DISEÑO DE UN MODELO DE GESTIÓN DE SEGURIDAD PARA EL CAPITAL INTELECTUAL DE CENTROS Y GRUPOS DE INVESTIGACIÓN: CASO INNOTEC

MARCELA CONTRERAS CRUZ
LEIDY JOHANNA CÁRDENAS SOLANO

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FÍSICO-MECÁNICAS
ESCUELA DE ESTUDIOS INDUSTRIALES Y EMPRESARIALES
BUCARAMANGA
2012

DISEÑO DE UN MODELO DE GESTIÓN DE SEGURIDAD PARA EL CAPITAL INTELECTUAL DE CENTROS Y GRUPOS DE INVESTIGACIÓN: CASO INNOTEC

MARCELA CONTRERAS CRUZ
LEIDY JOHANNA CÁRDENAS SOLANO

Proyecto de grado en modalidad "Pasantía de investigación" presentado como requisito para optar al título de Ingeniero Industrial

Director:
Ing. Luis Eduardo Becerra Ardila
Ms.C. en Administración
Docente Escuela de Estudios Industriales y Empresariales

Codirector:
Ing. Hugo Ernesto Martínez Ardila
Ms.C. en Ingeniería Área Electrónica
Investigador Grupo INNOTEC

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FÍSICO-MECÁNICAS
ESCUELA DE ESTUDIOS INDUSTRIALES Y EMPRESARIALES
BUCARAMANGA
2012

AGRADECIMIENTOS

A Dios, por su fortaleza y sustento a lo largo de este proceso de aprendizaje, porque en todo momento fue nuestro apoyo y sólo por su divina intervención fue posible llegar a la culminación satisfactoria de esta etapa de nuestras vidas.

A nuestras familias por su apoyo incondicional, por su paciencia y por el empuje que nos daban cada vez que nuestro ánimo desfallecía.

A los ingenieros Luis Eduardo y Hugo Ernesto por brindarnos su acompañamiento, orientación, y por su dedicación, y amabilidad con que nos trataron desde nuestro ingreso al grupo INNOTEC.

A los demás integrantes del grupo de investigación INNOTEC, por su amplia colaboración a lo largo del proceso investigativo, por sus consejos y por su cordial participación en las múltiples encuestas y pruebas pilotos.

Y a todos aquellos que directa o indirectamente aportaron a nuestro desarrollo personal, académico y profesional.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

LISTA DE ABREVIATURAS

CTI: Ciencia tecnología e Innovación

DIEF: Dirección de Investigación y Extensión de la Facultad

I+D: Investigación y desarrollo

INNOTEC: Centro para la Gestión y la Innovación Tecnológica

ISO: Organización Internacional de Normalización

MICMAC: Matriz de Impactos Cruzados – Multiplicación aplicada para una clasificación

MID: Matriz de Influencias Directas

MIDI: Matriz de Influencias Directas e Indirectas

PYME: Pequeña y Mediana Empresa

SI: Sistema de información

SGSI: Sistema de gestión de seguridad de la información

TICS: Tecnologías de la Información y la Comunicación

UAA: Unidad académico administrativa

UIS: Universidad Industrial de Santander

VIE: Vicerrectoría de Investigación y Extensión

GLOSARIO

ACTIVO DE INFORMACIÓN: se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para el grupo de investigación[1].

ACTIVO INTANGIBLE: es una fuente de futuros beneficios, pero en contraste con los activos tangibles, los intangibles no tienen una connotación física[2].

ADMINISTRACIÓN DEL RIESGO: actividades coordinadas para dirigir y controlar las medidas necesarias para la observación del riesgo dentro de la organización.

AMENAZA: aquello puede dañar o intentar dañar un activo de información[3]. Suelen clasificarse por su origen: naturales, humanas (intencionales o no intencionales), accidentales.

CVLAC: es el directorio de Currículum Vitae en Ciencia y Tecnología de acceso en la plataforma web del Departamento Administrativo de Ciencia, Tecnología e Innovación Colciencias.

DISPOSITIVOS MÓVILES: aparatos de pequeño tamaño, con algunas capacidades de procesamiento, con conexión permanente o intermitente a una red, memoria limitada, que ha sido diseñado específicamente para una función, pero que puede llevar a cabo otras funciones más generales. Ejemplos:

[1]NEIRA, Agustín; RUIZ, Javier. Glosario. En: Portal de ISO 27001 en español. [En línea]. [Consultado 10 enero 2012]. Disponible en <http://www.iso27000.es/glosario.html>
[2]LEV, Baruch (2003). Intangible Assets: Concepts and Measurements. *Encyclopedia of Social Measurement,* (Volumen 2, pp. 299).
[3]BACHMAIER, Carlos. Riesgo (Risk): ¿Qué es? Conceptos Previos. En: Revista Auditoria y Seguridad. [En línea]. [Consultado 23 marzo 2012]. Disponible en <http://www.revista-ays.com/DocsNum03/Academia/Carlos.pdf>

reproductores de audio portátiles, navegadores GPS, teléfonos móviles, los PDAs, los Tablet PCs[4].

EVALUACIÓN DE RIESGO: proceso de comparar los riesgos estimados contra los criterios de riesgo establecidos o dados, para determinar el grado de significancia del riesgo.

EVENTOS DE SEGURIDAD DE LA INFORMACIÓN: ocurrencia de un evento identificado sobre un sistema, servicio o red, cuyo estado indica una posible brecha en la política de seguridad de la información o falla en el almacenamiento de la misma; también cualquier situación previa desconocida que pueda ser relevante desde el punto de vista de la seguridad.

GRUPLAC: aplicación en línea que COLCIENICAS pone a disposición de la comunidad, la cual permite actualizar y consultar la información de grupos de investigación de Ciencia y Tecnología, de acceso en la plataforma web del Departamento Administrativo de Ciencia, Tecnología e Innovación Colciencias.

INCIDENTE DE SEGURIDAD: uno o varios eventos de seguridad de la información, no deseados o inesperados que tienen una cierta probabilidad de comprometer las operaciones de la empresa y amenazan a la seguridad de la información.

INFORMACIÓN CONFIDENCIAL: es toda información que por su naturaleza no puede ser revelada a terceros, y que por lo tanto no es pública. Ejemplos:avances o resultados de proyectos, datos recopilados en una investigación, información personal de los investigadores, propuestas o planes de proyectos. Pueden existir distintos niveles de confidencialidad.

[4]BAZ, Arturo; FERREIRA, Irene; ÁLVAREZ, María; GARCÍA, Rosana. Dispositivos móviles. [En línea]. [Consultado 20 marzo 2012]. Disponible en: <http://156.35.151.9/~smi/5tm/09trabajos-sistemas/1/Memoria.pdf>

ISI WEB OF KNOWLEDGE: es una plataforma integrada de información vía web, de la Thomson Corporation, para la búsqueda científica de información estructurada. Ofrece acceso a la Web of Science que cuenta con más de 9.200 revistas en 45 idiomas diferentes en los campos de las ciencias, ciencias sociales, artes y humanidades para encontrar los documentos más relevantes del área de interés.

MITIGACIÓN DE RIESGOS: planificación y ejecución de medidas de intervención dirigidas a reducir o disminuir el riesgo existente. La mitigación asume que en muchas circunstancias no es posible controlar el riesgo totalmente, es decir, que en muchos casos no es posible impedir o evitar totalmente los daños y sus consecuencias, sino más bien reducirlos a niveles aceptables por la propia organización.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN: documento que indica el compromiso y apoyo de la dirección, así como la definición del papel que debe jugar la seguridad de la información en la consecución de la misión y visión de la organización.

RIESGO: un evento no certero o condición que, si ocurriese, tendría un efecto positivo o negativo sobre los objetivos del proyecto. Los riesgos negativos pueden llamarse "amenazas", y los riesgos positivos "oportunidades". Normalmente expresado como impacto y probabilidad. Entonces es la probabilidad de que una amenaza ataque un activo de información a través de una vulnerabilidad concreta[5].

RIESGO RESIDUAL: un riesgo que permanece después de implementar los controles apropiados, basados en los resultados y conclusiones de la valoración y los procesos de tratamiento de riesgos.

[5] NEIRA y RUIZ, Op cit.

SEGURIDAD DE LA INFORMACIÓN: preservación de la confidencialidad, integridad y disponibilidad de la información, adicionalmente pueden considerarse otras propiedades como autenticación, autorización, registro de actividad, no repudio y confiabilidad.

SCOPUS: es una plataforma integrada de información vía web de Elsevier B.V., que permite la búsqueda de información científica estructurada, cuenta con una base de datos de citaciones y resúmenes, en una ventana de tiempo consultada a partir de 1960, de 16500 revistas revisadas por pares de las áreas de ciencias, tecnología, medicina y ciencias sociales, incluyendo artes y humanidades.

SISTEMA DE INFORMACIÓN: conjunto de componentes interrelacionados que recolectan (o recuperan), procesan, almacenan y distribuyen información para apoyar la toma de decisiones y el control de una organización[6].

SOCIEDAD DEL CONOCIMIENTO: "Es una sociedad con capacidad para generar, apropiar, y utilizar el conocimiento para atender las necesidades de su desarrollo y así construir su propio futuro, convirtiendo la creación y transferencia del conocimiento en herramienta de la sociedad para su propio beneficio. En la sociedad del conocimiento y del aprendizaje, las comunidades, empresas y organizaciones avanzan gracias a la difusión, asimilación, aplicación y sistematización de conocimientos creados u obtenidos localmente, o accesados del exterior. El proceso de aprendizaje se potencia en común, a través de redes, empresas, gremios, comunicación inter e intrainstitucional, entre comunidades y países"[7].

[6]LAUDON, Keneth C. y LAUDON, Jane P. Sistemas de información gerencial. Octava Edición. México : Pearson Educación, 2004, p. 8.

[7] UNIVERSIDAD INDUSTRIAL DE SANTANDER. Plan de Desarrollo Institucional 2008-2018. En: Grupo de Estudios Prospectivos Sociedad Economía y Ambiente – GEPSEA. .La Sociedad del Conocimiento. [En línea]. [Consultado 25 julio 2011]. Disponible en Internet en: <http://personales.com/venezuela/merida/gepsea/sc.htm>

STAKEHOLDERS: aquellos grupos que pueden afectar o ser afectados por el logro de los propósitos de la organización[8].

TI: se conoce como tecnología de información (TI) a la utilización de tecnología para el manejo y procesamiento de información – específicamente la captura, transformación, almacenamiento, protección, y recuperación de datos e información[9].

TRATAMIENTO DEL RIESGO: proceso de selección e implementación de mediciones para modificar el riesgo.

VALORACIÓN DE RIESGO: totalidad de los procesos de análisis y evaluación de riesgo.

VENTAJA COMPETITIVA: una organización posee una ventaja competitiva cuando tiene alguna característica diferencial respecto de sus competidores, que le confiere la capacidad para alcanzar unos rendimientos superiores a ellos, de manera sostenible en el tiempo[10].

VULNERABILIDAD: defecto o debilidad en los procedimientos y controles de seguridad, que podrían ser aprovechados por una amenaza y resultar en un incidente de seguridad o violación de la política de seguridad de la información.

---

[8] FREEMAN, R. Edward. Ethical leadership and creating value for stakeholders. En: PETERSON, Robert y FERRELL, O.C. Ethical leadership and creating value for stakeholders (2004). En: Business ethics: challenges for business schools and corporate leaders. Armonk, NY: M.E. Sharpe, 2005.

[9] Tecnología de información. En: Degerencia.com. [En línea]. [Consultado 9 marzo 2012]. Disponible en <http://www.degerencia.com/tema/tecnologia_de_informacion>

[10] RODRIGUEZ, Juan Manuel. La ventaja competitiva. En: El Ergonomista. [En línea]. [Consultado 8 enero 2012]. Disponible en <http://www.elergonomista.com/3ab12.html>

RESUMEN

TITULO: Diseño de un modelo de gestión de seguridad para el capital intelectual de centros y grupos de investigación: Caso INNOTEC.[11]

AUTORES: CÁRDENAS SOLANO, Leidy Johanna
CONTRERAS CRUZ, Marcela.[12]

PALABRAS CLAVES: Análisis de riesgos, análisis estructural, capital intelectual, grupo de investigación, política, seguridad de la información.

DESCRIPCIÓN:

En este proyecto se diseña un modelo de gestión de seguridad cuya finalidad es proteger los activos de información y conocimiento de un grupo o centro de investigación, y el cual es desarrollado a través de la adaptación de distintas metodologías encontradas en la literatura.

En primer lugar se desarrolla un ejercicio de análisis estructural, tomando como sistema de estudio la seguridad de la información en un grupo de investigación y como variables, los diferentes componentes que tienen influencia sobre esta. A partir de los resultados, se determinan las variables estratégicas del sistema sobre las cuales estará enfocado el modelo de gestión.

Posteriormente, se realiza un diagnóstico exploratorio de los grupos de investigación de la Facultad de Ingenierías Físico Mecánicas, que incluye la aplicación de un cuestionario y el análisis de los resultados obtenidos, con el objeto de conocer y analizar la situación actual de la seguridad de la información en grupos de investigación.

Por otra parte, se lleva a cabo un estudio del nivel de riesgo al cual se encuentra expuesto el grupo INNOTEC, a partir del cual se priorizan los riesgos y se asignan controles apropiados. Finalmente, se realiza la aplicación piloto del modelo de gestión en el grupo de investigación INNOTEC, a través de la formulación de la política de seguridad que le permitirá contar con lineamientos claros a la hora de tomar acciones preventivas y correctivas en esta área; y adicionalmente, servirá como punto de partida para la gestión de seguridad de la información en otros grupos de investigación.

[11] Proyecto de Grado
[12] Facultad de Ingenierías Físico Mecánicas. Escuela de Estudios Industriales y Empresariales. Director: Luis Eduardo Becerra Ardila. Codirector: Hugo Ernesto Martínez.

ABSTRACT

TITLE: Design of a security management model for the intellectual capital of research centers and groups: INNOTEC case.[13]

AUTORES: CÁRDENAS SOLANO, Leidy Johanna
CONTRERAS CRUZ, Marcela.[14]

KEY WORDS: Information security, intellectual capital, policy, research group, risk analysis, structural analysis.

DESCRIPTION:

In this project a security management model is design which aims to protect the knowledge and information assets of a research center or group; this model is developed through the adaptation of different methodologies.

Initially, a structural analysis exercise is developed, establishing the information security in a research group as the system for study, and the aspects that influence the security, were taking as variables. From these results, the strategic variables of the system are found, and they will be the main focus on the management model.

Subsequently, an exploratory diagnosis is carried through the research groups of the Faculty of Physical and Mechanic Engineering, which includes the application of one questionnaire and the analysis of the results, in order to understand and determine the current state of information security in research groups.

On the other hand, a study of the risk level to which INNOTEC is exposed was carried out, and permitted the prioritization of the risks and the assignation of the appropriate controls. Finally, the pilot application of the management model is made in INNOTEC, through the development of a security policy which will allow the researchers to have clear guidelines when taking preventive and corrective actions in this area. Additionally, it will serve as a starting point for the information security management of other research groups.

[13] Degree Project
[14] Faculty of Physique Mechanics Engineering.School of Industrial and Managerial Studies.Director: Luis Eduardo Becerra Ardila. Codirector: Hugo Ernesto Martínez.

TABLA DE CUMPLIMIENTO DE OBJETIVOS

OBJETIVO	LOGRO - REFERENCIA	PÁGINAS
Objetivo 1 Identificar y analizar buenas prácticas de seguridad de la información y protección del capital intelectual, a través de la consulta en bases de datos de revistas indexadas y estudios de casos.	**Capítulo 4** Estado del Arte (Ver **¡Error! El resultado no es válido para una tabla.**)	44–54 171–192
Objetivo 2 Establecer las condiciones actuales en materia de seguridad de la información a nivel institucional, a través de la consulta en fuentes primarias y secundarias acerca de las prácticas de seguridad de la información utilizadas en los grupos de investigación de la UIS.	**Capítulo 7** Análisis y valoración de riesgos	90–124
Objetivo 3 Identificar, caracterizar y valorar los riesgos potenciales relacionados con la seguridad de la información del grupo INNOTEC, a través de análisis estructural y matriz de valoración de riesgos, y con base en los controles descritos en la norma ISO/IEC 27001:2005.	**Capítulo 7** Análisis y valoración de riesgos	90–124
Objetivo 4 Describir y proponer un modelo de seguridad de la información basado en los riesgos identificados y valorados, adaptable al contexto de cualquier centro o grupo de investigación.	**Capítulo 6** Modelo de Gestión	76–90
Objetivo 5 Realizar aplicación piloto del modelo desarrollado, en el grupo INNOTEC, mediante la definición y aprobación de la política de seguridad usando la metodología policy capturing.	**Capítulo 8** Policy Capturing	125–138

Objetivo 6 Documentar la experiencia para posibles réplicas, sintetizando la metodología desarrollada.	**Capítulos 2 - 8**	28–138
LOGROS ADICIONALES		
• Presentación de ponencia En: Colombia. 2012. Evento: IV Congreso Iberoamericano SOPORTE AL CONOCIMIENTO CON LA TECNOLOGÍA. El título de la ponencia es: "A risk level management study for the Intellectual Capital Security: an approximation". (Ver ANEXO 1) • Participación en el Módulo de Seguridad de la Información brindado en la Especialización en Telecomunicaciones de la Escuela de Ingenierías Eléctrica, Electrónica y Telecomunicaciones de la UIS. Este modulo fue dictado por el Profesor Jorge Medina Villalobos, CSO del Banco de la República.		

INTRODUCCIÓN

El entorno competitivo actual ha generado la necesidad de una gestión eficiente de los recursos de las organizaciones, siendo el conocimiento uno de los más valiosos estratégicamente y una herramienta para generar valor en las mismas, a lo que algunos autores llaman la visión de la empresa basada en el conocimiento[15]. Con el fin de que dicho conocimiento genere valor, debe estar disponible y accesible para quien necesite hacer uso del mismo, lo cual se traduce en ser recopilado y almacenado en diferentes medios físicos o electrónicos. Esto sumado al auge de las tecnologías de comunicación e información – TICs, ha conducido a las organizaciones a una transformación de sus entornos de trabajo, que con frecuencia han dejado de ser físicos y se han convertido en entornos virtuales.

En este contexto, los flujos de información y el traslado de recursos de un sitio a otro hace que surjan vulnerabilidades que ponen en riesgo la seguridad de la información y el conocimiento en ella contenido. Proteger la información y el conocimiento, además de ser una tarea continua, es de vital importancia para las organizaciones. Lo anterior, generalmente es el resultado de la toma de conciencia (awareness) de sus directivos, sobre el impacto que pueden llegar a tener las amenazas y vulnerabilidades en los activos tangibles e intangibles. Por tanto, es importante que toda organización que quiera tener un mayor control de su capital intelectual, defina una estrategia de seguridad fundamentada en modelos que soporten políticas de seguridad, así como procedimientos y controles adaptados al contexto de cada tipo de organización, de manera que se optimicen la protección de la información y el conocimiento como recursos estratégicos y de gran valor.

[15] Grant, Robert. Toward a knowledge-based theory of the firm. En: Strategic Management Journal. Vol. 17 (1997); p. 110.

En este sentido, el presente proyecto constituye la primera iniciativa estructurada en la cual se describe el estado de la gestión de la seguridad de la información en los grupos de investigación de la Facultad de Ingenierías Fisicomecánicas y se propone una aproximación a un modelo de gestión de la seguridad del capital intelectual para organizaciones basadas en conocimiento, tales como grupos o centros de investigación, permitiendo identificar aspectos importantes para el desarrollo práctico de esta temática.

En el primer capítulo se presentan las especificaciones del proyecto en cuanto su descripción general, justificación, objetivos y alcance. En el capítulo 2, se describen de manera general las siete etapas que enmarcan la metodología del proyecto. Por otra parte, el tercer capítulo corresponde al marco referencial, y el cuarto, a la revisión del estado del arte, donde se definen los conceptos de modelo de gestión, análisis estructural, gestión de riesgos, y policy capturing, tal como se entienden y aplican en los ejercicios realizados.

El desarrollo del ejercicio de análisis estructural donde se analizan las relaciones entre las variables definidas para el sistema de seguridad de la información en grupos de investigación y, se definen las variables estratégicas del mismo, se presenta en el capitulo 5. Asimismo, el capítulo 6, muestra el modelo de gestión de seguridad de la información desarrollado y la explicación de cada uno de sus componentes.

Los capítulos 7 y 8 presentan el proceso de análisis y valoración de riesgos, y la aplicación de la metodología policy capturing para la formulación de la política para el grupo. Finalmente, se presentan las conclusiones y recomendaciones en torno a los ejercicios, actividades y análisis realizados.

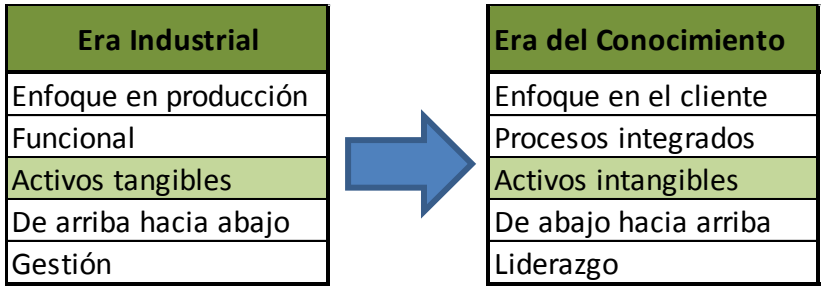
1. ESPECIFICACIONES DEL PROYECTO

1.1. DESCRIPCIÓN Y FORMULACIÓN DEL PROBLEMA DE INVESTIGACIÓN

En la economía actual, también llamada “economía basada en el conocimiento”[16][17][18], las organizaciones ya no son valoradas solo por la cantidad de activos físicos que poseen, sino por el conocimiento incluido en sus formas de administrar, procesos, infraestructura, personal, etc.; convirtiendo al capital intelectual en uno de los indicadores más importantes al valorar una compañía[19][20]. Por ejemplo, se estima que del 50 al 90 por ciento del valor creado hoy por una firma, proviene del capital intelectual de su gestión, en lugar del uso y la producción de bienes materiales[21] (ver Figura 1) .“Sólo del 6 al 30 por ciento del valor de una compañía es obtenido de activos tangibles, lo demás proviene de activos intangibles”[22].

[16]MORTAZAVI, S. Habib y BAHRAMI, Mahdi. Integrated approach to entrepreneurship – knowledge based economy: a conceptual model. En: Procedia – Social and Behavioural Sciences. Vol. 41 (2012); p. 283.
[17]SABAU, Gabriela. Know, live and let live: towards a redefinition of the knowledge-based economy – sustainable development nexus. En: Ecological Economics. Vol. 69, No. 6 (Abr. 2010); p. 1193.
[18] GRANT, Robert M. Toward a knowledge-based theory of the firm. En: Strategic Management Journal. Vol. 17 (Edición especial de invierno,1996); p. 110.
[19]SALLEBRANT, Tobias, et al. Managing risk with intelectual capital statements. En: Management Decision. Vol. 45, No. 9 (2007); p. 1471.
[20]AMIRI, Ali Naghi, RAMEZAN, Majid, y OMRANI, Abdollah. Studying the impacts of organizational organic structure on knowledge productivity effective factors case study: Manufacturing units in a domestic large industrial group. En: European Journal of Scientific Research. Vol. 40, No. 1 (2010); p. 99.
[21] GUTHRIE, J. y YONGVANICH, K. Using content analysis as a research method to inquire into intellectual capital reporting. En: Journal of Intellectual Capital. Vol. 5, No. 2 (2004); p. 282-293.
[22]VOLVOK, Dimitry. yGARINA, Tatiana. (2007). Intangible Assets: importance in the knowledge based economy and the role in value creation of a company. En: The Electronic Journal of Knowledge Management. Vol. 5, No. 4 (2007); p. 540.

Figura 1. Evolución en el estilo de gestión



Fuente. Propia basada en CHAREONSUK, C. y CHUVEJ, C. Intangible asset management framework for long-term financial performance. En: Industrial Management & Data Systems. Vol. 108, No. 6 (2008); p. 812.

Lo ideal es que todo el conocimiento que reside en una organización pueda ser utilizado por quien lo necesite para actuar de manera adecuada en cada momento[23]. Con el fin de lograr dicho objetivo, la información debe ser manejada de forma correcta y eficiente, tal como se manejan los demás recursos organizativos. Asimismo, la información debe ser considerada como un recurso dinámico que está en constante movimiento y constituye un flujo desde que se crea hasta que se destruye. Por tanto, es importante conocer cómo es transferida, a través de que canales, y qué personas tienen acceso a ella[24]; todo esto para garantizar su confidencialidad, integridad y disponibilidad (dimensiones de la seguridad de la información).

[23] CANALS, A. y PEREZ, M. Hacia la gestión del conocimiento. En: La Vanguardia. [en línea]. (2001) [Consultado el 5 de Agosto de 2011]. Disponible en <http://www.uoc.edu/web/esp/art/uoc/canals/canals_imp.html>

[24] CABRERA, R. y GARCÍA, R. Entorno Actual de Protección de Información en México. En: Revista Online Software Gurú. (2011) [Consultado el 5 de Agosto de 2011]. Disponible en: <http://www.sg.com.mx/content/view/1186/2/>

Sin embargo, debido a la complejidad de las organizaciones modernas, la globalización de la economía y el creciente auge de las tecnologías de información, mantener la información relevante dentro de los límites de acción de las empresas se ha convertido en un reto para las mismas, siendo la pérdida o fuga de información unos de los problemas más frecuentes y con mayor repercusión en su competitividad. En este sentido, el gerente general de Ingenium Soluciones informáticas*, Eduardo Gómez del Valle, afirma que "la causa principal de este problema radica en que las empresas no cuentan con políticas adecuadas en seguridad de la información, y por tanto, son los propios empleados, quienes realizan esta práctica delincuencial de forma diaria, esporádica o cuando se efectúa el despido o cese de funciones"[25].

Por otra parte, los resultados de la encuesta mundial "La seguridad en los complejos entornos TI del siglo XXI", elaborada por Check Point y Ponemon Institute, publicada en febrero de 2011, muestran que el 48,8% de los encuestados cree que los empleados tienen poca o muy poca conciencia sobre la protección de los datos y las políticas corporativas. Lo más grave de esta situación es que además de perder ventaja competitiva, la pérdida de información puede originar grandes pérdidas económicas; Larry Ponemon, presidente y fundador del Ponemon Institute, sostiene que "las pérdidas económicas derivadas de sufrir ataques en la información para una empresa

* Ingenium es una empresa española de vanguardia dedicada al diseño y desarrollo de la más alta tecnología domótica. Sitio web: *http://www.ingeniumsl.com*

[25] MEDINA, E. Evitar fuga de información, nuevo foco de inversión. En: La Republica. (2011). [Consultado el 31 de Agosto de 2011], Disponible en: http://www.larepublica.com.co/archivos/TECNOLOGIA/2011-02-02/evitar-fuga-de-informacion-nuevo-foco-de-inversion_120725.php

* Check Point es una empresa líder de seguridad en Internet, que ofrece seguridad total para redes, datos y criterios de valoración. Sitio web: *www.checkpoint.com*

** Ponemon Institute es una firma de investigación especializada en políticas de seguridad de la información. Sitio web: *www.ponemon.org*

pueden variar desde 237.000 a 52 millones de dólares"[26]. Otro estudio realizado por el mismo instituto sobre la pérdida de datos en 45 empresas de los Estados Unidos dio como resultado en 2009 que las pérdidas de información alcanzaron una cifra de $6,7 millones de dólares[27].

Tomando como base el valor que tiene la información corporativa para cualquier empresa actual, se vuelve evidente que para las "empresas basadas en el conocimiento"[282930], en particular las universidades y los grupos o centros de investigación que hacen parte de estas, el problema de la seguridad de la información cobra mayor relevancia estratégica debido al actual sistema de financiación en la educación superior. En vista de esta realidad, se requiere que las universidades exploten sus derechos de propiedad intelectual a un nivel mucho más alto que en el pasado, como fuente alternativa de ingresos, (diferente a los estudiantes y el gobierno)[3132]. Por lo que es importante ser eficiente en la protección de la información y el conocimiento a través de la formulación de modelos que establezcan normas, procedimientos y controles para la protección de la información. Según Kok[33], estos modelos deben incluir:

[26] PONNEMON INSTITUTE. Understanding Security Complexity in 21st Century IT Environments: A study of IT practitioners in the US, UK, France, Japan & Germany. 2011, p. 1.
[27] PONNEMON INSTITUTE y LLC. 2009 Annual Study: Cost of Data Breach. Understanding Financial Impact, Customer Turnover, and Preventive Solutions.2010, p. 4.
[28]ALVESSON, M. Management of Knowledge Intensive Companies. Berlin/New York: de Gruyter, 1995, p. 6
[29] ROBERTSON, M. y SWAN, J. Modes of organizing in an expert consultancy: a case study of knowledge, power and egos. En: Organization. Vol. 5, No. 4 (1998); p. 544.
[30]STARBUCK, W. H. Learning by knowledge-intensive firms .En: Journal of Management Studies. Vol. 3, No. 4 (1992); p. 715.
[31]MOK, Ka Ho. Fostering entrepreneurship: changing role of government and higher education governance in Hong Kong. En: Research Policy. Vol. 34, No. 4 (2005); p. 540.
[32]KOK, A. Intellectual Capital Management as Part of Knowledge Management Initiatives at Institutions of Higher Learning. En: The Electronic Journal of Knowledge Management. Vol. 5, No. 2 (2007); p. 183.
[33]Ibid.

- Medidas para proteger, resguardar y mercadear la propiedad intelectual producida por profesores y estudiantes; y
- Políticas para asegurar que todos los participantes compartan en el ingreso derivado de la propiedad intelectual sobre una base que sea justa, equitativa y de una naturaleza tal que, anime a la divulgación de los inventos y los descubrimientos.

Por su parte, la Universidad Industrial de Santander al considerar la investigación como eje fundamental de la misión institucional, en el año 2011 invirtió cerca de 34 mil 300 millones de pesos en Investigación, Fomento y Desarrollo[34]. Esta cifra corresponde al rubro destinado para proyectos de investigación que se ejecutan a través de los diferentes grupos de investigación, y en los cuáles la información y conocimiento generados representan un valor incalculable para la Universidad, y requieren ser gestionados con la mayor responsabilidad y confidencialidad posible. Cabe resaltar que el monto anteriormente mencionado representa la inversión realizada en un solo año, y que los proyectos financiados por la universidad generalmente tienen una duración superior a este periodo, por lo cual, si se deseara calcular el total de la inversión el monto sería mucho mayor, y por consiguiente, se espera que, mediante la venta de servicios, este produzca un retorno económico igualmente significativo para la Universidad. Se tiene estimado en el presupuesto anual que estos beneficios representan cerca del 54% del total de los ingresos recibidos por la universidad y valorados en 214 mil millones de pesos.[35]

1.2. JUSTIFICACIÓN DEL PROBLEMA DE INVESTIGACIÓN

[34] Fuente: Sistema de Información financiero. Universidad Industrial de Santander. 19 de Septiembre de 2011.
[35] Fuente: Sistema de Información financiero. Universidad Industrial de Santander. 10 de Diciembre de 2011.

El campo de la seguridad de la información ha crecido y evolucionado considerablemente en los últimos años, convirtiéndose en "una disciplina cada vez más crítica, necesaria y obligatoria" y en "un elemento integral de la capacidad de una organización para que ésta sea competitiva"[36]. Sin embargo, en Latinoamérica, aún está en proceso de crecimiento y evolución, en donde los esfuerzos por proteger este valioso recurso, han estado enfocados en herramientas tecnológicas, dejando descuidada una de las principales fuentes de riesgo que es el recurso humano; y solo un 26,7% del presupuesto de las organizaciones es destinado a la concientización y formación del usuario final[37].

En particular, son pocos los esfuerzos realizados en este campo dentro de las universidades. Según Rezgui y Marks[38], las universidades americanas están entre los entornos menos protegidos en seguridad de la información, puesto que solo una fracción de ellas, lleva a cabo actividades de sensibilización sobre este tema. Además, los fondos destinados a su implementación, son bajos en comparación con otras áreas. Según un estudio realizado en Australia, "Más del 80% de las universidades destina 5% o menos del presupuesto de TI al tema de la seguridad de la información"[39]. De ahí, la importancia y la novedad de esta investigación, que apunta directamente a mejorar la

[36]AREITIO, Javier. Seguridad de la información: redes, informática y sistemas de información. Madrid: Editorial Paraninfo, 2008, p 2.
[37] CANO, Jeimy. Seguridad de la Información en Latinoamérica. Tendencias 2009. En: Revista Sistemas de la Asociación Colombiana de Ingenieros. [en línea]. No. 110 (2009); p. 36. [Consultado el 31 de Agosto de 2011]. Disponible en <http://www.acis.org.co/fileadmin/Revista_110/05investigacion1.pdf>
[38]REZGUI, Yacine y MARKS, Adam. Information security awareness in higher education: an exploratory study. En: Computers & Security. Vol. 27 (2008); p. 241.
[39] LANE, Tim (2007). Information security management in Australian universities: an exploratory analysis. Tesis de grado para el título de Magister en Tecnologías de Información. Queensland University, Brisbane, Australia, p. 196.
* Unidades Académico Administrativas

gestión del riesgo en este tipo específico de organizaciones donde el conocimiento y la información son sus capitales más importantes.

Del mismo modo, este tema es importante para la Universidad Industrial de Santander, teniendo en cuenta que se trata de una institución creadora y transformadora de conocimiento, gran parte del cual reposa bajo la forma de conocimiento codificado (i.e. tesis de grado, informes, artículos publicados y demás productos de los proyectos llevados a cabo). Además recientemente se inició el proceso para implementar la norma ISO/IEC 27001 en la división de Servicios de Información de la Universidad, con proyección hacia el resto de UAAs* en el largo plazo, demostrando así el interés por el tema a nivel institucional.

En particular, el grupo de investigación INNOTEC no cuenta con información clara y estructurada sobre cómo crear una estrategia de seguridad de la información, cómo definir las políticas de seguridad, cuáles son los recursos que se deben proteger, qué procedimientos debe tener un grupo de investigación para cumplir los objetivos de seguridad, qué personas están involucradas en el establecimiento de las políticas y quiénes deben velar por hacerlas cumplir; se hace importante la apropiación de conocimiento en el tema y el desarrollo un modelo de gestión de seguridad que sirva de soporte para capacitar a los investigadores.

1.3. OBJETIVOS

1.3.1. Objetivo general

Diseñar un modelo de gestión de seguridad para el capital intelectual de entidades generadoras de conocimiento (como centros o grupos de investigación), basado en los principios fundamentales de seguridad de la información y la valoración de riesgos; el cual les permita minimizar la probabilidad de pérdidas materiales e intangibles.

1.3.2. Objetivos específicos

- Identificar y analizar buenas prácticas de seguridad de la información y protección del capital intelectual, a través de la consulta en bases de datos de revistas indexadas y estudios de casos.
- Establecer las condiciones actuales en materia de seguridad de la información a nivel institucional, a través de la consulta en fuentes primarias y secundarias acerca de las prácticas de seguridad de la información utilizadas en los grupos de investigación de la UIS.
- Identificar, caracterizar y valorar los riesgos potenciales relacionados con la seguridad de la información del grupo INNOTEC, a través de análisis estructural y matriz de valoración de riesgos, y con base en los controles descritos en la norma ISO/IEC 27001:2005.
- Describir y proponer un modelo de seguridad de la información basado en los riesgos identificados y valorados, adaptable al contexto de cualquier centro o grupo de investigación.
- Realizar aplicación piloto del modelo desarrollado, en el grupo INNOTEC, mediante la definición y aprobación de la política de seguridad usando la metodología policy capturing.
- Documentar la experiencia para posibles réplicas, sintetizando la metodología desarrollada.

1.4. ALCANCE

El alcance de este proyecto es proponer un modelo de gestión de la seguridad del capital intelectual en organizaciones generadoras de conocimiento, mediante una previa caracterización y evaluación de riesgos potenciales relacionados con este tópico. Asimismo busca fortalecer la estructura investigativa de la Universidad Industrial de Santander, mediante un marco de referencia estructurado sobre cómo definir políticas de seguridad, cuáles recursos proteger, qué procedimientos llevar, las personas a involucrar y quiénes garantizarán el cumplimiento.

2. METODOLOGÍA

Para llevar a cabo los objetivos específicos, el presente proyecto se desarrolló en siete etapas tal como lo ilustra la Figura 2. En el

ANEXO 2, se presentan las definiciones de las herramientas utilizadas durante el desarrollo del ejercicio.

a) Revisión de la literatura: En la primera etapa del estudio se realizó la revisión de la literatura sobre la gestión de la seguridad de la información. Para ello, se utilizó la base de datos ISI Web of Knowledge, teniendo en cuenta que es una plataforma que incluye revistas indexadas y que realiza una rigurosa selección de contenidos para obtener artículos de alta calidad. Además, gracias a que en la actualidad las diferencias entre esta base de datos y Scopus son mínimas, y trabajos realizados muestran que tanto ISI como Scopus están estadísticamente equilibrados en términos de temas, países, idioma y editores[40][41], se resalta el uso de la plataforma ISI en el desarrollo de este proyecto y su traslape de aproximadamente el 80% de los artículos de Scopus, ya que la mayoría de los estudios realizados entre ISI y Scopus, concluyen con resultados muy similares entre ambas[42][43]. Otro estudio[44], demuestra que "el 54% de las revistas indexadas

[40]BRAUN, T, GLÄNZEL, W y SCHUBERT, A. The Web of Knowledge: A Festschrift in Honor of Eugene Garfield, chapter How balanced is the Science Citation Index's journal coverage? A preliminary overview of macro level statistical data. Medford: ASIS, 2000. Citado por: IBAÑEZ, Alfonso, CONCHA, Bielza y LARRAÑAGA, Pedro. Productividad y visibilidad científica de los profesores funcionarios de las Universidades públicas españolas en el área de tecnologías informáticas, Investigadores. Universidad Politécnica de Madrid, 2011, p. 11. [Consultado 20 Agosto de 2012]. Disponible en: http://oa.upm.es/9407/1/analisis-bibliometrico.pdf

[41] MOYA-ANEGÓN, F. et al. Coverage analysis of Scopus: A journal metric approach. En: Scientometrics. Vol. 73 No. 1 (2007); p. 53-78. Citado por: IBAÑEZ, Alfonso, CONCHA, Bielza y LARRAÑAGA, Pedro. Productividad y visibilidad científica de los profesores funcionarios de las Universidades públicas españolas en el área de tecnologías informáticas, Investigadores. Universidad Politécnica de Madrid, 2011, p. 11. [Consultado 20 Agosto de 2012]. Disponible en: http://oa.upm.es/9407/1/analisis-bibliometrico.pdf

[42] ARCHAMBAULT, E. et al. Comparing bibliometric statistics obtained from the Web of Science and Scopus. En: Journal of the American Society for Information Science and Technology. Vol. 60, No. 7 (2009); p, 1320-1326. Citado por: IBAÑEZ, Alfonso, CONCHA, Bielza y LARRAÑAGA, Pedro. Productividad y visibilidad científica de los profesores funcionarios de las Universidades públicas españolas en el área de tecnologías informáticas. Universidad Politécnica de Madrid, 2011, p. 11. [Consultado 20 Agosto de 2012]. Disponible en: http://oa.upm.es/9407/1/analisis-bibliometrico.pdf

[43] LOPEZ-ILLESCAS, C, MOYA-ANEGÓN, F y MOED, HF. Comparing bibliometric country-by country rankings derived from the Web of Science and Scopus: the effect of poorly cited journals in oncology. En: Journal of Information Science. Citado por: IBAÑEZ, Alfonso, CONCHA, Bielza y LARRAÑAGA, Pedro. Productividad y visibilidad científica de los profesores funcionarios de las Universidades públicas españolas en el área de tecnologías informáticas, Investigadores.

por Scopus y el 84% de las indexadas por ISI Web of Knowledge son las mismas, produciendo resultados muy parecidos". También, se tuvieron en cuenta las bases de datos Ebsco Host, ScienceDirect, Springerlink, ProQuest, y la herramienta Google Scholars para complementar la búsqueda. La revisión inicial se encuentra plasmada en el estado del arte y el marco referencial. Igualmente, es importante mencionar que dicha revisión se actualizó en el transcurso de todo el proyecto, ya que es necesaria una constante revisión de las nuevas publicaciones en diversos medios de información.

b) Identificación de las áreas estratégicas del sistema de seguridad de la información: En la segunda etapa del proyecto se aplicó la técnica de análisis estructural, con el fin de caracterizar el sistema de seguridad de la información en la UIS e identificar las variables estratégicas del sistema de seguridad de la información, sobre las cuáles se debe actuar primeramente y que influirán sobre el resto del sistema hasta que se logre la estabilidad y aparición de nuevas variables estratégicas. Para ello, se llevaron a cabo tres pasos que caracterizan la técnica: elaboración del listado de variables, identificación de las interrelaciones por medio de la matriz de impacto cruzado e identificación de las variables clave. En el desarrollo de esta etapa se empleó el software MICMAC® el cual se alimentó con la información recolectada de diferentes actores, quienes apoyaron el proceso de diligenciamiento de la matriz y validaron los resultados encontrados en la identificación de las variables clave.

Universidad Politécnica de Madrid, 2011, p. 11. [Consultado 20 agosto 2012]. Disponible en: http://oa.upm.es/9407/1/analisis-bibliometrico.pdf

[44] GEVEL, Y y ISELID L. Web of Science and Scopus: A journal title overlap study. En: Online Information Review. Vol. 32, No. 1; (2008); p. 8-21. Citado por: IBAÑEZ, Alfonso, CONCHA, Bielza y LARRAÑAGA, Pedro. Productividad y visibilidad científica de los profesores funcionarios de las Universidades públicas españolas en el área de tecnologías informáticas, Investigadores. Universidad Politécnica de Madrid, 2011, p. 11. [Consultado 20 agosto 2012]. Disponible en: <http://oa.upm.es/9407/1/analisis-bibliometrico.pdf>

c) Análisis del estado de la gestión de la seguridad de la información (GSI) en la Universidad Industrial de Santander: En esta etapa se buscaba conocer el estado de la gestión de la seguridad de la información en la UIS. Para ello, se realizó un diagnóstico general sobre las prácticas y uso de controles de seguridad de la información en los grupos de investigación de la universidad, utilizando como técnica de recolección de la información un cuestionario desarrollado por las autoras del proyecto. Primero, se realizó una prueba piloto del instrumento de medición con algunos de los estudiantes de INNOTEC. Luego, el instrumento mejorado, fue aplicado en los grupos de investigación de la Facultad de Ingenierías Fisicomecánicas.

d) Análisis del estado de la gestión de seguridad de la información en el grupo de investigación INNOTEC: En esta etapa se realizó un diagnóstico de la GSI en INNOTEC. Para esto, se analizaron los 26 controles que según Layton[45] son indicadores claves de riesgo, y corresponden a la categoría de gestión. Se utilizó como técnica de recolección de la información un cuestionario, en el cual se solicitaba a los integrantes del grupo de investigación calificar el nivel de implementación de cada uno de los controles.

e) Análisis y valoración de riesgos en el grupo de investigación INNOTEC: En esta etapa se buscaba conocer los principales riesgos relacionados con la información, y a partir de estos identificar los requerimientos de seguridad del grupo INNOTEC. Para ello se utilizó la metodología GISAM, descrita en el libro Information Security de Timothy Layton, la cual incluye la identificación de amenazas, vulnerabilidades, y consecuencias, y, a partir de estos, el análisis de probabilidad e impacto, los cuales condujeron a la elaboración de la matriz de nivel de riesgo.

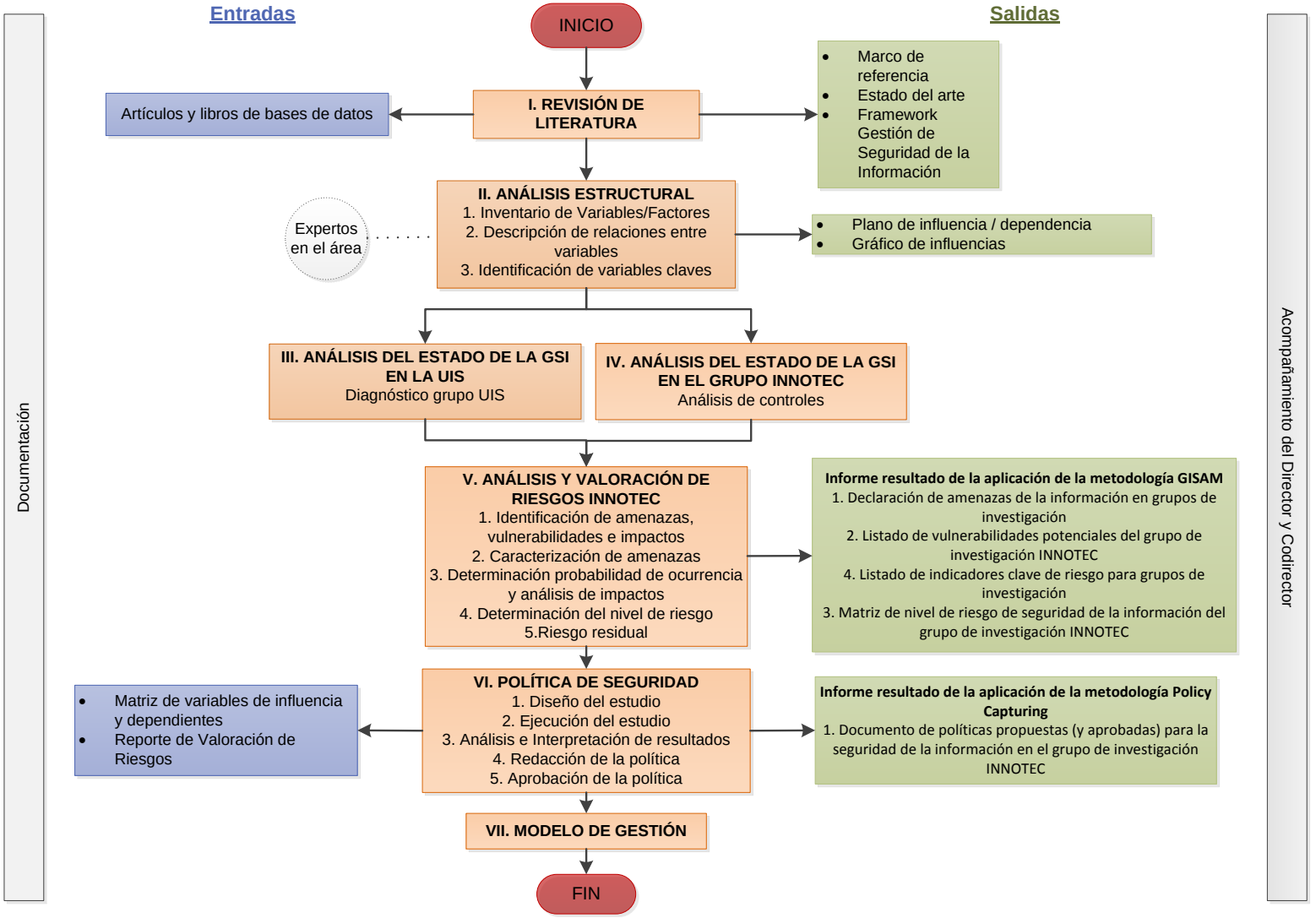
[45]LAYTON, Op. cit., p. 31.

f) Desarrollo de la política de seguridad de la información para el grupo de investigación INNOTEC: en esta etapa se buscaba desarrollar una política de seguridad de la información para INNOTEC, la cual definiera la(s) área(s) sobre la(s) cual(es) debe enfocarse la atención en lo que concierne a la seguridad de la información. Para ello, se utilizó la metodología policy capturing, mediante la cual se compilaron las perspectivas y criterios de los miembros del grupo de investigación. Se utilizó como técnica de recolección de la información un cuestionario en el cual se les pidió a las personas tomar una decisión concerniente a la seguridad de la información basadas en escenarios hipotéticos de un proyecto de investigación.

g) Modelo de gestión de la seguridad de la información en el grupo de investigación INNOTEC: En esta etapa se diseñó una aproximación a un modelo de GSI, el cual es de aplicación general para cualquier organización de conocimiento, y cuyo piloto se realizó en INNOTEC, a partir de la revisión de la literatura y de los resultados de las etapas previas del proyecto. El modelo está compuesto por las etapas que hacen parte de la GSI y una descripción general de las etapas.

Así mismo, como métodos y técnicas de recolección de datos se utilizó la revisión de literatura, las encuestas, la entrevista, observación y se hizo uso de información primaria y secundaria.

Figura 2. Diagrama de flujo de la metodología



Fuente. Autores del proyecto

3. MARCO REFERENCIAL

Para tener claridad acerca de la temática a tratar, se debe partir de la diferencia entre los conceptos de dato, información y conocimiento, los cuales son usados comúnmente de manera indistinta llevando a una errónea interpretación de su significado. Una manera sencilla de diferenciarlos es pensar que "los **datos** están localizados en el mundo y el **conocimiento** está localizado en las personas que conforman las organizaciones, mientras que la **información** adopta un papel mediador entre ambos"[46].

Según Davenport y Prusak[47], "un dato es un conjunto discreto, de factores objetivos sobre un hecho real". Un dato no dice nada sobre el porqué de las cosas, y por sí mismo tiene poca o ninguna relevancia o propósito. "A diferencia de los datos, la información tiene significado, relevancia y propósito. Los datos se convierten en información cuando su creador les añade significado"[48].

La información puede existir en muchas formas. Puede estar impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en películas o hablada en una conversación. Cualquiera que sea la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre debiera estar apropiadamente protegida[49].

El estándar ISO/IEC 27002:2005 define la seguridad de la información como "la protección de la información de un rango amplio de amenazas para poder

[46] CARRIÓN MAROTO, Juan. Introducción conceptual a la gestión del conocimiento. [en línea]. (2002). [Consultado el 10 de agosto de 2011]. Disponible en <http://manuelgross.bligoo.com/content/view/642641/Introduccion-Conceptual-a-la-Gestion-del-Conocimiento.html>

[47] DAVENPORT, Thomas y PRUSAK, Lawrence. Working knowledge: how organizations manage what they know. Cambridge, MA: Harvard Business School Press, 1998, p. 2.

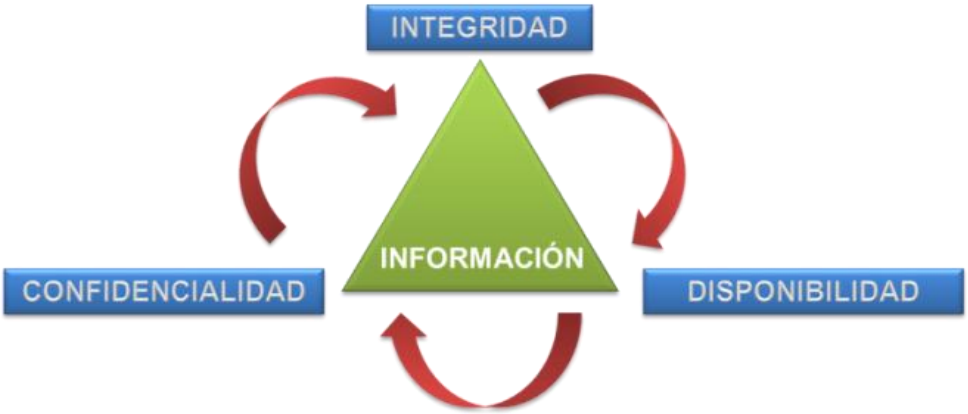
[48] Ibid. p. 4.

[49] INTERNATIONAL STANDARDS ORGANIZATION.ISO/IEC 27002:2005. Código para la práctica de la gestión de la seguridad de la información. 2005, p. 7

asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales. (…) Se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, y estructuras organizativas (…)"[50].

Asimismo, se encuentran en la literatura una amplia serie de conceptos y definiciones realizadas por varios autores para referirse a las dimensiones de seguridad de la información (Ver Figura 3). En la presente investigación se han seleccionado algunas de ellas, las cuales se presentan en la Tabla 1.

Figura 3. Dimensiones de Seguridad de la Información



Fuente. Autores del proyecto.

Tabla 1. Definiciones de las dimensiones de seguridad de la información

Autor	Confidencialidad	Integridad	Disponibilidad
Timothy Layton[51]	Asegurar que la información sea accesible solo a aquellos autorizados para su acceso		Asegurar que solo usuarios autorizados tengan acceso a información apropiada y sistemas de información cuándo ellos lo requieran.

[50] Ibid.
[51] LAYTON, T. Information Security: Design, implementation, measurement and compliance. Boca Raton: Auerbach Publications, 2007, p. 8.

Autor	Confidencialidad	Integridad	Disponibilidad
ISO 27000:2009 [52]	Propiedad de que la información no esté disponible o divulgada a individuos, entidades o procesos desautorizados	Propiedad de proteger la exactitud e integridad de los activos	Propiedad de estar accesible y utilizable cuando sea solicitado por una entidad autorizada
Witman y Mattord[53]	La información tiene confidencialidad cuando se previene la divulgación o exposición a individuos o sistemas desautorizados	La información tiene integridad cuando está toda completa e incorrupta.	La disponibilidad permite a los usuarios autorizados - personas o sistemas de cómputo - acceder a información sin interferencia u obstrucción, y recibirla en el formato requerido.
Boddington y Hill[54]	Proteger información sensible de divulgación desautorizada o intercepción inteligible.	Asegurar que la información sea precisa y completa en almacenamiento y transporte; y sea correctamente procesada	Asegurar que la información esté disponible para aquellos que están autorizados para tenerla, cuando y donde ellos deban tenerla.
Mitchell, Marcella y Baxter[55]	Proteger la información sensible de divulgación desautorizada o intercepción ininteligible	Salvaguardar la precisión y completitud de la información	Asegurar que la información y servicios vitales estén disponibles para usuarios autorizados cuando sea requerido.

Fuente: Autores del proyecto a partir de los autores mencionados en la tabla.

[52] INTERNATIONAL STANDARDS ORGANIZATION.ISO/IEC27000:2009.Information security management systems — Overview and vocabulary. 2005, p. 2-3.
[53] WHITMAN, Michael y MATTORD, Herbert J. Introduction to information security. En: _____. Principles of information security. 4 ed. Boston: Cengage Learning, 2011, p. 12-14.
[54] BODDINGTON, T. y HILL, S. Preparing for BS 7799 certification. En: GERBER, Mariana, VON SOLMS, Rossouw y OVERBEEK, Paul. Formalizing information security requirements. En: Information Management & Computer Security. Vol. 9, No. 1; p. 34.
[55] MITCHELL, Ruth; MARCELLA, Rita y BAXTER, Graeme. Corporate information security management. En: New Library World. Vol. 100, No. 5 (1999); p. 214.

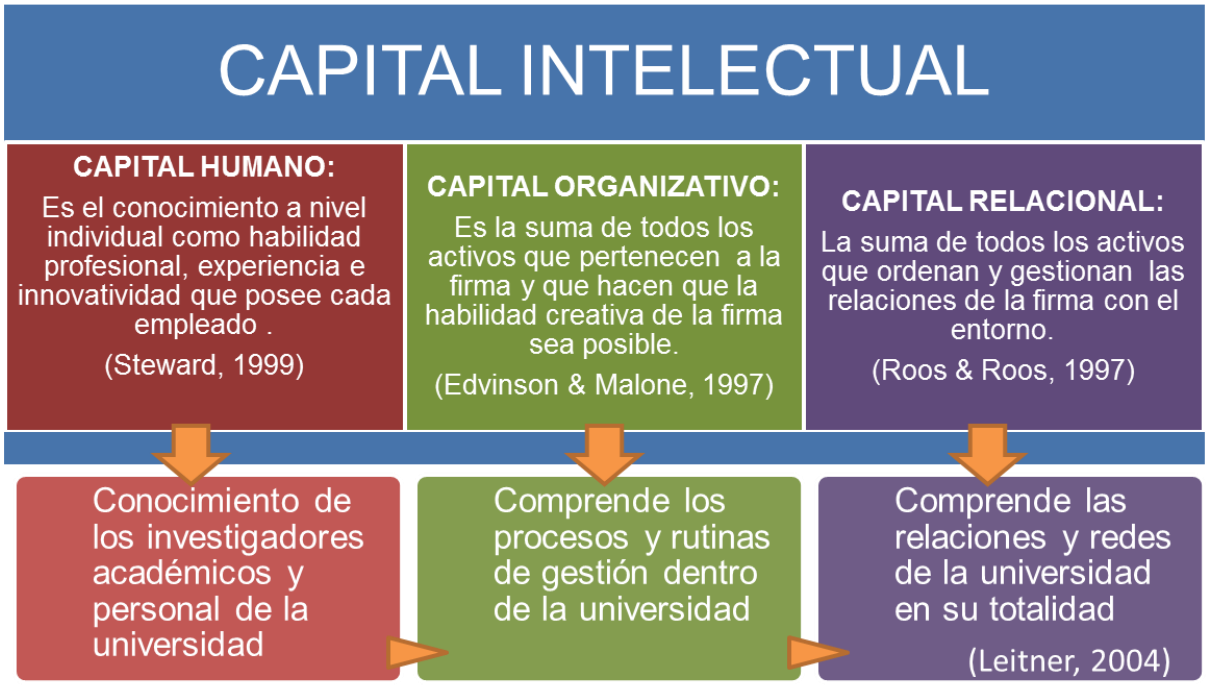
Por otra parte, conocimiento es una mezcla de experiencia, valores, información y "saber hacer" que sirve como marco para la incorporación de nuevas experiencias e información, y es útil para la acción. Se origina y aplica en la mente de los conocedores. En las organizaciones con frecuencia no sólo se encuentra dentro de documentos o almacenes de datos, sino que también está en rutinas organizativas, procesos, prácticas, y normas.

Ahora bien, el capital intelectual de una organización, es un concepto más complejo que ha venido evolucionando significativamente en los últimos años[56]. Este incluye aquellos factores de creación de valor de una organización que no se muestran en el tradicional balance general, pero que son de importancia crítica para la rentabilidad a largo plazo de una compañía[57]. Considerado como un activo intangible, el capital intelectual está constituido principalmente por tres partes: capital humano, capital estructural y capital relacional[58] (Ver Figura 4).

El capital humano representa la combinación del conocimiento, habilidades, capacidad de innovación y competencias de los individuos de la compañía. El capital estructural representa los almacenes de conocimiento no-humanos alojados en tecnología, software, bases de datos, estructura y rutinas, y el capital relacional representa el conocimiento alojado en las relaciones de negocios con clientes y proveedores[59] [60].

[56] SÄLLEBRANT, Op. Cit., p. 1473.
[57] ANDREOU, Andreas y BONTIS, Nick. A model for resource allocation using operational knowledge assets. En: The Learning Organization: An International Journal. Vol. 14, No. 4 (2007); p. 355.
[58] BONTIS, Nick. There's a price on your head: managing intellectual capital strategically. En: Ivey Business Journal (actualmente Business Quarterly). Vol. 60, No. 40 (1996); p. 43.
[59] SÄLLEBRANT, Op. Cit., p. 1473.
[60] BONTIS, Nick. Intellectual capital: an exploratory study that develops measures and models. En: Management Decision. Vol. 36, No. 2 (1998); p. 65-67.

Figura 4. Elementos del capital intelectual y el contexto de las universidades



Fuente: Autores del proyecto a partir de MARTÍNEZ, Hugo. Gestión de los activos intangibles en la educación superior. [Diapositivas]. Bogotá: 2010.

Habiendo entendido los anteriores conceptos puede definirse la gestión del conocimiento como la gestión del capital intelectual en una organización, con la finalidad de añadir valor a los productos y servicios que ofrece la organización en el mercado y de diferenciarlos competitivamente. Otra definición propuesta por William Wallace[61] considera a la gestión del conocimiento como "una nueva disciplina para habilitar personas, equipos y organizaciones completas en la creación, compartición y aplicación del conocimiento, colectiva y sistemáticamente, para mejorar la consecución de los objetivos de negocio".

[61] WALLACE, William. La Gestión del Conocimiento. En: Knowledge Management Today. Sevilla, Diciembre 1999. Definición disponible en http://www.a3net.net/es/gescon/definiciones.htm

Teniendo en cuenta que la gestión del conocimiento es más estratégica en algunas organizaciones que en otras, se ha definido una nueva categoría: "empresas basadas en el conocimiento"[62] [63] [64], la cual se refiere a aquellas organizaciones donde la mayor parte del trabajo es de naturaleza intelectual y donde empleados bien calificados y educados conforman la mayor parte de la fuerza de trabajo[65]. Ejemplos típicos de KIFs incluyen firmas de abogados y contadores, compañías de consultoría en administración, ingeniería y computación, agencias publicitarias, unidades de investigación y desarrollo, y empresas de alta tecnología.

En cuanto a la Seguridad de la Información, es preciso anotar, además, que esta no se da de manera repentina, sino que es un proceso continuo que hay que gestionar conociendo siempre las vulnerabilidades, amenazas y riesgos que afectan cualquier información (o conocimiento), así como sus causas, probabilidad de ocurrencia, e impacto.

En una empresa basada en el conocimiento, la necesidad de gestionar recursos de forma eficiente, dadas las diversas interrelaciones, la cantidad de tareas a realizar, el importante número de personas con diferentes cargos, todo sumado a la complejidad en el manejo de la información y limitado por el factor tiempo y recursos, exige diseñar modelos de gestión para este tipo de instituciones.

3.1. MODELO DE GESTIÓN

Antes de llegar a describir en qué consiste un modelo de gestión, se hace necesario acotar un marco común de definición para cada concepto: modelo y

[62] ALVESSON (1995), Op. Cit., p. 6.
[63] ROBERTSON, Maxine y SWAN, Op. Cit., p. 543.
[64] STARBUCK, Op. Cit.., p. 715.
[65] ALVESSON, Mats. Social identity and the problem of loyalty in knowledge-intensive companies. En: Journal of Management Studies. Vol. 37, No.8 (2000); p. 1101-1123.

gestión. Es así como, Chestnut[66], define modelo como "una representación cualitativa o cuantitativa de un proceso o una tentativa que muestra los efectos de aquellos factores que son importantes para los propósitos que se consideran". Además, según la Real Academia Española[67], se denomina modelo a "un esquema teórico, generalmente en forma matemática, de un sistema o de una realidad compleja, que se elabora para facilitar su comprensión y el estudio de su comportamiento".

Por otro lado, la gestión está caracterizada por una visión más amplia de las posibilidades reales de una organización, para resolver determinada situación o arribar a un fin determinado. Puede asumirse, como "la disposición y estructuración de los recursos de un individuo, o grupo, para obtener los resultados esperados. Puede generalizarse, también, como una forma de alinear los esfuerzos y recursos para alcanzar un fin determinado"[68].

Definida por Díaz et al.[69], la gestión es "la principal dimensión de una organización, en ella debe existir una necesidad permanente de interpretar el entorno, proyectar los cambios en él, y con un modelo de gestión estratégico poder dar respuesta a la realidad que exige dicho entorno". A su vez, Levy[70]

[66]CHESTNUT Harold.Systems engineering Tools. Nueva York: John Wiley, 1965. Citado en LÓPEZ, Rodrigo y TORRES Luis. Teoría de Sistemas. Universidad Nacional de Colombia. Departamento de Ingeniería de Sistemas e Industrial. 2009, p. 75

[67] REAL ACADEMIA ESPAÑOLA. Diccionario de la lengua española. 22 ed., Madrid: Espasa, 2001.

[68] BARROSO, Héctor. Diseño de un modelo de gestión para el centro de sangre de concepción "Dra. Marcela Contreras Arriagada". Concepción, 2009. Tesis para optar al grado de Magíster en Ingeniería Industrial. Universidad del Bio-Bio. Facultad de Ingeniería. Departamento de Ingeniería Industrial. P. 29

[69] DIAZ et al. Gestión estratégica del cambio institucional Citado en AGUILAR, José, et al. Metodología para la elaboración de un modelo de gestión en una institución pública venezolana: Fundacite-Mérida. En: Interciencia. Vol. 27, No. 6 (Jun. 2002); p. 293.

[70] LEVY, Alberto. El cómo y el porqué: un camino hacia el desarrollo empresario. Buenos Aires: Grupo Editorial Norma, 1989. Citado por AGUILAR, José, et al. Metodología para la elaboración de un modelo de gestión en una institución pública venezolana: Fundacite-Mérida. En: Interciencia. Vol. 27, No. 6 (Jun. 2002); p. 293.

señala que para interpretar y dirigir el cambio es necesario contar con un esquema de trabajo que se define en un modelo de gestión.

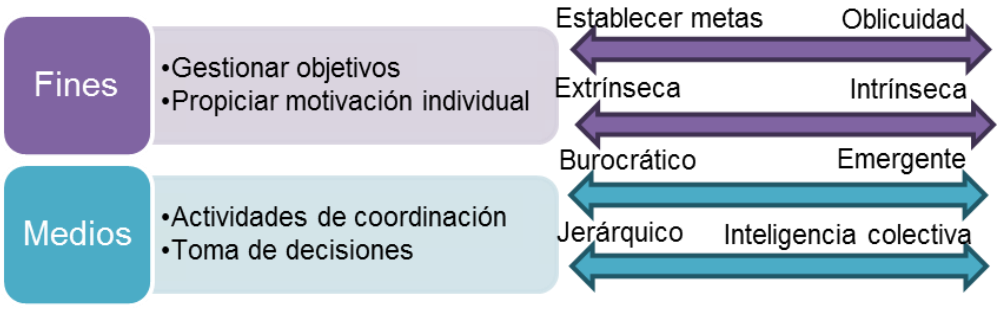
Por consiguiente, un modelo de gestión puede considerarse como un esquema o marco de referencia para la administración de una organización. En este contexto, un modelo de gestión es una forma de definir prioridades y tomar decisiones[71] y para ello, será necesario considerar acciones concretas de planificación, organización, coordinación, dirección y control generando de esta forma un lazo de retro-alimentación que le permita a los directivos verificar si el rumbo de la organización va en el sentido deseado o debe ser intervenido para corregir eventuales distorsiones.

Según Birkinshaw y Goddard[72], un modelo de gestión son las elecciones hechas por los altos ejecutivos de una compañía acerca de cómo se definen objetivos, se motiva el esfuerzo, se coordinan actividades y se asignan recursos; en otras palabras, como se define el trabajo de gestión. Un modelo de gestión involucra las decisiones al nivel más fundamental acerca como se maneja la empresa. Estas decisiones dan forma a las prácticas y comportamientos específicos de la empresa. Debido a que estos principios son invisibles y raramente se hacen explícitos, con mucha frecuencia las organizaciones son inconscientes de los modelos de gestión que están usando[73].

Estos mismos autores, identificaron cuatro conjuntos básicos de las actividades de gestión, y dos puntos polares de vista de cómo cada grupo de actividades se puede llevar a cabo (Ver Figura 5).

[71] TOBAR, Federico. Modelos de Gestión: La encrucijada de la reconversión. En: Énfasis Management. Vol. 5, No. 8 (Ago. 1999); p. 8.
[72] Ibid.
[73] BIRKINSHAW, Julian y GODDARD, Jules. What is your management model? En: MIT Sloan Management Review. Vol. 50, No. 2 (2009); p. 82.

Figura 5. Un marco de trabajo para dimensionar la gestión



Fuente. Autores del proyecto. Adaptado de BIRKINSHAW, Julian y GODDARD, Jules. What is your management model? En: MIT Sloan Management Review. Vol. 50, No. 2 (2009); p. 84.

Gestionar objetivos: una manera común de gestionar objetivos es tomar un enfoque directo. Los directivos definen un conjunto claro de objetivos para su equipo y un marco temporal en el cual estos deben ser alcanzados (establecer metas). Un principio alternativo es gestionar los objetivos oblicuamente, es decir, establecer una meta A, y en el proceso de alcanzarla, llegar al cumplimiento de una meta B (oblicuidad).

Motivación individual: en los años 50, Douglas McGregor identificó dos principios distintivos de motivación humana. La teoría X fue construida con base en la suposición de que los trabajadores son por naturaleza perezosos y requieren premios extrínsecos, principalmente dinero, para realizar bien sus trabajos. La teoría Y fue construida con base en la suposición de que los trabajadores son ambiciosos, auto-motivados, y valoran premios intrínsecos, como el sentimiento de realización[74].

Actividades de coordinación: La mayoría de las compañías grandes son burocracias, en donde se aplican regulaciones y estructuras formales para asegurar conformidad en el comportamiento y generar resultados consistentes.

[74] MCGREGOR, Douglas. The human side of enterprise. New York: McGraw Hill, 1960.

Por el contrario, hay compañías donde la coordinación se da de manera espontánea a través del comportamiento de interés personal de actores independientes.

Toma de decisiones: el principio de jerarquía les proporciona a los directivos responsabilidad directa por las decisiones que toman, les provee con autoridad legítima sobre sus subordinados y les concede el poder porque valora su experiencia y conocimiento. El principio alternativo es la inteligencia colectiva sugiere que bajo condiciones de incertidumbre la experticia agregada de un gran número de personas puede producir pronósticos más precisos y mejores decisiones que las de un pequeño número de expertos.

Autores como Dezerega[75] y Levy[76] hacen énfasis en que para administrar el cambio no es suficiente contar con un modelo de gestión, también es importante definirlo con claridad para que la organización tenga un estilo de trabajo en donde las fuerzas de todos se integren. Otro elemento importante a considerar cuando se realiza un modelo es la facilidad para identificar y entender a la organización, y con ello, aprovechar las fortalezas y realizar mejoras en las debilidades de una forma más eficiente. Se debe tener en cuenta que no hay un modelo único de gestión, ya que este se debe generar a partir del perfil de la organización (misión, visión, esquemas internos/externos, cadena de valor, entre otros).

Teniendo en cuenta los atributos de un modelo de gestión, Díaz et al.[77] expone diversos modelos de referencia que ilustran cambios institucionales, tales como: burocrático, evolucionista, cognitivo, educativo, político, hegemónico, relacional y estratégico.

[75]DEZEREGA, V. (1995).Control de la Gestión Empresarial. Centro de Desarrollo Gerencial. IESA. Caracas, Venezuela. Citado en AGUILAR, José, et al. Metodología para la elaboración de un modelo de gestión en una institución pública venezolana: Fundacite-Mérida. En: Interciencia. Vol. 27, No. 6 (Jun. 2002); p. 293.
[76] LEVY, Op. Cit.
[77] DÍAZ et al., Op. Cit.

Ahora bien, estos tipos de modelos sirven para entender y describir a las organizaciones, sin embargo no se puede generalizar ni enmarcar una institución a un sólo tipo de modelo, es por esto que se debe pensar en escoger elementos de cada uno y evitar otros. Basado en ello, cada organización deberá diseñar su propio modelo de gestión según lo que pretenda administrar, puesto que existen diferentes tipos, entre ellos, la gestión social, gestión de proyectos, gestión ambiental, gestión financiera, gestión del conocimiento y gestión de riesgos. Sin lugar a duda, tener claro el objetivo del modelo de gestión, enfocarse y acotarlo, generara resultados más eficientes y eficaces.

4. ESTADO DEL ARTE

Con el fin de obtener información reciente, relevante y relacionada con el problema de investigación, se utilizaron varias bases de datos a las cuáles la UIS tiene suscripción con acceso desde el campus universitario como: ISI Web of Science, Ebsco Host, ScienceDirect, Scopus, ProQuest, y Springerlink.

La revisión de la literatura partió de una búsqueda realizada en ISI WOS, utilizando el campo "tópico" con la frase *"Information Security"*, entre comillas para asegurar que las dos palabras aparecieran juntas, y con un horizonte de tiempo de 2001 – 2012. El principal foco de esta revisión fue investigar lo que se ha dicho acerca de la gestión de seguridad de la información en las organizaciones.

Primeramente, se examinaron los títulos de los artículos, con el fin de excluir aquellos que no estuvieran aquellos que no estuvieran directamente relacionados con el foco de la revisión. Posteriormente, se realizó un Posteriormente, se realizó un segundo filtro por el contenido y temática tratada en el resumen, para finalmente el resumen, para finalmente organizar las publicaciones de acuerdo a las palabras claves en nueve categorías (Ver claves en nueve categorías (Ver

ANEXO 3), que dieron origen al desarrollo de un marco de trabajo, o *framework,* sobre gestión de seguridad de la información (Ver

ANEXO 4).

Adicionalmente, se incluyeron en la revisión artículos de los autores más relevantes en el tema, y documentos relacionados, utilizando el método "bola de nieve", que consiste en descubrir otros documentos de interés mediante la revisión de la bibliografía citada en los documentos iniciales. Como consecuencia, se encontraron documentos de años anteriores al 2001, y se pudo identificar algunos autores relevantes sobre los cuales se profundizó la búsqueda.

Además para complementar los resultados, se realizó una búsqueda utilizando las mismas palabras claves (*"Information Security"*), en la herramienta Google Académico, incluyendo los documentos relevantes diferentes a los que ya se tenían. Finalmente, se obtuvieron más de 100 publicaciones para el análisis. A continuación se presenta una breve reseña de los artículos consultados.

Hace más de 20 años, algunos académicos como Drucker[78], Porter y Millar[79], fueron los primeros en reconocer que una "Revolución de la Información" estaba teniendo lugar, la cual tuvo un impacto inmediato, con efectos significativos en todos los aspectos de la vida organizativa[80]. A través de los años, la experiencia ha comprobado que una buena gestión de la información, no sólo puede mejorar significativamente el desempeño organizativo[818283], sino que también puede transformar radicalmente los procesos, estructura y cultura de la organización[8485].

[78] DRUCKER, Peter. The coming of the new organization. En: Harvard Business Review. Vol. 66, No. 1 (1988); p. 47.
[79] PORTER, Michael y MILLAR, Victor. How information gives you competitive advantage. En: Harvard Business Review. Vol. 64, No. 4 (1985); p. 149.
[80] ZAMMUTO, Raymond, et al. Information technology and the changing fabric of organization. En: Organization Science. Vol. 18, No. 5 (Sep. 2007); p. 751.
[81] BRYNJOLFSSON, Erik y HITT, Lorin. Paradox lost? Firm-level evidence on the returns to information systems spending. En: Management science. Vol. 42, No. 4 (Abr. 1996).Citado por DOHERTY, Neil; ANASTASAKIS, Leonidas y FULFORD, Heather. The information security policy unpacked: a critical study of the content of university policies. En: International Journal of Information Management. Vol. 29, No. 6 (Dic. 2009); p. 449.
[82] SIRCAR, Sumit y CHOI, Jung. A study of the impact of information technology on firm performance: a flexible production function approach. En: Information Systems Journal. Vol. 19, No.

Dada su creciente importancia, la información es a menudo vista como análoga a la "sangre" de la organización[86] [87] [88]. Por consiguiente, si el flujo de información es continuo, los procesos y tareas se ejecutarán de manera óptima; por el contrario, si este es restringido o seriamente perturbado, entonces la organización puede deteriorarse o incluso morir, lo cuál se constituye en un riesgo de seguridad de la información. Acerca de cómo prevenir estos riesgos, Kevin Mitnick hizo la siguiente afirmación: "Nunca se confíe de los mecanismos de seguridad en la red para proteger su información. Revise su punto más vulnerable. En la mayoría de los casos descubrirá que este se encuentra en las personas"[89]. De esta forma, se resalta que los controles técnicos por si mismos no aseguran la seguridad de los activos de información de una organización, y tampoco resolverán los problemas relacionados con seguridad de la información. Sin embargo, en el mundo empresarial no siempre se ha visto la información desde la misma perspectiva.

Con el tiempo, el enfoque de seguridad de la información ha evolucionado desde la seguridad física orientada a la protección de computadores y dispositivos de

---

3 (2009).Citado por DOHERTY, Neil; ANASTASAKIS, Leonidas y FULFORD, Heather. The information security policy unpacked: a critical study of the content of university policies. En: International Journal of Information Management. Vol. 29, No. 6 (Dic. 2009); p. 449.

[83] WARD, Jhon y PEPPARD, Joe. Strategic planning for information systems. 3 ed. Chichester: Wiley Publishing, 2002. Citado por DOHERTY, Neil; ANASTASAKIS, Leonidas y FULFORD, Heather. The information security policy unpacked: a critical study of the content of university policies. En: International Journal of Information Management. Vol. 29, No. 6 (Dic. 2009); p. 449.

[84] DOHERTY, Neil; KING, Malcolm y AL-MUSHAYT, Omar. The impact of inadequacies in the treatment of organizational issues on information systems development projects. En: Information & Management. Vol. 41, No. 1 (Oct. 2003); p. 50.

[85] MARKUS, Lynne. Technochange management: using IT to drive organizational change. En: Journal of Information Technology. Vol. 19, No. 1 (2004); p. 4.

[86]HALLIDAY, S., BADENHORST, K. y VON SOLMS, R.A business approach to effective information technology risk analysis and management. En: LATEGAN, Neil y VON SOLMS, Rossouw. Towards enterprise information risk management: a body analogy. En: Computer Fraud & Security. Vol. 2006, No. 12 (Dic. 2006); p. 17

[87] WILLS M. Personal communication. En: GERBER, Mariana y VON SOLMS, Rossouw. Management of risk in the information age. En: Computers & Security. Vol. 24 (2005); p. 17.

[88] PEPPARD, Joe. The conundrum of IT management. En: European Journal of Information Systems. Vol. 16, No. 1 (2007); p. 339.

[89] SIMON, William y MITNICK, Kevin. The art of deception: controlling the human element of security. Indianapolis: Wiley Publishing, 2002, p. 79.

almacenamiento de información, pasando por la seguridad de sistemas y redes de tecnologías de información, y actualmente se concentra en la gestión de alto nivel mediante políticas, procedimientos y controles basados en las personas[90].

Según von Solms[91], el desarrollo del campo de la seguridad de la información se puede describir a partir de cinco etapas, llamadas "olas", comprendidas entre el comienzo de la década de los 80's y el periodo actual. Sin embargo, estas etapas no son excluyentes sino que cada nueva etapa complementa a la anterior dándole un énfasis diferente a cada uno de los aspectos relacionados con seguridad de la información; y, por tanto, deben ser vistas como etapas paralelas entre sí.

La etapa anterior al comienzo de los años 80, es decir, la primera ola, se conoce como la "Ola Técnica" (*"Technical Wave"*), la cual estuvo caracterizada por un enfoque bastante técnico, donde la responsabilidad de seguridad recaía fundamentalmente sobre los expertos técnicos de la organización. Durante esta ola, los principales mecanismos de protección utilizados estaban condicionados a formas simples de identificación y autorización de acceso como listas de control de acceso, y contraseñas; por el contrario, aspectos como políticas de seguridad y concientización de los usuarios, aún no habían adquirido ninguna relevancia.

Más adelante, al inicio de la década de los 80's, la aparición de nuevas tecnologías como el computador personal y el internet, junto con el hecho de que la información ya no estaba almacenada en un solo computador central, sino en computadores de escritorio conectados a través de redes, crearon la necesidad de implementar nuevos mecanismos de seguridad para ejercer control sobre quien accedía a la información. Como resultado de estas dos primeras etapas, los

[90] NNOLIM, Anene. A framework and methodology for information security management. Southfield, 2007. Dissertation (Doctor of Management in Information Technology).Lawrence Technological University. Graduate Faculty of the College of Management.P.2

[91] VON SOLMS, Bassie. The 5 Waves of Information Security: From Kristian Beckman to the Present. En: 25th IFIP TC-11 International Information Security Conference. (2010); p. 1.

profesionales del área obtuvieron la atención de los gerentes y altos mandos de las empresas, por lo cual la segunda ola ha sido denominada “Ola Administrativa” (*“Management Wave”*[92]). De esta manera, se mejoró significativamente la seguridad de la información y comenzó a ser más notorio que en la dimensión humana estaba el reto más grande para la seguridad de las organizaciones.

De acuerdo con Cano[93], los últimos diez años se han distinguido por un nuevo cambio de rumbo en la seguridad de la información: los negocios se efectúan en un contexto global y virtual que desafía a las organizaciones “a ofrecer condiciones de seguridad concretas y viables que balanceen las necesidades de los procesos empresariales y los principios de seguridad de la información: confidencialidad integridad y disponibilidad”. Por ende, la seguridad de la información pasa de ser un fin en sí mismo, a ser un medio para lograr asegurar la competitividad de las empresas que hacen parte de este entorno global altamente riesgoso.

Debido a estos acontecimientos durante la segunda ola, las compañías empezaron a investigar los aspectos relacionados con mejores prácticas en seguridad de la información. Las empresas empiezan a preocuparse por conocer los principales componentes de un buen plan de seguridad, entonces aparecen nuevos intereses como establecer políticas de seguridad, evaluar la seguridad de la información frente a los *stakeholders* mediante monitoreo y medición, obtener algún tipo de certificación oficial, todo manejado bajo una cultura de seguridad[94].

Además, el rol del empleado como usuario final de la información llama la atención y con esto cobra importancia la dimensión humana en este proceso, conduciendo

[92] VON SOLMS, Bassie. Information Security: the third wave? En: Computers & Security. Vol. 19 (2000); p. 616.
[93] Cano, Op. cit., p. 6.
[94] VON SOLMS, Bassie. Information Security: the fourth wave. En: Computers & Security. Vol. 25, No. 3 (May. 2006); p. 165.

por tanto a una tercera ola, comprendida entre mediados de los 90´s y el 2005, llamada "Ola Institucional" (*"Institucional Wave"*), que buscaba contar con una estandarización de la seguridad de la Información en las empresas, haciendo evidente que la seguridad de la información está constituida por varias dimensiones interrelacionadas, y no solamente una dimensión técnica como se había creído en un comienzo.

De manera general, la gestión de seguridad de la información puede ser vista desde tres niveles principales: estratégico, táctico y operacional. Estos tres niveles corresponden a los tipos de asuntos que conciernen a la alta dirección, incluyendo la naturaleza general de los conocimientos necesarios para administrar la seguridad, en esos niveles[95].

Ante esta necesidad de un claro direccionamiento, en 1995 fue publicada por la British Standards Institution[96], la norma BS 7799, cuyo propósito era el de proporcionar a cualquier empresa, sin importar su país de origen, un conjunto de prácticas de referencia para la gestión de la seguridad de su información. "La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente"[97].Hoy en día, la primera parte de la norma se conoce como ISO/IEC 27002, y la segunda como ISO/IEC 27001, cuyas versiones más recientes son del año 2005.

---

[95] BELSIS, Petros; KOKOLAKIS, Spyros y KIOUNTOUZIS, Evangelos. Information systems security from a knowledge management perspective. En: Information Management &Computer Security. Vol. 13, No. 3 (2005); p. 193.

[96] BSI Group ofrece ahora una completa cartera de servicios de negocio a los clientes, ayudándoles a elevar su rendimiento y mejorar su competitividad en todo el mundo. Sitio web: http://www.bsigroup.com/

[97] LÓPEZ, Agustín y RUIZ, Javier. Origen de ISO 27000. En: EL PORTAL DE ISO 27001 EN ESPAÑOL. [En línea]. [Consultado el 10 de agosto de 2011]. Disponible en <http://www.iso27000.es/iso27000.html#section3a>

Otro tema que tomó relevancia durante esta época fue la concientización en seguridad de la información, dado que un trabajador desinformado acerca de los riesgos de seguridad puede poner en peligro la ventaja competitiva de la empresa.

A pesar de todos estos esfuerzos, ninguna de las directrices de ISO proporciona la base teórica necesaria para un marco y una metodología para la gestión de la seguridad[98]. Algunos autores, como Hong et al.[99] sugieren que la ausencia de un marco y una metodología para la gestión de la seguridad han contribuido a la falta de teoría en gestión de la seguridad.

Alrededor de 2005, se empieza a hablar de una nueva fase, caracterizada básicamente por manejar el tema de la gestión de la seguridad de la información; esta se conoce como Ola de Gobernanza de Seguridad de la Información" (*"Information Security Governance Wave"*).

Como se mencionó antes, en la tercera ola las empresas comienzan a crear técnicas para medir el estado y nivel de cumplimiento de seguridad, esto origina informes que son evaluados por la alta dirección. Es claro, entonces, que un buen gobierno corporativo y el papel que este juega en la compañía, indican un nivel más elevado de compromiso de la compañía respecto a la manera en que se gestiona la Seguridad de la Información.

Antes de discutir sobre la quinta y última ola de la seguridad de la información, es conveniente mencionar que como consecuencia del creciente énfasis en la seguridad de la información, se da lugar a la aparición del concepto de gestión de la seguridad de la información[100], con lo que se busca asegurar los datos y la

[98] NNOLIM, Op. Cit., p. 5.
[99] HONG, Kwo-Shing, et al. An integrated system theory of information security management. En: Information Management & Computer Security. Vol. 11, No. 5 (2003); p. 243.
[100] VON SOLMS (2006), Op. Cit., p. 167.

información de la empresa, delegando responsabilidades tanto a la alta gerencia como a los empleados. El objetivo principal es garantizar la confidencialidad, integridad, y conservación de la información, con el propósito de no perder la ventaja competitiva de la compañía. El cual se logra a través de un despliegue importante de medidas de seguridad, fuerte inversión en infraestructura de tecnologías de información y comunicaciones [TICs]; llevando a muchas empresas a extender sus sistemas en la internet y la World Wide Web; obligando a los millones de usuarios, clientes y/o consumidores a entrar en la era cibernética.

Esto llevó a la quinta y última oleada de seguridad de la información hasta el momento, que se llama la "Ola de Seguridad Cibernética" (*"Cyber Security Wave")*, y se originó a partir del año 2006, como consecuencia de los riesgos que Internet ha traído para las compañías, puesto que estas al actualizarse y trabajar bajo sistemas basados en la red, proveen a los ciberdelincuentes la oportunidad de atacar sus sistemas y apropiarse de información valiosa a través de tácticas como el *malware, phishing, spoofing*, entre otras[101].

Según Symantec[102], "La internet se ha convertido en una herramienta de negocios fundamental, sin embargo, trabajar en la web nunca había sido más peligroso". Este autor afirma que, se ha llegado a la etapa en que es imposible asegurar y proteger adecuadamente algunos sistemas basados en internet, sumado a que algunos especialistas en seguridad de la información, la mayoría de los casos no son realmente profesionales. Sin duda, esta ola cuestiona las garantías que se tienen y desafía a las compañías para que reconsideren el papel que han desempeñado en este ámbito.

[101] VON SOLMS (2010), Op Cit., p.4.
[102] SYMANTEC. The wild, wild web: how to ensure 360-degree border security. Symantec, 2010.

Otros autores, como Rungta et al.[103] proponen un nuevo enfoque a la gestión de seguridad de la información, y basan su propuesta afirmando que las estructuras de seguridad existentes en las empresas son insuficientes. Tal parece que la gestión de seguridad de la información aún no ha alcanzado el punto de madurez, en el que se convierte en un proceso continuo de gestión[104]. Vermeulen y von Solms[105] consideran que una profunda arquitectura de seguridad de la información es necesaria para la gestión eficaz de la seguridad. Esto es corroborado por un estudio de Mitchell, Marcella y Baxter[106] acerca de las cuestiones que influencian la gestión de seguridad de la información corporativa, en dónde observaron que la mayoría de las organizaciones estudiadas no eran proactivas en la gestión de seguridad de la información.

Pero no es sólo el uso de la información lo que causa conmoción en las organizaciones; durante los últimos años, se ha generado la necesidad de reconocer la importancia de gestionar de forma activa y explícita el conocimiento como fuente de ventaja competitiva sostenible[107]. Uno de los aspectos que muchas organizaciones dejan de lado radica en que no basta con preservar la confidencialidad, integridad y disponibilidad de la información, también es necesario garantizar la protección del conocimiento o capital intelectual, pues es este último el que les aporta mayor valor, especialmente en el caso de las KIFs* como las universidades. Según Mok[108], este tipo de instituciones deben tener un mayor enfoque del tema, puesto que son organizaciones con intensiva generación

[103] RUNTGA, Sanjay, et al. Bringing security proactively into the enterprise. En: Intel Technological Journal. Vol. 08, No. 04 (2004); p. 304.
[104] NNOLIM, Op. Cit., p. 7.
[105] VERMEULEN, Clive y VON SOLMS, Rossouw. The information security management toolbox: taking the pain out of security management. En: Information Management & Computer Security. Vol. 10, No. 3 (2002, pp. 120.
[106] MITCHELL, MARCELLA y BAXTER. Op. cit., p. 213.
[107] JOHANNESSEN, Jon-Arild y OLSEN, Bjørn. Knowledge management and sustainable competitive advantages: the impact of dynamic contextual training. En: International Journal of Information Management. Vol. 23, No. 4 (Ago. 2003); p. 278.
*KIFs: knowledge-intensive firms, empresas basadas en conocimiento.
[108] MOK, Op. cit. p. 540.

de conocimiento; la calidad y la seguridad de sus activos de información debería ser una prioridad muy alta.

En este tipo de instituciones la realización efectiva de sus actividades educativas y de investigación es cada vez más dependiente de la disponibilidad, integridad y exactitud de los recursos de información. Sin embargo, según una investigación realizada por Doherty, Anastasakis y Fulford[109], en la que se estudió una muestra de 61 universidades pertenecientes "World University Ranking 2007" del Times Higher Education Supplement, "solo el 7% de las políticas de seguridad de las universidades seleccionadas contenían una mención explícita de la prioridad especial concedida a la seguridad de la información, dada la naturaleza de conocimiento que tiene la organización".

Para asegurar el éxito, las organizaciones deben tratar de maximizar el nivel de conocimiento exclusivo utilizable dentro de sí mismas. Actualmente, este objetivo se aborda desde dos campos de actividad principales: Gestión del Conocimiento y Gestión de la Seguridad de la Información. El triunfo de ambas disciplinas depende fuertemente de las personas.

En la Gestión del Conocimiento, las personas tienen que compartir su conocimiento individual – tanto tácito como explícito – con otros para formar y establecer un cuerpo de conocimiento comprensible que pueda ser usado (y aprovechado) por toda la organización. Lo mismo es cierto acerca de la Seguridad de la Información. Después de décadas de acercamientos meramente técnicos, ahora es ampliamente aceptado que "las personas son la piedra angular de la seguridad de la información"[110].

[109] DOHERTY, Neil; ANASTASAKIS, Leonidas y FULFORD, Heather. The information security policy unpacked: a critical study of the content of university policies. En: International Journal of Information Management. Vol. 29, No. 6 (Dic. 2009); pp. 455.
[110] BISHOP, Matt y FRINCKE, Deborah. A human endeavor: lessons from Shakespeare and beyond. En: IEEE Security & Privacy Magazine. Vol. 3, No. 4 (Jul. 2005); p. 49.

Para lograr que la seguridad de la información funcione, las personas deben comportarse de una manera segura, sin eludir los mecanismos y procedimientos de seguridad establecidos, tomando decisiones correctas en caso de eventos imprevistos[111]. La forma de responder a esta brecha de seguridad es a través de un mecanismo ampliamente reconocido como único: la política de seguridad de la información[112] [113] [114]. Por lo tanto, es particularmente importante revisar el papel y alcance de una política de seguridad.

[111] GLASER, Timo y PALLAS, Frank. Information security and knowledge management: solutions through analogies? Berlin: Universidad Técnica de Berlín, 2007, p. 17.
[112] VON SOLMS, Bassie y VON SOLMS, Russouw. The 10 deadly sins of information security management. En: Computers & Security. *V*ol. 23, No. 5 (Jul. 2004); p. 372.
[113] WADLOW, Thomas. The process of network security: designing and managing a safe network. Reading: Addison-Wesley Professional, 2000, p. 304.
[114] WHITMAN, Michael. In defense of the realm: understanding threats to information security. En: International Journal of Information Management. Vol. 24 (2004); p. 51.

Dentro de la literatura se llega a un acuerdo; una política de seguridad de la información es un documento de alto nivel, que define los objetivos de la organización, las intenciones y prioridades[115] [116], por tanto, da condiciones inmejorables que protegen de manera proactiva la disponibilidad, confidencialidad e integridad de la información empresarial[117] [118]. Entonces una buena política debería: destacar roles, derechos y responsabilidades individuales; definir explícitamente los usos autorizados; proporcionar condiciones a los empleados que les permita reportar amenazas identificadas o sospechosas; definir sanciones por violaciones a la seguridad de la información; y, facilitar la retroalimentación que mantenga actualizadas las políticas de seguridad en la organización[119].

A pesar de la creciente preocupación de profesionales y académicos por la ausencia de una base teórica y un acercamiento formal a la gestión de seguridad de la información, Herath[120] advierte que la investigación empírica sobre las conductas en los usuarios de la información y los factores que influyen en ellas apenas ha comenzado.

[115] HÖNE, Karin y ELOFF, J.H.P. Information security policy – what do international information security standards say? En: Computers & Security. Vol. 21, No. 5 (2002); p. 402.
[116] HONG, Op. Cit., p. 244.
[117] BASKERVILLE, Richard y SIPONEN, Mikko. An information security meta-policy for emergent organizations. En: Logistics Information Management. Vol. 15, No. 5/6 (2002); p. 338.
[118] DAVID, Jon. Policy enforcement in the workplace. En: Computers & Security. Vol. 21, No. 6 (2002); p. 513.
[119] WHITMAN, Op. Cit., p. 52.
[120] HERATH, Tejaswini. Essays on information security practices in organizations. Buffalo, 2008.Dissertation (Doctor of Philosophy).University of New York. Faculty of the graduate school.P. 9.

5. ANÁLISIS ESTRUCTURAL

Con el objetivo de entender una realidad o problema específico, es interesante abordarlo, entendiéndolo como un sistema. Se crea entonces un modelo, en este caso, basado en conocimientos, en el que se "sintetiza en pocas variables el funcionamiento de un aspecto complejo". "La estructura de las variables en un sistema definido, conserva cierta permanencia, lo que varía son las relaciones entre ellas"[121], su evolución y las nuevas maneras de medirlas. Todas estas características enmarcan el *análisis estructural*, y lo hacen ser una herramienta versátil, y por esta razón práctica para un proyecto en el que se quiere conocer escenarios reales y potenciales, en el "corto" y "largo" plazo – Fotos instantáneas de la situación.

En general, el análisis estructural es "una herramienta diseñada para el enlace de ideas", que se utiliza en la construcción de escenarios, principalmente con el fin de "encontrar las variables influyentes, dependientes y esenciales para entender la evolución del sistema y predecir su comportamiento futuro. El principal mérito de este método radica en la ayuda que presta a un grupo para plantearse las buenas preguntas y estructurar una reflexión colectiva"[122], tal reflexión, debe ser lo suficientemente sencilla para apropiar fácilmente el proceso y los resultados[123]. Esta herramienta permite describir un sistema con la ayuda de una matriz en donde los diferentes actores del mismo, relacionan los elementos que lo constituyen. Su objetivo es revelar las principales variables influyentes y dependientes y de esta manera los elementos esenciales entre aquellos

[121] GARAVITO, Edwin. Presentación 2. Material académico para la asignatura Técnicas modernas de optimización. Presentación en formato PDF [En línea]. [Consultado el 15 de febrero de 2012] Disponible en: http://gavilan.uis.edu.co/~garavito/index_general.htm
[122] BALLESTEROS, Diana Paola. Análisis estructural prospectivo aplicado al sistema logístico. En: Scientia et Technica. Vol. 14, No. 39 (2008); p. 194.
[123] GODET, Michel. La caja de herramientas de la prospectiva estratégica. 4 ed. París: Gerpa con la colaboración de Electricité de France, Mission Prospective, 2000, p.74.

constitutivos de un problema, para la evolución del sistema[124]. En otras palabras, permite "identificar el peso de los fenómenos y la gobernabilidad que se tiene sobre ellos dentro del sistema"[125]; reduciendo de esta forma la complejidad del sistema de estudio.

Este proceso debe ir acompañado del juicio de los evaluadores[126] y tiene la ventaja de estimular la reflexión dentro del grupo, y hacer que los participantes analicen ciertos aspectos que algunas veces son poco intuitivos[127], pues si bien en general el 80% de los resultados de un ejercicio de análisis estructural confirma las intuiciones y puntos de vista de los evaluadores, el 20% restante genera preguntas entre los participantes por su carácter no intuitivo, lo que además, permite validar el método al mostrar que sus resultados no distan de las percepciones del grupo de evaluadores. Es de anotar, que la realización de este tipo de ejercicio tiene consigo limitaciones derivadas de la subjetividad de las variables y la evaluación de las relaciones que se dan entre ellas.

En general, el proceso que se lleva a cabo en la realización de un análisis estructural consta de tres etapas[128]: Elaboración del listado de variables, identificación de las interrelaciones por medio de la matriz de análisis estructural e identificación de las variables clave[129]. A continuación se detallan las especificidades de cada una de ellas.

[124] GODET, Op. cit. p.68.
[125] MOJICA, Francisco José. La construcción del futuro. Bogotá: Universidad Externado de Colombia, 2005, p.123.
[126] MOJICA S., Francisco. Prospectiva: Técnicas para visualizar el futuro. Bogotá: Legis, 1991. 116p.
[127] ARCADE, Jacques, et al. Análisis estructural con el Método Micmac y estrategia de los actores con el Método Mactor. 2004. [En línea]. [Consultado el 20 de febrero de 2012]. Disponible en: <http://guajiros.udea.edu.co/fnsp/cvsp/politicaspublicas/godet_analisis_estructural.pdf>
[128] ARISTA, Anarrosa, et al. Prospectiva: Construcción social del futuro. Santiago de Cali: ILPES, 1997, p. 116
[129]GODET, Op.cit,

5.1. DEFINICIÓN DEL SISTEMA Y VARIABLES A EVALUAR

Como paso fundamental para la identificación de las variables que serán sujeto de evaluación es preciso especificar el sistema a analizar. En este sentido, se parte de la definición de sistema dada por O'Brien, quien establece que un sistema es "un grupo de componentes interrelacionados que trabajan juntos hacia un fin común, aceptando inputs y produciendo outputs en un proceso de transformación organizado"[130].

Un sistema es más complejo mientras más componentes y más interrelaciones existan entre estos. Como consecuencia, surgen propiedades o características nuevas que no pueden explicarse analizando de forma aislada cada elemento del sistema. En este caso, se considera como sistema de estudio, el sistema de seguridad de la información en grupos de investigación, el cual esta conformado por diferentes componentes, de tipo tecnológico o humano, que pueden aumentar o disminuir el nivel de seguridad en este tipo específico de organizaciones basadas en conocimiento.

Asimismo, se pueden establecer los factores en que se divide el sistema y en los cuales se deben clasificar las variables. Esta etapa, aunque es la menos formal, es crucial para el resto del proceso, ya que en ella se generan no solo las variables sino la estructura del sistema bajo estudio; en el curso de esta fase conviene ser lo más exhaustivo posible y no excluir a priori ninguna pista de investigación[131].

---

[130] O'BRIEN, J. Management Information Systems: A Managerial End User Perspective. 2 ed. Boston: Irwin, 1998.

[131] Prospectiva. Análisis Estructural, Mic Mac. Matriz de Impactos cruzados – Multiplicación Aplicada a una clasificación, p. 7. [Consultado 2 febrero de 2012] Disponible en: <http://www.ucol.mx/acerca/coordinaciones/cgic/cgic/Ejeinvestigacion/Bibliografia/Micmac_instrucciones.pdf>

Con base en el esquema general del sistema se realizó inicialmente una lluvia de ideas a fin de construir un listado ideas a fin de construir un listado inicial de variables que sirviera de soporte para la identificación final de las variables la identificación final de las variables a analizar. Este listado se construyó previa revisión bibliográfica, estudiando revisión bibliográfica, estudiando diferentes documentos alusivos a la seguridad de la información, entre los que se la información, entre los que se encuentran, el libro "Information Security" de Layton; normas de referencia o Layton; normas de referencia o metodologías para valoración de riesgos, como, OCTAVE[132], MAGERIT, e ISO/IEC OCTAVE[132], MAGERIT, e ISO/IEC 27002:2005; guías de seguridad de la información, como la proporcionada por información, como la proporcionada por NIST[133]; estudios institucionales y de organismos internacionales; entre organismos internacionales; entre otros. Luego de reuniones iniciales no estructuradas tipo tormenta de ideas en que estructuradas tipo tormenta de ideas en que emergieron más de 70 variables, la discusión se estructuró alrededor de discusión se estructuró alrededor de una propuesta de 59 variables, que pueden ser detalladas en el ser detalladas en el

[132]Operationally Critical Threat, Asset, and Vulnerability Evaluation.Ver Capitulo 3. Estado del Arte
[133]National Institute of Standards and Technology.Sitio web: http://www.nist.gov/index.html

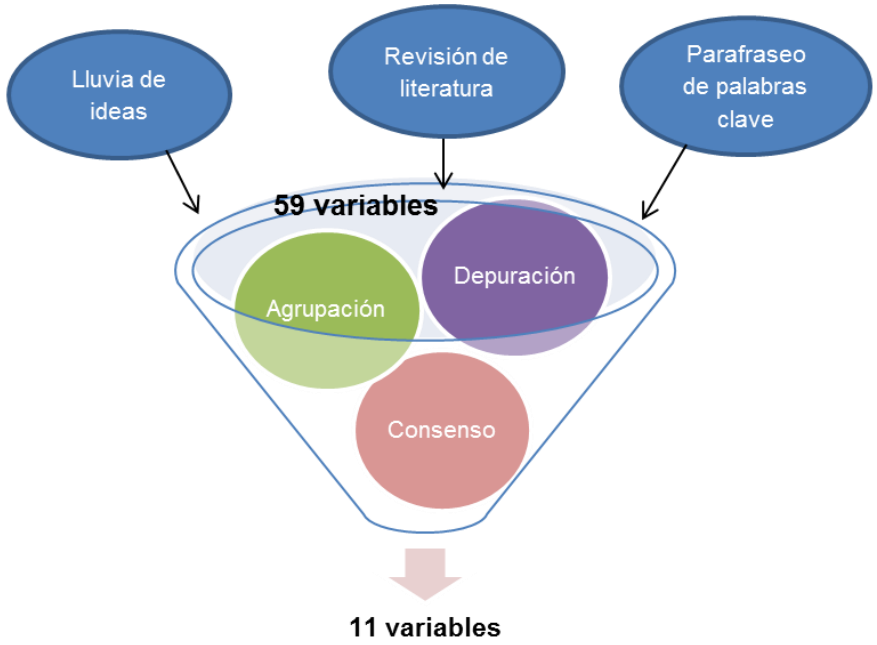
ANEXO 5. Es importante aclarar que en este primer paso se eliminó cualquier tipo de restricción en la consideración de las variables, evitando la crítica de las mismas así como la exploración de las implicaciones de cada una, lo que generó una lista extensa y posiblemente redundante.

Teniendo en cuenta la lista anterior, y luego de un proceso de depuración, agrupación según relaciones y semejanzas agrupación según relaciones y semejanzas existentes y un consenso entre las autoras y el director y codirector del autoras y el director y codirector del proyecto, se obtuvo como resultado una lista final de variables a evaluar que final de variables a evaluar que logran explicar las 59 anteriores de una manera más general. En el más general. En el

ANEXO 5, se presenta la lista de variables definidas, 11 en total, con su respectiva definición, que componen el sistema, el cual no es elevado, pues este ejercicio no busca describir con precisión el funcionamiento del sistema estudiado, sino destacar sus principales características[134].

[134]GODET, Op. cit. p. 106.

Figura 6. Consolidación de variables



Fuente. Autores del proyecto

5.2. IDENTIFICACIÓN DE LAS INTERRELACIONES ENTRE LAS VARIABLES

La evaluación de la influencia que ejerce cada variable sobre las otras fue desarrollada por los evaluadores señalados en el

ANEXO 6, los cuales fueron seleccionados de acuerdo a su trayectoria en la realización de actividades de investigación o administración en los grupos de investigación y UAA de la UIS, y su conocimiento sobre el funcionamiento del sistema, validados por el director del proyecto. Éstos recibieron el instructivo que se muestra en el

ANEXO 7, con las indicaciones necesarias para realizar correctamente la actividad requerida.

5.3. INFLUENCIA ENTRE LAS VARIABLES

La influencia entre las variables se presenta en alguno de los siguientes tipos:

- Real Directa: La variable A influye sobre B, por lo que los cambios en A modifican a B.
- Real Indirecta: Si la variable A influye sobre B y B influye sobre C, entonces A influye indirectamente sobre C.
- Potencial: Se da cuando la influencia de una variable sobre otra no acontece en el momento presente, pero se piensa que debería darse. Es decir, la influencia se sitúa no al nivel del ser sino del deber ser[135].

De esta forma, se empleó una matriz de doble entrada en la que los evaluadores valoraron únicamente las influencias directas y potenciales entre variables. Finalmente la matriz fue diligenciada por los evaluadores empleando cualquiera de los símbolos de la Tabla 2 según la evaluación realizada.

Tabla 2. Simbología para el diligenciamiento de la matriz

Símbolo	Tipo de Influencia
1	Directa débil
2	Directa Moderada
3	Directa fuerte
4	Potencial.

Fuente: Autores con base en las instrucciones del software MIC MAC®

5.4. IDENTIFICACIÓN DE LAS VARIABLES CLAVE

A partir de las valoraciones dadas por los evaluadores, se aplicó la metodología explicada en el ANEXO 8, con el fin de generar consenso entre las respuestas obtenidas, y así obtener la matriz de influencias directas que se introdujo en el

[135] MOJICA. Op. cit., p. 43.

software MICMAC® para ser procesada por el mismo. En el ANEXO 9, se muestra la matriz obtenida.

Para esta fase se empleó el software libre MICMAC® (Matriz de Impactos Cruzados Multiplicación Aplicada a una Clasificación)[136], a través del cual se realizó la jerarquización de las variables en términos de su influencia y dependencia. Para este fin, el software sitúa las variables en planos de Influencia/Motricidad -Dependencia de acuerdo al valor obtenido en los índices de estos dos criterios, cuya definición se presenta en la Tabla 3.

Tabla 3. Índices de motricidad y dependencia

Indicador	Definición	Caracterización
Índice de motricidad	Suma de las influencias de cada variables o el porcentaje de influencia. Sumatoria horizontal.	Muestra la fuerza que una variable tiene sobre las demás.
Índice de dependencia	Suma de las influencias que tienen las variables sobre una. Sumatoria vertical.	Indica el grado de subordinación de una variables respecto a las otras

Fuente: Autores con base en MOJICA S., Francisco. Prospectiva: Técnicas para visualizar el futuro

El plano se encuentra explícitamente divido en cuatro zonas, sin embargo, se contempla la existencia de una quinta en la parte media del mismo; en éstas las variables son ubicadas de acuerdo a su relación de motricidad- dependencia, denotando con esto características especiales, las cuales son descritas en la **¡Error! No se encuentra el origen de la referencia.** y la **¡Error! No se encuentra el origen de la referencia.**.

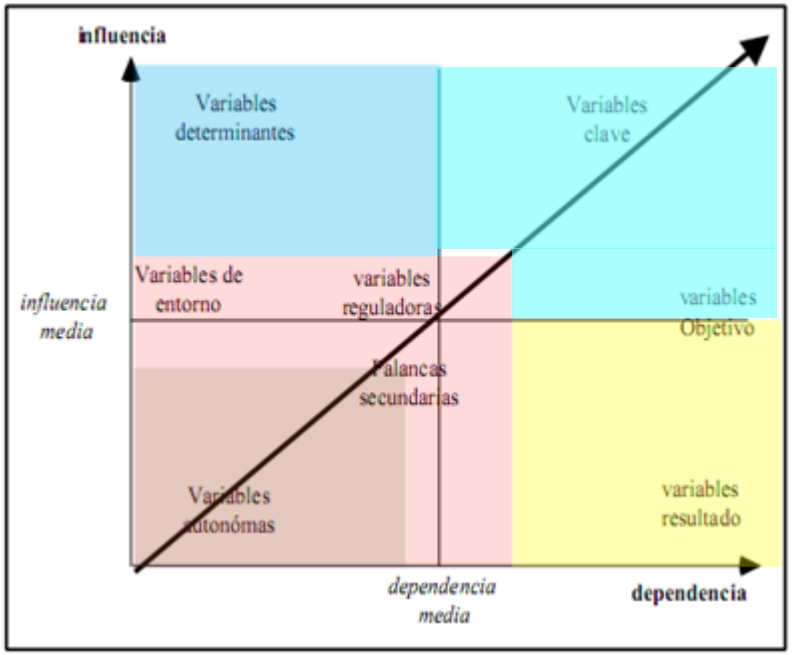
[136] Software desarrollado por el Laboratorio de Investigación en Prospectiva, Estrategia y Organización LIPSOR, el Instituto de Innovación Informática para la Empresa 3IE y la Escuela para la Informática y Técnicas Avanzadas EPITA.

Tabla 4. Zonas en los planos Motricidad/Influencia – Dependencia

Zona	Motricidad	Dependencia	Característica de las variables
Poder	Alta	Baja	Sus modificaciones repercuten en todo el sistema.
Conflicto/ Trabajo	Alta	Alta	Las variaciones sobre ellas tienen efecto en sí mismas y en la zona de salida.
Salida	Baja	Alta	Son producto de las variables de las zonas anteriores.
Autónoma	Baja	Baja	No constituyen parte determinante para el futuro del sistema.
Pelotón	Media	Media	No se puede decir nada *a priori* sobre estas variables.

Fuente: FLÓREZ, María Camila y SERRANO, Ximena Paola. Identificación de líneas estratégicas de investigación para la Universidad Industrial de Santander a partir de herramientas de vigilancia tecnológica y prospectiva área: salud. Trabajo de grado Ingeniería Industrial. Bucaramanga: Universidad Industrial de Santander. Facultad de Ingenierías Fisicomecánicas. Escuela de Estudios Industriales y Empresariales, 2011, p. 86.

Figura 7. Plano Motricidad/Influencia - Dependencia MICMAC



La ventaja que ofrece el método MICMAC® radica en que permite determinar los efectos producidos por las influencias indirectas ejercidas entre las variables revelando de esta forma el poder oculto que tienen algunas de ellas y que difícilmente se puede apreciar por medio de una clasificación directa. Para este fin, el software eleva la matriz de influencias directas a una potencia definida según el número de iteraciones que defina el usuario para buscar la estabilidad, puesto que se ha demostrado que toda matriz debe converger hacia una estabilidad al cabo de un cierto número de interacciones ("generalmente 4 o 5 para una matriz de tamaño 50"[137]), cuyos resultados pueden visualizarse en un plano de características semejantes a los descritos anteriormente.

Una vez se ha tomado la decisión de explorar y conocer las condiciones de un sistema en el presente y en el futuro una vez se intervenga, la primera acción que se debe efectuar es la determinación de los elementos que serán fundamentales en el futuro de la organización o sistema tomado[138], entendiendo esto como la identificación de las variables clave.

Esta fase consiste en la identificación de variables esenciales a la evolución del sistema, en primer lugar mediante una clasificación directa (de realización fácil, mediante simples sumas de valores de motricidad/influencia y de dependencia para cada una de las variables), y posteriormente por una clasificación indirecta (llamada MICMAC® para matrices de impactos cruzados Multiplicación Aplicada para una Clasificación). Esta clasificación indirecta se obtiene después de la elevación en potencia de la matriz. La comparación de la jerarquización de las variables en las diferentes clasificación (directa, indirecta y potencial) es un proceso rico en enseñanzas. Ello permite confirmar la importancia de ciertas variables, pero de igual manera permite desvelar ciertas variables que en razón de

[137] MATRIZ DE IMPACTOS CRUZADOS. Op. cit. p. 7.
[138] DE JOUVENEL, Hugues. Sur la démarch eprospective, un brief guide méthodologique. Futuribles. 1993, Citado por ARISTA, Anarrosa, *et al*. Op, cit., p. 154.

sus acciones indirectas juegan un papel principal (y que la clasificación directa no ponía de manifiesto)[139].

Es de resaltar que en esta clasificación indirecta no se tienen en cuenta las relaciones potenciales, las cuáles son evaluadas en un plano potencial que concede alta intensidad a estas relaciones permitiendo contrastar los resultados[140].

Para este análisis se tuvieron en cuenta 11 variables (Ver

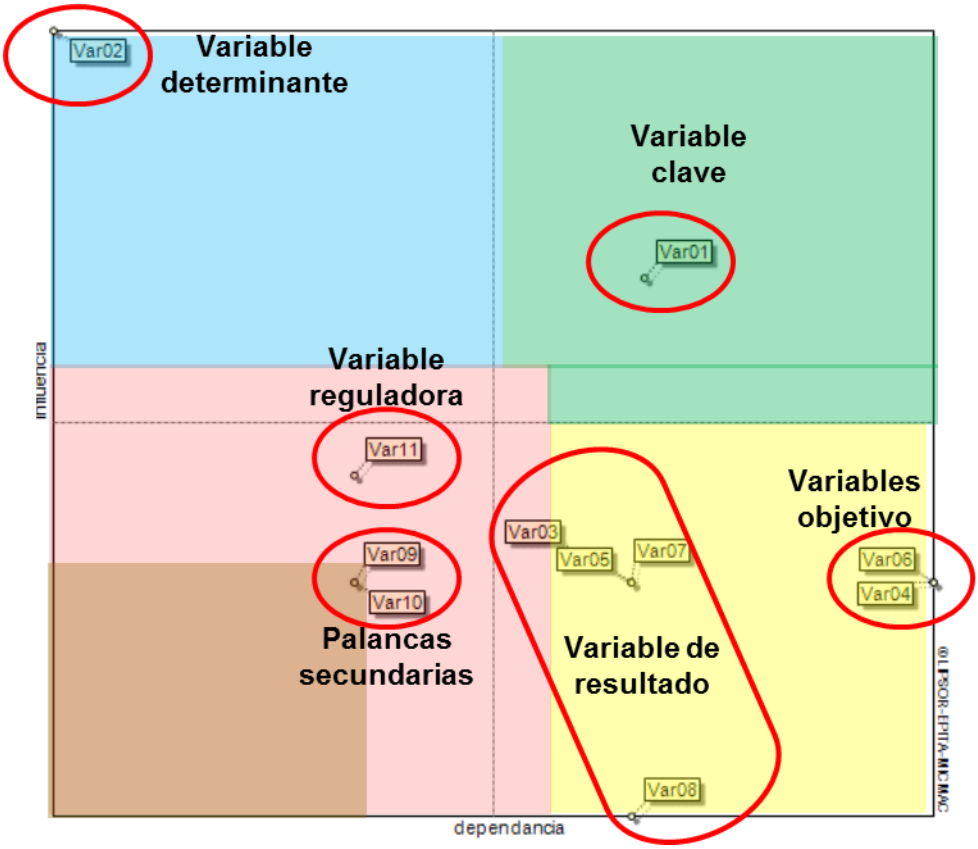
[139] MATRIZ DE IMPACTOS CRUZADOS. Op. cit. p. 12.
[140]GODET, Op. cit., p. 93

ANEXO 5), las cuales fueron procesadas en el software MICMAC® de acuerdo a los criterios establecidos anteriormente.

La matriz de influencias directas producto de las valoraciones de los evaluadores se presenta en el ANEXO 9. Producto de dicho procesamiento se obtuvo como primer insumo el *plano de influencia/ dependencia directa* y el *plano de influencia/dependencia indirecta*, los cuales fueron analizados en conjunto por medio del *plano de desplazamiento directo/indirecto*, visible en el ANEXO 10. En este se aprecia una aparente estabilidad del sistema al presentar desplazamientos imperceptibles a la vista de las variables, lo cual significa que no existe una caracterización distinta debido a su posición en el plano.

De esta forma, el análisis preliminar del sistema partió del *plano de influencia/dependencia indirecto* (Figura 8), que permite apreciar las influencias ocultas entre las variables, revelando la influencia que se puede ejercer sobre una variable a través de terceros, es decir que se puede modificar el estado de una variable de interés a través de la acción sobre otra sin atacarla directamente, dándole a quienes toman las decisiones (actores) la posibilidad de diversificar sus opciones para influenciar el sistema.

Figura 8. Plano de influencias / dependencias indirectas



Fuente: Software MicMAc®

En el plano, se llama la atención sobre los siguientes puntos:

- La variable 2, es decir, la organización de seguridad de la información, ubicada en una posición completamente influyente e independiente del resto de variables, se puede entender como una variable de gran poder, y corresponde al área en la que se pueden realizar acciones que afecten todo el sistema, es decir, variables de entrada, fuertemente motrices. Según la perspectiva de los evaluadores, la seguridad en los grupos de investigación depende de la presencia de una estructura que gestione en diferentes niveles (estratégico, táctico y operativo). Es decir, se requiere que se definan directrices y se apoye activamente desde la dirección de los grupos de investigación, la gestión de la

seguridad de la información, este compromiso debe verse reflejado a través de un comité encargado del área, la asignación de responsabilidades, la aprobación de un documento de políticas de seguridad de la información, la exigencia del cumplimiento de dichas políticas, la revisión periódica y monitoreo del estado general de la seguridad de la información, entre otras actividades de alto nivel relacionadas con la seguridad de la información[141]. En conclusión, esta variable determina el sistema en un inicio, es decir, cuando se quiere dar los primeros pasos de implementación de seguridad en toda la organización; es a través de esta primera gestión que se debe fomentar la cooperación y la colaboración de todos los integrantes del grupo de investigación[142], y con esta variable se puede por tanto, influenciar y afectar todas las demás variables.

- Las variables 5 y 7 tienen una naturaleza común y son posibles variables "pelotón", ya que ambas son, en esencia, áreas relacionadas con el control de acceso; la primera, corresponde al acceso físico, y la segunda, al acceso lógico. Asimismo, la variable 3, gestión de activos se relaciona directamente con el nivel de seguridad de la información. Las tres se encuentran en una zona de salida, dan cuenta de los resultados de funcionamiento del sistema, estas variables son poco influyentes y muy dependientes. Se les califica igualmente como variables sensibles. Se pueden asociar a indicadores de evolución, pues se traducen frecuentemente como objetivos. Esto revela que para los evaluadores, los resultados de las acciones implementadas se pueden medir a través de estas variables, es decir si existe una organización y una política de seguridad, entonces seguramente, el resultado es que, estén

[141] SISTESEG. Organización de la Seguridad de la Información. [en línea] [consultado 15 agosto 2012]. Disponible en: <http://www.sisteseg.com/files/Microsoft_Word_-_Organizaci_n_de_la_seguridad_de_la_informaci_n.pdf>

[142] PORTAL DE SOLUCIONES TÉCNICAS Y ORGANIZATIVAS A LOS CONTROLES DE ISO/IEC 27002. Capítulo 6: Organización de la seguridad de la información. [en línea]. [consultado 15 agosto 2012]. Disponible en: <http://iso27002.wiki.zoho.com/6-1-Organizaci%C3%B3n-Interna.html>

definidas las responsabilidades sobre los activos del grupo de investigación[143], y se mantenga una protección adecuada de los mismos, por ello, se requiere que las áreas, los recursos de tratamiento de la información, los procesos de negocio y la información como tal sensible, estén protegidos por controles adecuados que garanticen el acceso únicamente al personal autorizado, y que los propietarios de los activos que son responsables en el grupo de la protección de "sus" activos cumplan con la reglas de control[144].

- Las variables 4 y 6, seguridad de los recursos humanos y gestión de comunicaciones y operaciones, se encuentran en una zona altamente dependiente y medianamente influyente, constituyéndose en variables objetivo del sistema. Es decir, que sobre ellas se pueden aplicar líneas de trabajo para el mejoramiento de las condiciones de seguridad. Esto coincide con la teoría, puesto que las personas son consideradas el eslabón más débil en la gestión de la seguridad. Según Ashenden[145], la seguridad de la Información sigue madurando como una función de la organización, dependiente de la tecnología, los procesos y las personas; pero aún sigue siendo más fácil ser expertos en gestión de la tecnología y los procesos, que tener éxito en la gestión de personas. Por consiguiente, el reto del sistema es desarrollar vínculos entre la gestión de la organización y la gestión de seguridad de la información.

- La variable 8, adquisición, desarrollo y mantenimiento de sistemas de información, se encuentra en una zona con cero influencia, indicando que actualmente las actividades relacionadas con los sistemas de información de los grupos de investigación no están jalonando la seguridad de la información,

[143] Ibid.
[144] Ibid.
[145] ASHENDEN, Debi. Information security management: a human challenge?. En: Information Security Technical Report. Vol. 13, No. 4 (Nov. 2008); p. 195–201. Link: http://ac.els-cdn.com/S1363412708000484/1-s2.0-S1363412708000484-main.pdf?_tid=74ad3970-1d2e-11e2-a061-00000aacb35e&acdnat=1351009793_1301b0facfbc62ffccc05cb243b73190

principalmente porque se constituyen en procesos aislados, manejados por la división de servicios de información, y completamente ajenos a las actividades del investigador.

- Las variables 9 y 10, gestión de incidentes de seguridad de la información y gestión de la continuidad respectivamente, se encuentran ubicadas exactamente en el mismo punto, el cual es medianamente dependiente y poco influyente. La primera variable, gestión de incidentes, establece procedimientos formales de reporte y busca asegurar que los eventos y debilidades de la seguridad de la información sean comunicados de una manera "automática" y rápida, que permita que se realice una acción correctiva oportuna, sin embargo, en el panorama actual debido a la ausencia de una política, es la dirección de cada grupo de investigación quien debe estar al tanto de los procedimientos de reporte de los diferentes eventos que podrían impactar los activos de información, al igual que la variable gestión de la continuidad, que busca minimizar el impacto sobre la organización para recuperarse de las pérdidas de activos de información.

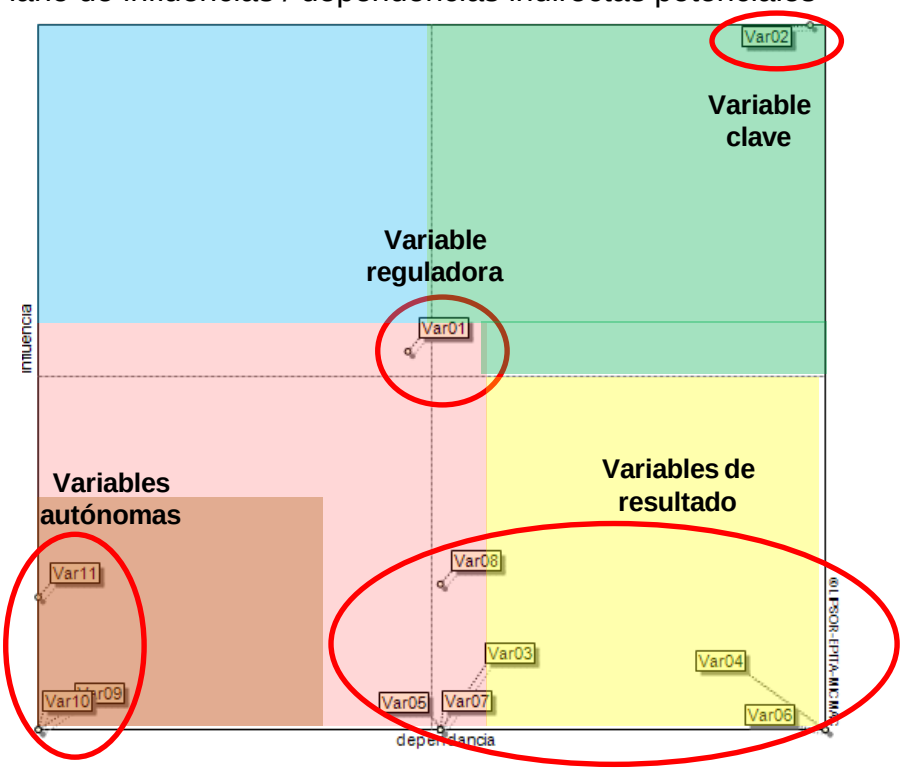
  En el análisis se encuentra que dependen de la organización de seguridad de la información, ya que según lo consensuado por los evaluadores primero se establece un marco referencial para iniciar y controlar la seguridad lo cual implica aprobar y adoptar la política de seguridad, luego se establecen compromisos de la dirección del grupo para que apoyen activamente la seguridad y, como consecuencia se gestiona la continuidad de los procesos y los incidentes de seguridad.

- La variable 11(conformidad o cumplimiento), ya sea de los requerimientos legales o de las políticas y estándares de seguridad, está ubicada cerca al centro del plano, y se puede identificar en la zona de "palanca secundaria". Sobre ella, la variable organización que implica compromiso fuerte de la

dirección del grupo tiene una influencia importante, debido a que una dirección clara con unas responsabilidades definidas puede evitar o no las violaciones de cualquier ley o requerimiento de seguridad. También, actúa de forma recíproca pero en un grado mediano la variable política. Además, ésta variable tiene una influencia media indirecta sobre la gestión de los recursos humanos y de las comunicaciones y operaciones en el sistema, puesto que los evaluadores piensan que, son los integrantes del grupo de investigación, los responsables de la seguridad y el cumplimiento de sus responsabilidades legales, gracias a un desarrollo idóneo de sus roles; y si existe gestión del cumplimiento se espera que se asegure la operación correcta y segura de los medios de procesamiento de la información.

Finalmente, a la hora de definir las variables estratégicas del sistema de investigación en el área de seguridad de la información, el plano de influencias/dependencias indirectas no es contundente; por tanto, es indispensable incluir el efecto de las relaciones potenciales definidas por los evaluadores que darán como resultado un estado de evolución del sistema en un contexto futuro, lo que puede implicar un desplazamiento de cada variable respecto a su posición inicial (ver ANEXO 10). De esta forma se obtiene el plano de influencias/dependencias indirectas potenciales, visible en la Figura 9.

Figura 9. Plano de influencias / dependencias indirectas potenciales



Fuente: Software MicMAc®

Como panorama inicial, se observa que todas las variables se han movido a través del plano, donde algunas conservan su zona mientras que otras cambian radicalmente de posición, lo que puede justificarse dadas las influencias indirectas, es decir, la existencia de una “tercera variable” afectando a través de otra. Según su distribución en el plano, las variables se caracterizan de la siguiente forma[146]:

- **Variables determinantes:** También se consideran variables de entrada del sistema y como su nombre lo indica son las que determinan el funcionamiento del mismo, según su evolución pueden ser frenos o motores, debido a su comportamiento poco dependiente dicha evolución no está dada por la acción de otras variables sobre estas. Se encuentran ubicadas en la parte superior

[146]GONOD P. Dynamique des systèmes et méthodes prospective.Travaux et recherches de prospective. Futuribles International, nº2. 1996.

izquierda del plano, es decir son poco dependientes y muy motrices. El sistema no presenta ninguna variable ubicada en esta zona.

- **Variables de entorno:** Están ubicadas en la zona de pelotón, y son aquellas que condicionan fuertemente el sistema pero no pueden ser controladas por este. Sin embargo, este sistema no presenta ninguna variable ubicada en esta zona.
- **Variables reguladoras:** Son las situadas en la zona central del plano, se convierten en "llave de paso" para alcanzar el cumplimiento de las variables-clave y que estas vayan evolucionando tal y como conviene para la consecución de los objetivos del sistema. Corresponden a esta denominación:

Tabla 5. Variable Reguladora Política de Seguridad de la Información

Política de Seguridad de la Información
En todos los planos de influencia dependencia analizados (directo, potencial, indirecto, e indirecto potencial), esta variable siempre conserva el segundo lugar más influyente después de la organización de la seguridad de la información (Ver ANEXO 11). Su ubicación en la zona de poder se justifica al tratarse de una variable netamente de gobierno, pues es en la política donde se definen los lineamientos de actuación para todas las demás dimensiones de seguridad de la información. Además, expresa las intenciones y objetivos de la alta dirección respecto a la protección de los activos de información y conocimiento, que son áreas resultado en el sistema**.**

Fuente. Autores del proyecto

- **Variables autónomas:** En la zona próxima al origen, se sitúan estas variables, son poco influyentes o motrices y poco dependientes, estas variables parecieran en gran medida no coincidir con el sistema ya que por un lado no detienen su evolución, pero tampoco permiten obtener ninguna ventaja del mismo. Se corresponden con tendencias pasadas o inercias del

sistema o bien están desconectadas de él. No constituye en parte determinante para el futuro del sistema. Se constata frecuentemente un gran número de acciones de comunicación alrededor de estas variables que no constituyen un reto. Se encuentra aquí la variable:

- Cumplimiento legal (conformidad)
- Gestión de la continuidad
- Gestión de incidentes de seguridad de la información

Tabla 6. Variables autónomas

Cumplimiento legal, gestión de la continuidad, y gestión de incidentes
Estas variables se ubican en este cuadrante, ya que se relacionan con actividades cotidianas (continuas) que se deben desarrollar dentro de la organización. Por tanto, como consecuencia de gestionar la seguridad de la información, estas dimensiones se convierten en inercias del sistema, y pueden llegar a ser vistos como procesos comunes del sistema que se cumplen bajo cualquier condición, y no como procesos estratégicos del mismo.

Fuente. Autores del proyecto

- **Variables palanca secundaria:** Son menos motrices que las reguladoras, sin embargo, su importancia está dada por la influencia que puedan ejercer sobre estas, que a su vez afectan la evolución de las variable-claves.
- **Variables resultado:** Son las variables resultado de la interacción de todas las que están excluidas en esta clasificación, su modificación no se logra abordándolas de frente sino a través de las que depende en el sistema. Es decir, son variables de salida del sistema, de naturaleza muy dependiente y poco influyente. Son esencialmente sensibles a la evolución de las variables influyentes. Dan cuenta de los resultados del funcionamiento del sistema. Se pueden asociar a indicadores de evolución, pues se traducen frecuentemente como objetivos. Se encuentran en este grupo:

- Seguridad de recursos humanos
- Gestión de comunicaciones y operaciones
- Control de acceso
- Gestión de activos
- Seguridad física y ambiental
- Adquisición, desarrollo y mantenimiento de sistemas de información

Tabla 7. Variables resultado

Seguridad de recursos humanos
Se puede interpretar su ubicación en la zona de salida, teniendo en cuanta que al contar con un sistema de gestión de la seguridad de la información totalmente estructurado y eficiente, se garantiza la aplicación y revisión continua de controles, lo que en un mediano o largo plazo conduce a la concientización de los trabajadores acerca de la importancia de cumplir con las políticas y procedimientos establecidos por la alta dirección. Por tanto, esta dimensión, se convierte en un resultado del sistema, pues en ella se ven reflejados los efectos de las acciones tomadas en otras dimensiones estratégicas como la organización de la seguridad de la información.
Gestión de comunicaciones y operaciones
Esta variable es resultado de las acciones tomadas en otras dimensiones, cuando el sistema se encuentra en un estado equilibrado, se puede garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información.
Control de acceso
Es una variable con una influencia nula, y dependencia media. Esto implica que para tener efecto sobre ella se deben tomar acciones en otras dimensiones. Según el gráfico de influencias (ANEXO 12), la variable que ejerce una influencia relativamente importante sobre ella es la organización de seguridad de la información.

Gestión de activos
Esta variable al igual que la anterior tiene una influencia nula, y dependencia media. Como resultado sirve para evaluar cual es el nivel de protección de los activos de información en la organización y que tan bien se están gestionando. En el gráfico de desplazamientos se observa que esta variable es influenciada por la organización de la seguridad de la información.
Seguridad física y ambiental
De igual manera, se pueden establecer indicadores de seguridad física y ambiental, esta variable es fuertemente influida por la organización de la seguridad.
Adquisición, desarrollo y mantenimiento de sistemas de información
También, esta variable constituye una salida del sistema, puesto que al dar cumplimiento a normas, y políticas de seguridad se vuelve un deber controlar los procesos de adquisición, desarrollo y mantenimiento de sistemas de información, en dónde se presentan varias de las vulnerabilidades y amenazas.

Fuente. Autores del proyecto

5.5. VARIABLES ESTRATÉGICAS

Por su ubicación en el plano, se consideraron como variables estratégicas del área las situadas en la **zona de conflicto del *plano influencia/dependencia indirectas potenciales***. Es importante recordar que la lectura de los resultados presentados por MICMAC no es única, pues atiende a las interpretaciones dada por evaluadores[147]. Así, continuando con la clasificación de las variables que se ha venido presentando, son variables clave las:

[147]GODET, Op. cit., p. 96.

- **Variables objetivo:** Ubicadas en la zona limítrofe entre la zona de conflicto/trabajo y la zona de salida, de alta dependencia y mediana influencia. Su denominación viene dada porque su nivel de dependencia permite actuar directamente sobre ellas para que evolucionen en la forma deseada ayudando a la consecución de las variables clave.
- **Variables clave:** Este tipo de variables tienen una alta motricidad (influencia) y alta dependencia, ubicadas en la zona de trabajo/conflicto, por tanto, cualquier cambio en ellas afecta el resto del sistema. De naturaleza inestable y corresponden a los retos, modificarlas implica alterar la evolución del sistema a un escenario deseado. Sobre ellas se establecen líneas de acción con el fin de transformar para mejorar el sistema. Se encuentra aquí únicamente la variable:

Tabla 8. Variable estratégica Organización de la seguridad de la información

Organización de la seguridad de la información
La ubicación de esta dimensión dentro de la zona de conflicto se explica en el hecho de que a través de ella se pueden ejecutar planes de acción que influencien todo el sistema. Al tener una estructura de gestión de seguridad de la información, la organización puede ejercer control sobre todas las áreas, y regular las acciones que permiten proteger los activos de información y conocimiento. La alta dirección debe establecer y dar un mecanismo de aprobación de la política de seguridad de la información y orientar la aplicación de la seguridad de la información en toda la organización. Las personas dentro de la organización deben conocer y comprender sus responsabilidades para la seguridad de la información.

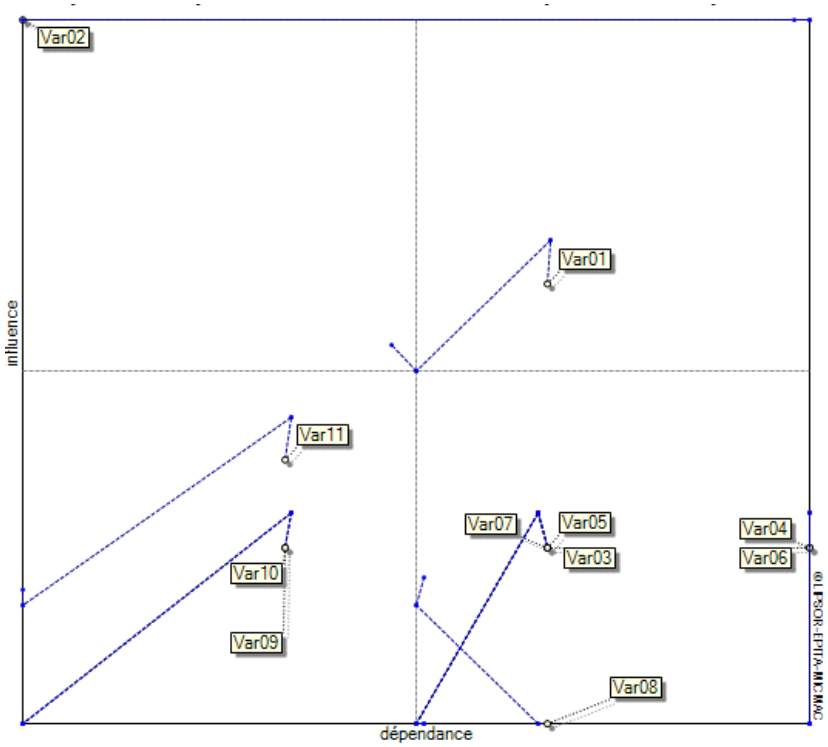
Organización de la seguridad de la información
Según el gráfico de influencias indirectas potenciales, la organización de la seguridad de la información ejerce influencia relativamente importante sobre la política de seguridad, seguridad física y ambiental, gestión de activos, y la adquisición, desarrollo y mantenimiento de sistemas de información. Además ejerce influencia más importante sobre seguridad de recursos humanos y gestión de comunicaciones y operaciones.

Fuente: Autores del proyecto a partir de ISO/IEC 27002:2005

Finalmente, el análisis estructural es aprovechado como una herramienta para identificar o describir el funcionamiento del sistema de seguridad de la información, mediante las relaciones de influencia y dependencia entre las variables o dimensiones incluidas. Por tanto, más allá de identificar las variables estratégicas futuras, se logró identificar que variables determinan el sistema, que causas, efectos o impactos generan y de qué forma se deben controlar.

Todo lo anterior basado en el conocimiento tácito de los evaluadores que fueron encuestados a nivel institucional como muestra representativa de la UIS. Ahora se verá materializado el conocimiento y los criterios de evaluación recolectados mediante la matriz de impactos.

Figura 10. Plano de desplazamientos: directo/indirecto/directo potencial/indirecto potencial



Fuente: Software MicMAc®

Los resultados obtenidos se detallan en el plano de desplazamientos (ver Figura 10), que permite ver el comportamiento de las variables a través del tiempo mientras el sistema se estabiliza. Allí se observa que la variable “Política de Seguridad de la Información”, en el plano directo se encontraba en la zona de poder y en el plano indirecto potencial se desplazó a la zona de conflicto. Dados estos comportamientos, se puede pensar hipotéticamente que en una organización, y en este caso un grupo de investigación de una universidad pública, donde el conocimiento es el activo más importante, no puede abordarse asuntos específicos de seguridad de la información sin antes implementar una política que permita tener una aproximación holística de los riesgos, puesto que la política ayudará a escoger los controles adecuados para disminuir los riesgos identificados, y tener una priorización clara de los asuntos de seguridad a tratar para que los controles implementados sean coherentes con los requerimientos de seguridad del grupo.

6. MODELO DE GESTIÓN

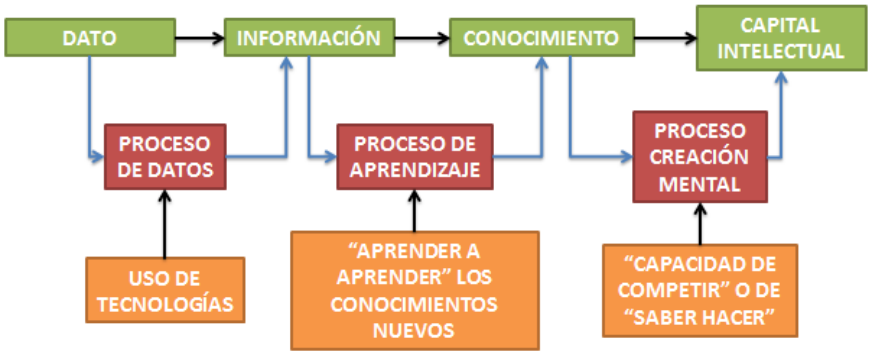
Según Bontis[148], "el capital intelectual ha sido considerado por muchos, definido por algunos, entendido por pocos y formalmente valorado por prácticamente nadie", lo cual supone uno de los desafíos más importantes para los directivos y académicos del presente y del futuro. Para el desarrollo del modelo, y siguiendo a Lev[149], se utilizó indiferentemente los términos capital intelectual, activos intangibles y activos de conocimiento. Entendiendo que el capital intelectual abarca las relaciones con los *stakeholders*, los esfuerzos innovadores, la infraestructura del grupo de investigación, el conocimiento y la pericia de los integrantes del grupo[150][151][152]. Bajo esta misma línea, Bradley[153] propone que el capital intelectual consiste en la capacidad para transformar el conocimiento en recursos que crean riqueza tanto en la organización como en el país.

El desarrollo del modelo comienza diferenciando lo que es información de conocimiento. Mientras que la información es la materia prima, el conocimiento puede ser ya considerado como el producto final[154]. De este modo, los integrantes del grupo reciben como *input* la información construida a través de los datos y, tras su análisis, obtienen como *output* el conocimiento; que da como resultado el

[148] BONTIS, N. Intellectual capital: an exploratory study that develops measures and models. En: Management Decision. Vol. 36, No. 2 (1998); p. 63.
[149] LEV, Baruch. Intangibles: management, measurement and reporting. Washington, DC: Brookings Institute, 2001, p. 5.
[150] EDVINSSON, Leif y MALONE, Michael. El capital intelectual. Barcelona: Gestión 2000, 1999, p. 27.
[151] EDVINSSON, Leif. Intellectual capital of nations.En: HOLSAPPLE, Clyde. Knowledge Management 1: Knowledge matters. Birkhäuser, 2004, p. 153.
[152] ISRAEL. MINISTRY OF INDUSTRY, TRADE AND LABOR. The intellectual capital of the state of Israel: a look to the future – The hidden values of the desert. Jerusalem: Office of the Chier Scientist, 2007, p. 10. [En línea]. [Consultado el 7 de agosto de 2012]. Disponible en <http://www.moital.gov.il/NR/rdonlyres/C973239E-F6C2-453A-A4D9-5A30F59258E3/0/intellectualcapital.pdf>
[153] BRADLEY, K. Intellectual capital and the new wealth of nations. En: Business Strategy Review. Vol. 8, No. 1 (1997). Citado por SÁNCHEZ, A. J., MELIÁN, A., HORMIGA, E. El concepto de capital intelectual y sus dimensiones. En: Investigaciones Europeas de Dirección y Economía de la Empresa, Vol. 13, No. 2 (2007); p. 98-99.
[154] RENDÓN, Miguel. Relación entre los conceptos: información, conocimiento y valor. Semejanzas y diferencias. En: Ciência da Informação, Brasília. Vol. 34, No. 2 (2005); p. 53.

capital intelectual del grupo o centro de investigación, luego de la suma del conocimiento de sus miembros y de la interpretación práctica del mismo (ver Figura 11).

Figura 11. Proceso de creación del capital intelectual

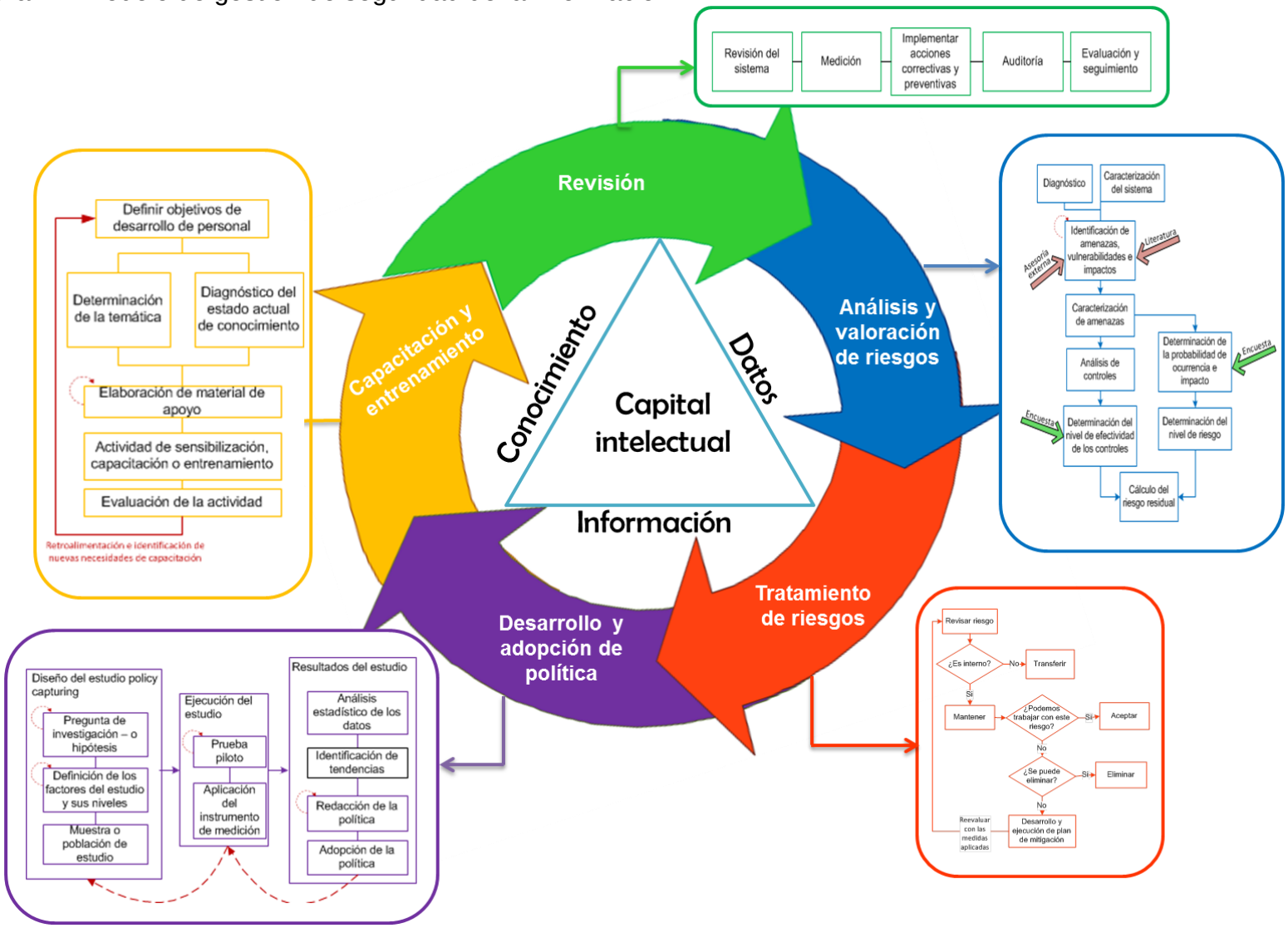


Fuente: Autores del proyecto. Adaptado de BUENO, Eduardo. La gestión del conocimiento: nuevos perfiles profesionales. [En línea]. (1999). [Consultado el 6 de agosto de 2012]. Disponible en <http://www .sedic.es/bueno.pdf>

Por tanto, lo que se busca mediante el modelo propuesto es la protección de este conocimiento a través de la gestión de la seguridad de la información, dado que "la información es la base fundamental sobre la cual la seguridad desarrolla su dinámica y propone las acciones de protección"[155]. De esta manera, el modelo está fuertemente relacionado con la gestión del conocimiento, enmarcado en el proceso de protección del conocimiento. Para ello, se explican las cinco fases recomendadas para evolucionar con las exigencias de un ambiente altamente competitivo, ágil y de alto riesgo propio de una organización basada en conocimiento, que debe enfrentar y asegurar, según Wilbanks[156], "un escenario interconectado, global, poco regulado, altamente consultado y vulnerable".

[155] LACEY, D. Managing the human factor in information security: how to win over staff and influence business managers. Chichester: John Wiley & Sons, 2009, p. 15-16.
[156] WILBANKS, L. Need to share vs. need to assure. En: IEEE IT Professional. Vol. 10, No. 3 (2008); p. 64.

Figura 12. Modelo de gestión de seguridad de la información



Fuente. Autores del proyecto

La Figura 12, presenta un modelo que caracteriza cinco dimensiones o fases, que a su vez se enmarcan en cuatro conceptos clave, ubicados en el centro de la figura. Asimismo, cada dimensión desarrolla una estructura compuesta por procesos específicos que se detallan en los cuadros laterales. El objetivo del modelo es proteger adecuadamente la información, como activo que posee valor para cualquier grupo o centro de investigación, para asegurar la continuidad del mismo, minimizar los daños y maximizar el retorno de la inversión en capital intelectual.

A continuación se presenta la descripción de cada una de las fases del modelo con el propósito de aclarar su interpretación.

Cabe aclarar que en el presente proyecto, las primeras tres fases del modelo propuesto, se desarrollaron de una manera intensiva, y se tratarán a profundidad en los capítulos 7 y 8 de este documento. Por otra parte, las dos últimas etapas fueron formuladas de manera pasiva, por lo cual únicamente se presenta una caracterización conceptual de las mismas.

6.1. DIAGNÓSTICO Y CARACTERIZACIÓN DEL SISTEMA

La preocupación de las organizaciones por la seguridad de la información no debe estar centrada sólo en los aspectos y controles técnicos aplicados a las TICs[157], sino es necesario proponer estrategias de gestión de seguridad de la información que abarque el desarrollo, revisión y cumplimiento de las políticas de seguridad; para lo cual se debe determinar qué hay que proteger y por qué, de qué se debe proteger y cómo protegerlo. Además, se

[157]VERMEULEN y VON SOLMS. Op. cit., p. 119.

requiere conocer qué tanto, los miembros de la universidad que hacen parte de la investigación, son conscientes de la importancia y las prácticas que llevan a cabo sobre el tema.

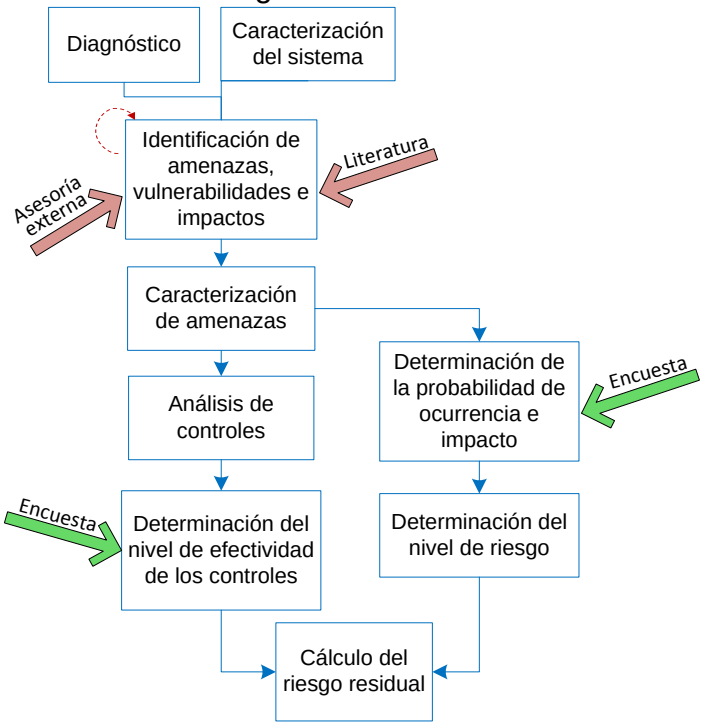
Por lo anterior, y conforme a la norma ISO/IEC 27002:2005, se requiere tener un inventario de activos de información, que habitualmente incluyen software, hardware, documentos, informes, bases de datos, aplicaciones, entre otros; que deben ser clasificados en función de su importancia desde el punto de vista de cada grupo de investigación, teniendo en cuenta el nivel de impacto, la dimensión de seguridad de la información comprometida.

6.2. ANÁLISIS Y VALORACIÓN DE RIESGOS

Esta fase constituye la parte principal del modelo de gestión; en ella se identifican, valoran y priorizan los riesgos de seguridad a los que está expuesto el grupo de investigación, para posteriormente identificar y asignar el conjunto más adecuado de controles de acuerdo a los requerimientos. En este sentido, el análisis de riesgos, consiste en el proceso de identificar los riesgos de seguridad de un sistema y determinar su probabilidad de ocurrencia, su impacto, y los mecanismos que mitiguen ese impacto[158]. A su vez, la valoración de riesgos, consiste en la determinación del nivel de riesgo, a partir de las medidas anteriores, y el cálculo del riesgo residual, producto de los controles existentes. El diagrama de flujo de esta fase se muestra en la Figura 13. En el desarrollo de esta fase, se generan registros y documentación propia de cada actividad, a saber: listado de vulnerabilidades, amenazas, impactos, y controles, y matriz de nivel de riesgo.

[158]SYALIM, Amril, HORI, Yoshiaki y SAKURAI, Kouichi. Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide, En: International Conference on Availability, Reliability and Security. 2009, p. 726.

Figura 13. Procesos de análisis y valoración de riesgos



Fuente. Autores del proyecto.

6.3. TRATAMIENTO DE RIESGOS

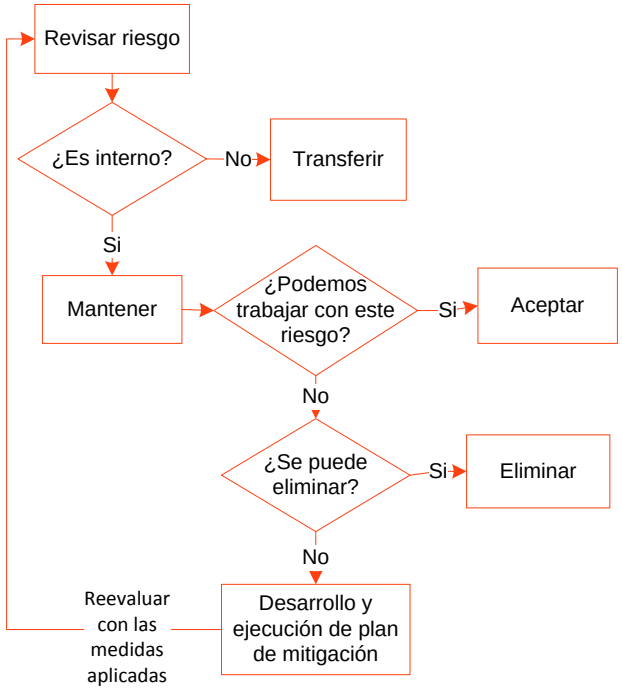
En esta fase, se planea lo que se debe hacer con respecto a los riesgos identificados. Esta decisión debe ser abordada por personal con conocimiento, experiencia y disposición, para analizar y desarrollar estrategias

tendientes a disminuir, eliminar o transferir los riesgos. La Figura 14 presenta una visión detallada de las decisiones progresivas que deben tomarse durante la planeación de riesgos.

En primera instancia, cada riesgo es revisado para asegurar que es entendido y está claramente documentado. Si el riesgo no es inherente al grupo de investigación, se transfiere a una entidad externa (dentro o fuera de la universidad) para que se encargue de gestionarlo. En caso contrario, se evalúa el nivel de riesgo y la opción de aceptarlo. De no ser aceptado, se contemplan la posibilidad de eliminar la acción que da origen al mismo. Finalmente, si en definitiva, el riesgo debe mitigarse, se procede a determinar el plan de mitigación de riesgo, para su desarrollo e implementación.

En el desarrollo de esta fase, se generan algunos registros y documentación propia de cada actividad como: fichas de riesgo, y plan de mitigación de riesgos.

Figura 14. Procesos de elección de medidas de tratamiento de riesgos



Fuente. Autores del proyecto. Adaptado de DOROFEE, Audrey, et al. Continuous risk management guidebook. Hanscom: Carnegie Mellon University Software Engineering Institute, 1996, p. 562.

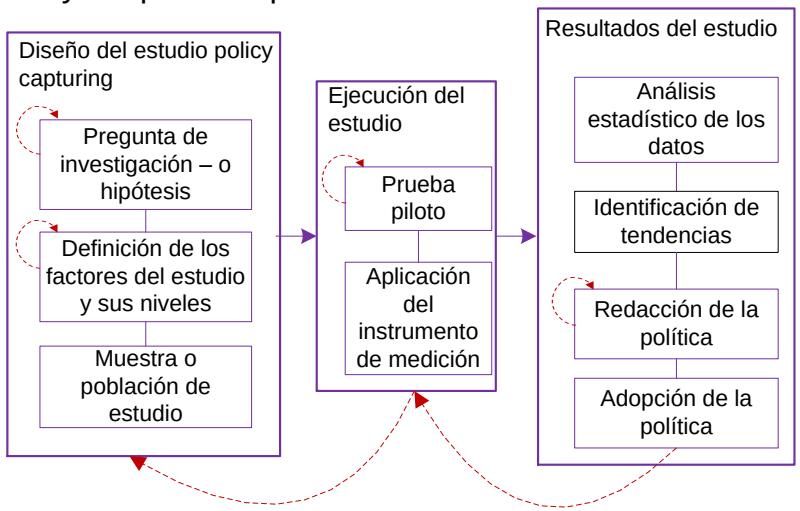
6.4. DESARROLLO Y ADOPCIÓN DE POLÍTICA

Para implementar un estándar para la seguridad de la información, es indispensable disponer de una política de seguridad precisa. La política debe transmitir claramente el compromiso de la dirección en relación a la protección de la información y establecer el marco general de seguridad para el grupo de investigación y su orientación. Aquí

se tienen en cuenta los riesgos críticos de la fase anterior, los resultados del estudio de policy capturing, los objetivos de seguridad de la información, reglas, normas y procedimientos que regulan el funcionamiento del grupo.

En el desarrollo de esta fase, el principal documento generado es la política de seguridad de la información, debidamente aprobada por la dirección del grupo, y comunicada a todos los integrantes del mismo.

Figura 15. Procesos de desarrollo y adopción de política



Fuente. Autores del proyecto

6.5. CAPACITACIÓN Y ENTRENAMIENTO

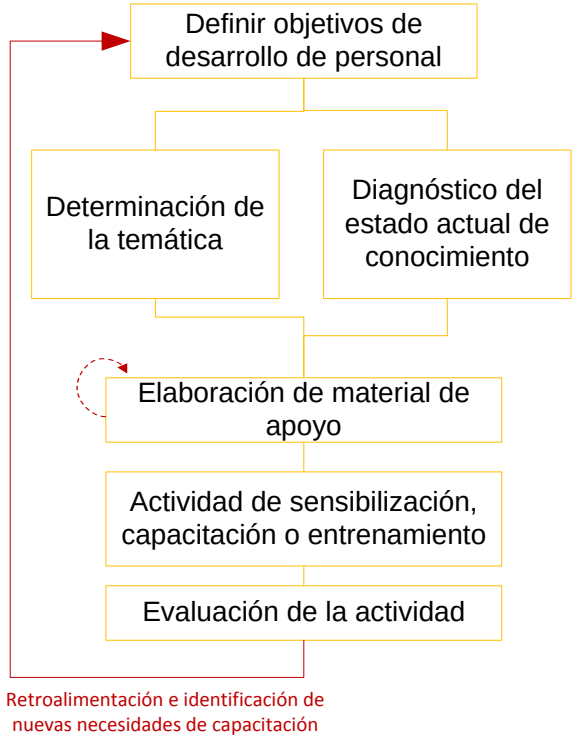
En esta fase, se planean y ejecutan las diferentes actividades de sensibilización, formación y, capacitación de los investigadores, estudiantes, y demás personal que labore o tenga compromisos con el grupo de investigación. La importancia de esta parte se determina en la medida en que los integrantes cumplan con la política de seguridad establecida.

Autores como Johnson y Goetz[159], en un reporte de gestión de seguridad de una gran compañía internacional, citan a Theresa Jones de Dow Chemical quien afirma: *"*El mayor desafío es cambiar el comportamiento. Si se pudiera cambiar el comportamiento de la mano de obra, entonces posiblemente se habrá resuelto el problema*".*

Para lograr lo anterior, previamente, se definen los objetivos de las actividades a desarrollar, se determina la temática a tratar, y se realiza un diagnóstico del estado actual de conocimiento que tienen las personas sobre dicha temática. Con esta información, se elabora el material de apoyo, por ejemplo, diapositivas, folletos, plegables, videos, etc. Finalmente, se ejecutan las actividades planeadas, buscando la participación activa de los integrantes del grupo, y la realización de discusiones abiertas que permitan dar claridad al tema. Se recomienda posteriormente, llevar a cabo una evaluación con el fin de verificar el cumplimiento de los objetivos. Durante el desarrollo de esta fase, se generan algunos registros y documentación propia de cada actividad; algunos como, registro de asistencia, material de apoyo utilizado, informe de la actividad, entre otros.

[159] JOHNSON, M. Eric y GOETS, Eric. Embedding Information Security into the Organization. En: IEEE Security & Privacy. Vol. 5, No. 3 (2007); p. 17.

Figura 16. Procesos de entrenamiento



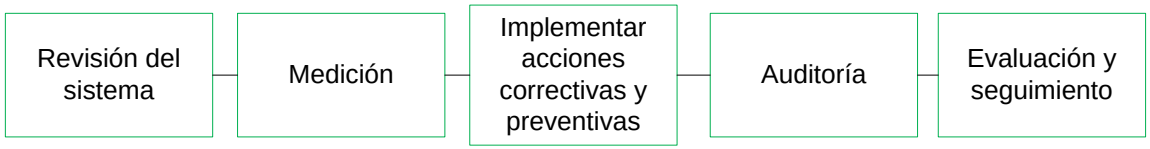
Fuente. Adaptado de PUHAKAINEN, Petri y SIPONEN, Mikko. Improving employees' compliance through information systems security training: an action research study. En: MIS Quarterly. Vol. 34, No. 4 (Dic. 2010); p. 764.

6.6. REVISIÓN

En coherencia con el principio de mejora continua que se enfatiza en todos los estándares establecidos por ISO, la última fase del modelo de gestión propuesto consite en la revisión de las acciones tomadas en las fases anteriores. A partir de la revisión, se realiza la medición de indicadores, para establecer e implementar acciones y/o ajustes correctivos y preventivos; seguidos de la auditoría, evaluación y seguimiento necesarios.

En el desarrollo de esta fase, se generan algunos registros y documentación propia de cada actividad como: planes de mejora, plan de acciones correctivas y preventivas, e informe de auditoría.

Figura 17. Procesos de revisión de gestión de seguridad

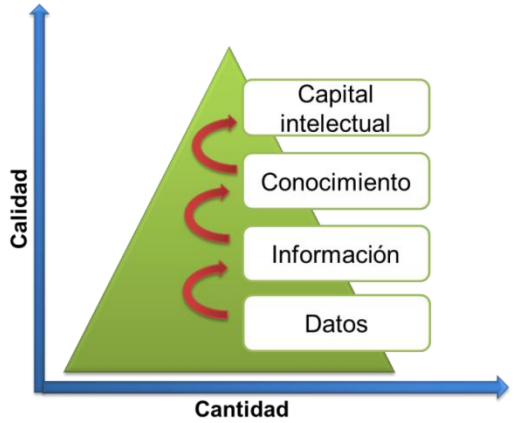


Fuente. Autores del proyecto

6.7. JERARQUÍA DEL CONOCIMIENTO

Finalmente, se consideró importante enriquecer la propuesta de gestión incluyendo los cuatro componentes de la jerarquía del conocimiento (Ver Figura 18), como conceptos claves alrededor de los cuales se debe desarrollar el modelo de gestión planteado.

Figura 18. Jerarquía del conocimiento



Fuente. Autores del proyecto. Adaptado de PAÉZ URDANETA, I. Gestión de la inteligencia: aprendizaje tecnológico y modernización del trabajo informacional. Retos y oportunidades. Caracas: Instituto de Estudios del Conocimiento de la Universidad Simón Bolívar, 1992, p. 10.

Dado que a menudo se cita, o se utiliza de forma implícita, las definiciones de datos, información y conocimiento en los sistemas de gestión de información, y en la literatura de gestión del conocimiento[160] . Los principales puntos de vista sobre la pirámide de la sabiduría o llamada en otros casos como “pirámide del conocimiento”, quizá se expresa mejor en las fuentes tradicionales de Adler[161], Ackoff[162] y Zeleny[163].

[160] ROWLEY, Jennifer. The wisdom hierarchy: representations of the DIKW hierarchy. En: Journal of Information Science. Vol. 33, No. 2 (Feb. 2007); p. 163
[161] ADLER, Mortimer Jerome. A guidebook to learning: for a lifelong pursuit of wisdom. New York: Macmillan,1986.
[162] ACKOFF, R.L. From data to wisdom. En: Journal of Applied Systems Analysis. Vol. 16 (1989).
[163] ZELENY, M. Management support systems: towards integrated knowledge management. En:, Human Systems Management. Vol. 7, No. 1 (1987).

Ackoff[164] fue de los primeros autores en plantear la transformación del dato en información y de esta en conocimiento hasta llegar a la sabiduría, que adaptado a la situación de los grupos de investigación en una universidad, podría decirse que se llega al capital intelectual, a través de la gestión del conocimiento. Aunque autores como Durant-Law[165], considera que "la distinción entre conocimiento y sabiduría carece de unas sólidas bases epistemológicas", por lo cual, el conocimiento es el techo de cualquier proceso de conversión.

Finalmente, algunos autores han integrado el concepto de "la pirámide de Ackoff"[166] con "la espiral de Nonaka y Takeuchi"[167] en un concepto denominado por Durant-Law[168] como "el conducto del conocimiento", el cual es el pilar de la productividad, que se entiende como la generación de valor a partir de este recurso.

En este sentido, Arias y Aristizábal[169], plantean que el conocimiento llega a ser productivo cuando las organizaciones brindan unas condiciones de orden contextual que les permiten a los individuos capturar los datos y

[164] ACKOFF, R. On learning and systems that facilitate it.En: Center for Quality of Management Journal. Vol. 5, No. 2 (1996); p.30.
[165] DURANT-LAW, Graham. Tardis: a journey throught an Enterprise knowledge space. [En línea]. Citado por: ARIAS, José y ARISTIZÁBAL, Carlos. El dato, la información, el conocimiento y su productividad en empresas del sector público de Medellín. En: Semestre Económico. Vol. 14, No. 28 (2004); p. 98.
[166]ACKOFF, R. (1996). On learning and systems that facilitate it. En: Center for quality of management journal, Vol. 5, No 2, p. 30. Citado por ARIAS, José y ARISTIZÁBAL, Carlos. El dato, la información, el conocimiento y sum productividad en empresas del sector público de Medellín. En: Semestre Económico. Vol. 14, No. 28 (2011); p. 99.
[167]NONAKA, I. y TAKEUCHI, H. (1995). The Knowledge-Creating Company, Oxford: Oxford University Press. Citado por ARIAS, José y ARISTIZÁBAL, Carlos. El dato, la información, el conocimiento y su productividad en empresas del sector público de Medellín. En: Semestre Económico. Vol. 14, No. 28 (2011); p. 99.
[168] DURANT-LAW, G. (2004). Tardis: a journey through an enterprise knowledge space. [En línea]. Citado por ARIAS, José y ARISTIZÁBAL, Carlos. El dato, la información, el conocimiento y su productividad en empresas del sector público de Medellín En: Semestre Económico. Vol. 14, No. 28 (2011); p. 99
[169] ARIAS, José y ARISTIZÁBAL, Carlos. El dato, la información, el conocimiento y sum productividad en empresas del sector público de Medellín. En: Semestre Económico. Vol. 14, No. 28 (2011); p. 99

la información, movilizarlos a través del conducto hasta convertirse en conocimiento que pasa de tácito a explícito, tomando forma para generar valor.

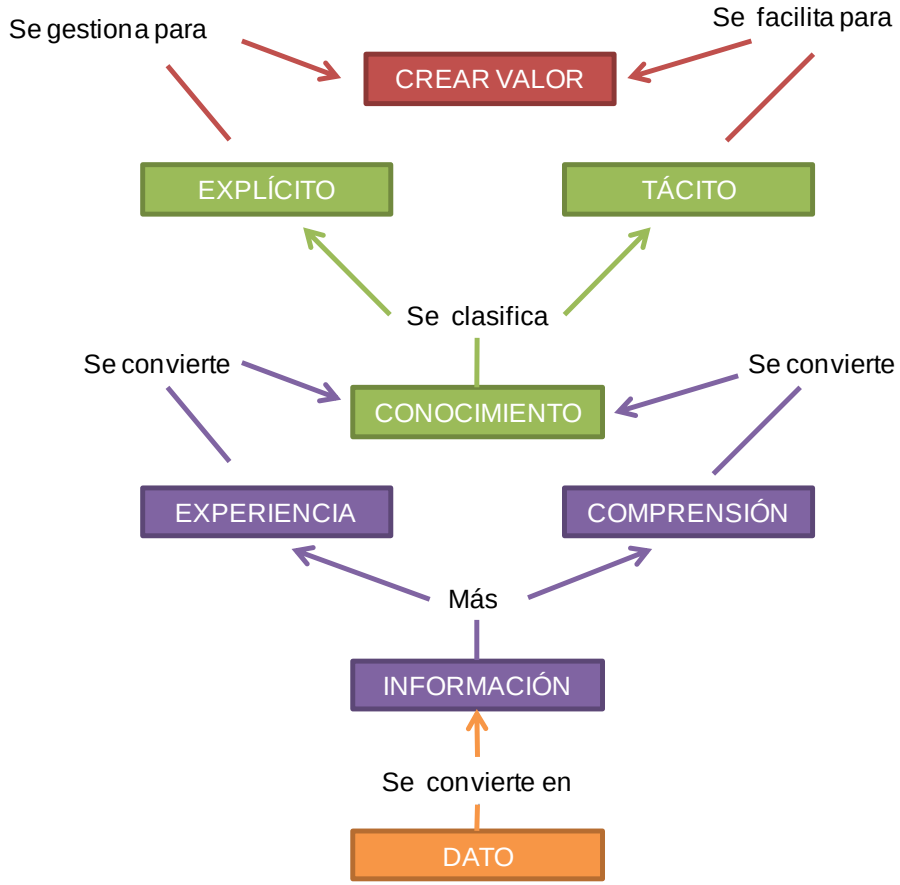
De otra parte, cabe resaltar que los expertos en gestión del conocimiento del sector público consideran que no hay ninguna diferencia entre información y conocimiento explícito, porque ambos conceptos aluden a aquello que le pertenece a la organización, y que además, según Simó y Sallán[170], el conocimiento explícito, está asociado al capital estructural; una de las clasificaciones de Bontis et al.[171]. Así mismo, estos expertos plantean que sólo el conocimiento tácito puede considerarse como conocimiento y este a su vez se asocia al capital humano, otra de las clasificaciones de Bontis et al. (Ver

[170] SIMÓ, Pep y SALLÁN, José María. Capital Intangible y capital Intelectual: Revisión, definiciones y líneas de investigación. En: Estudios de Economía Aplicada, Vol. 26, No. 2 (2008); p. 75

[171] BONTIS, N.; KEOW, W. C. C. y RICHARDSON, S. Intellectual capital and business performance in Malaysian industries. En: Journal of Intellectual Capital. Vol. 1, No. 1 (2000). Citado por SIMÓ, Pep y SALLÁN, José María. Capital Intangible y capital Intelectual: Revisión, definiciones y líneas de investigación. En: Estudios de Economía Aplicada, Vol. 26, No. 2 (2008); p. 75.

Figura **19**).

Figura 19. Dato, información y conocimiento en el proceso de creación de valor



Fuente: Autores del proyecto. Adaptado de ARIAS, José y ARISTIZÁBAL, Carlos. El dato, la información, el conocimiento y su productividad en empresas del sector público de Medellín. Semestre Económico, Vol. 14, No. 28 (2011); p. 105.

Incluso, Simó y Sallán, y otros autores como Sullivan[172] y Viedma[173], proponen de forma similar, la siguiente definición de capital intelectual:

"El capital intelectual es el conocimiento propiedad de la organización (conocimiento explícito) o de sus miembros (conocimiento tácito) que crea o produce valor presente para la organización". Teniendo en cuenta lo anterior y los cuestionamientos de expertos sobre si realmente es procedente hablar de gestión del conocimiento tácito; se ha llegado a la conclusión que esto no es posible; en lugar de ello, el que en realidad se puede gestionar es el explícito. Por lo tanto, el modelo de gestión planteado en esta investigación se enfoca en la seguridad de este tipo de conocimiento, el cual crea valor para la organización.

[172] SULLIVAN, P. H. Profiting from intellectual capital: extracting value from innovation. NY, Wiley, New York, 1998. Citado por SIMÓ, Pep y SALLÁN, José María. Capital Intangible y capital Intelectual: Revisión, definiciones y líneas de investigación. En: Estudios de Economía Aplicada, Vol. 26, No. 2 (2008); p. 71.

[173] VIEDMA, J. M. In search of an Intellectual Capital comprehensive theory. En: Electronic Journal of Knowledge Management. Vol. 2, No. 5 (2007).Citado por SIMÓ, Pep y SALLÁN, José María.Capital Intangible y capital Intelectual: Revisión, definiciones y líneas de investigación. En: Estudios de Economía Aplicada. Vol. 26, No.2 (2008); p. 71.

7. ANÁLISIS Y VALORACIÓN DE RIESGOS

En este apartado se describirá paso a paso el proceso de análisis de riesgos, que se define como "el uso sistemático de la información para identificar fuentes de riesgo y estimar su valor, como un requisito previo para la gestión de riesgos"[174]. Luego de una breve justificación del tema, se empezará por describir el panorama de los grupos de la Facultad de Ingenierías Físicomecánicas, en el tema de seguridad de la información y las prácticas formales o informales adoptadas por los mismos. Seguido del análisis de controles, su nivel de efectividad, la declaración de amenazas y riesgos, finalizando con la matriz de valoración de riesgos, la priorización de riesgos, la asignación de controles, el cálculo y análisis del riesgo residual, una vez se determina la medida de administración del riesgo.

La gestión de riesgos esta relacionada con la gestión de la información, la cual implica un esfuerzo sostenido por parte de la dirección de la organización, apoyada en elementos de planificación, organización y control que permitan cumplir con los objetivos de la seguridad de la información. La ausencia de esta herramienta conduce, ineludiblemente, a la dispersión de esfuerzos, el reproceso y, por regla general, a resultados poco satisfactorios.

Asimismo, Gordon et al.[175] resaltan la creciente importancia de la gestión efectiva de seguridad de la información, debido al aumento de la frecuencia y costo de los incidentes de seguridad. Además, las restricciones

[174] OZKAN, Sevgi y KARABACAK, Bilge. Collaborative risk method for information security management practices: a case context within Turkey. En: International Journal of Information Management. Vol. 30, No. 6 (2010); p. 567.
[175] GORDON, Lawrence et al. 2005 CSI/FBI Computer Crime and Security Survey. En: Computer Security Journal. Vol. 21, No. 3. (2005); p. 2.

presupuestarias son señaladas como uno de los principales obstáculos para esta[176].En general, el análisis de riesgos es un proceso usado como herramienta de diagnóstico para poder establecer la exposición real a los riesgos por parte una organización, estos riesgos por su parte, se basan en la probabilidad de que una amenaza ataque con éxito un activo a través de una vulnerabilidad concreta. Por lo tanto, el riesgo depende de tres componentes: activo, vulnerabilidad y amenaza. Este análisis tiene como objetivos identificar los riesgos (mediante la identificación de sus elementos) y lograr establecer el riesgo total (o exposición bruta al riesgo) y luego el riesgo residual, tanto sea en términos cuantitativos o cualitativos[177].

7.1 DIAGNÓSTICO GRUPOS UIS

Partiendo de la necesidad mencionada de fomentar una gestión apropiada del capital intelectual (Ver MODELO DE GESTIÓN en Capítulo 6),como recurso estratégico para generar valor y ventaja competitiva en las organizaciones (Ver DESCRIPCIÓN Y FORMULACIÓN DEL PROBLEMA DE INVESTIGACIÓN en Capítulo 1),a lo que algunos autores llaman la "visión de la empresa basada en el conocimiento"[178], se inició por hacer un diagnóstico y valoración de los grupos de investigación UIS de la Facultad de Ingenierías Fisicomecánicas, mediante encuestas en materia de seguridad de la información.

7.1.1 Población y muestra

[176] ERNST & YOUNG. Global information security survey 2003, Ernst & Young LLP, 2003, p. 1.
[177] SENA, Leonardo y TENZER, Simón. Introducción a riesgo informático. FCEA – Cátedra Introducción a la computación. Agosto 2004, p. 4. [en línea] [Consultado 25 agosto 2012]. Disponible en: <http://www.ccee.edu.uy/ensenian/catcomp/material/riesgo.pdf>
[178] GRANT, Robert M. Prospering in dynamically-competitive environments: organizational capability as knowledge integration. En: Organization Science. Vol. 7, No. 4 (1996); p. 385.

La muestra se determinó por conveniencia (muestreo no probabilístico), teniendo en cuenta la asequibilidad a los grupos de investigación de la universidad. Por lo cual, de los 105 grupos de investigación asociados a las cinco facultades (Ver Figura 20), se escogieron para el estudio únicamente aquellos pertenecientes a la Facultad de Ingenierías Fisicomecánicas, es decir, un total de 23 grupos, que representan aproximadamente el 22% del universo inicial. Además, se tuvo en cuenta que al pertenecer a la misma facultad, los grupos evaluados tendrían características afines con el grupo INNOTEC, en dónde se llevará a cabo la aplicación piloto del modelo de gestión. Una de las actividades que caracterizan a los grupos de investigación de esta facultad es la venta de servicios de conocimiento, puesto que corresponden a áreas de aplicación en lugar de generación, como ocurre por ejemplo en Ciencias Básicas.

Figura 20. Facultades de la Universidad Industrial de Santander

Fuente. Autores del proyecto.

7.1.2 Desarrollo del instrumento de medición

El instrumento de medición se diseñó a partir de la revisión bibliográfica de fuentes como: norma ISO/IEC 27002:2005[179], la herramienta de medición de riesgos de BITS[180], la guía de gestión de riesgos para sistemas de tecnologías de información[181] y Layton[182]. Considerando que se trataba de una encuesta exploratoria, solo se incluyeron preguntas relacionadas con los indicadores claves de riesgo (KRI por sus siglas en inglés); Según Layton[183], estos controles se consideran medidas esenciales que debe implementar una organización con el fin de preservar la seguridad de su información.

Se redactó inicialmente un borrador que tenía preguntas para cada indicador, y luego se agruparon las preguntas de acuerdo a temáticas relacionadas, cambiando las preguntas dicotómicas por preguntas de opción múltiple con múltiple respuesta. El instrumento de medición desarrollado, se muestra en el ANEXO 13.

7.1.3 Aplicación del instrumento de medición

[179] INTERNATIONAL STANDARDS ORGANIZATION. Op. Cit.
[180] BITS. Bits key risk measurement tool for information security operational risks. Washington DC: BITS, 2004.
[181] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Risk management guide for information technology systems: recommendations of the National Institute of Standards and Technology. Gaithersburg: NIST, 2002.
[182] LAYTON. Op. cit..
[183] Ibid.

La aplicación del instrumento de medición se realizó mediante una entrevista semi-estructurada, a fin de dar libertad al entrevistador para efectuar las preguntas que creyera oportunas y hacerlo en los términos que estimara convenientes, explicando su significado, pidiendo aclaraciones cuando no entendiera algún punto y profundizando en algún extremo cuando le pareciera necesario.

Se contactó personalmente a los directores de los grupos de investigación seleccionados, y en caso que el director no estuviera disponible, se entrevistó a otros investigadores del grupo, que en algunos casos, fueron profesionales de apoyo, docentes o estudiantes de maestría y doctorado. De esta manera, el instrumento de medición fue diligenciado por aquellas personas con conocimiento amplio y suficiente de la situación actual del grupo, es decir, que están involucrados directamente con la dinámica de funcionamiento. La muestra se refleja en el siguiente cuadro:

Tabla 9. Tipo de vinculación con el grupo

Vinculación con el grupo de investigación	% encuestado
Profesor de planta, cátedra o jubilado	89%
Estudiante en trabajo de grado de postgrado	5%
Profesional de apoyo	5%
Total	**100%**

Fuente. Autores del proyecto

En el estudio no se tuvieron en cuenta auxiliares de investigación, administrativos ni estudiantes en trabajo de grado de pregrado, puesto que el tiempo de permanencia de estas personas es corto y su conocimiento de las actividades del grupo es limitado e insuficiente para dar respuesta a la especificidad de las preguntas formuladas en la encuesta, las cuales requerían de una visión amplia del tema.

No existieron intenciones de evaluación, y la información recolectada fue soporte para complementar y fortalecer las primeras bases conceptuales del modelo de gestión a desarrollar posteriormente. Además, sólo fueron registradas las respuestas de 21 grupos debido a que no se pudo contactar a los directores de los dos grupos restantes (Ver

ANEXO 6).

7.1.4 Análisis de resultados

La aplicación del instrumento de medición permitió tener una visión más amplia de la dinámica de los grupos de investigación, la percepción que tienen sus directores e investigadores sobre el tema de seguridad de la información, las situaciones problema que se pueden presentar, y cómo son afrontadas en cada caso. Asimismo, un beneficio extra fue el interés que se despertó en cada una de las personas por conocer la temática tratada y reflexionar acerca de la necesidad de implementarla en sus procesos de investigación.

Por otro lado, se hicieron preguntas a los directores e investigadores sobre la antigüedad del grupo, y tipos de proyectos desarrollados, con la intención de caracterizar los grupos de investigación encuestados, y divisar el nivel de madurez, factor que puede influir en la forma como se utiliza y protege el conocimiento generado. Además se consultó el número de estudiantes e investigadores, mediante la plataforma ScienTI, en la aplicación de ingreso GrupLAC (Ver ANEXO 14). Una vez finalizadas las entrevistas que fueron realizadas con una frecuencia promedio de tres por día, se procedió a la codificación y tabulación de la información para el recuento, y estructuración de los datos obtenidos. La interpretación en detalle de cada pregunta formulada en la encuesta esta a continuación.

7.1.4.1 Política de seguridad de la información

La totalidad (100%) de los grupos de investigación encuestados no cuentan con una política de seguridad de la información documentada y actualizada. Algunos de los factores que contribuyen a que se presente esta situación son la falta de conciencia sobre la necesidad de generar una cultura de protección del conocimiento, ausencia de políticas institucionales sobre seguridad de la información y la no ocurrencia de incidentes graves o brechas de seguridad evidentes. Asimismo, la no claridad del objetivo de la seguridad de la información, el cual consiste en proteger la información y sus elementos críticos[184].

También se evidenciaron comportamientos atípicos en algunos de los grupos encuestados, cuyas prácticas son contrarias a lo que se espera normalmente se haga con el conocimiento generado al interior de un grupo de investigación, puesto que rechazan la idea de proteger la información explicando que el desarrollo de productos (por ejemplo, software) debe darse bajo el paradigma de sistemas blandos. Otro aspecto manifestado textualmente por aproximadamente el 21% de los grupos entrevistados, y de manera implícita por el resto, fue el desconocimiento y la falta de capacitación sobre las prácticas adecuadas para el manejo, control y seguridad de la información.

7.1.4.2 Aspectos relacionados con la política de seguridad

Debido a que ninguno de los grupos encuestados tienen política de seguridad, no fue posible analizar aspectos tales como:

- Canales a través de los cuales se comunica la política
- Frecuencia en que se actualiza y comunica la política

[184] WHITMAN y MATTORD. Op. cit., p. 8.

- Elementos incluidos dentro de la política

7.1.4.3 Controles implementados

La ausencia de lineamientos sobre la seguridad de la información, permite que cada investigador (profesor o estudiante) aplique los controles que considere necesarios, de manera intuitiva.

Cada entrevistado podía seleccionar más de una casilla de verificación, por lo que se calculó una frecuencia absoluta y relativa para cada control mencionado. Entre los controles más comunes implementados actualmente en los grupos se encuentran las copias de seguridad o back ups y la protección de las instalaciones físicas. Seguidamente se muestra la tabla con los resultados para la pregunta *"¿Cuáles de los siguientes controles se encuentran implementados actualmente?"*

Tabla 10. Frecuencia de los controles implementados en grupos de investigación

Control	Frecuencia	Porcentaje
Acuerdos de confidencialidad en seguridad de la información	13	65%
Reportes en caso de incidentes de seguridad de la información	1	5%
Copias de seguridad de la información (back up)	20	100%
Destrucción segura de información	3	15%
Seguridad de la red interna (intranet)	5	25%
Acceso a equipos (computadores), software e información	13	65%
Instalación de software	10	50%
Uso, publicación o divulgación de la información	11	55%
Protección de las instalaciones físicas donde opera el grupo de investigación	14	70%
Creación y eliminación de cuentas de usuario	5	25%

Fuente. Autores del proyecto

- Otros controles, como los **acuerdos de confidencialidad,** se utilizan solo en los casos específicos donde sea necesario, dependiendo del proyecto a ejecutar; en algunos grupos son firmados por el director del grupo o los investigadores responsables de ejecutar el proyecto; y en otros grupos los acuerdos se hacen firmar a todos los integrantes del grupo, independiente del rol que desempeñen dentro del proyecto de extensión, ya sea auxiliar, estudiante en pasantía de pregrado o postgrado, profesional de apoyo o investigador.
- Solamente un grupo (5% de los encuestados) realiza **reportes de incidentes**. Los demás consideran que esta práctica es innecesaria puesto que no tienen conocimiento ni conciencia de haberlos experimentado. Lo anterior, puede deberse a no tener definida una política de seguridad, y dentro de ella un proceso para reportar los incidentes.

- Todos los grupos afirmaron utilizar **copias de seguridad** de la información, sin embargo, es una práctica realizada de manera individual, y no existen lineamientos generales, establecidos por la dirección del grupo. Cada investigador determina, de acuerdo a su criterio, la frecuencia de las copias.
- Casi ningún grupo (solo el 15%) controla la **destrucción segura de información.** Una razón para ello, es que los grupos son muy jóvenes (menos de 10 años) y por tanto, no se ha realizado una renovación en los equipos de cómputo, además, la mayoría de investigadores trabaja en su computador personal y es responsable de su propia información. Por otra parte, los documentos físicos (impresos), después de cumplir su propósito dentro del proyecto, son utilizados como papel reciclaje, práctica que no se considera como destrucción segura de la información.
- En cuanto a la **seguridad de la red interna,** los controles aplicados corresponden a las indicaciones dadas por la División de Servicios de Información. Por otra parte, la mayoría de redes informáticas en las universidades no fueron diseñadas originalmente pensando en la seguridad. A diferencia de las redes corporativas y otras redes comerciales, que son más cerradas y segmentadas con énfasis en la protección de los recursos valiosos de la información, las redes de la universidad están diseñadas para funcionar como proveedores del servicio de Internet, facilitar el acceso a los usuarios y facilitar el flujo de la información.
- El **control de acceso** a equipos, software e información se aplica en 13% de los grupos. Los derechos de control de acceso se otorgan de acuerdo a características como: antigüedad en el grupo, rol desempeñado, proyecto en el que participa, nivel de responsabilidad, etc.
- La **instalación de software** se controla únicamente en los casos dónde se tienen salas de cómputo asignadas, esto se hace mediante el uso de claves de administrador para realizar cambios/actualizaciones en el software.

- La **protección de las instalaciones físicas** es una práctica bastante común entre los grupos, el 70% de ellos aplican controles de este tipo. No obstante, los controles aplicados radican en la instalación de chapas y puertas corrientes. En algunos casos, se maneja un formato de control con las personas que tienen acceso a la llave.
- La **creación y eliminación de cuentas de usuario** es el control menos común entre los grupos entrevistados ya que los equipos de cómputo utilizados son, en su mayoría, propiedad de los mismos estudiantes. Los grupos que aplican este control son aquellos que cuentan con una sala de cómputo asignada por la universidad.

7.1.4.4 Importancia dada a los aspectos de seguridad de la información

La importancia dada a la seguridad de la información es baja en la mayoría de los casos (35%), esto se puede explicar por la falta de difusión del tema desde las diferentes instancias en la Universidad, esto causa que muchos de los investigadores no consideren la temática dentro de sus actividades cotidianas de no ser por la encuesta realizada, la cual despertó interés en cada uno de ellos. De igual forma, la ausencia de sucesos críticos, a excepción del incendio de las oficinas de DSI,

Para el rol desempeñado, responsabilidad en seguridad y clasificación de la información, la respuesta más popular fue “alta”. Esto muestra que las respuestas están basadas están basadas en la percepción de la persona que contestó la encuesta y no en hechos concretos, puesto que no se observa coherencia entre la importancia dada a los aspectos de seguridad de la información y los controles implementados.

Tabla 11. Frecuencia relativa de la importancia dada a los aspectos evaluados

Aspecto	Nula	Poca	Media	Alta	Muy alta
Seguridad de la información	0%	35%	20%	25%	20%
Rol desempeñado por cada integrante en la SI	0%	30%	15%	40%	15%
Responsabilidad de la seguridad de la información	0%	20%	15%	45%	20%
Clasificación de la información	5%	30%	20%	40%	5%
Reporte de incidentes	35%	30%	0%	35%	0%
Usos autorizados de los activos	15%	5%	35%	30%	15%

Fuente. Autores del proyecto

En cuanto a los dos últimos aspectos: reporte de eventos y usos autorizados de activos, las opiniones están divididas entre las opciones alta y nula o media, lo cual indica que no hubo mucha claridad en la formulación de la pregunta pues algunas personas contestaron basados en los hechos que se dan en el grupo de investigación mientras que otros contestaron de acuerdo a su apreciación personal sin indicar esto que por ser importante un aspecto existan medidas adecuadas para su aplicación en el grupo.

7.1.4.5 Procedimientos de ingreso de integrantes

Con esta pregunta se buscaba si actualmente, cuando ingresa un nuevo integrante a un grupo de investigación, se usan procedimientos relacionados con la seguridad de la información, y de qué tipo (Ver Tabla 12).

Tabla 12. Frecuencia de utilización de procedimientos para nuevos integrantes

Procedimiento	Frecuencia	Porcentaje

Programa de sensibilización, formación o educación	11	55%
Firma de acuerdo de confidencialidad	3	15%
Entrega de normatividad del grupo	5	25%
Presentación de los demás miembros	18	90%
Asignación de activos	11	55%
Asignación de responsabilidades	15	75%
Ninguna acción	0	0%
Otro	0	0%

Fuente. Autores del proyecto

- **Programa de sensibilización, formación o educación.** En cuanto al ingreso de nuevos integrantes, se realiza de manera bastante informal, aunque en el **55%** de los grupos contestaron que tienen un programa de sensibilización y formación, este consiste en un par de charlas que tiene el director del grupo con el nuevo miembro, en las cuales se le informa muy superficialmente acerca de las actividades del grupo, proyectos ejecutados y niveles de responsabilidad.
- **Firma de acuerdo de confidencialidad.** Solamente en dos grupos (10%), se firman acuerdos de confidencialidad cada vez que ingresa un nuevo integrante. Uno de ellos, hace firmar políticas de cumplimiento a los nuevos miembros sin importar si son de pregrado o postgrado. El otro utiliza acuerdos únicamente cuando se realizan proyectos de extensión con una empresa privada que lo exige.
- **Entrega de normatividad del grupo.** Solo el 25% de los grupos hacen entrega de la normatividad, la cual consiste en lineamientos generales sobre comportamiento con los compañeros y uso de los equipos de cómputo, así como información sobre la misión del grupo y sus líneas de investigación. Algunos medios de

divulgación de la normatividad incluyen: wikis, folletos, documentos. En algunos grupos, se les pide a los estudiantes que lean el reglamento estudiantil de la Universidad.

- **Presentación de los demás miembros.** En la mayoría de los grupos (90%) se realiza una presentación informal de los demás miembros durante la primera reunión grupal a la que asista el nuevo integrante. En grupos demasiado pequeños (2 o 3 miembros) se hace innecesaria esta práctica.
- **Asignación de activos.** Solo en el 55% de los grupos se utiliza este procedimiento, los casos en los que no se lleva a cabo son justificados por la ausencia de activos propios del grupo, es decir, cada investigador utiliza su portátil personal, en el cual maneja la información y documentos necesarios para la realización del proyecto en el que participe.
- **Asignación de responsabilidades.** El 75 % de los grupos asigna responsabilidades a sus miembros, estas están altamente relacionadas con los productos (artículos, ponencias, informes, manuales) que deben entregar al final del proyecto, y poco relacionadas con la seguridad de la información.

7.2 CARACTERIZACIÓN DEL SISTEMA

En la evaluación de los riesgos de un sistema que requiere gestionar la seguridad de la información según NIST, el primer paso es definir el alcance del esfuerzo. Aquí, se deben identificar los recursos y la información que constituye el mismo, para ello, se requiere de un profundo conocimiento del entorno de procesamiento del sistema. Puesto que la caracterización del sistema permite delinear el alcance de la evaluación del riesgo, la primera acción consistió en recoger información que permitiera dar una definición de los usuarios, los productos, los procesos misionales y las

tecnologías de información, para el caso INNOTEC. Para observar con detalle cada una de las características del grupo de investigación, relacionadas en la Tabla 13, ver ANEXO 15 y ANEXO 16.

Tabla 13. Principales características del Grupo de Investigación INNOTEC

Tipo de variable	Características
Grupo de Investigación	Definición Grupo de investigación Definición INNOTEC Misión, visión, trayectoria y objetivos Líneas de investigación Dominios de investigación Fortalezas Investigadores principales Equipo de Trabajo
Integrante del Grupo de Investigación	Horas de dedicación al grupo Fecha de inicio de vinculación Nivel de educación Vinculación
Infraestructura Tecnológica (Recursos)	Redes científicas Software especializado Bases de datos especializadas
Productos	Productos de nuevo Conocimiento Productos de circulación e impacto Productos de formación de RR.HH

Fuente. Autores del proyecto

7.3 EVALUACIÓN DE RIESGOS: CASO INNOTEC

Consiguiente a esta contextualización, se inició el análisis de riesgos en el grupo de investigación INNOTEC, el cual se ha destacado en los últimos 4 años por su participación en la ejecución de proyectos de gran importancia, en cuanto a su alcance y presupuesto. Algunos ejemplos son: Identificación de áreas estratégicas, PILA Network, Towards Sustainable Financial Management of Universities in Latin América - SUMA, Gestión financiera en instituciones de educación superior – GEFIES,

Este proceso se define como el uso sistemático de la información para identificar fuentes y estimar el riesgo, dado que es un requisito previo para la gestión de riesgos. Si el análisis del riesgo no se realiza correctamente, la selección de medidas no será efectiva y su éxito será muy poco probable.

El proceso de análisis y valoración de riesgos, se realizó según la metodología GISAM (Ver Global Information Security Assessment Methodology en

ANEXO 4), puesto que aprovecha los dos tipos de evaluación (cuantitativa y cualitativa) y se considera que es un tipo de modo mixto de evaluación, razones por las que fue utilizada en el estudio, ésta metodología se compone de los siguientes pasos:

7.3.1 Análisis de controles

Uno de los componentes principales dentro de la metodología de evaluación de riesgos escogida, GISAM, es el análisis de controles, que consiste en una evaluación del nivel de efectividad de las prácticas, procedimientos o mecanismos existentes en el grupo de investigación, que reduzca el nivel de riesgo.

7.3.1.1 Selección de los controles

La selección de la norma ISO/IEC 27002 se fundamenta en que es el código de práctica para seguridad de la información más ampliamente aceptado a nivel mundial. No obstante, y debido al alcance definido en los objetivos del presente proyecto, el estudio de riesgos se limitó a una aplicación piloto que no se considera un análisis definitivo ni concluyente. Por tanto, para realizar la evaluación de controles, se tomó como punto de partida los 35 controles indicadores claves de riesgo (KRI) según Layton[185], quien, basado en su amplia experiencia trabajando con empresas que han implementado la norma ISO/IEC 27002, considera que estos son fundamentales y necesarios para mantener la seguridad de la información en una organización, independiente del entorno o industria de los cuales haga parte. La razón por la cual se escogió el listado presentado por este autor, radica en la clasificación y priorización que realiza sobre los controles de seguridad de la información enlistados por ISO/IEC 27002.

Dado que la gestión de seguridad de la información puede ser vista desde tres niveles principales: estratégico, táctico y operacional. Y considerando que estos tres niveles corresponden a los tipos de asuntos que conciernen a la alta dirección, incluyendo la naturaleza general de los conocimientos necesarios para administrar la seguridad, se decidió partir de los 35 controles principales, y se escogieran para la valoración únicamente aquellos que correspondieran a la categoría de Management (M) puesto que el modelo a desarrollar es un modelo de gestión. Pese a que los controles operativos y técnicos son relevantes para cualquier organización, para efectos de practicidad y por el enfoque del grupo de investigación INNOTEC, no se consideraron en la evaluación de riesgos. El listado final es de 26 controles que se muestran en el ANEXO 17 con su correspondiente valoración del nivel de efectividad y análisis.

[185] LAYTON, Op, cit., p. 23 – 40

7.3.1.2 Escala de valoración

Para la valoración se utilizaron los siguientes niveles de efectividad del control:

Tabla 14. Niveles de efectividad de control

Nivel	Descripción
0	El control es aplicable pero no ha se ha reconocido la necesidad de implementarlo
1	Existe conciencia, pero no hay acción. No existe un esfuerzo formal de implementación.
2	Parcialmente implementado. Se reconoce la aplicabilidad de este control y se han hecho algunos intentos de implementación.
3	Control implementado. Se revisa por lo menos una vez al año, pero el proceso y los resultados no siempre se documentan.
4	Control gestionado. Se tienen políticas y procedimientos documentados. El control se revisa de manera regular, y el proceso y los resultados se documentan adecuadamente.
5	Comprensible. Alto nivel de consciencia sobre las responsabilidades con este control. Se revisa continuamente y los resultados se documentan completamente.

Fuente: Autores del proyecto. Adaptado de LAYTON, T. Information Security: Design, implementation, measurement and compliance. Boca Raton: Auerbach Publications, 2007, p. 8.

7.3.1.3 Participantes

Se aplicó un cuestionario con 26 controles de riesgo, el cual fue aplicado a través de la herramienta de formularios de Google Docs, a todos los investigadores y estudiantes de doctorado, maestría y pregrado, el cual permitió establecer las condiciones actuales del grupo de investigación INNOTEC, en el área de seguridad de la información. El formulario completo se puede observar en el ANEXO 18. En la Tabla 15 se muestra la conformación del equipo que completo esta valoración.

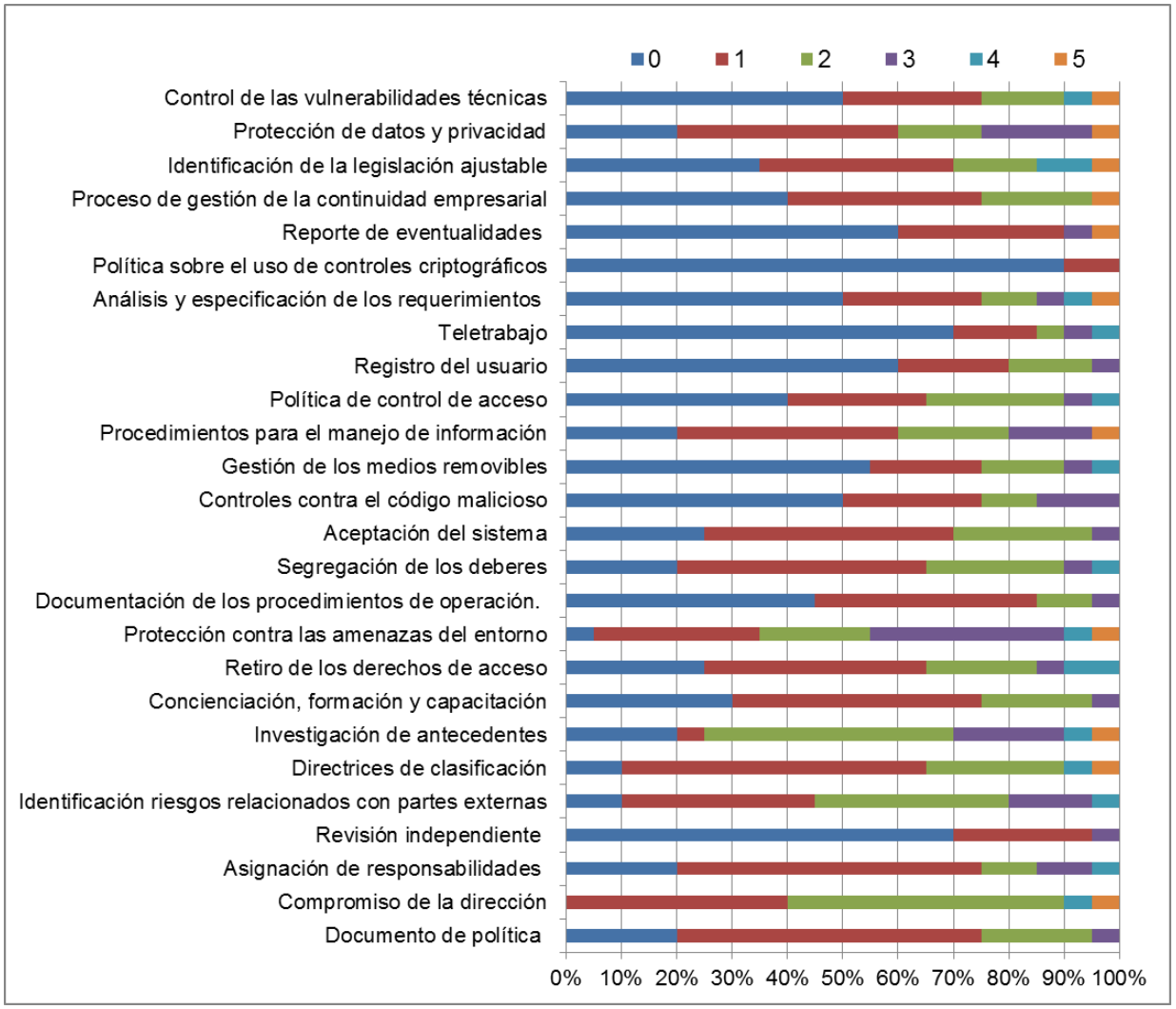
Tabla 15. Tipo de participantes según su vinculación con el grupo

Tipo de vinculación	Frecuencia	Porcentaje
Profesor de planta, cátedra o jubilado	3	15%
Auxiliar (de investigación o administrativo)	1	5%
Estudiante en trabajo de grado de pregrado	5	25%
Estudiante en trabajo de grado de posgrado (maestría y doctorado)	10	50%
Profesional de apoyo	1	5%

Se observa que la mayor parte de las personas que respondieron el cuestionarios está conformada por estudiantes en trabajo de grado de posgrado (50%), es decir estudiantes de maestría y doctorado. Asimismo, la segunda categoría con mayor frecuencia es la de estudiantes de trabajo de grado de pregrado, con un 25%. En el

ANEXO 19 se encuentra el listado de las personas que contestaron el cuestionario.

Figura 21. Controles y su nivel de implementación



Fuente. Autores del proyecto con ayuda del software Microsoft Excel.

7.3.1.4 Análisis e interpretación de resultados

Una vista general de la Figura 21 nos muestra que los niveles 4 y 5 de efectividad del control que recomiendan tener políticas y procedimientos documentados, con revisiones continuas o de manera regular, acompañada de la adecuada documentación de resultados; sólo son el 5,19 % del número de respuestas de los integrantes de INNOTEC, incluso en el 57% de los controles evaluados ninguna persona contesto que existiera un nivel de efectividad de 5. En cuanto al nivel 3, que señala que el control esta implementado, que se revisa al menos una vez al año, pero que el proceso no se documenta, sólo fue indicado en el 7,5% de las respuestas comparado con el 85,42% que suman la frecuencia de las respuestas seleccionadas para los niveles de efectividad 0, 1 y 2, donde lo máximo que existe en la actualidad para el grupo INNOTEC son controles parcialmente implementados, es decir, se reconoce su aplicabilidad pero no se han hecho intentos de implementación. Con más detalle, el 36,15% y 33,08% de las respuestas pertenecen a los niveles de control 0 y 1 respectivamente, lo cual se observa con las franjas de la Figura 21, donde los colores azul y rojo son predominantes en los 26 controles evaluados. Todos los porcentajes anteriores muestran la necesidad de mejorar ese 85,42%.

Sin embargo, para ver con mayor especificidad los resultados de cada control evaluado por los integrantes del grupo y su respectivo análisis, ver ANEXO 17.

7.3.2 Identificación de amenazas, vulnerabilidades e Impactos

Se realizó un listado de amenazas, vulnerabilidades e impactos (Ver ANEXO 20, ANEXO 21 y ANEXO 22), a partir de la revisión bibliográfica de fuentes como: ISO/IEC 27002[186], BITS[187], NIST[188], Layton[189], Whitman[190 191], entre otras[192 193], y

[186] INTERNATIONAL STANDARDS ORGANIZATION. Op. cit.
[187] BITS. Op. cit., p. 13.

se complementaron con los resultados de la encuesta exploratoria aplicada a los grupos de investigación.

7.3.3 Caracterización de amenazas

En este punto se agruparon las amenazas identificadas de acuerdo a la fuente de la cual provienen. Considerando los listados propuestos en la literatura, se tomaron como fuentes de amenaza para el grupo las siguientes:

- Personas externas: personas ajenas al grupo de investigación que actúan de manera maliciosa, violando la seguridad de la información.
- Criminal informático: Según Symantec, "es una persona que comete un delito en el que se haya utilizado un equipo, una red o un dispositivo de hardware"[194].
- Personas internas: Se refiera a integrantes del grupo, que pueden causar incidentes de seguridad.
- Vándalo: En el contexto universitario, se trata de personas que participan en desordenes civiles tales como cierre de la universidad, atentados contra edificios, detonación de explosivos, entre otros.
- Naturaleza: En esta categoría se encuentran amenazas producidas por fenómenos naturales.
- Proveedor de servicios informáticos: Entidad que suministra soluciones de hardware, software y redes al grupo de investigación, encargado a su vez de los

---

[188] NIST. Op. cit., p. 13-14.
[189] LAYTON. Op. cit., p. 24-26.
[190] WHITMAN (2004). Op. cit., p. 46.
[191] WHITMAN, Michael E. Enemy at the gate: threats to information security. En: Communications of the ACM. Vol. 46, No. 8 (2003); p. 92.
[192] REED, Simón. Riesgos y amenazas de la fuga de información en las empresas. En: Revista a+ - Auditoría y seguridad. No. 20 (Mar. 2008); p. 80-81.
[193] Top information security risks for 2008. En: CISSP forum and ISO27k implementer's forum. [En línea]. [Consultado 5 Junio 2012]. Disponible en: http://www.iso27001security.com/Top_information_security_risks_for_2008.pdf
[194] SYMANTEC CORPORATION. Definición de cibercrimen. [En línea]. [Consultado el 29 de junio de 2012]. Disponible en <http://mx.norton.com/cybercrime/definition.jsp>

servicios postventa que ello implique, tales como, mantenimiento, asesoría o actualización.

- Entorno: Serie de fuerzas que tienen incidencia sobre el desarrollo de las actividades del grupo de investigación.

7.3.4 Determinación de la probabilidad de ocurrencia y análisis de impactos

A partir de los listados iniciales, se creo una tabla en la cual se asociaron las vulnerabilidades e impactos con las vulnerabilidades e impactos con las diferentes amenazas (Ver

).

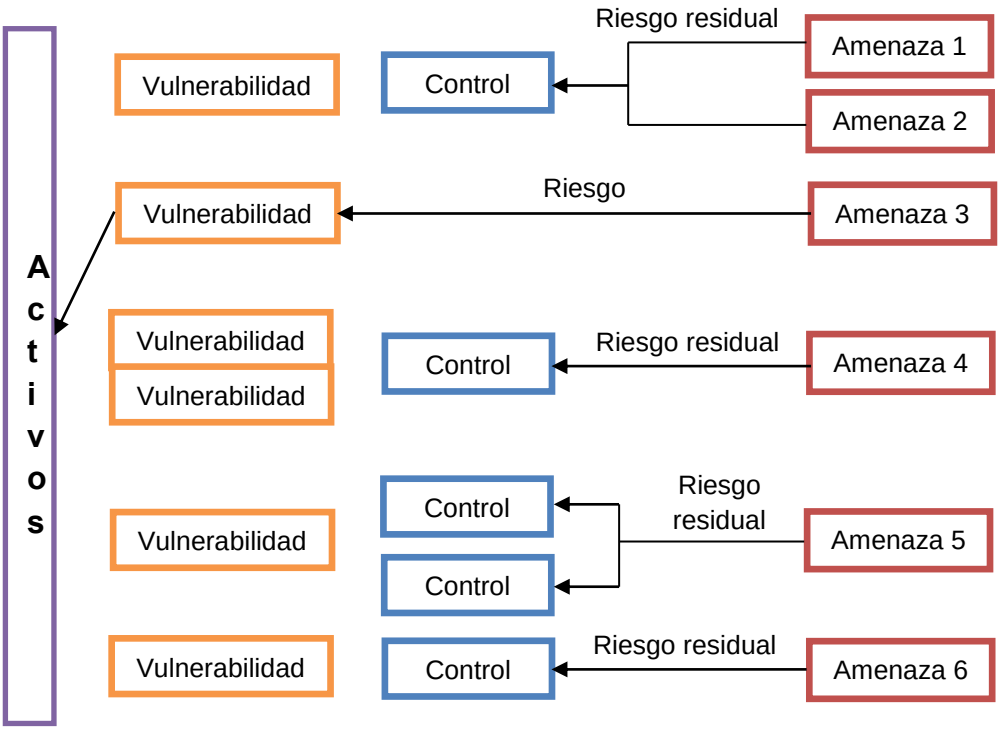
Al realizar dicha asociación, se tuvieron en cuenta los diferentes tipos de relaciones existentes, los cuales se pueden observar claramente en la Figura 22. A modo de ejemplo, más de una amenaza puede potencialmente explotar una sola vulnerabilidad (ver amenazas 1 y 2). Una sola amenaza puede potencialmente explotar más de una vulnerabilidad (ver amenaza 4). Cuando no se aplican controles, el activo queda completamente expuesto y la amenaza explota la vulnerabilidad ocasionando el riesgo; por el contrario, cuando se aplican controles, el nivel de riesgo es reducido hasta cierto punto, quedando un riesgo residual.

Posteriormente, se construyó un listado de riesgos, el cual fue revisado por Jorge Medina Villalobos[195], especialista en seguridad de la información. De acuerdo a sus recomendaciones, se mejoró la redacción y estructura de los riesgos.

En este punto, de nuevo se hizo importante la participación de todos los miembros del grupo de investigación INNOTEC con el fin de conocer su percepción del nivel de riesgo en seguridad de la información. Para ello, se diseñó un instrumento de medición cuyo objetivo fue medir la percepción de cada persona en cuanto a la probabilidad de ocurrencia y el impacto de cada uno de los riesgos identificados.

Figura 22. Relación entre vulnerabilidades, amenazas y riesgos

[195] Ingeniero Electrónico de la Universidad Industrial de Santander. Postgrado en telecomunicaciones de la misma Universidad. Certified Information Systems Security Professional (CISSP). Desde hace varios años trabaja como Ingeniero especialista en seguridad en la Unidad de Seguridad Informática del Banco de la República. Catedrático de seguridad informática de la Universidad Javeriana y del Diplomado en Seguridad Informática de la Universidad Sergio Arboleda.



Fuente. Autores del proyecto. Adaptado de VON SOLMS, S.H. y VON SOLMS, Rossouw. IT risk management. En: _____. Information security governance. Springer Publishing Company, 2009, p. 92.

7.3.4.1 Población de estudio

El instrumento de medición desarrollado fue enviado vía electrónica a todos los miembros del grupo de investigación INNOTEC. Además, se incluyeron las opiniones de dos profesionales de apoyo que trabajan con el grupo. En total se recolectaron 24 encuestas completas. En el siguiente cuadro se muestra el número de personas que participaron y sus respectivos roles dentro del grupo:

Tabla 16. Participante del Estudio

Tipo de vinculación	Número personas	% encuestado
Profesor de planta, cátedra o jubilado	3	12,5%
Estudiante en trabajo de grado de postgrado	13	54,2%
Estudiante en trabajo de grado de pregrado	7	29;2%
Profesional de apoyo	1	4,2%

Fuente. Autores del proyecto

7.3.4.2 Diseño del instrumento de medición

El instrumento de medición se diseñó teniendo en cuenta el conocimiento sobre seguridad de la información que seguridad de la información que tienen los miembros del grupo INNOTEC (Ver **ANEXO 23. TABLA DE AMENAZAS, VULNERABILIDADES, IMPACTOS, RIESGOS Y CONTROLES**

Amenaza	Vulnerabilidad Asociada	Impacto	Riesgo	Control que aplica
(1) Suplantación de identidad	Controles de acceso lógico y/o físico inadecuados.	Costo de oportunidad	Suplantación de identidad por baja efectividad de los controles de seguridad físicos y/o errores humanos, que conlleva a perdidas de información confidencial a un costo muy alto.	8.3.3 Retirada de los derechos de acceso
	Descuidos, errores humanos	Incapacidad de cumplir con los objetivos organizativos		10.1.1 Documentación de los procedimientos de operación
	Integrantes del grupo no cumplen con la política de seguridad de la información.	Pérdida de confianza		10.7.3 Procedimientos de manipulación de la información
	La dirección no exige el cumplimiento de la política de seguridad de la información.	Pérdida de diferenciación y crecimiento		11.1.1 Política de control de acceso
	La dirección no apoya el desarrollo de una política de seguridad de la información.	Fuga de información		11.2.1 Registro de usuario
	La dirección no apoya los programas de capacitación y sensibilización para los	Pérdida de la privacidad		12.3.1 Política de uso de los controles criptográficos
	Integrantes del grupo no capacitados / inconscientes	Pérdida de ventajas competitivas		6.1.6 Contacto con las autoridades
	Contacto poco estrecho entre los integrantes del grupo.	Pérdidas financieras		8.1.3 Términos y condiciones de contratación
	Ausencia de programas de capacitación y sensibilización			8.2.1 Responsabilidades de la Dirección
	Ausencia de política de seguridad de la información			8.2.3 Proceso disciplinario
	Falta de controles de acceso lógido y/o físico			9.1.1 Perímetro de seguridad física
				9.1.2 Controles fisicos de entrada
				9.1.3 Seguridad de oficinas, despachos e instalaciones
				9.2.1 Emplazamiento y protección de equipos
				9.2.7 Retirada de materiales propiedad de la empresa
				10.7.4 Seguridad de la documentación del sistema
				10.8.1 Políticas y procedimientos de intercambio de información
				10.8.2 Acuerdos de intercambio
				10.10.1 Registros de auditoría
				10.10.3 Protección de la información de los registros
				10.10.4 Registros de administración y operación
				11.2.2 Gestión de privilegios
				11.2.3 Gestión de contraseñas de usuario
				11.2.4 Revisión de los derechos de acceso de usuario
				11.3.1 Uso de contraseñas
				11.3.2 Equipo de usuario desatendido
				11.4.2 Autenticación de usuario para conexiones externas
				11.5.1 Procedimientos seguros de inicio de sesión
				11.5.2 Identificación y autenticación de usuario
				11.5.3 Sistema de Gestión de contraseñas
				11.5.5 Desconexión automática de sesión
				11.5.6 Limitación del tiempo de conexión
				12.3.2 Gestión de claves
				12.5.4 Fugas de información
				15.1.6 Regulación de los controles criptográficos

ANEXO 24). Para cada uno de los riesgos identificados, se evaluaron tres aspectos: probabilidad de ocurrencia, impacto, y medida de tratamiento. En el primer caso, se utilizó una escala de tres niveles cualitativos (alto, medio y bajo) asociada a unos valores porcentuales establecidos teniendo en cuenta lo sugerido por BITS[196]. En cuanto a la descripción cualitativa de cada nivel, se utilizaron las descripciones proporcionadas por Layton[197] y NIST[198]. (Ver Tabla 17).

[196] BITS. Op. cit., p. 14.
[197] LAYTON. Op. cit., p. 36.
[198] NIST. Op. cit., p. 21.

Tabla 17. Escala de valoración para la probabilidad de ocurrencia

% Prob.	Descripción
70-100%	Pueden existir vulnerabilidades y amenazas y el nivel de efectividad del control es muy bajo o no es aceptable. Existen otras variables del entorno que pueden aumentar el rating de la probabilidad de ocurrencia. La fuente de la amenaza esta altamente motivada y es suficientemente capaz de hacerse efectiva.
40-69%	Existen amenazas y vulnerabilidades, pero el nivel de efectividad del control se considera que esta en el límite aceptable o las variables del entorno que existen causan que la probabilidad de ocurrencia sea menor que alta y mayor que la baja. La fuente de la amenaza tiene la motivación y la capacidad de hacerse efectiva.
10-39%	Existen amenazas y vulnerabilidades, el nivel de efectividad del control esta ranqueado en 4 o 5, es decir que puede impedir significativamente la ocurrencia de la amenaza sobre la vulnerabilidad. No existen variables del entorno que pudiesen incrementar la posibilidad de ser explotada y ejercida. La fuente de la amenaza le falta motivación o capacidad.

Fuente. Autores del proyecto. Adaptado de BITS[199] y NIST[200].

Según BITS[201], “una probabilidad del 0% no es una opción puesto que, por definición, siempre existe la probabilidad de que una amenaza ocurra sin importar que tan baja sea esa probabilidad”. Por tanto, se establecieron 3 rangos de 30% de amplitud cada uno, siendo la menor asignación posible de 10%.

En el caso del impacto, se utilizó una escala ordinal de 6 niveles: No hay impacto, menor, tangible, significativo, serio, y grave. Sin embargo para practicidad en el diligenciamiento del instrumento de medición, se asocio cada nivel a un número

[199] BITS. Op. cit., p. 14.
[200] LAYTON Op. cit., p. 36.
[201] BITS. Op. cit., p. 14.

del 0 al 5, siendo 5 el nivel con mayor impacto (Ver Tabla 18). Las definiciones para cada nivel fueron tomadas de la herramienta BITS[202].

Tabla 18. Escala de valoración para el impacto

Nivel	Valor	Descripción
Grave	5	Incapacidad para recuperarse. Cierre permanente del grupo o pérdida permanente de las instalaciones. Es muy probable una pérdida total de los negocios y operaciones.
Serio	4	Posible daño a la reputación del grupo. Cese prolongado de las actividades del grupo. Requiere la activación de un plan de contingencia. Meses de refuerzo son necesarios para la reparación/recuperación. Pérdida temporal de las instalaciones.
Significativo	3	Semanas de esfuerzo son necesarias para la reparación/recuperación. Hay gastos importantes y pérdidas de ingresos.
Tangible	2	Días de esfuerzo son necesarios para la reparación / recuperación. Hay gastos significativos y/o cierta pérdida de ingresos
Menor	1	Se requiere de algunos esfuerzos para reparar el daño. Los costos de recuperación son mínimos. No hay pérdidas de ingresos.
No hay impacto	0	Sin impacto medible en este momento

Fuente. Autores del proyecto. Adaptado de BITS[203], NIST[204] y LAYTON[205].

Finalmente, se le pidió a las personas que seleccionaran una de las cuatro opciones de tratamiento de riesgo (Ver Tabla 19) que plantea la norma ISO/IEC 27002[206].

[202] BITS. Op. cit., p. 18.
[203] BITS. Op. cit., p. 18.
[204] NIST. Op. cit., p. 23.
[205] LAYTON Op. cit., p. 16.
[206] ISO. Op. Cit.

Tabla 19. Opciones de tratamiento de riesgo

OPCIONES DE TRATAMIENTO DEL RIESGO	
ACEPTAR	Aceptar los riesgos consciente y objetivamente, siempre que no se vean afectados el objetivo ppal del grupo.
REDUCIR	Aplicar los controles apropiados para reducir los riesgos.
TRANSFERIR	Transferir los riesgos asociados a otras partes; por ejemplo, aseguradores o proveedores.
ELIMINAR	Evitar los riesgos no permitiendo acciones que podrían causar que el riesgo ocurra.

Fuente: Adaptado de Norma ISO/IEC 27002:2005.

7.3.4.3 Aplicación del instrumento de medición

La aplicación del instrumento de medición se realizó a través del diligenciamiento individual del instrumento de medición. En algunos casos en que las personas así lo solicitaron, y por la necesidad de agilizar el proceso de recolección de respuestas, se brindo acompañamiento por parte de las autoras del proyecto.

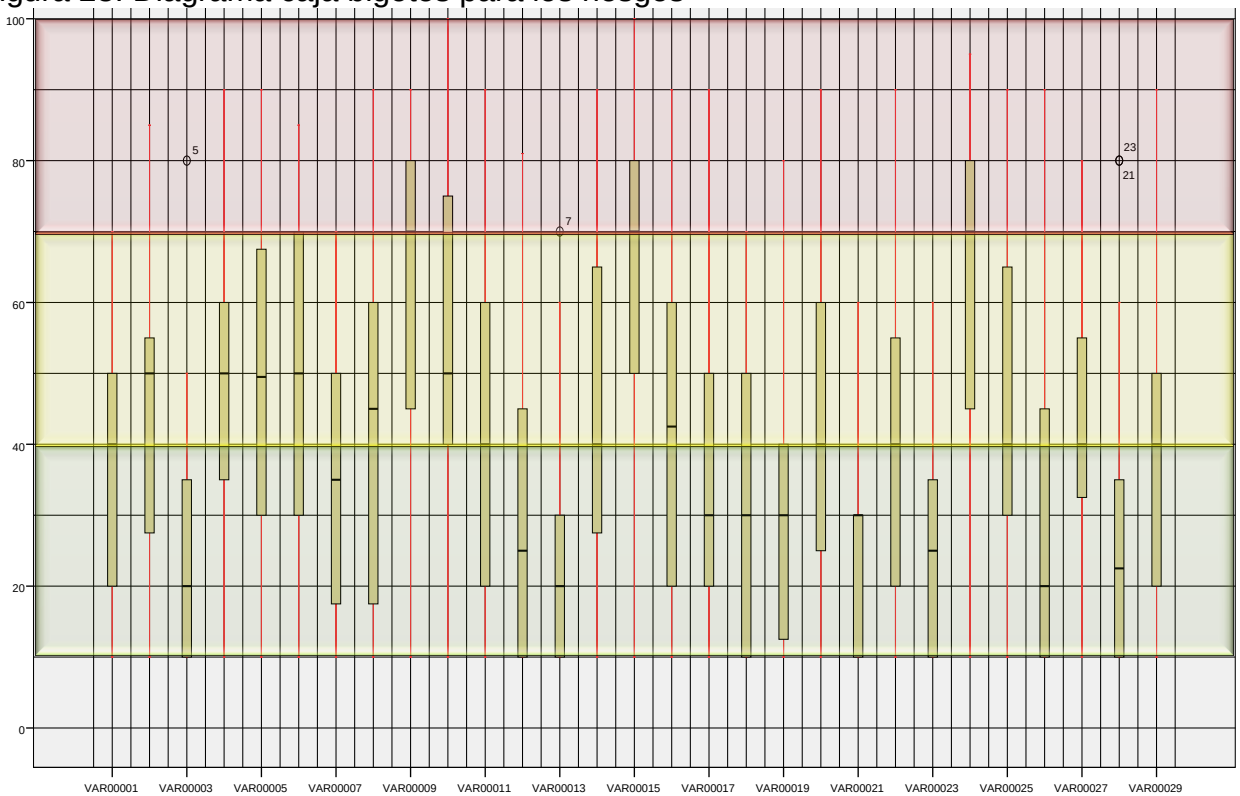
7.3.4.4 Análisis de resultados

- **Probabilidad**

Con el fin de visualizar y conocer el tipo de distribución estadística de las respuestas, se elaboró el diagrama de caja bigotes para la variable probabilidad. Se escogió este diagrama por su utilidad para realizar comparaciones entre conjuntos de datos, dado su alto impacto visual y fácil interpretación. En la Figura 23, se muestra el gráfico correspondiente, dónde en el eje Y se ubica el valor de probabilidad y en el eje X los riesgos evaluados.

En la Figura 23 se puede notar una gran dispersión en los datos dada la longitud de los bigotes, además que están ordenados de manera asimétrica, lo cual es entendible puesto que se están midiendo percepciones de las personas, las cuales dependiendo del riesgo se inclinan hacia arriba o hacia abajo. Por lo tanto, se eligió la mediana como valor representativo de los datos para determinar la ubicación del riesgo en la matriz de nivel de riesgo. Entonces, se demarcaron tres zonas, las correspondientes a los tres intervalos definidos de probabilidad (bajo= 10-40%, medio= 40-70%, alto=70-100%), y según en la zona en que se ubicara la mediana, se decidía que nivel de probabilidad tenía el riesgo en evaluación.

Figura 23. Diagrama caja bigotes para los riesgos

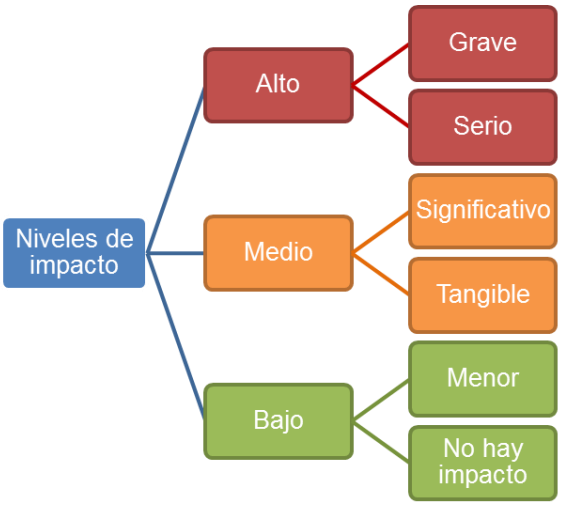


Fuente. Autores del proyecto con ayuda del software SPSS®

- **IMPACTO**

En este caso, la variable que se midió era categórica, por lo cual se uso la moda como valor representativo de los datos. Se realizaron gráficos de tortas para cada uno de los riesgos (Ver ANEXO 25). Además, con el fin de simplificar el análisis, los 6 niveles de impacto se agruparon en tres niveles cualitativos: alto, medio y bajo (Ver Figura 24).

Figura 24. Agrupación de niveles de impacto



Fuente. Autores del proyecto

- **MEDIDA DE TRATAMIENTO**

Al igual que el impacto, la medida de tratamiento del riesgo es una variable categórica. Por lo cuál su análisis se realizo mediante el cálculo de moda. Los gráficos de torta para cada uno de los 28 riesgos se encuentran en el ANEXO 25. A continuación se resaltan algunos aspectos que llaman la atención:

- Para la mayoría de los riesgos (25 de 28), la medida más popular para su tratamiento, según las personas encuestadas, es la reducción del mismo,

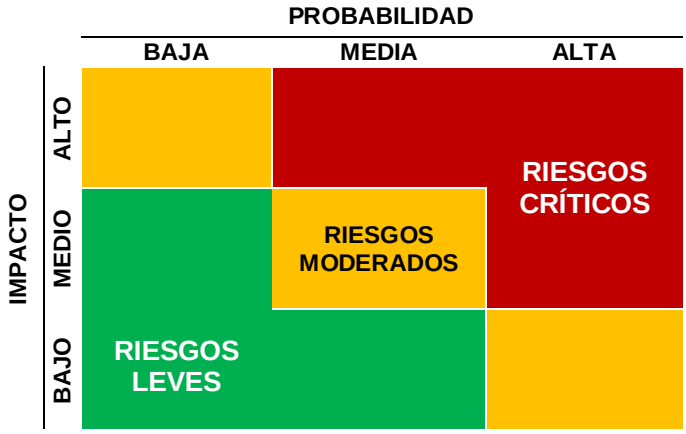
entendida como la aplicación de controles que minimicen ya sea su probabilidad de ocurrencia, su impacto, o ambos.

- Para el riesgo relacionado con desastres naturales, el 50% de las personas eligieron la opción de aceptar el riesgo, lo cuál es completamente coherente puesto que a parte de algunas medidas de prevención, es poco lo que se puede hacer con respecto al factor naturaleza.
- Tanto para el riesgo de ataques físicos, vandalismo y desordenes civiles como para siniestros, la medida con mayor número de respuestas fue “transferir”, entendida como la acción de encargar a una entidad externa al grupo para que gestione el riesgo en cuestión.

7.3.5 Determinación del nivel de riesgo

Una vez obtenidas las cuantificaciones de probabilidad e impacto para cada riesgo, se procedió a utilizar la matriz de riesgos, en la que se relacionan estas dos medidas, y de donde se obtiene el nivel de riesgo, clasificado en niveles bajo, medio y alto (Figura 25). En el ANEXO 27, se muestra la matriz de riesgo completa y en la Tabla 20, se muestran los niveles obtenidos como resultado del análisis de riesgos.

Figura 25. Matriz de nivel de riesgo



Fuente: Autores del proyecto.

Tabla 20. Resultados de análisis de riesgos

No	Riesgo	% Prob. de ocurrencia	Prob. cualitativa	Nivel de impacto	Impacto cualitativo	Nivel de riesgo
1	Suplantación de identidad	40	Media	2	Medio	Medio
2	Sabotaje o vandalismo contra la información y/o sistemas de información del grupo	50	Media	4	Alto	Alto
3	Extorsión a los integrantes del grupo	20	Baja	4	Alto	Medio
4	Personas malintencionadas acceden y/u obtienen información confidencial	50	Media	4	Alto	Alto
5	Daños en TI (equipos)	49,5	Media	4	Alto	Alto
6	Robo o pérdida accidental	50	Media	3	Medio	Medio
7	Ingeniería social	35	Baja	3	Medio	Bajo
8	Penetración desautorizada al sistema de información a través de la red	45	Media	4	Alto	Alto
9	Ataques de malware	70	Alta	2	Medio	Alto
10	Pérdida de información gestionada en la nube	50	Media	3	Medio	Medio
11	Fallas en el hardware	40	Media	2	Medio	Medio
12	Obsolescencia tecnológica.	25	Baja	4	Alto	Medio
13	Robo por integrantes del grupo.	20	Baja	3	Medio	Bajo
14	Violaciones de propiedad intelectual.	40	Media	4	Alto	Alto
15	Expansión del uso de ordenadores personales y dispositivos móviles	70	Alta	3	Medio	Alto
16	Daño de las copias de seguridad.	42,5	Media	3	Medio	Medio
17	Usuarios con sobre-privilegios alteran los datos o interceptan información	30	Baja	3	Medio	Bajo

No	Riesgo	% Prob. de ocurrencia	Prob. cualitativa	Nivel de impacto	Impacto cualitativo	Nivel de riesgo
18	Incumplimiento de acuerdos de confidencialidad o privacidad establecidos	30	Baja	4	Alto	Medio
19	Información confidencial es divulgada por integrantes del grupo	40	Media	3	Medio	Medio
20	Incumplimiento de responsabilidades por modificaciones en los sistemas de información	30	Baja	3	Medio	Bajo
21	Acceso a software especializado con fines no académicos	40	Media	4	Alto	Alto
22	Modificación de información confidencial por integrantes del grupo.	25	Baja	3	Medio	Bajo
23	Fuga de conocimiento	70	Alta	3	Medio	Alto
24	Ataques físicos, vandalismo y/o desordenes civiles.	40	Media	4	Alto	Alto
25	Desastres naturales.	20	Baja	5	Alto	Medio
26	Fallas técnicas en equipos, redes o software	40	Media	3	Medio	Medio
27	Interrupción de las actividades cotidianas por siniestros	22,5	Baja	4	Alto	Medio
28	Fallas en el suministro de energía.	40	Media	2	Medio	Medio

Fuente. Autores del proyecto

7.3.6 Asignación de Controles

Una vez se han determinado los requerimientos de seguridad a partir de los riesgos identificados, se debe seleccionar los controles apropiados que deberán implementarse e incorporarse en la formulación de la política de seguridad de la información del grupo de investigación. Esta asignación de controles se efectuó de manera independiente para cada uno de los 28 riesgos, teniendo en cuenta la amenaza y sus vulnerabilidades asociadas, buscando contrarrestar estas últimas. Para este ejercicio se utilizó el estándar ISO/IEC 27002:2005, que establece 133 controles, y los cuales fueron examinados y designados según lo requerido por cada riesgo.

En concordancia con el objetivo de este trabajo, en la estrategia de mitigación contenida en la hoja de información de cada riesgo crítico, sólo se tuvieron en cuenta los controles KRI del área de gestión (ver ANEXO 31).

Al realizar el análisis se observó que de los 26 controles KRI del área de gestión, 6 de estos son aplicables no sólo para INNOTEC sino para cualquier otro grupo de investigación, puesto que, favorecen la gestión tanto de los riesgos críticos como de los 18 riesgos restantes que están en niveles: leve y moderado (ver Tabla 21). Asimismo, en los puntos de inicio de la seguridad de la información que recomienda la norma ISO/IEC 27002:2005[207], sugieren 5 de estos 6 controles por ser considerados práctica común en la mayoría de organizaciones y en la mayoría de escenarios. Otro hallazgo importante, fue que de los 26 controles KRI, 7 no se requerían asignar a los 10 riesgos críticos definidos en la evaluación de riesgos (ver Tabla 22), por el contrario fue necesaria la inclusión de otros controles que a pesar de no ser parte de la lista sugerida por Layton, son pertinentes para un grupo de investigación, esos controles son entre otros, 10.8.2 Acuerdo de confidencialidad, 6.1.6 Contacto con las autoridades, 11.3.1 Uso de contraseñas, y

[207] INTERNATIONAL STANDARDS ORGANIZATION. Op. Cit, p. 11.

15.1.2 Derechos de propiedad intelectual. Este último control además es considerado en la norma ISO/IEC 27002:2005[208] como esencial para una organización desde el punto de vista legislativo.

El detalle de la asignación de controles realizada por el equipo de trabajo del proyecto esta en el proyecto esta en el

[208] Ibid.

, y para conocer la definición de cada uno de estos controles es preciso consultar la norma ISO/IEC 27002:2005.

Tabla 21. Controles KRI Management seleccionados como práctica común para todos los riesgos evaluados en INNOTEC

Control	NOMBRE DEL CONTROL
5.1.1	Documento de política de seguridad de la información
6.1.1	Compromiso de la Dirección con la seguridad de la información
6.1.3	Asignación de responsabilidades relativas a la seguridad de la
8.2.2	Concienciación, formación y capacitación en seguridad de la
13.1.1	Notificación de los eventos de seguridad de la información
14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio

Fuente. Autores del proyecto

Tabla 22. Controles no seleccionados para mitigar los riesgos críticos de INNOTEC

Control	NOMBRE DEL CONTROL
6.1.8	Revisión independiente de la seguridad de la información.
10.1.1	Documentación de los procedimientos de operación
10.3.2	Aceptación del sistema
10.7.1	Gestión de soportes extraíbles
12.1.1	Análisis y especificación de los requisitos de seguridad
15.1.1	Identificación de la legislación aplicable
15.1.4	Protección de datos y privacidad de la información de carácter

Fuente. Autores del proyecto

7.3.7 Riesgo Residual

Luego de establecer los controles para mitigar el nivel de riesgo de la organización, permanece un remanente de riesgo, pues reducirlo en un 100% no es posible en la práctica. Al respecto, Spafford, citado por el consultor Vicente Aceituno[209], señaló que "El único sistema verdaderamente seguro es aquel que se encuentra apagado, encerrado en una caja fuerte de titanio, enterrado en un bloque de hormigón, rodeado de gas nervioso y vigilado por guardias armados y muy bien pagados. Incluso entonces yo no apostaría mi vida por ello".

El riesgo residual es entonces el riesgo que permanece después del tratamiento del riesgo, y en esencia, es el riesgo que no puede ser tratado y, por tanto, debe ser aceptado por la organización. Como el objetivo de la gestión del riesgo es reducir al máximo el riesgo residual, este proceso puede requerir de múltiples réplicas para alcanzar su objetivo[210]. El cálculo del riesgo residual se encuentra en el ANEXO 29. Este cálculo se hizo teniendo en cuenta la situación actual del grupo de investigación, y se espera que una vez se implemente el modelo de gestión y se efectúe la política de seguridad de la información, al realizar de nuevo la evaluación de controles el resultado del riesgo residual cambie y sea despreciable.

El riesgo residual puede calcularse de varias formas, en este proyecto se siguió la guía BITS key risk measurement tool for information security opertional risks, para lo cual, se utilizaron los valores de probabilidad e impacto obtenidos del análisis de

[209] ACEITUNO, Vicente. Definición de seguridad de la información y sus limitaciones. [En línea]. Disponible en: http://www.fistconference.org/data/presentaciones/queesseguridad.pdf. Citado por: RAYME SERRANO, Rubén. Gestión de seguridad de la información y los servicios críticos de las universidades: un estudio de tres casos en Lima Metropolitana Tesis de maestría en gestión empresarial. Universidad Nacional Mayor de San Marcos. Facultad de ciencias administrativas. p. 24.

[210] HALVORSON, Nick. Information risk management: a process approach to risk diagnosis and treatement. En: TIPTON, Harold y KRAUSE, Micki. Information security management handbook. 6 ed. Vol. 2. Boca Raton: Auerbah Publications, 2008.

riesgos y se uso la moda como estadístico representativo del nivel de efectividad de los controles. Lo siguiente fue observar en la matriz de puntuación numérica de 0-a-10 la cuantificación de la intersección del nivel de efectividad del control y el valor del impacto.

La matriz de puntuación se define como sigue:
10 = Control Bajo vs Impacto Alto → Considerable margen de mejora
0 = Control Bueno vs Impacto Bajo → No hay lugar para la mejora.

Por ejemplo, si el control se había aplicado completamente la puntuación siempre era cero, porque no hay espacio para la mejora en la acción / control. Incluso si el impacto era cero, un control de cero produciría una puntuación de riesgo de 5 a causa de que el impacto puede cambiar con el tiempo y el grupo de investigación debe estar practicando por lo menos algún nivel de control diferente de cero.

En general, el puntaje de los 28 riesgos varió entre 1,42 y 5,16, esta puntuación son resultado de la intersección del grado de implementación del control y el impacto multiplicado por el porcentaje de probabilidad de ocurrencia. A partir de este análisis los integrantes del grupo pueden tener un punto de referencia para la próxima evaluación de riesgo y de esa forma tomar decisiones como la de continuar o abandonar la actividad dependiendo del nivel de riesgos; fortalecer controles o implantar nuevos controles; o finalmente, podrían tomar posiciones de cobertura. Esta decisión está delimitada a un análisis de costo beneficio y riesgo.

8. POLICY CAPTURING

Policy capturing aparece en la literatura de toma de decisiones, comúnmente utilizada para estudiar los procesos de toma de decisión, cuyo propósito es valorar como los tomadores de decisiones utilizan información disponible al momento de realizar juicios evaluativos[211]. Es muy aplicada en el campo de los estudios organizativos y utiliza principalmente el diseño de experimentos.

Se trata de una metodología de captura de decisiones basada en regresión en donde se les solicita a los participantes que tomen decisiones en respuesta a una serie de escenarios de decisión o problemáticas presentados por el investigador[212]. Esto implica la existencia de una variable dependiente, es decir la decisión tomada, y dos o más variables independientes, también llamadas factores del estudio, que consisten en fragmentos claves de información que son manipulados en los escenarios. A partir de las respuestas obtenidas (conjunto de decisiones tomadas por los participantes del estudio), el investigador realiza una regresión, en donde la estimación de los coeficientes indica la importancia o peso relativo de los diferentes factores y define los patrones o estrategias para cada tomador de decisión[213].

En el presente proyecto, se utilizó policy capturing con el objetivo de analizar la importancia que tienen las tres dimensiones de seguridad de la información en la toma de decisiones sobre la implementación de medidas de control en los proyectos de investigación; y de esta manera, poder definir una política de seguridad de la información para el grupo INNOTEC, que permita controlar los

[211] KARREN, Ronald y BARRINGER, Melissa. A review and analysis of the policy-capturing methodology in organizational research: guidelines for research and practice. En: Organizational Research Methods. Vol. 5, No. 4 (2002); p. 337.
[212] AIMAN-SMITH, Lynda, SCULLEN, Steven y BARR, Steve. Conducting studies of decision making in organizational contexts: a tutorial for policy-capturing and other regression-based techniques. En: Organizational Research Methods. Vol. 5, No. 4 (Oct. 2002); p. 390.
[213] Ibid. p. 388.

riesgos identificados, dado que si estos ocurren, tienen un impacto en al menos una de las tres dimensiones de la seguridad de la información (Ver Figura 26).

Figura 26. Riesgos críticos identificados y su relación con las dimensiones de seguridad de la información

Principios de Seguridad de la información			
Confidencialidad	**Integridad**	**Disponibilidad**	**Continuidad de las actividades de investigación**
Personas malintencionadas obtienen acceso a información confidencial	Sabotaje o vandalismo contra la información o TI	Sabotaje o vandalismo contra la información o TI	Acceso a software académico
Ingreso desautorizado	Ataques de malware	Daños en TI	Violaciones de propiedad intelectual
Expansión del uso de ordenadores personales	Expansión del uso de ordenadores personales	Ataques de malware	
		Expansión del uso de ordenadores personales	
		Fuga de Conocimiento	
		Ataques físicos, vandalismo	

Fuente. Autores del proyecto

8.1 JUSTIFICACIÓN DEL ESTUDIO

La justificación para la aplicación de esta metodología proviene de sus múltiples ventajas con respecto a otros enfoques para examinar las políticas de decisión, como por ejemplo el auto-reporte de calificación de atributos, en el cual los participantes califican y jerarquizan las variables de interés según su importancia. Estudios sobre dicho método han generado inquietudes acerca de su validez al encontrar que las políticas expresadas difieren de las verdaderas políticas

(observadas)[214]. La discrepancia puede deberse a que los individuos no sean transparentes en sus respuestas a causa de su deseo de ser "socialmente correcto". En contraste, policy capturing evita dichos efectos indeseados al evaluar indirectamente la importancia explicativa de las variables y, por esta razón, es considerada preferible que el método de auto-reporte de atributos.

Otra fortaleza de la metodología, proviene de la posibilidad que tiene el investigador de manipular experimentalmente los niveles de los factores. Mediante el uso de muestreo sistemático de los estímulos, y la presentación aleatoria de estos a los tomadores de decisión, el investigador puede enfocarse en estímulos particulares o combinaciones de estímulos[215] [216]; asimismo, al repetir algunos estímulos, puede evaluar la confiabilidad de los datos[217]. Incluso, el hecho de pedirles a las personas que realicen juicios acerca de escenarios con atributos múltiples es más similar a los problemas de toma de decisión y, por tanto más realista[218].

Por último, policy capturing se lleva a cabo al nivel individual; esto significa que se genera un modelo para cada tomador de decisión, aunque se pueden generalizar los resultados para grupos de individuos.

Por lo general, el proceso que se lleva a cabo en la aplicación de policy capturing consta de cinco etapas principales[219]: diseño del estudio, ejecución del estudio, análisis, interpretación y reporte de resultados. Seguidamente se detallan los pormenores de cada una de ellas.

---

[214] HITT, Michael y MIDDLEMIST, Dennis. A methodology to develop the criteria and criteria weightings for assessing subunit effectiveness in organizations. En: Academy of Management Journal. Vol. 22, No. 2 (1979); p. 356.
[215] CAROLL, John y JOHNSON, Eric. Decision research: a field guide. Newbury Park, CA: Sage, 1990.
[216] MCGRATH, Joseph. Dilemmaticas: The study of research choices and dilemmas. En: American behavioral scientist. Vol. 25, No. 2. (Nov./Dic. 1981); p. 179.
[217] AIMAN-SMITH, SCULLEN y BARR, Op. Cit. p. 390
[218] KARREN y BARRINGER, Op. Cit. p. 338
[219] AIMAN-SMITH, SCULLEN y BARR, Op. Cit. p. 390

8.2 DISEÑO DEL ESTUDIO

Antes de comentar los detalles del diseño y ejecución del estudio, vale la pena aclarar algunos supuestos y limitaciones que este implica.

- En el cuestionario se repitieron dos escenarios, como método de control, cuyas respuestas no fueron incluidas en el análisis.
- La participación individual en el cuestionario es confidencial. De esta manera, las investigadoras aseguran la plena cooperación de los participantes.
- El alcance de este estudio se limita a los estudiantes de pregrado, posgrado, profesores y profesionales de apoyo del grupo de investigación INNOTEC.
- El estudio se enfoca a un solo grupo de investigación, lo que impide la generalización de los resultados. Por tanto la política que se desarrolle a partir de lo encontrado tendrá aplicación únicamente en el grupo INNOTEC. Sin embargo, esto no implica que se no se pueda adaptar a otros grupos, ya que de alguna manera la similitud de propósitos y objetivos la harían aplicable potencialmente para otros grupos de la Facultad, e incluso para organizaciones o dependencias de la Universidad.

Ahora bien, según la literatura revisada, existen varios aspectos que deben ser considerados y definidos claramente en el diseño del estudio, como lo son la naturaleza del estudio, la muestra o población, los factores y sus niveles, los escenarios, y la pregunta a realizar.

8.2.1 Naturaleza de la pregunta

El primer aspecto a considerar en el diseño del estudio es la naturaleza de la pregunta de investigación, es decir, si se busca examinar los resultados de la decisión individual o tendencias generales de resultados agregados de muchos tomadores de decisión. Los estudios que abordan la primera opción se conocen

como idiográficos, mientras que aquellos basados en la segunda se conocen como nomotéticos, y son los más comunes en la investigación organizativa.
Debido a que lo que se buscaba era obtener una visión global de la toma de decisiones en el grupo de investigación, y no evaluar la visión de cada integrante por separado, la naturaleza de la pregunta del estudio se clasifica como nomotética. Al respecto, Aiman-smith, Scullen y Barr[220] señalan que los investigadores aplican esta orientación asumiendo que los distintos participantes pueden ser sustituidos por otros; en el caso del presente proyecto, se podría intercambiar uno o varios participantes por otros investigadores del mismo grupo, y se esperaría una variación poca o nula en los resultados.

En definitiva, la pregunta se planteó de la siguiente manera: ¿Cuál dimensión de la seguridad de la información (confidencialidad, integridad o disponibilidad) tiene mayor influencia en la decisión de un integrante del grupo INNOTEC, que participa en un proyecto de investigación, de aplicar medidas de control sobre el mismo?

8.2.2 Población

En este punto, se consideró el tema de determinar quienes participarían en el estudio. Una selección apropiada de sujetos está directamente relacionada con la representatividad del estudio; este es un principio estadístico de gran importancia que implica la capacidad de reproducir a pequeña escala las características de la población.

Buscando involucrar a la mayor cantidad de personas posibles, y con el fin de analizar los diferentes comportamientos que se presentan entre los investigadores, se determinó como población de estudio, la totalidad de los integrantes del grupo de investigación activos en el momento del diseño del estudio. La forma en que

[220]AIMAN-SMITH, SCULLEN y BARR, Op. Cit. p. 390

esta conformada la población se observa en la Figura 27, con un total de 34 personas, incluyendo profesores y estudiantes de pregrado y posgrado.

Figura 27. Conformación de la población de estudio

Fuente. Autores del proyecto

8.2.3 Elección de los factores

Se debe recordar que los modelos de policy capturing no pueden incluir todas las variables que influencian la toma de decisiones. Los investigadores deben buscar la concordancia entre la interpretación y la pregunta de investigación. Además, es conveniente usar información cualitativa obtenida a través de entrevistas realizadas luego de la ejecución del estudio para enriquecer la interpretación de resultados.

Para determinar los factores a incluir en los escenarios de policy capturing, se tuvo en cuenta los resultados de la evaluación de riesgos. De acuerdo al análisis de los 10 riesgos críticos, cada uno de ellos se puede relacionar con una de las tres dimensiones de seguridad de la información (Ver Figura 26).

Las definiciones utilizadas para cada factor fueron:

- *Confidencialidad:* “Es la necesidad de que la información sensible de la organización solo sea conocida por personas autorizadas”[221].
- *Integridad:* “Es la característica que hace que el contenido de la información permanezca inalterado, a menos que sea modificado o eliminado por personal autorizado”[222].
- *Disponibilidad:* “Es la capacidad de la información de estar siempre disponible en el momento que la necesiten, para ser procesada por las personas autorizadas”[223].

8.2.4 Niveles de los factores

Según Aiman-Smith, Scullen y Barr[224], los escenarios en un diseño factorial completo deberían incluir no más de cinco factores; asimismo, dos o tres niveles por factor deberían ser suficientes para la mayoría de los diseños factoriales completos. Teniendo en cuenta lo anterior, para cada factor se establecieron dos niveles: alto y bajo. El nivel alto representa la condición de total cumplimiento de la dimensión de seguridad de la información; por el contrario, el nivel bajo representa la completa violación o transgresión a la misma. En seguida se muestra una descripción específica de cada nivel para los tres factores en cuestión.

[221] ESET COLOMBIA. Guía del empleado seguro. [en línea]. [consultado el 15 de mayo de 2012]. Disponible en http://endpoint.eset-la.com/guia_del_empleado_seguro.pdf
[222] ESET. Op. cit., p. 3
[223] ESET. Op. cit., p. 3
[224] AIMAN-SMITH, SCULLEN y BARR, Op. Cit. p. 396.

Tabla 23. Descripciones de los niveles de los factores

Factor	Nivel	Descripción
Confidencialidad	Alta	Toda información del proyecto es considerada confidencial y su divulgación está prohibida previa publicación oficial de los resultados.
	Baja	La información del proyecto, clasificada como confidencial, se hace pública sin autorización. La información del proyecto está siendo divulgada sin autorización
Disponibilidad	Alta	La información puede ser usada por personas directamente involucradas en el proyecto de investigación en el momento que lo requieran.
	Baja	La información no se encuentra disponible en el momento en que la necesitan.
Integridad	Alta	Toda la información del proyecto puede ser modificada únicamente por personas directamente involucradas en el mismo
	Baja	La información del proyecto puede ser modificada por cualquier persona dentro o fuera del grupo.

Fuente. Autores del proyecto

8.2.5 Construcción de los escenarios

Los escenarios se construyeron de la misma forma en que se hace en los estudios factoriales, es decir, los factores y sus niveles, fueron sistemáticamente variados. Considerando que se trataba de un diseño factorial completo $\mathbf{2^3}$ (3 factores con 2 niveles cada uno) se construyeron un total de **8 escenarios**, utilizando todas las posibles combinaciones de los factores y sus niveles. Estos pueden observarse en el ANEXO 32. De esta manera, se garantizó la ortogonalidad, que es un tema importante en la selección y descripción de los escenarios. También se tuvo en cuenta en la redacción que los escenarios fueran relevantes y realistas para que no se viera afectada la validez del estudio.

Tabla 24. Matriz del diseño

CORRIDA	FACTOR		
	Confidencialidad	Integridad	Disponibilidad
1	-	-	-
2	+	-	-
3	-	+	-
4	+	+	-
5	-	-	+
6	+	-	+
7	-	+	+
8	+	+	+

Fuente. Autores del proyecto

8.2.6 Instrumento de medición

El instrumento de medición se diseñó utilizando la opción de Formulario en Google Docs (Ver ANEXO 32). Se incluyeron algunas preguntas sobre la vinculación con el grupo como: tipo de vinculación, años de experiencia, y participación en proyectos como autor, director o codirector. Esto con el fin de caracterizar a cada participante y estudiar posibles diferencias entre subgrupos.

Asimismo, para asegurar una adecuada comprensión de los escenarios, se incluyeron en el cuestionario definiciones breves de los tres factores que se enmarcan en cada escenario. Adicionalmente, se redactó un párrafo introductorio que describía el contexto general para todos los escenarios.

Los ocho escenarios fueron ordenados aleatoriamente en el cuestionario, y se repitieron dos escenarios a manera de preguntas de control, para un total de 10 escenarios. Después de revisar cada escenario, cada participante debía indicar el tipo de medida de control que aplicaría en cada caso, utilizando una escala de 5 puntos que se muestra en la Tabla 25. Se determinó de esta manera, debido a

que algunas investigaciones[225] [226] sugieren que la confiabilidad de la escala de Likert tiende a estabilizarse aproximadamente en las escalas de 5 a 7 puntos.

Tabla 25. Escala de respuesta

Opción	Definición
Ningún control	Las condiciones no ameritan la implementación de medidas de control, usted se siente tranquilo.
Control leve	Se requieren algunos controles, con un costo mínimo y de rápida implementación, con tan sólo horas para que usted solucione la situación.
Control moderado	Se requieren controles que implican costos significativos y algunos días para su implementación. Usted puede hacerse cargo de la situación.
Control fuerte	La situación causa daños en la calidad del proyecto, pero se pueden reparar, incurriendo en costos altos, intervención de la dirección del grupo y algunos meses para implementar controles.
Control muy fuerte	Se requiere completo compromiso de la dirección, costos altos, e incluso pueden existir daños irreparables. Se necesitarán meses para implementar controles.

Fuente. Autores del proyecto

8.3 EJECUCIÓN DEL ESTUDIO

Esta etapa se focaliza en los procedimientos e instrumentos para recolectar los datos. Se debe informar a los participantes acerca de la naturaleza de la tarea que se les va a encomendar, incluyendo las suposiciones que deberán realizar. Luego se debe proveer la información de los atributos de una forma accesible y comprensible. Y por último asegurarse que los participantes no empleen demasiado tiempo en responder las preguntas, evitando fatigas y molestias.

[225] CICCHETTI, D. V., SHOWALTER, D., yTYRER, P. J. The effect of number of rating scale categories on levels of inter-rater reliability: a Monte-Carlo investigation. En: Applied Psychological Measurement. Vol. 9 (1985); p. 35.
[226] PRESTON, Carolyn y COLMAN, Andrew. Optimal number of response categories in rating scales: reliability, validity, discriminating poser and respondent preferences. En: Acta Phychologica. Vol. 104, No. 2 (2000); p. 9.

8.3.1 Aplicación del cuestionario

Todos los datos fueron recolectados mediante correo electrónico usando cuestionarios basados en computador (Herramienta para formularios de Google Docs). Se les explico a los participantes, que iban a leer una serie de escenarios descriptivos de una situación en la cual se debe tomar una decisión respecto al nivel de implementación de medidas de control en un proyecto de investigación.

Además, se les instruyó para que tuvieran en cuenta los tres fragmentos de información proporcionados para tomar la decisión. Igualmente, se hizo énfasis en que leyeran cada situación cuidadosamente y la asumieran como propia y real, indicándoles que no volvieran a atrás, en otras palabras, que consideraran cada situación como única y aislada.
La participación fue voluntaria; la anonimidad y confidencialidad de las respuestas fueron garantizadas desde el inicio. Cada participante recibió un cuestionario idéntico a los demás. Finalmente, se obtuvieron respuestas de 30 personas (aprox. 85% de la población).

8.4 ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Debido a que los factores son variables cualitativas, fue necesario utilizar la codificación dummy para los niveles, siendo 1 el nivel alto y 0 el nivel bajo.

8.4.1 ANÁLISIS ESTADÍSTICO ANOVA

Utilizando únicamente los 8 escenarios sin repeticiones, y las respuestas recolectadas de todos los participantes, se obtuvo la tabla de ANOVA para los efectos principales y las interacciones de los factores, mediante el software SPSS®.

Para el análisis estadístico, se plantearon las siguientes hipótesis:

- H_0= Los efectos principales de los factores y sus interacciones son iguales
- H_1= Al menos uno de los efectos principales de los factores y sus interacciones es diferente a los demás.

Tabla 26. Análisis de varianza

Fuente de variación	Grados de libertad	SC sec.	SC ajust.	MC ajust.	F	P
Confidencialidad	1	71,5	71,5	71,5	93,56	0,000
Disponibilidad	1	24,7	24,7	24,7	32,33	0,000
Integridad	1	0,1	0,1	0,1	0,14	0,712
Confidencialidad *Disponibilidad	1	17,6	17,6	17,6	23,04	0,000
Confidencialidad*Integridad	1	1,2	1,2	1,2	1,48	0,211
Disponibilidad*Integridad	1	7,7	7,7	7,7	10,08	0,002
Confidencialidad* Disponibilidad*Integridad	1	6,3	6,3	6,3	8,29	0,004
Error	**232**	**177,30**	**177,3**	**0,764**		
Total	**239**	**306,46**				

Fuente. Autores del proyecto con ayuda del software SPSS®

En el modelo a analizar, consistente en tres factores, los efectos de interés son siete: los tres efectos principales, los tres efectos de las interacciones dobles (uno por cada interacción entre cada dos factores) y el efecto de la interacción triple (entre los tres factores). Para conocer el efecto de un factor es suficiente con hacerlo variar entre dos valores[227]. Los más adecuados en este estudio fueron los extremos de su dominio experimental: entre el nivel 0 y 1.

En la Tabla 26 se observa que los efectos principales de la confidencialidad y la disponibilidad son altamente significativos (P valor <<< 0,05); por lo que, usando un nivel de confianza del 5%, se rechaza Ho en ambos casos. Mientras que, para

[227] FERRÉ, Joan. El diseño factorial completo 2^k. Universidad Rovira i Virgili. Departamento de química analítica y química orgánica. Grupo de Quimiometría y cualimetría. Tarragona, p. 4. <http://argo.urv.es/quimio/general/doecast.pdf>.

el efecto principal de la integridad, se acepta Ho dado que el nivel de significancia en este caso es mayor que alfa, es decir, para los integrantes del grupo no es relevante la aplicación de medidas de control cuando la dimensión que está en el nivel más bajo es la integridad.

Por otro lado, el efecto de la interacción entre integridad y disponibilidad es significativo, dado que en ese caso con un P valor de 0,002 se rechaza Ho, es decir, en un contexto donde la disponibilidad y la integridad sean al mismo tiempo bajas, los integrantes del grupo estarían dispuestos a aplicar medidas de control de mayor nivel. Asimismo, el efecto de la interacción de confidencialidad y disponibilidad es significativo, quiere decir, que cuando el escenario muestra estas dos dimensiones afectadas (o en niveles bajos), igualmente se siguen tomando medidas de control y se rechaza Ho con un P valor igual a 0,000. Sin embargo, el efecto de la interacción de los factores confidencialidad e integridad es contrario, ya que se acepta Ho con un P valor de 0,211, e indica que ante un contexto donde se afecten negativa y simultáneamente estos dos factores, el nivel de medida de control no varía.

8.4.2 ANÁLISIS INTRA-SUJETOS

Se utilizó el análisis de regresión múltiple para evaluar los efectos de la combinación lineal de los tres factores independientes (confidencialidad, integridad y disponibilidad) relacionados con la decisión de implementar medidas de control. Se calculó una ecuación de regresión para cada participante, utilizando la herramienta POLICY-PC ®.

El análisis de regresión para cada participante conllevó a la obtención de 30 ecuaciones, cuyos resultados se resumirán a continuación (una tabla que contiene la totalidad de las ecuaciones puede ser solicitada a los autores del proyecto). En primer lugar, hubo una amplia variación en el grado en que la combinación lineal

de factores entre-sujetos predijo el nivel en que cada participante decidía aplicar el control (el coeficiente R^2 varió de 0,12 a 0,96). El promedio de R^2 para los 30 participantes fue de 0,70 (SD= 0,19).

Por otra parte, de acuerdo a las situaciones planteadas en los escenarios, la persona tomaba la decisión de aumentar o no el nivel de control en cada uno, es decir, era diferente la importancia que cada integrante le daba a cada dimensión de seguridad de la información según el contexto. Por consiguiente, el peso relativo variaba entre los factores y estadísticamente era más significativo para alguno de éstos, según cada persona. Entonces, con estos pesos relativos, se observó que factor tenía el mayor y se determinó, el porcentaje de participantes para los cuales tenía mayor peso cada factor así: confidencialidad 53.33%, disponibilidad 30% e integridad 10%. A la par, se presentaron dos casos atípicos: para una persona la confidencialidad e integridad tenían el mismo peso relativo, esto es el 3,33% de la población piensa que estos dos factores son igual de importantes, y para el otro caso, en una de las personas la integridad y disponibilidad tenían el mismo peso y por tanto el restante 3,33% de la población opina que tanto la integridad como la disponibilidad son igual de relevantes.

CONCLUSIONES

- Dado que la información (y el conocimiento) se está convirtiendo en una fuente de riqueza y de riesgo para las compañías (sea que decidan protegerla activamente o no), aquellos involucrados en la gestión de información necesitan entender la complejidad e importancia de su aseguramiento. No obstante, el reporte de publicaciones de ISI Web of Science en la ventana de tiempo 2001 – 2012 en el tópico "information security", muestra que la seguridad de la información es una temática con un rápido crecimiento, cuyo número de artículos por año en 2011 fue 3,3 veces los del año 2001 (Ver ANEXO 34), pero que aún no llega a su etapa de madurez, reflejado en los incrementos porcentuales positivos. Lo anterior, da la oportunidad de seguir explorando en la temática y enriquecerla a futuro.

- A pesar de los esfuerzos hechos por cambiar el enfoque técnico por un enfoque de gestión, las evaluaciones de riesgo presentes en los artículos analizados, están encaminadas en su mayoría a la identificación de amenazas técnicas, descuidando el análisis de otras esferas o ámbitos igualmente importantes, como el recurso humano, considerado el eslabón más débil de la seguridad de la información[228] [229]. Además, lo encontrado en la evaluación de riesgos, muestra lo erróneo de este enfoque, pues el 50% de los riesgos provienen de una fuente interna, es decir, son causados por las acciones intencionales o accidentales de los mismos investigadores. Entonces, una estrategia favorable consiste en profundizar en el estudio de amenazas y vulnerabilidades originadas por el capital humano e implementar los controles alineados con el resultado de este estudio.

[228] VROOM, Cheryl y VON SOLMS, Rossouw.Towards information security behavioural compliance.En: Computers & Security. Vol. 23, No. 3 (May. 2004); p. 193.
[229] BULGURCU, Burcu, CAVUSOGLU, Hasan y BENBASAT, Izak. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. En: Mis Quarterly. Vol. 34, No. 3 (Sep. 2010); p. 523.

- Los grupos de investigación analizados en el diagnóstico exploratorio, se pueden clasificar en dos categorías según el enfoque que tienen sobre la protección del conocimiento. La primera corresponde a aquellos que trabajan bajo el paradigma de conocimiento libre. “El conocimiento libre es aquel que puede adquirirse libremente, sin requerir ningún permiso, que puede compartirse con otros, puede modificarse de acuerdo a las necesidades, y permite que esas modificaciones se distribuyan de nuevo para beneficiar a todos”[230]. Por otro lado, existe otra categoría de grupos, los cuales trabajan bajo el paradigma de la sociedad (o economía) del conocimiento, según el cual, el conocimiento hace parte del capital de trabajo y es el activo más importante, y principal fuente de ventaja competitiva para la organización, razón por la cual debe ser gestionado cuidadosamente[231]. A partir de esta clasificación, se concluye que el modelo de gestión desarrollado será de interés para aquellos grupos de investigación que consideren el conocimiento generado como una fuente de financiamiento, más allá de ser únicamente un recurso estratégico para generar reconocimiento dentro de la comunidad académica.

- Uno de los resultados más valiosos del estudio fue la inquietud generada en los grupos de investigación de la Facultad de Ingenierías Fisicomecánicas ante el desconocimiento de la temática. Puesto que ninguno de los grupos estudiados cuenta con un sistema de seguridad de la información, aunque en algunos se practican procesos aislados de seguridad de la información de manera implícita, sin embargo esto no garantiza ni evidencia plenamente que se esté protegiendo el capital intelectual en los grupos. Por otro lado, se identificó que ante la ausencia de una política de seguridad de la información, al momento de implementar medidas de protección, preventivas o correctivas, sobre sus activos de información y conocimiento, los investigadores toman decisiones sin evaluar el riesgo que

[230] PLUSS, Ricardo. ¿Qué es conocimiento libre? En: Conocimiento Libre. [En línea]. [Consultado 18 marzo 2012]. Disponible en <http://conocimientolibre.wordpress.com/sobre-conocimiento-libre/>
[231] HERNANDEZ, Ysmael A. La sociedad de la información: sociedad del conocimiento un paradigma alternativo. En: Gestiopolis. [En línea]. [Consultado 18 marzo 2012]. Disponible en <http://www.gestiopolis.com/canales7/ger/la-gestion-y-la-sociedad-del-conocimiento.htm>

puede conllevar esta situación. Esto sumado a que el estudio exploratorio reveló también la ausencia de una cuantificación real del capital intelectual y de un inventario de sus activos de conocimiento e información, se ratifica la necesidad latente en la universidad, por generar una cultura de gestión de seguridad de la información mediante la extensión del modelo de gestión generado en este proyecto, como una primera iniciativa para la protección del capital intelectual.

- Para que el resultado conserve la calidad que permite obtener el modelo desarrollado en este proyecto, y no sea influenciado por sesgos; es necesario, no sólo la construcción de una taxonomía que facilite la identificación de riesgos, sino también la formulación de un modelo conceptual que logre integrar sus principales elementos y explique la interacción que existe entre ellos. Asimismo, el equipo de evaluación debe conocer del valor del capital intelectual, entender previamente la metodología, y además saber sobre la temática de riesgos de seguridad de la información, esto puede obtenerse al conjugar la experiencia con una revisión de la literatura en el área.

- Al utilizar una escala de riesgo netamente matemática, la evaluación de riesgos se dificulta, puesto que, no se cuenta con una valoración de los activos de conocimiento (y de información) tangibles e intangibles del grupo. Lo que conlleva una pérdida de significancia para los directivos del grupo, dificultando interpretar la información necesaria para la toma de decisiones correctivas o preventivas. Por ello, se hizo uso de una metodología mixta de evaluación de riesgos, como GISAM, que permitió aprovechar los datos cuantitativos y expresar el nivel de riesgo en términos cualitativos; puesto que facilitaba comprender y luego explicar los resultados de las entrevistas semiestructuradas con los integrantes del grupo, permitiendo la construcción del plan de tratamiento de riesgos.

- Al finalizar la etapa de análisis de riesgos, con base en la documentación teórica y mediante el debate en conjunto de los autores del proyecto, se

clasificaron los diez riesgos críticos de acuerdo con la dimensión de seguridad afectada (confidencialidad, disponibilidad e integridad), obteniendo como resultado, que el 60% de estos impide garantizar la disponibilidad de la información. Sin embargo, los riesgos críticos relacionados con el uso a software especializado y propiedad intelectual, no afectaban ninguna de las tres dimensiones directamente, sino la continuidad de las actividades y operaciones del grupo de investigación como tal. Para ello, considerando la norma ISO/IEC 27002, desde el punto de vista legislativo es esencial contar con el control, “Derechos de propiedad intelectual (DPI)”, aunque no sea KRI, e incluirlo dentro de un listado adaptado de controles claves para la gestión de riesgos, al igual que el control “acuerdos de confidencialidad”, que apoye la gestión de la seguridad del capital intelectual en una organización basada en conocimiento.

- Mediante la aplicación de la metodología policy capturing, se reunieron los requerimientos necesarios para el desarrollo de la política de seguridad de la información definida para el grupo de investigación INNOTEC. Esta política se redactó tomando en cuenta las decisiones e intereses de los integrantes del grupo de investigación, buscando favorecer la conservación de la confidencialidad, integridad y disponibilidad de la información, con un énfasis especial en la confidencialidad, por ser la dimensión de mayor importancia para el 55,33% de los investigadores del grupo INNOTEC. Asimismo, la política, recomendada y aprobada, permite ser extendida a cualquier grupo o centro de investigación que le interese salvaguardar los resultados de proyectos de gran impacto e importancia estratégica para ellos, e implementarla en función de las necesidades de seguridad que identifiquen y los riesgos priorizados como críticos de acuerdo a las escalas establecidas para su probabilidad e impacto.

RECOMENDACIONES

- En vista de la existencia de un alto riesgo de ataques hacia las instalaciones físicas de la Universidad, se sugiere a la misma ofrecer a los grupos de investigación, la posibilidad de administrar su información en servidores ubicados fuera del Campus Universitario, permitiendo así el acceso a la información en el momento oportuno aun cuando existan estos incidentes.

- A la Vicerrectoría de Investigación y Extensión - VIE, contar con un repositorio institucional de los proyectos y estudios estratégicos realizados por grupos de investigación de las diferentes Facultades, a fin de evitar el reprocesamiento de información, agilizar los procesos de investigación y fortalecer el trabajo colaborativo e interdisciplinario. Igualmente, es conveniente que la información contenida en el repositorio sea clasificada de acuerdo a su confidencialidad, y se cuente con diferentes niveles de acceso a la misma. Además, se le recomienda diseñar los instrumentos o herramientas necesarias para concientizar la comunidad académica, sobre una adecuada gestión de la seguridad de la información y el conocimiento, con apoyo de la socialización de los resultados de este proyecto, y de esta manera promover la formulación y ejecución de proyectos de este tipo a nivel institucional.

- Con el objeto de proteger la confidencialidad de la información, y mantenerla disponible sin interrupciones o degradación del acceso, se les recomienda a los grupos y centros de investigación la implementación de un data center propio, en donde se administren y preserven de manera centralizada, los productos de conocimiento obtenidos a partir de los proyectos de investigación que desarrollen. A su vez, para apoyar la conservación del conocimiento, se sugiere que existan sesiones regulares de transferencia del conocimiento desarrollado o apropiado por el grupo, con el fin de mantener la dinámica de investigación.

- Al director del grupo de investigación INNOTEC, liderar la revisión y actualización periódica de la política de seguridad de la información en pro de la mejora continua y el enriquecimiento del modelo de gestión, de manera que se tomen decisiones acertadas en este ámbito. Adicionalmente, y debido a la amplitud y complejidad del entorno investigativo, es aconsejable determinar períodos de tiempo para realizar ejercicios posteriores de análisis y valoración de riesgos que permitan llegar a un mayor detalle en la identificación de amenazas, vulnerabilidades e impactos, para tipos de proyectos específicos, y dar un adecuado tratamiento a nuevos riesgos que pudieran surgir.

- En la distribución del diagrama de Pareto (Ver Anexo 35) se observa el predominio de los riesgos con valoración alta y media, lo que constituye un mensaje de alerta para el grupo de investigación, sobre la necesidad de aplicar medidas de control en el corto y mediano plazo. Teniendo en cuenta estos resultados**,** la dirección del grupo de investigación INNOTEC deberá determinar la acción de gestión apropiada e implementar inmediatamente controles que protejan el grupo especialmente de los riesgos críticos.

- Al definir el plan de tratamiento de riesgos y la política de seguridad, se buscó un equilibrio entre la protección excesiva y la divulgación abierta de resultados, para evitar reducir la disponibilidad del capital intelectual causada por la aplicación de demasiadas restricciones; lo anterior, considerando que en el estudio de policy capturing, se evidenció en los integrantes dan una mayor relevancia a la confidencialidad y disponibilidad de la información. Por consiguiente, se recomienda a las organizaciones basadas en conocimiento interesadas en formular su política y gestionar la seguridad de su información, definir sus propios niveles de confidencialidad y disponibilidad, dependiendo del tipo de conocimiento, la esencia de cada grupo y el alcance de los proyectos que manejen.

BIBLIOGRAFÍA

ACKOFF, R. On learning and systems that facilitate IT. En: Center for Quality of Management Journal. Vol. 5, No. 2 (1996); p.27-35.

ACKOFF, R.L. From data to wisdom. En: Journal of Applied Systems Analysis. Vol. 16 (1989). p. 3-9.

ADLER, Mortimer Jerome. A guidebook to learning: for a lifelong pursuit of wisdom. New York: Macmillan,1986. 163 p.

AIMAN-SMITH, Lynda, SCULLEN, Steven y BARR, Steve. Conducting studies of decision making in organizational contexts: a tutorial for policy-capturing and other regression-based techniques. En: Organizational Research Methods. Vol. 5, No. 4 (Oct. 2002); p. 388-414

ALVESSON, M. Management of Knowledge Intensive Companies. Berlin/New York: de Gruyter, 1995. 367 p.

ALVESSON, Mats. Social identity and the problem of loyalty in knowledge-intensive companies. En: Journal of Management Studies. Vol. 37, No.8 (2000); p. 1101-1123.

AMIRI, Ali Naghi, RAMEZAN, Majid, y OMRANI, Abdollah. Studying the impacts of organizational organic structure on knowledge productivity effective factors case study: Manufacturing units in a domestic large industrial group. En: European Journal of Scientific Research. Vol. 40, No. 1 (2010); p. 91-101.

ANDREOU, Andreas y BONTIS, Nick. A model for resource allocation using operational knowledge assets. En: The Learning Organization: An International Journal. Vol. 14, No. 4 (2007); p. 345-374.

ARCADE, Jacques, et al. Análisis estructural con el Método Micmac y estrategia de los actores con el Método Mactor. 2004. [En línea]. [Consultado el 20 de febrero de 2012]. Disponible en: http://guajiros.udea.edu.co/fnsp/cvsp/politicaspublicas/godet_analisis_estructural.pdf

ARCHAMBAULT, E. et al. Comparing bibliometric statistics obtained from the Web of Science and Scopus. En: Journal of the American Society for Information Science and Technology. Vol. 60, No. 7 (2009); p, 1320-1326. Citado por: IBAÑEZ, Alfonso, CONCHA, Bielza y LARRAÑAGA, Pedro. Productividad y visibilidad científica de los profesores funcionarios de las Universidades públicas españolas en el área de tecnologías informáticas. Universidad Politécnica de Madrid, 2011, p.

11. [Consultado 20 Agosto de 2012]. Disponible en: http://oa.upm.es/9407/1/analisis-bibliometrico.pdf
AREITIO, Javier. Seguridad de la información: redes, informática y sistemas de información. Madrid: Editorial Paraninfo, 2008, p 2.

ARIAS, José y ARISTIZÁBAL, Carlos. El dato, la información, el conocimiento y sum productividad en empresas del sector público de Medellín. En: Semestre Económico. Vol. 14, No. 28 (2011); p. 99

ARISTA, Anarrosa, et al. Prospectiva: Construcción social del futuro. Santiago de Cali: ILPES, 1997, p. 116

ASHENDEN, Debi. Information security management: a human challenge?. En: Information Security Technical Report. Vol. 13, No. 4 (Nov. 2008); p. 195–201. Link: http://ac.els-cdn.com/S1363412708000484/1-s2.0-S1363412708000484-main.pdf?_tid=74ad3970-1d2e-11e2-a061-00000aacb35e&acdnat=1351009793_1301b0facfbc62ffccc05cb243b73190

BALLESTEROS, Diana Paola. Análisis estructural prospectivo aplicado al sistema logístico. En: Scientia et Technica. Vol. 14, No. 39 (2008); p. 194.

BARROSO, Héctor. Diseño de un modelo de gestión para el centro de sangre de concepción “Dra. Marcela Contreras Arriagada”. Concepción, 2009. Tesis para optar al grado de Magíster en Ingeniería Industrial. Universidad del Bio-Bio. Facultad de Ingeniería. Departamento de Ingeniería Industrial. p. 29.

BASKERVILLE, Richard y SIPONEN, Mikko. An information security meta-policy for emergent organizations. En: Logistics Information Management. Vol. 15, No. 5/6 (2002); p. 337-346.

BASKERVILLE, Richard y SIPONEN, Mikko. An information security meta-policy for emergent organizations. En: Logistics Information Management. Vol. 15, No. 5/6 (2002); p. 338.

BEAUTEMENT, Adam y SASSE, Angela. The economics of user effort in information security. En: Computer Fraud & Security. Vol. 2009, No. 10 (2009); p. 8

BEAUTEMENT, Adam, et al. Modelling human and technological costs and benefits of USB memory stick security. En: Workshop on economics in information security 2008. (2008).

BELSIS, Petros; KOKOLAKIS, Spyros y KIOUNTOUZIS, Evangelos. Information systems security from a knowledge management perspective. En: Information Management & Computer Security. Vol. 13, No. 3 (2005); p. 193

BIRKINSHAW, Julian y GODDARD, Jules. What is your management model? En: MIT Sloan Management Review. Vol. 50, No. 2 (2009); p. 82

BISHOP, Matt y FRINCKE, Deborah. A human endeavor: lessons from Shakespeare and beyond. En: IEEE Security & Privacy Magazine. Vol. 3, No. 4 (Jul. 2005); p. 49.

BITS. Bits key risk measurement tool for information security operational risks. Washington DC: BITS, 2004.

BODDINGTON, T. y HILL, S. Preparing for BS 7799 certification. En: GERBER, Mariana, VON SOLMS, Rossouw y OVERBEEK, Paul. Formalizing information security requirements. En: Information Management & Computer Security. Vol. 9, No. 1; p. 34.

BOJANC, Rok y JERMAN-BLAŽIČ, Borka. An economic modeling approach to information security risk management. En: International Journal of Information Management. Vol. 28, No. 5 (2008); p. 413.

BONTIS, N. Intellectual capital: an exploratory study that develops measures and models. En: Management Decision. Vol. 36, No. 2 (1998); p. 63.

BONTIS, N.; KEOW, W. C. C. y RICHARDSON, S. Intellectual capital and business performance in Malaysian industries. En: Journal of Intellectual Capital. Vol. 1, No. 1 (2000). Citado por SIMÓ, Pep y SALLÁN, José María. Capital Intangible y capital Intelectual: Revisión, definiciones y líneas de investigación. En: Estudios de Economía Aplicada, Vol. 26, No. 2 (2008); p. 75.

BONTIS, Nick. Intellectual capital: an exploratory study that develops measures and models. En: Management Decision. Vol. 36, No. 2 (1998); p. 65-67.

BONTIS, Nick. There's a price on your head: managing intellectual capital strategically. En: Ivey Business Journal (actualmente Business Quarterly). Vol. 60, No. 40 (1996); p. 43.

BRAUN, T, GLÄNZEL, W y SCHUBERT, A. The Web of Knowledge: A Festschrift in Honor of Eugene Garfield, chapter How balanced is the Science Citation Index's journal coverage? A preliminary overview of macro level statistical data. Medford: ASIS, 2000. Citado por: IBAÑEZ, Alfonso, CONCHA, Bielza y LARRAÑAGA, Pedro. Productividad y visibilidad científica de los profesores funcionarios de las Universidades públicas españolas en el área de tecnologías informáticas, Investigadores. Universidad Politécnica de Madrid, 2011, p. 11. [Consultado 20 Agosto de 2012]. Disponible en: http://oa.upm.es/9407/1/analisis-bibliometrico.pdf

BRYNJOLFSSON, Erik y HITT, Lorin. Paradox lost? Firm-level evidence on the returns to information systems spending. En: Management science. Vol. 42, No. 4 (Abr. 1996). Citado por DOHERTY, Neil; ANASTASAKIS, Leonidas y FULFORD, Heather. The information security policy unpacked: a critical study of the content of university policies. En: International Journal of Information Management. Vol. 29, No. 6 (Dic. 2009); p. 449.

BUENO, Eduardo. La gestión del conocimiento: nuevos perfiles profesionales. [En línea]. (1999). [Consultado el 6 de agosto de 2012]. Disponible en http://www .sedic.es/bueno.pdf

BULGURCU, Burcu, CAVUSOGLU, Hasan y BENBASAT, Izak. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. En: Mis Quarterly. Vol. 34, No. 3 (Sep. 2010); p. 523-548.

CABRERA, R. y GARCÍA, R. Entorno Actual de Protección de Información en México. En: Revista Online Software Gurú. (2011) [Consultado el 5 de Agosto de 2011]. Disponible en: http://www.sg.com.mx/content/view/1186/2/

CANALS, A. y PEREZ, M. Hacia la gestión del conocimiento. En: La Vanguardia. [en línea]. (2001) [Consultado el 5 de Agosto de 2011]. Disponible en http://www.uoc.edu/web/esp/art/uoc/canals/canals_imp.html

CANO, Jeimy. Seguridad de la Información en Latinoamérica. Tendencias 2009. En: Revista Sistemas de la Asociación Colombiana de Ingenieros. [en línea]. No. 110 (2009); p. 36. [Consultado el 31 de Agosto de 2011]. Disponible en http://www.acis.org.co/fileadmin/Revista_110/05investigacion1.pdf

Características y ventajas de OCTAVE. [en línea]. [consultado el 10 de agosto de 2011] Disponible en: http://www.cert.org/octave/

CAROLL, John y JOHNSON, Eric. Decision research: a field guide. Newbury Park, CA: Sage, 1990.

CARRIÓN MAROTO, Juan. Introducción conceptual a la gestión del conocimiento. [en línea]. (2002). [Consultado el 10 de agosto de 2011]. Disponible en http://manuelgross.bligoo.com/content/view/642641/Introduccion-Conceptual-a-la-Gestion-del-Conocimiento.html

CHANG, Shuchih y LIN, Chin-Shien. Exploring organizational culture for information security management. En: Industrial Management & Data Systems. Vol. 107, No. 3 (2007); p. 438.

CHAREONSUK, C. y CHUVEJ, C. Intangible asset management framework for long-term financial performance. En: Industrial Management & Data Systems. Vol. 108, No. 6 (2008); p. 812 – 828.

CHESTNUT Harold. Systems engineering Tools. Nueva York: John Wiley, 1965. Citado en LÓPEZ, Rodrigo y TORRES Luis. Teoría de Sistemas. Universidad Nacional de Colombia. Departamento de Ingeniería de Sistemas e Industrial. 2009, p. 75

CICCHETTI, D. V., SHOWALTER, D., yTYRER, P. J. The effect of number of rating scale categories on levels of inter-rater reliability: a Monte-Carlo investigation. En: Applied Psychological Measurement. Vol. 9 (1985); p. 35.

COMISIÓN ECONÓMICA Y SOCIAL DE LAS NACIONES UNIDAS. ¿Qué es gobernanza? ¿y buen gobierno? [en línea]. [consultado el 8 de mayo de 2012]. Disponible en <http://www.casaasia.es/governasia/boletin2/3.pdf>

DA VEIGA, A. y ELOFF, J.H.P. A framework and assessment instrument for information security culture. En: Computers & Security. Vol. 29, No. 2 (2010); p. 203.

DAVENPORT, Thomas y PRUSAK, Lawrence. Working knowledge: How Organizations Manage What They Know. Cambridge, MA: Harvard Business School Press, 1998, p. 2.

DAVID, Jon. Policy enforcement in the workplace. En: Computers & Security. Vol. 21, No. 6 (2002); p. 513.

DE JOUVENEL, Hugues. Sur la démarche prospective, un brief guide méthodologique. Futuribles. 1993, Citado por ARISTA, Anarrosa, *et al*. Op, cit., p. 154.

DESOUZA, Kevin y VANAPALLI, Ganesh. Securing knowledge in organizations: lessons from the defense and intelligence sectors. En: International Journal of Information Management. Vol. 25, No. 1 (Feb. 2005); p. 85.

DEZEREGA, V. (1995). Control de la Gestión Empresarial. Centro de Desarrollo Gerencial. IESA. Caracas, Venezuela. Citado en AGUILAR, José, et al. Metodología para la elaboración de un modelo de gestión en una institución pública venezolana: Fundacite-Mérida. En: Interciencia. Vol. 27, No. 6 (Jun. 2002); p. 293.

DIAZ et al. Gestión estratégica del cambio institucional. Citado en AGUILAR, José, et al. Metodología para la elaboración de un modelo de gestión en una institución

pública venezolana: Fundacite-Mérida. En: Interciencia. Vol. 27, No. 6 (Jun. 2002); p. 293.

DOHERTY, Neil; ANASTASAKIS, Leonidas y FULFORD, Heather. The information security policy unpacked: a critical study of the content of university policies. En: International Journal of Information Management. Vol. 29, No. 6 (Dic. 2009); p. 455.

DOHERTY, Neil; KING, Malcolm y AL-MUSHAYT, Omar. The impact of inadequacies in the treatment of organizational issues on information systems development projects. En: Information & Management. Vol. 41, No. 1 (Oct. 2003); p. 50.

DOROFEE, Audrey, et al. Continuous risk management guidebook. Hanscom: Carnegie Mellon University Software Engineering Institute, 1996, p. 562.

DRUCKER, Peter. The coming of the new organization. En: Harvard Business Review. Vol. 66, No. 1 (1988); p. 47.

DURANT-LAW, Graham. Tardis: a journey throught an Enterprise knowledge space. [En línea]. Citado por: ARIAS, José y ARISTIZÁBAL, Carlos. El dato, la información, el conocimiento y su productividad en empresas del sector público de Medellín. En: SemestreEconómico. Vol. 14, No. 28 (2004); p. 98.

EDVINSSON, Leif y MALONE, Michael. El capital intelectual. Barcelona: Gestión 2000, 1999, p. 27

EDVINSSON, Leif. Intellectual capital of nations. En: HOLSAPPLE, Clyde. Knowledge Management 1: Knowledge matters. Birkhäuser, 2004, p. 153.

ERNST & YOUNG. Global information security survey 2003. Ernst & Young LLP, 2003, p.1.

ESET COLOMBIA. Guía del empleado seguro. P 1-18. [En línea]. [Consultado el 15 de mayo de 2012]. Disponible en http://endpoint.eset-la.com/guia_del_empleado_seguro.pdf

ESTADOS UNIDOS. US GENERAL ACCOUNTING OFFICE. Information Security Risk Assessment: Practices of Leading Organizations. 1999. P. 6-7.

FERRÉ, Joan. El diseño factorial completo 2^k. Universidad Rovira i Virgili. Departamento de química analítica y química orgánica. Grupo de Quimiometría y cualimetría. Tarragona, p. 4. <http://argo.urv.es/quimio/general/doecast.pdf>.

FLÓREZ, María Camila y SERRANO, Ximena Paola. Identificación de líneas estratégicas de investigación para la Universidad Industrial de Santander a partir

de herramientas de vigilancia tecnológica y prospectiva área: salud. Trabajo de grado Ingeniería Industrial. Bucaramanga: Universidad Industrial de Santander. Facultad de Ingenierías Fisicomecánicas. Escuela de Estudios Industriales y Empresariales, 2011, p. 86

GARAVITO, Edwin. Presentación 2. Material académico para la asignatura Técnicas modernas de optimización. Presentación en formato PDF [En línea]. [Consultado el 15 de febrero de 2012] Disponible en: http://gavilan.uis.edu.co/~garavito/index_general.htm

GERBER, Mariana y VON SOLMS, Rossouw. Management of risk in the information age. En: Computers & Security. Vol. 24, No. 1 (Ene. 2005); p. 28.

GEVEL, Y y ISELID L. Web of Science and Scopus: A journal title overlap study. En: Online Information Review. Vol. 32, No. 1; (2008); p. 8-21. Citado por: IBAÑEZ, Alfonso, CONCHA, Bielza y LARRAÑAGA, Pedro. Productividad y visibilidad científica de los profesores funcionarios de las Universidades públicas españolas en el área de tecnologías informáticas, Investigadores. Universidad Politécnica de Madrid, 2011, p. 11. [Consultado 20 agosto 2012]. Disponible en: <http://oa.upm.es/9407/1/analisis-bibliometrico.pdf>

GLASER, Timo y PALLAS, Frank. Information security and knowledge management: solutions through analogies? Berlin: Universidad Técnica de Berlín, 2007, p. 17.

GODET, Michel. La caja de herramientas de la prospectiva estratégica. 4 ed. París: Gerpa con la colaboración de Electricité de France, Mission Prospective, 2000, p.1-91.

GONOD P. Dynamique des systèmes et méthodes prospective. Travaux et recherches de prospective. Futuribles International, nº2. 1996.

GOODALL, John, LUTTERS, Wayne y KOMLODI, Anita. Developing expertise for network intrusion detection. En: Information Technology & People. Vol. 22, No. 2 (2009); p. 92-108.

GORDON, Lawrence et al. 2005 CSI/FBI Computer Crime and Security Survey. En: Computer Security Journal. Vol. 21, No. 3. (2005); p. 2.

GRANT, Robert M. Prospering in dynamically-competitive environments: organizational capability as knowledge integration. En: Organization Science. Vol. 7, No. 4 (1996); p. 385.

GRANT, Robert M. Toward a knowledge-based theory of the firm. En: Strategic Management Journal. Vol. 17 (Edición especial de invierno,1996); p. 110.

GRANT, Robert M. Toward a knowledge-based theory of the firm. En: Strategic Management Journal. Vol. 17 (Edición especial de invierno,1996); p. 110.

GUTHRIE, J. y YONGVANICH, K. Using content analysis as a research method to inquire into intellectual capital reporting. En: Journal of Intellectual Capital. Vol. 5, No. 2 (2004); p. 282-293

HALLIDAY, S., BADENHORST, K. y VON SOLMS, R. A business approach to effective information technology risk analysis and management. En: LATEGAN, Neil y VON SOLMS, Rossouw. Towards enterprise information risk management: a body analogy. En: Computer Fraud & Security. Vol. 2006, No. 12 (Dic. 2006); p. 17

HERATH, Tejaswini. Essays on information security practices in organizations. Buffalo, 2008. Dissertation (Doctor of Philosophy). University of New York. Faculty of the graduate school. P. 9.

HITT, Michael y MIDDLEMIST, Dennis. A methodology to develop the criteria and criteria weightings for assessing subunit effectiveness in organizations. En: Academy of Management Journal. Vol. 22, No. 2 (1979); p. 356.

HÖNE, Karin y ELOFF, J.H.P. Information security policy – what do international information security standards say? En: Computers & Security. Vol. 21, No. 5 (2002); p. 402.

HONG, Kwo-Shing, et al. An integrated system theory of information security management. En: Information Management & Computer Security. Vol. 11, No. 5 (2003); p. 243.

INTERNATIONAL STANDARDS ORGANIZATION. ISO/IEC 27000:2009 Information technology — Security techniques — Information security management systems — Overview and vocabulary. 2005, p. 2-3.

INTERNATIONAL STANDARDS ORGANIZATION. ISO/IEC 27002:2005. Código para la práctica de la gestión de la seguridad de la información. 2005, p 7.

ISRAEL. MINISTRY OF INDUSTRY, TRADE AND LABOR. The intellectual capital of the state of Israel: a look to the future – The hidden values of the desert. Jerusalem: Office of the Chier Scientist, 2007, p. 10. [En línea]. [Consultado el 7 de agosto de 2012]. Disponible en <http://www.moital.gov.il/NR/rdonlyres/C973239E-F6C2-453A-A4D9-5A30F59258E3/0/intellectualcapital.pdf>

JOHANNESSEN, Jon-Arild y OLSEN, Bjørn. Knowledge management and sustainable competitive advantages: the impact of dynamic contextual training. En: International Journal of Information Management. Vol. 23, No. 4 (Ago. 2003); p. 278.

JOHNSON, M. Eric y GOETS, Eric. Embedding Information Security into the Organization. En: IEEE Security & Privacy. Vol. 5, No. 3 (2007); p. 17.

JOHNSON, M. Eric y GOETZ, Eric. Embedding information security into the organization. En: IEEE Security & Privacy Magazine. Vol. 5, No. 3 (May. 2007); p. 16-24.

KARREN, Ronald y BARRINGER, Melissa. A review and analysis of the policy-capturing methodology in organizational research: guidelines for research and practice. En: Organizational Research Methods. Vol. 5, No. 4 (2002); p. 337.

KARYDA, Maria, KIOUNTOUZIS, Evangelos y KOKOLAKIS, Spyros. Information systems security policies: a contextual perspective. En: Computers & Security. Vol. 24, No. 3 (2005); p. 248.

KAYWORTH, Tim y WHITTEN, Dwayne. Effective information security requires a balance of social and technology factors. En: MIS Quarterly Executive. Vol. 9, No. 3 (Sep. 2010); p. 163-175.

KNAPP, Kenneth, et al. Information security policy: an organizational-level process model. En: Computers & Security. Vol. 28, No. 7 (Oct. 2009): p. 493-508.

KOK, A. Intellectual Capital Management as Part of Knowledge Management Initiatives at Institutions of Higher Learning. En: The Electronic Journal of Knowledge Management. Vol. 5, No. 2 (2007); p. 183.

KRAEMER, S., CARAYON, P. y CLEM, J.F. Characterizing violations in computer and information security systems. En: Proceedings of the 16th Triennial World Congress of the International Ergonomics Association (IEA). 2006.

LACEY, D. Managing the human factor in information security: how to win over staff and influence business managers. Chichester: John Wiley & Sons, 2009, p. 15-16.

LANE, Tim (2007). Information security management in Australian universities: an exploratory analysis. Tesis de grado para el título de Magister en Tecnologías de Información. Queensland University, Brisbane, Australia, p. 1-269.

LAYTON, T. Information Security: Design, implementation, measurement and compliance. Boca Raton: Auerbach Publications, 2007, p. 8.

LEV, Baruch. Intangibles: management, measurement and reporting. Whashington, DC: Brookings Institute, 2001, p. 5.

LEVY, Alberto. El cómo y el porqué: un camino hacia el desarrollo empresario. Buenos Aires: Grupo Editorial Norma, 1989. Citado en AGUILAR, José, et al.

Metodología para la elaboración de un modelo de gestión en una institución pública venezolana: Fundacite-Mérida. En: Interciencia. Vol. 27, No. 6 (Jun. 2002); p. 293.

LIM, Joo, et al. Exploring the relationship between organizational culture and information security culture. En: Proceedings of the 7th Australian information security management conference. (2009); p. 8-9..

LÓPEZ, Agustín y RUIZ, Javier. Origen de ISO 27000. En: EL PORTAL DE ISO 27001 EN ESPAÑOL. [En línea]. [Consultado el 10 de agosto de 2011]. Disponible en < http://www.iso27000.es/iso27000.html#section3a>

LOPEZ-ILLESCAS, C, MOYA-ANEGÓN, F y MOED, HF. Comparing bibliometric country-by country rankings derived from the Web of Science and Scopus: the effect of poorly cited journals in oncology. En: Journal of Information Science. Citado por: IBAÑEZ, Alfonso, CONCHA, Bielza y LARRAÑAGA, Pedro. Productividad y visibilidad científica de los profesores funcionarios de las Universidades públicas españolas en el área de tecnologías informáticas, Investigadores. Universidad Politécnica de Madrid, 2011, p. 11. [Consultado 20 agosto 2012]. Disponible en: http://oa.upm.es/9407/1/analisis-bibliometrico.pdf

MARABELLI, Marco y NEWELL, Sue. Knowledge risks in organizational networks: The practice perspective. En: The Journal of Strategic Information Systems. Vol. 21, No. 1 (Mar. 2012); p. 25.

MARKUS, Lynne. Technochange management: using IT to drive organizational change. En: Journal of Information Technology. Vol. 19, No. 1 (2004); p. 4.

MCGRATH, Joseph. Dilemmaticas: The study of research choices and dilemmas. En: American behavioral scientist. Vol. 25, No. 2. (Nov./Dic. 1981); p. 179.

MCGREGOR, Douglas. The human side of enterprise. New York: McGraw Hill, 1960.

MEDINA, E. Evitar fuga de información, nuevo foco de inversión. En: La Republica. (2011). [Consultado el 31 de Agosto de 2011], Disponible en: http://www.larepublica.com.co/archivos/TECNOLOGIA/2011-02-02/evitar-fuga-de-informacion-nuevo-foco-de-inversion_120725.php

MITCHELL, Ruth; MARCELLA, Rita y BAXTER, Graeme. Corporate information security management. En: New Library World. Vol. 100, No. 5 (1999); p. 213.

MOJICA S., Francisco. Prospectiva: Técnicas para visualizar el futuro. Bogotá: Legis, 1991., p. 116.

MOJICA, Francisco José. La construcción del futuro. Bogotá: Universidad Externado de Colombia, 2005, p.123.

MOK, Ka Ho. Fostering entrepreneurship: changing role of government and higher education governance in Hong Kong. En: Research Policy. Vol. 34, No. 4 (2005); pp. 540.

MORTAZAVI, S. Habib y BAHRAMI, Mahdi. Integrated approach to entrepreneurship – knowledge based economy: a conceptual model. En: Procedia – Social and Behavioural Sciences. Vol. 41 (2012); p. 283.

MOYA-ANEGÓN, F. et al. Coverage analysis of Scopus: A journal metric approach. En: Scientometrics. Vol. 73 No. 1 (2007); p. 53-78. Citado por: IBAÑEZ, Alfonso, CONCHA, Bielza y LARRAÑAGA, Pedro. Productividad y visibilidad científica de los profesores funcionarios de las Universidades públicas españolas en el área de tecnologías informáticas, Investigadores. Universidad Politécnica de Madrid, 2011, p. 11. [Consultado 20 Agosto de 2012]. Disponible en: http://oa.upm.es/9407/1/analisis-bibliometrico.pdf

NATIONAL CYBER SECURITY SUMMIT TASK FORCE. Information security governance: a call to action. [en línea]. [consultado el 15 de septiembre de 2012]. Disponible en <http://www.cyberpartnership.org/InfoSecGov4_04.pdf>

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Risk management guide for information technology systems: recommendations of the National Institute of Standards and Technology. Gaithersburg: NIST, 2002.

NNOLIM, Anene. A framework and methodology for information security management. Southfield, 2007. Dissertation (Doctor of Management in Information Technology). Lawrence Technological University. Graduate Faculty of the College of Management. P. 2

O'BRIEN, J. Management Information Systems: A Managerial End User Perspective. 2 ed. Boston: Irwin, 1998.

OZKAN, Sevgi y KARABACAK, Bilge. Collaborative risk method for information security management practices: a case context within Turkey. En: International Journal of Information Management. Vol. 30, No. 6 (2010); p. 567.

PAÉZ URDANETA, I. Gestión de la inteligencia: aprendizaje tecnológico y modernización del trabajo informacional. Retos y oportunidades. Caracas: Instituto de Estudios del Conocimiento de la Universidad Simón Bolívar, 1992, p. 10.

PEPPARD, Joe. The conundrum of IT management. En: European Journal of Information Systems. Vol. 16, No. 1 (2007); p. 339.

PONNEMON INSTITUTE y LLC. 2009 Annual Study: Cost of Data Breach. Understanding Financial Impact, Customer Turnover, and Preventive Solutions. 2010, p. 4

PONNEMON INSTITUTE. Understanding Security Complexity in 21st Century IT Environments: A study of IT practitioners in the US, UK, France, Japan & Germany. 2011, p. 1

PORTAL DE SOLUCIONES TÉCNICAS Y ORGANIZATIVAS A LOS CONTROLES DE ISO/IEC 27002. Capítulo 6: Organización de la seguridad de la información. [en línea]. [consultado 15 agosto 2012]. Disponible en: <http://iso27002.wiki.zoho.com/6-1-Organizaci%C3%B3n-Interna.html>

PORTER, Michael y MILLAR, Victor. How information gives you competitive advantage. En: Harvard Business Review. Vol. 64, No. 4 (1985); p. 149.

POSTHUMUS, Shaun y von Solms, Rossouw. A framework for the governance of information security. En: Computers & Security. Vol. 23, No. 8 (2004); p. 638-646.

PRESTON, Carolyn y COLMAN, Andrew. Optimal number of response categories in rating scales: reliability, validity, discriminating poser and respondent preferences. En: Acta Phychologica. Vol. 104, No. 2 (2000); p. 9.

Prospectiva. Análisis Estructural, Mic Mac. Matriz de Impactos cruzados – Multiplicación Aplicada a una clasificación, p. 7. [Consultado 2 febrero de 2012] Disponible en: <http://www.ucol.mx/acerca/coordinaciones/cgic/cgic/Ejeinvestigacion/Bibliografia/Micmac_instrucciones.pdf>

PUHAKAINEN, Petri y SIPONEN, Mikko. Improving employees' compliance through information systems security training: an action research study. En: Mis Quarterly. Vol. 34, No. 4 (Dic. 2010); p. 757-778.

PUHAKAINEN, Petri y SIPONEN, Mikko. Improving employees' compliance through information systems security training: an action research study.En: MIS Quarterly. Vol. 34, No. 4 (Dic. 2010); p. 764.

REAL ACADEMIA ESPAÑOLA. Diccionario de la lengua española. 22 ed., Madrid: Espasa, 2001.

RENDÓN, Miguel. Relación entre los conceptos: información, conocimiento y valor. Semejanzas y diferencias. En: Ciência da Informação, Brasília. Vol. 34, No. 2 (2005); p. 53.

REZGUI, Yacine y MARKS, Adam. Information security awareness in higher education: an exploratory study. En: Computers & Security. Vol. 27 (2008); p. 241.

ROBERTSON, M. y SWAN, J. Modes of organizing in an expert consultancy: a case study of knowledge, power and egos. En: Organization. Vol. 5, No. 4 (1998); p. 543-64.

ROWLEY, Jennifer. The wisdom hierarchy: representations of the DIKW hierarchy. En: Journal of Information Science. Vol. 33, No. 2 (Feb. 2007); p

RUNTGA, Sanjay, et al. Bringing security proactively into the enterprise. En: Intel Technological Journal. Vol. 08, No. 04 (2004); p. 304.

SABAU, Gabriela. Know, live and let live: towards a redefinition of the knowledge-based economy – sustainable development nexus. En: Ecological Economics. Vol. 69, No. 6 (Abr. 2010); p. 1193.

SÄLLEBRANT, Tobias et al. Managing risk with intelectual capital statements. En: Management Decision. Vol. 45, No. 9 (2007);p. 1471.

SALMELA, Hannu. Analysing business losses caused by information systems risk: a business process analysis approach. En: Journal of Information Technology. Vol. 23, No. 3 (2007); p. 185.

SÁNCHEZ MEDINA, A. J., MELIÁN GONZÁLEZ, A., HORMIGA PÉREZ, E. El concepto de Capital Intelectual y sus dimensiones. En: Investigaciones Europeas de Dirección y Economía de la Empresa. Vol. 13, No. 2 (2007); p. 98-99.

SHEDDEN, Piya et al. Incorporating a knowledge perspective into security risk assessments. En: Vine. Vol. 41, No. 2 (2011); p. 152.

SHEDDEN, Piya, SMITH, Wally y AHMAD, Atif. Information security risk assessment: towards a business practice perspective. En: 8th Australian Information Security Management Conference. (Nov. 2010); p. 1119.

SIMÓ, Pep y SALLÁN, José María. Capital Intangible y capital Intelectual: Revisión, definiciones y líneas de investigación. En: Estudios de Economía Aplicada, Vol. 26, No. 2 (2008); p. 75

SIMON, William y MITNICK, Kevin. The art of deception: controlling the human element of security. Indianapolis: Wiley Publishing, 2002, p. 79.

SIRCAR, Sumit y CHOI, Jung. A study of the impact of information technology on firm performance: a flexible production function approach. En: Information Systems Journal. Vol. 19, No. 3 (2009). Citado por DOHERTY, Neil; ANASTASAKIS, Leonidas y FULFORD, Heather. The information security policy unpacked: a

critical study of the content of university policies. En: International Journal of Information Management. Vol. 29, No. 6 (Dic. 2009); p. 449.

SISTESEG. Organización de la Seguridad de la Información. [en línea] [consultado 15 agosto 2012]. Disponible en: <http://www.sisteseg.com/files/Microsoft_Word_-_Organizaci_n_de_la_seguridad_de_la_informaci_n.pdf>

STARBUCK, W. H. Learning by knowledge-intensive firms. En: Journal of Management Studies. Vol. 3, No. 4 (1992); p. 715.

SULLIVAN, P. H. Profitingfromintellectual capital: extractingvaluefrominnovation. NY, Wiley, New York, 1998. Citado por SIMÓ, Pep y SALLÁN, José María. Capital Intangible y capital Intelectual: Revisión, definiciones y líneas de investigación. En: Estudios de EconomíaAplicada, Vol. 26, No. 2 (2008); p. 71.

SYALIM, Amril, HORI, Yoshiaki y SAKURAI, Kouichi. Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide, En: International Conference on Availability, Reliability and Security. 2009, p. 726

SYMANTEC CORPORATION. Definición de cibercrimen. [En línea]. [Consultado el 29 de junio de 2012]. Disponible en <http://mx.norton.com/cybercrime/definition.jsp>

SYMANTEC. The wild, wild web: how to ensure 360-degree border security. Symantec, 2010

THOMSON, Kerry-Lynn, VON SOLMS, Rossouw y LOUW, Lynette. Cultivating an organizational information security culture. En: Computer Fraud & Security. Vol. 2006, No. 10 (Oct. 2006); p. 49-50.

TOBAR, Federico. Modelos de Gestión: La encrucijada de la reconversión. En: Énfasis Management. Vol. 5, No. 8 (Ago. 1999); p. 8.

TRKMAN, Peter y DESOUZA, Kevin. Knowledge risks in organizational networks: An exploratory framework. En: The Journal of Strategic Information Systems. Vol. 21, No. 1 (Mar. 2012); p. 5.

VAN NIEKERK, Johan y VON SOLMS, Rossouw. Understanding information security culture: a conceptual framework. En: Proceedings of the ISSA 2006 from Insight to Foresight Conference. (2006).

VERMEULEN, Clive y VON SOLMS, Rossouw. The information security management toolbox: taking the pain out of security management. En: Information Management & Computer Security. Vol. 10, No. 3 (2002); p. 120.

VIEDMA, J. M. In search of an Intellectual Capital comprehensive theory.En: Electronic Journal of Knowledge Management. Vol. 2, No. 5 (2007).CitadoporSIMÓ, Pep y SALLÁN, José María.Capital Intangible y capital Intelectual: Revisión, definiciones y líneas de investigación. En: Estudios de Economía Aplicada. Vol. 26, No.2 (2008); p. 71.

VOLVOK, Dimitry. y GARINA, Tatiana. (2007). Intangible Assets: importance in the knowledge based economy and the role in value creation of a company. En: The Electronic Journal of Knowledge Management. Vol. 5, No. 4 (2007); p. 540

VON SOLMS, Basie. Information security: a multidimensional discipline. En: Computers & Security. Vol. 20, No. 6 (2001); p. 505.

VON SOLMS, Bassie y VON SOLMS, Rossouw. From information security to… business security? En: Computers & Security. Vol. 24, No. 4 (Jun. 2005); p. 271.

VON SOLMS, Bassie y VON SOLMS, Russouw. The 10 deadly sins of information security management. En: Computers & Security. *V*ol. 23, No. 5 (Jul. 2004); p. 372.

VON SOLMS, Bassie. Information Security: the fourth wave. En: Computers & Security. Vol. 25, No. 3 (May. 2006); p. 165.

VON SOLMS, Bassie. Information Security: the third wave? En: Computers & Security. Vol. 19 (2000); p. 616.

VON SOLMS, Bassie. The 5 Waves of Information Security: From Kristian Beckman to the Present. En: 25th IFIP TC-11 International Information Security Conference. (2010); p. 1.

VON SOLMS, Rossouw y VON SOLMS, Bassie. From policies to culture. En: Computers & Security. Vol. 23, No. 4 (Jun. 2004); p. 275-279.

VROOM, Cheryl y VON SOLMS, Rossouw. Towards information security behavioural compliance. En: Computers & Security. Vol. 23, No. 3 (May. 2004); p. 191-198.

WADLOW, Thomas. The process of network security: designing and managing a safe network. Reading: Addison-Wesley Professional, 2000, p. 304

WALLACE, William. La Gestión del Conocimiento. En: Knowledge Management Today. Sevilla, Diciembre 1999. Citado por http://www.a3net.net/es/gescon/definiciones.htm

WARD, Jhon y PEPPARD, Joe. Strategic planning for information systems. 3 ed. Chichester: Wiley Publishing, 2002. Citado por DOHERTY, Neil; ANASTASAKIS, Leonidas y FULFORD, Heather. The information security policy unpacked: a critical study of the content of university policies. En: International Journal of Information Management. Vol. 29, No. 6 (Dic. 2009); p. 449.

WEI, June y LI, Yi. Computer information systems threat analysis on security. En: 2004 IRMA International Conference. 2004.

WEIRICH, Dirk. Persuasive password security. Londres, 2005. Tesis para optar al título de doctor en filosofía. University of London. Department of Computer Science. P. 51,

WHITMAN, Michael E. Enemy at the gate: threats to information security. En: Communications of the ACM. Vol. 46, No. 8 (2003); p. 92.

WHITMAN, Michael y MATTORD, Herbert J. Introduction to information security. En: _____. Principles of information security. 4 ed. Boston: Cengage Learning, 2011, p. 12-14.

WHITMAN, Michael. In defense of the realm: understanding threats to information security. En: International Journal of Information Management. Vol. 24 (2004); p. 51.

WIANT, Terry. Information security policy's impact on reporting security incidents. En: Computers & Security. Vol. 24, No. 6 (Sep. 2005); p. 449.

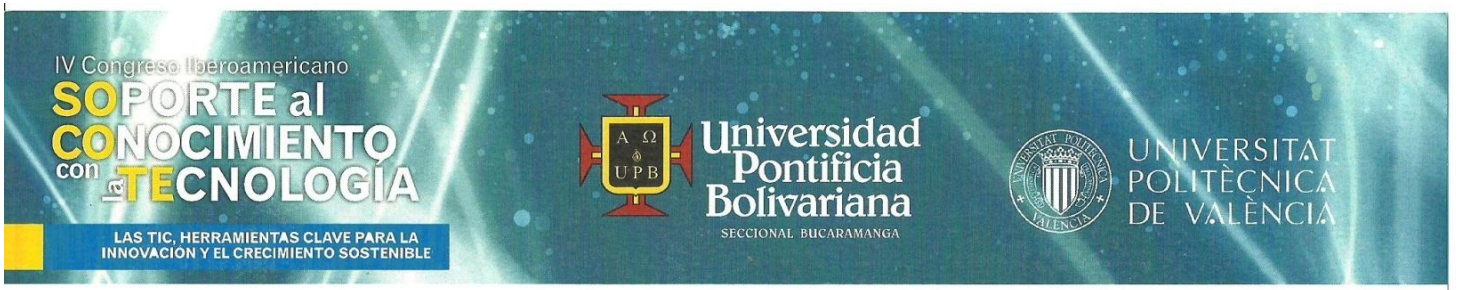
WILBANKS, L. Need to share vs. need to assure. En: IEEE IT Professional. Vol. 10, No. 3 (2008); p. 64.

WILLS M. Personal communication. En: GERBER, Mariana y VON SOLMS, Rossouw. Management of risk in the information age. En: Computers & Security. Vol. 24 (2005); p. 17.

ZAMMUTO, Raymond, et al. Information technology and the changing fabric of organization. En: Organization Science. Vol. 18, No. 5 (Sep. 2007); p. 751.

ZELENY, M. Management support systems: towards integrated knowledge management. En:, Human Systems Management. Vol. 7, No. 1 (1987)

ANEXO 1. CERTIFICADO DE PRESENTACIÓN DE LA PONENCIA



Grupo de I+D Integración de las Tecnologías de la Información en las Organizaciones

EL COMITÉ ORGANIZADOR

Certifica que la Ponencia

A risk level management study for the Intellectual Capital Security: an approximation

ha sido presentada por

LEIDY J. CARDENAS SOLANO

en el IV Congreso Iberoamericano

SOPORTE AL CONOCIMIENTO CON LA TECNOLOGÍA - SOCOTE-

Las TIC, herramientas clave para la innovación y el crecimiento sostenible

Realizado en Bucaramanga los días 4 y 5 de Octubre de 2012
con una intensidad de 16 horas.

MANUEL RODENES ADAM
Presidente Comité Organizador UPV

ALBA SORAYA AGUILAR JIMÉNEZ
Presidente Comité Organizador UPB

Grupo de I+D Integración de las Tecnologías de la Información en las Organizaciones

EL COMITÉ ORGANIZADOR

Certifica que la Ponencia

A risk level management study for the Intellectual Capital Security: an approximation

ha sido presentada por

MARCELA CONTRERAS CRUZ

en el IV Congreso Iberoamericano

SOPORTE AL CONOCIMIENTO CON LA TECNOLOGÍA - SOCOTE-

Las TIC, herramientas clave para la innovación y el crecimiento sostenible

Realizado en Bucaramanga los días 4 y 5 de Octubre de 2012
con una intensidad de 16 horas.

MANUEL RODENES ADAM
Presidente Comité Organizador UPV

ALBA SORAYA AGUILAR JIMÉNEZ
Presidente Comité Organizador UPB

ANEXO 2. HERRAMIENTAS DE BÚSQUEDA Y PROCESAMIENTO DE INFORMACIÓN

BUSCADORES Y METABUSCADORES
(Información no estructurada)

Google

Herramienta:	Meta buscador de información no estructurada
Tipo de Herramienta:	Herramientas de Búsqueda de Información
Interfaz:	Web – Online
Funciones:	Motor de búsqueda de información general y específica. Su alcance permite profundizar en bases especializadas tales como Google Académico, Centros de Noticias, Libros, Mapas, entre otros. Su última actualización plantea la intención de incorporar algoritmos semánticos a su motor de búsqueda.
Página Web:	www.google.com

PLATAFORMAS DE BUSQUEDA CIENTÍFICA Y TECNOLÓGICA
(Información Estructurada)

ISI Web of Knowledge (Thomson)

Compañía:	The Thomson Corporation
Herramienta:	Buscador de información científica estructurada
Producto:	Web of Science
Tipo de Herramienta:	Plataformas Integradas de Información vía Web
Características:	Plataforma integrada accesible vía Web y diseñada para brindar apoyo a todos los niveles de investigación científica y académica. En la actualidad cubre: 1. Más de 22.000 revistas 2. 23 millones de patentes 3. 192.000 conferencias 4. 5.500 Sitios Web 5. 5.000 libros 6. 2 millones de estructuras químicas, etc. Entre sus principales productos se destaca ISI Web of Science que accede a los índices de citaciones en Ciencias (6126 revistas incluidas), Ciencias Sociales (1802 revistas incluidas), Artes y Humanidades (1136 revistas incluidas)
Interfaz:	Plataforma Web con Acceso Restringido.

Funciones:	Combina contenidos de calidad evaluados con herramientas diversas herramientas que permiten usar, analizar y gestionar dichos contenidos.
Página Web:	http://portal.isiknowledge.com/

SCOPUS

Compañía:	Elsevier B.V.
Herramienta:	Buscador de información científica estructurada
Tipo de Herramienta:	Plataformas Integradas de Información vía Web
Características:	Base de Datos de citaciones y abstract con más de: 1. 15.000 revisiones 2. 125 colecciones de libros 3. 700 relaciones de conferencias 4. 500 accesos a publicaciones abiertas 5. 29 millones de registros de abstract 6. 265 millones de referencias agregadas a todos los abstract. 7. Incluye más de 265 millones de fuentes confiables en Internet 8. 18 millones de patentes.
Interfaz:	Web – On line. Acceso Restrictivo.
Funciones:	Combina contenidos de calidad evaluados con herramientas diversas herramientas que permiten usar, analizar y gestionar dichos contenidos.
Página Web:	www.scopus.com

Science Direct

Compañía:	Elsevier B.V.
Herramienta:	Buscador de información científica estructurada
Tipo de Herramienta:	Plataformas Integradas de Información vía Web
Características:	Base de datos de texto completo que ofrece artículos de revistas y capítulos de libros. En la actualidad cubre: 1. Más de 2500 revistas revisadas por pares 2. Más de 11.000 libros 3. Más de 11 millones de artículos o capítulos 4. Crece a un ritmo de casi 0,5 millones de adiciones por año 5. 25 expertos están brindando soporte técnico las 24 horas
Interfaz:	Plataforma Web con Acceso Restringido.
Funciones:	La plataforma ofrece una sofisticada búsqueda avanzada y la funcionalidad de recuperación que permite al usuario aprovechar al máximo la eficacia de su proceso de descubrimiento de conocimiento.

Página Web:	www.sciencedirect.com

Ebsco Host

Compañía:	EBSCO Industries
Herramienta:	Buscador de información científica estructurada
Tipo de Herramienta:	Plataformas Integradas de Información vía Web
Características:	EBSCOhost es un poderoso sistema de referencia en línea a través de Internet. Ofrece una variedad de bases de datos de texto completo y bases de datos populares de los principales proveedores de información. Las bases de datos completas van desde las colecciones de referencia generales hasta las bases de datos diseñadas especialmente, sobre temas específicos para bibliotecas públicas, académicas, médicas, empresariales y universiades.
Interfaz:	Plataforma Web con Acceso Restringido.
Página Web:	http://search.ebscohost.com

ProQuest

Compañía:	ProQuest
Herramienta:	Buscador de información científica estructurada
Tipo de Herramienta:	Plataformas Integradas de Información vía Web
Características:	Es la aplicación de búsqueda de bases de datos que diseñó ProQuest (la empresa) para llevar a cabo su misión de conectar a personas e información, y caminar hacia su visión de futuro de ser una empresa clave en materia de investigación en todo el planeta. 1. Áreas temáticas: Artes, economía y negocios, salud y medicina, historia, literatura e idiomas, ciencia y tecnología, ciencias sociales. 2. Tipos de fuentes: Periódicos, tesis doctorales y tesinas (ProQuest es el archivo oficial de tesis de la Biblioteca del Congreso de los Estados Unidos), revistas científicas, emisiones de televisión y radio, agencias de noticias y comunicados de prensa, instantáneas e informes anuales de empresas, libros, archivos y documentos gubernamentales, mapas.
Interfaz:	Plataforma Web con Acceso Restringido.
Página Web:	http://search.proquest.com

Springerlink

Compañía:	Springer Science+Business Media
Herramienta:	Buscador de información científica estructurada
Tipo de Herramienta:	Plataformas Integradas de Información vía Web
Características:	SpringerLink es una de las principales bases de datos interactivas del mundo en los campos de las ciencias, la técnica, la medicina y la recopilación de archivos en línea. Contiene 1.300 títulos de revistas electrónicas del alto impacto en texto completo con cobertura desde 1997 hasta la fecha y aproximadamente 9.300 títulos de libros electrónicos de 13 colecciones en todas las áreas científicas desde el año 2005 con derecho completo y perpetuo de la propiedad de estos libros.
Interfaz:	Plataforma Web con Acceso Restringido.
Página Web:	http://www.springerlink.com

HERRAMIENTAS DE APLICACIÓN Y TRATAMIENTO DE INFORMACIÓN

Microsoft Excel ®

Compañía:	Microsoft
Herramienta:	Procesamiento de información.
Interfaz:	Aplicación PC
Utilidad para el Informe:	Procesamiento de datos alfanuméricos, graficas resultados sobre probabilidad e impacto de los riesgos, nivel de efectividad de controles, etc.

MIC MAC ®

Compañía:	Laboratorio de Investigación en Prospectiva, Estrategia y Organización LIPSOR
Herramienta:	Procesamiento de información
Interfaz:	Aplicación PC
Funciones:	El programa micmac tiene por objeto ayudar en un estudio micmac de análisis estructural. Permite, a partir de una lista de variables estructurales y una matriz que representa las influencias directas entre las variables, extraer e identificar las variables claves del problema estudiado, con la ayuda de cuadros y gráficos que permiten la modelización del problema a abordar.

Utilidad para el informe:	Procesamiento de la matriz de impactos cruzados para generar las MID, MII, MIDP, MIIP y sus respectivos gráficos de influencias/dependencias, necesarios para el análisis estructural

SPSS ®

Compañía:	IBM
Herramienta:	Procesamiento de información
Interfaz:	Aplicación PC
Funciones:	SPSS es un sistema global para el análisis de datos. Puede adquirir datos de casi cualquier tipo de archivo y utilizarlos para generar informes tabulares, gráficos y diagramas de distribuciones y tendencias, estadísticos descriptivos y análisis estadísticos complejos.
Utilidad para el informe:	Procesamiento de datos alfanuméricos, creación de informes y gráficos de estadísticos descriptivos.

ANEXO 3. CLASIFICACIÓN DE PALABRAS CLAVES PARA FRAMEWORK

Buenas prácticas	Políticas	Gestión de Riesgos	Recursos humanos	Gestión del Conocimiento	Governanza	Sistemas de Información y redes	Economía	Incidentes de Seguridad
Balanced scorecard	Information Security Policies	Asset classification	Awareness	Customer capital	Corporate governance	Computer networks	Cost of security	Computer Crime
Best practices	Information Security Policy	Asset identification	Behavioral issues of information security	Human capital	Evaluation model	Hacker learning	Cost sharing	Data Security
BS 7799	Internet Use Policy	Business impact analysis	Behavioral operations management	Intellectual assets	Framework	ICT security tools	Economics of IS	Disclosures
Business practice.	IS security policies	Business information risk	Behavior	Knowledge	Governance	ICTs	Experimental economics	Downtime Loss
Certification	National information security policy	Controls	Corporate culture	Knowledge creation	Information security governance	Information and communication technologies	Information security economics	Event Studies
Compliance	Optimal policy	Countermeasures	Employee perspectives	Knowledge management	Information technology governance	Information systems	Market value	Information Leakage
Conformity Assessment Procedure	Policy	Information assets	Employees' compliance with security policies	Knowledge management capability	IT governance	Information systems outsourcing	Optimal security investment	Insider Trading
Guidelines	Policy Content	Information security risk	End-user security	Knowledge security	Management frameworks	Information systems security	Technology investment	Missing Data
Information security certification	Power And Politics	Information security risk analysis	Information Security Awareness	Knowledge sharing	Management levels	Information systems security management	Transaction cost economics	Nonmalicious Security Violation
Information security compliance	Security Policy	Information security risk management	Information security culture	Knowledge transfer	Reference model	Information systems services	Business administration/ economics	Organizational Effectiveness
Information security management system	Security Policy Adoption	Information security threats	Information Security Culture	Practice perspective of knowledge	Organization	Information technology capabilities		Security Breaches
Information security requirements	Security Policy Implementation	Information security vulnerabilities	IS security training	Structural perspective of knowledge	Business process analysis	Information technology security		Security Shocks
Information systems security	Technology policy	Information systems risk	Online protection behavior	Structure capital		Internet		

Buenas prácticas	Políticas	Gestión de Riesgos	Recursos humanos	Gestión del Conocimiento	Governanza	Sistemas de Información y redes	Economía	Incidentes de Seguridad
standards								
Institutionalization		Information systems risk management	Organizational behavior			Internet misuse		
International standards		IS threats	Organizational culture			Intrusion detection		
ISO 17799		Paper-based risk analysis	Participation			Network effects		
ISO 27001		Perceived security risk	Security awareness			Network security		
ISO/IEC 27001:2005		Quantitative risk analysis	Security behavior			Networks		
ISO/IEC 27002:2005		Risk	Security culture			Organizational networks		
Legal requirements		Risk Analysis	Security education			Patch management		
Measurements		Risk Assessment	User participation			Pensamiento sistémico		
Metrics		Risk Level	Users			Virtual organizations		
Performance measures		Risk Management				Virtual work		
Quality control		Risk Model				Virus		
Regulation		Risk Reduction				Web misuse		
Security compliance		Security Risk Management						
Security management code of practice		Security Risks						
Standard		Security threats						
Work practice		Survey						
Workgroup norms		Threat mitigation						
		Value-at-risk (VaR)						
		Violations						
		Vulnerabilities						

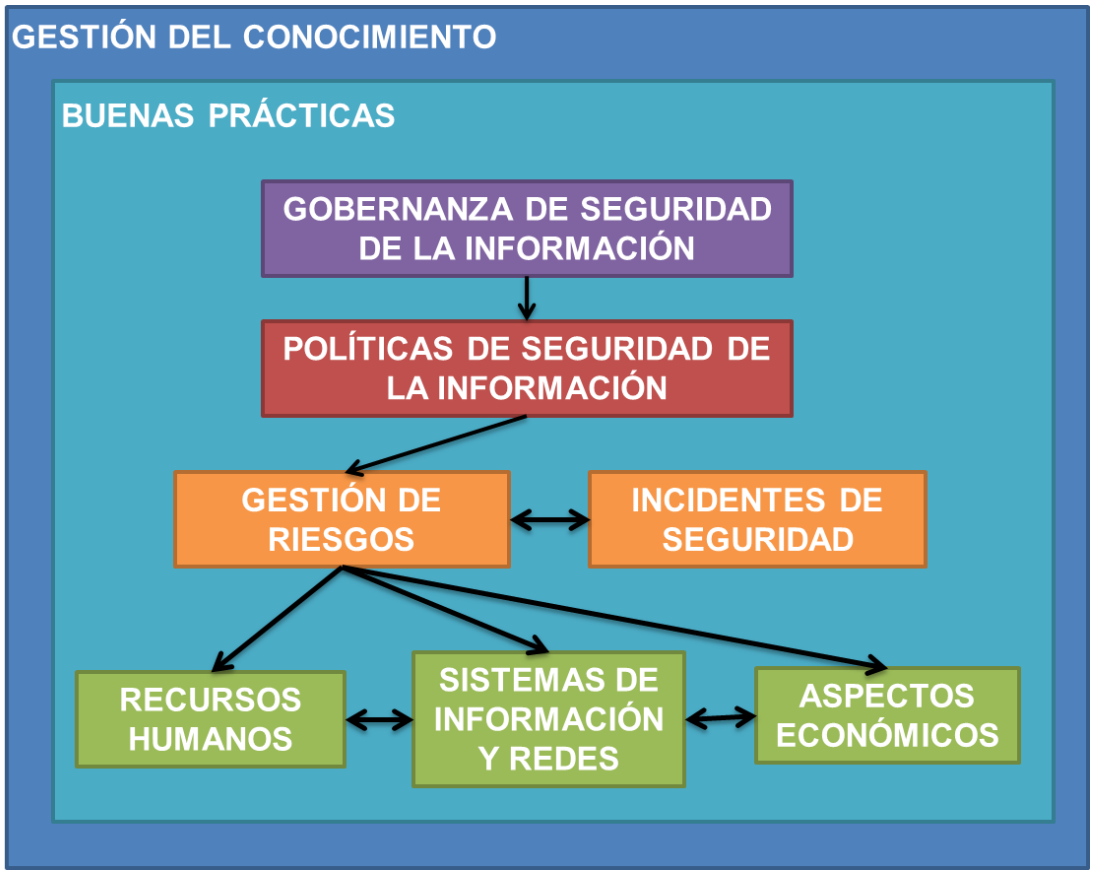
ANEXO 4. FRAMEWORK

Como principal resultado de la revisión de literatura realizada, se desarrollo un marco de trabajo, en el cual se agruparon las temáticas tratadas en las publicaciones en nueve categorías relacionadas entre sí como se muestra en la Figura 28. En esta, el elemento de mayor nivel jerárquico es la gobernanza de seguridad de la información, en donde se toman las decisiones de carácter estratégico que afectan directamente el desarrollo de políticas. Es normal que exista una política general de seguridad de la información, y a partir de ella se pueden desencadenar políticas específicas para distintas áreas de la organización. En la política, también se establecen lineamientos sobre cómo, cuándo y quién lleva a cabo la evaluación y tratamiento de riesgos, actividades que constituyen la gestión de riesgos. Esta última es alimentada por los incidentes de seguridad que brindan alertas sobre riesgos no identificados o no controlados.

Como base de todas las actividades realizadas, se encuentran siempre los estándares, lineamientos o guías de buenas prácticas, los cuales permiten a las organizaciones conocer los requisitos mínimos para gestionar la seguridad de la información.

Finalmente como tema transversal se encuentra la gestión del conocimiento, ya que cualquier esfuerzo realizado en la organización se convierte en conocimiento y experiencia que debe ser apropiado por los individuos. Asimismo, no solo la información debe ser protegida sino también el conocimiento existente en las personas, es allí donde surgen nuevos riesgos que deben evaluarse y tratarse.

Figura 28. Marco de trabajo de seguridad de la información



Fuente. Autores del proyecto.

1. Gestión del conocimiento

Actualmente el interés por este campo sigue creciendo a un ritmo asombroso, aunque son escasos los estudios cómo proteger los activos basados en conocimiento[232]; por tanto, existe un gran interés en el diseño y desarrollo de marcos de trabajo (frameworks) de gestión de seguridad de la información[233], que proporcionen una guía en la protección de la información y conocimiento generado, gestionado y transferido en las organizaciones. En la Tabla 27, se

[232] DESOUZA, Kevin y VANAPALLI, Ganesh. Securing knowledge in organizations: lessons from the defense and intelligence sectors.En: International Journal of Information Management. Vol. 25, No. 1 (Feb. 2005); p. 85.
[233] NNOLIM, Op. cit., p. 13.

presenta un marco comparativo de los diferentes tipos de framework que se encuentran en la literatura de seguridad de la información.

A pesar de que existen muchas metodologías para evaluar los riesgos de seguridad asociados con las fugas, modificación no autorizada y la interrupción de la información utilizada por las organizaciones, Shedden et al.[234] y Shedden y Smith[235] argumenta que estos métodos tienen una orientación técnica hacia la identificación y evaluación de los activos de información. Esto opaca los principales riesgos asociados con el desarrollo y la utilización del conocimiento organizativo. Por lo cual es preciso explorar los métodos de evaluación de riesgos de seguridad de una manera más efectiva para identificar y tratar los conocimientos asociados a los procesos de negocio.

[234]SHEDDEN, Piya et al. Incorporating a knowledge perspective into security risk assessments. En: Vine. Vol. 41, No. 2 (2011); p. 152.
[235]SHEDDEN, Piya, SMITH, Wally y AHMAD, Atif. Information security risk assessment: towards a business practice perspective. En: 8th Australian Information Security Management Conference. (Nov. 2010); p. 119.

Tabla 27. Frameworks de seguridad de la información

Tipo	Descripción	Componentes	Autores
Gestión de riesgos	Con base en las relaciones entre activo, amenaza y vulnerabilidad, proponen la relación de objetivos para TOE (Target de evaluación) y los requerimientos funcionales de seguridad. Los requisitos funcionales de seguridad y los requisitos de aseguramiento de seguridad pueden proporcionar las protecciones adecuadas para la vulnerabilidad y la amenaza del Sistema de Gestión de Seguridad de la Información - SGSI.	- Amenazas - Políticas de seguridad organizativas - Activos **Objetivos de seguridad:** - Para el target de evaluación - Para el entorno - Para el entorno operacional **Requerimientos de seguridad:** - Funcionales - De aseguramiento - De controles	Farn, Lin y Fung[236]
Gestión de riesgos	Sirve para poner un poco de la estructura en un área intrínsecamente no estructurada de la gestión de riesgos de conocimiento. Los administradores pueden utilizar el marco de trabajo como un dispositivo guía en la identificación de los principales tipos de riesgo que enfrenta su organización, y los posibles efectos perjudiciales de esos riesgos.	**Naturaleza de colaboración:** - Simétrica y asimétrica Naturaleza de la red: - Funcional, ágil, cobertura de riesgo, innovadora **Proximidad:** - Próximo y no próximo **Tipo de acción:** - Deliberada de la compañía, deliberada del individuo y no deliberada **Rango de riesgo:** - Unitario, dúo, red	Trkman y Desouza[237]

[236]FARN, Kwo-Jean, LIN, Shu-Kuo y FUNG, Andrew Ren-Wei. A study on information security management system evaluation: assents, threat and vulnerability. En: Computer Standards & Interfaces. Vol. 26, No. 6 (2004); p. 509.
[237] TRKMAN, Peter y DESOUZA, Kevin. Knowledge risks in organizational networks: An exploratory framework. En: The Journal of Strategic Information Systems. Vol. 21, No. 1 (Mar. 2012); p. 5.

Tabla 27. (Continuación)

Tipo	Descripción	Componentes	Autores
Cultura de seguridad de la información	El efecto global de la cultura de seguridad de la información de una organización puede ser vista como una acumulación de los efectos de cada uno de los niveles subyacentes de la cultura. Cada uno de estos niveles puede influenciar positiva o negativamente la cultura de seguridad de la información en general.	**Niveles de la cultura de seguridad de la información** - Línea base de mínimo aceptable - Nivel de seguridad neto - Artefactos - Valores adoptados - Supuestos tácitos compartidos - Conocimiento sobre seguridad de la información	van Niekerek y von Solms[238]
Cultura de seguridad de la información	Busca asistir a las organizaciones en la implementación de componentes de seguridad de la información de manera que puedan direccionar positivamente el comportamiento de los empleados hacia la protección de los activos de información	**Nivel organizativo:** - Componente estratégico - Componente de evaluación de riesgo - Política y procedimientos - Buenas prácticas **Nivel grupal:** - Componente de protección y operaciones de tecnología - Educación y capacitación - Confianza **Nivel individual:** - Concientización	Da Veiga y Eloff[239]

[238] VAN NIEKERK, Johan y VON SOLMS, Rossouw. Understanding information security culture: a conceptual framework. En: Proceedings of the ISSA 2006 from Insight to Foresight Conference. (2006).
[239] DA VEIGA, A. y ELOFF, J.H.P. A framework and assessment instrument for information security culture.En: Computers & Security. Vol. 29, No. 2 (2010); p. 203.

Tabla 27. (Continuación)

Tipo	Descripción	Componentes	Autores
Gestión de la seguridad de la información	Los autores utilizan un marco de trabajo de balancedscorecard (BSC) para establecer el índice de rendimiento para la gestión de la seguridad de la información en las organizaciones. Además, el BSC se utiliza para fortalecer el vínculo entre los indicadores de desempeño fundamentales y la estrategia de negocio. El mapa estratégico se construye con 12 objetivos estratégicos y 35 indicadores clave de rendimiento.	**Financiera:** **-** Reducción de pérdidas - Promover claridad **Cliente:** **-** Fortalecer transacción de seguridad - Respetar satisfacción externa **Procesos internos:** - Políticas integras - Disminución de ilegalidad - Mejorar habilidades del sistema - Cumplimiento de directrices **Aprendizaje y crecimiento:** **-** Custodia mejorada - Aumento de entrenamiento - Sostenibilidad fuerte - Recursos suficientes	Huang, Lee y Kao[240]
Gestión de la seguridad de la información	Puede ser utilizado como modelo para la documentación de la representación arquitectónica de la gestión de seguridad en la empresa. Las filas representan varios puntos de vista de la gestión de seguridad de la información, y las columnas representan varios elementos para cada punto de vista	**Stakeholder:** - Junta directiva - Estratega - Auditor - Profesional de seguridad - Arquitecto de información - Usuario (líder unidad de negocio) - Usuario (empleado) - Operaciones (Manager de TI)	Nnolim[241]

[240]HUANG, Shi-Ming, LEE, Chia-Ling y KAO, Ai-Chin. Balancing performance measures for information security management: a balanced scorecard framework. En: Industrial Management & Data Systems. Vol. 106, No. 2 (2006); p. 255.
[241] NNOLIM, Op. cit., p. 163.

Tabla 27. (Continuación)

Tipo	Descripción	Componentes	Autores
Gestión de la seguridad de la información	Según los autores, la seguridad efectiva se logra holísticamente a través de la aplicación de múltiples mecanismos de alineación social y organizativa combinados con competencia en tecnología. Este marco de trabajo provee una base para desarrollar prácticas de seguridad más detalladas, y finalmente procedimientos detallados de operación.	**Mecanismos de gestión de riesgo:** - Integración organizativa - Alineación social - Competencia técnica **Objetivos para la estrategia** - Balance entre la seguridad y las necesidades del negocio - Aseguramiento del cumplimiento - Mantenimiento de la cultura	Kayworth y Whitten[242]
Gobernanza de seguridad de la información	Los dos lados de la gobernanza de seguridad de la información son elementos esenciales que contribuyen a una estrategia eficaz para hacer frente a los riesgos empresariales de información a nivel de gobierno corporativo. El lado de gobernanza involucra a la dirección ejecutiva y la Junta. El lado de gestión se preocupa por la manera en que la estrategia de seguridad de la información se implementa y administra.	**El lado de gobernanza:** - Visión - Estrategia - Misión **El lado de gestión:** - Política	Posthumus y von Solms[243]

Fuente: Autores del proyecto a partir de los autores mencionados

[242] KAYWORTH, Tim y WHITTEN, Dwayne. Effective information security requires a balance of social and technology factors. En: MIS Quarterly Executive. Vol. 9, No. 3 (Sep. 2010); p. 166.
[243]POSTHUMUS, Shaun y VON SOLMS, Rossouw.A framework for the governance of information security.En: Computers & Security. Vol. 23 (2004); p. 644.

2. Gestión de riesgos

Gerber y von Solms[244] proponen adoptar un enfoque alternativo al análisis de riesgos tradicional, en el cual se analicen no solamente los riesgos de los activos tangibles, sino también los riesgos de los intangibles como la información; además, consideran relevantes los riesgos causados por asuntos culturales, legislativos, sociológicos, entre otros.

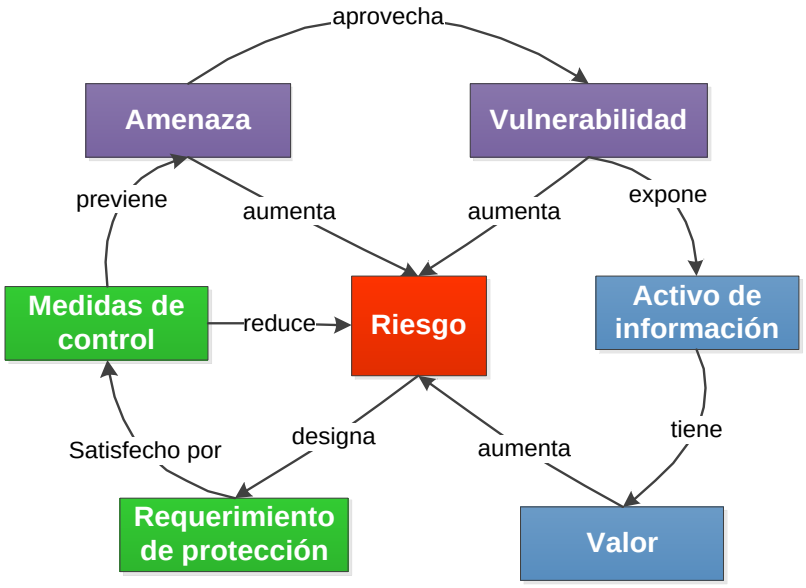
Asimismo, Lategan y von Solms[245], enfatizan en que las empresas hoy en día deben asegurar que los riesgos sean gestionados holísticamente y que la terminología y prácticas de riesgo relacionadas con TICs estén congruentemente alineadas con la terminología y prácticas de la empresa. Es decir, las TICs no pueden ser vistas como un componente independiente en cuanto a la gestión de riesgos se refiere.

De acuerdo con Layton[246], un **riesgo** está constituido por la probabilidad, impacto y consecuencia de eventos negativos que la organización debe considerar como parte de sus operaciones; mientras que una **vulnerabilidad** consiste en un defecto o debilidad en un sistema de información, procedimiento asociado, o **control** existente que tiene el potencial de ser ejercido (accidental o intencionalmente) y resultar en un incumplimiento o violación de la política de seguridad de la información. Por ende, las vulnerabilidades no tienen ningún impacto si una amenaza en cuestión no está presente. Por otra parte, la **amenaza** se refiere a un posible peligro del sistema o atacante que aprovecha las debilidades (vulnerabilidades del sistema). En la Figura 29, se observan las múltiples relaciones existentes entre los conceptos anteriores.

---

[244] GERBER, Mariana y VON SOLMS, Rossouw. Management of risk in the information age.En: Computers & Security. Vol. 24, No. 1 (Ene. 2005); p. 28.
[245] LATEGAN, Neil y VON SOLMS, Rossouw. Towards enterprise information risk management: a body analogy. En: Computer Fraud & Security. Vol. 2006, No. 12 (Dic. 2006); p. 17
[246] LAYTON, Op. cit., p. 7.

Figura 29. Relaciones entre los componentesdel riesgo



Fuente. Autores del proyecto. Adaptado de FARN, Kwo-Jean, LIN, Shu-Kuo y FUNG, Andrew Ren-Wei. A study on information security management system evaluation: assents, threat and vulnerability. En: Computer Standards& Interfaces. Vol. 26, No. 6 (2004); p. 507.

En este sentido, como uno de los primeros pasos en la implantación de un protocolo de seguridad de la información, se debe llevar a cabo una evaluación del riesgo (en inglés risk assessment), el cual consiste en el proceso de identificar los riesgos de seguridad de un sistema y determinar su probabilidad de ocurrencia, su impacto, y los mecanismos que mitiguen ese impacto[247].

Según la US General Accounting Office[248], la mayoría de las metodologías de evaluación de riesgos utilizadas incluyen los siguientes elementos básicos:

[247]SYALIM, Amril, HORI, Yoshiaki y SAKURAI, Kouichi. Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide, En: International Conference on Availability, Reliability and Security.2009, p. 726.
[248] ESTADOS UNIDOS. US GENERAL ACCOUNTING OFFICE. Information Security Risk Assessment: Practices of Leading Organizations. 1999, p. 6-7.

- Identificación de las amenazas.
- Estimación de la probabilidad de que dichas amenazas ocurran.
- Identificación y valoración de los activos que podrían estar en riesgo.
- Cuantificación del impacto.
- Recomendación de controles: Identificar las acciones costo-efectivas que podrían mitigar el riesgo.
- Determinación del riesgo: es el resultado de combinar la probabilidad de ocurrencia y el impacto de la amenaza, junto con la vulnerabilidad existente.
- Documentación de los resultados y elaboración de un plan de acción.

En particular, existen diferentes metodologías de evaluación del riesgo, entre las cuales se encuentran:

2.1. Magerit

Es una metodología abierta para análisis y gestión del riesgo, desarrollada por el Ministerio Español de Administración Pública, ofrecida como un marco de trabajo y guía para la Administración Pública. Dada su naturaleza abierta, también es usado fuera de la Administración[249].

Desde que Magerit fue publicada por primera vez en 1997, el análisis de riesgo ha sido consolidado como un paso necesario para la gestión de la seguridad, claramente reconocida en las directrices de la OECD[250].

Esta metodología es de interés para cualquiera que trabaje con información estructurada y sistemas de computación. Si esta información, o los servicios que

[249]ENISA - Agencia Europea de Seguridad de las Redes y de la Información (n.d). RiskManagement - RiskAssessmentMethods: Magerit. [en línea]. [Consultado el 10 de Octubre de 2011]. Disponible en: <http://rm-inv.enisa.europa.eu/methods_tools/m_magerit.html>

[250] La Organización para la Cooperación y el Desarrollo Económico es una organización de cooperación internacional, compuesta por 34 países (entre ellos Chile y México), cuyo objetivo es coordinar sus políticas económicas y sociales. Sitio web: http://www.oecd.org/about

son provistos a través de ella, son de valor, esta metodología permitirá conocer que tanto de ese valor está en riesgo y ayudará a protegerlo.

2.2. Operationally Critical Threat, Asset, and Vulnerability Evaluation

Desarrollada por el Carnegie Mellon Software Engineering Institute[251], consiste en una serie de herramientas, técnicas, y métodos para el proceso de planeación estratégica y evaluación basada en riesgos de seguridad de la información, los cuales se caracterizan por ser[252]:

- *A*uto-dirigidos*,* pequeños equipos de personal de la organización a través de unidades de negocio y de TI trabajan juntos para hacer frente a las necesidades de seguridad de la organización.
- *Flexible, cada* método se puede adaptar al entorno único de riesgo de la organización*,* objetivos de seguridad, y el nivel de habilidad*.*
- *E*volucionado, OCTAVE trasladó a la organización hacia una visión *de seguridad* basada en el riesgo operacional y se dirige hacia la tecnología en un contexto empresarial*.*

2.3. Global Information Security Assessment Methodology

Este tipo de evaluación tiene como propósito cuantificar y calificar los riesgos de seguridad de la información de manera holística a nivel organizacional. GISAM aprovecha los dos tipos de evaluación (cuantitativa y cualitativa) dentro de la metodología y se considera que es un tipo de modo mixto de evaluación, razones por las que será la metodología a utilizar en el presente proyecto.

---

[251] El Carnegie Mellon Software EngineeringInstitute es un centro de investigación y desarrollo financiado con fondos federales. Sitio web: http://www.sei.cmu.edu

[252] Características y ventajas de OCTAVE. [en línea]. [consultado el 10 de agosto de 2011] Disponible en: <http://www.cert.org/octave/>

Este tipo de evaluación brinda una perspectiva integral de seguridad de la información a nivel institucional, ya que considera los aspectos operativos y de gestión de seguridad de la información, así como la aplicación y uso de la tecnología. Además, es muy escalable ya que se puede aplicar tanto en pequeñas empresas como en organizaciones mundiales.

Según Layton[253], la metodología contempla los siguientes componentes del análisis y evaluación de riesgo:

- **Determinación de los activos dentro del alcance.** Estos pueden provenir de diferentes fuentes de información dentro de la organización y pueden encontrarse en diferentes soportes como papel o medios digitales.
- **Identificación de amenazas.** Durante el proceso de evaluación de riesgos, es crítico identificar las amenazas que podrían potencialmente dañar o afectar de manera adversa las operaciones y/o activos críticos de la organización. Dichas amenazas pueden ser clasificadas así: Humanas maliciosas, humanas no maliciosas, accidentales, y otras.
- **Caracterización de las amenazas.** Las amenazas pueden cuantificarse a partir de los siguientes atributos, a los cuales se les asigna un valor numérico específico.
    - Probabilidad de ocurrencia.
    - Impacto: consiste en realizar una estimación de las pérdidas o daños potenciales que podría causar la amenaza.
    - Velocidad (o tiempo) de ocurrencia
    - Nivel de efectividad de los controles existentes.
- **Identificación de vulnerabilidades.** Existen múltiples vulnerabilidades que puedan ser aprovechadas por las amenazas. El objetivo de este paso es desarrollar una lista de las vulnerabilidades de la organización (defectos o puntos débiles) que podría ser explotada por las amenazas potenciales.

[253] LAYTON, Op, cit., p. 23 – 40.

- **Análisis de controles.** Consiste en analizar los controles que se han implementado, o están previstos para su aplicación, por la organización para minimizar o eliminar la probabilidad de que una amenaza actúe sobre una vulnerabilidad de la organización.
- **Determinación de la probabilidad de ocurrencia.** La probabilidad de ocurrencia es un componente importante de la evaluación de riesgos, ya que proporciona a los tomadores de decisiones información crítica sobre la probabilidad de que un acontecimiento negativo ocurra. La calificación de probabilidad para cada control debe considerar las amenazas y las vulnerabilidades pertinentes y el nivel de eficacia de los controles.
- **Análisis de impactos.** Consiste en determinar el impacto adverso para la organización, como resultado de la explotación por parte de una amenaza de una determinada vulnerabilidad.
- **Determinación del riesgo.** Con el fin de evaluar el nivel de riesgo de la organización, se desarrolla una matriz de nivel de riesgo que correlacione la probabilidad de ocurrencia, el impacto y el nivel de efectividad del control actual. Los posibles niveles de riesgo para una organización son: leve, vigilado, moderado, alto y crítico.

3. Incidentes de seguridad

En comparación con otras áreas del framework, los incidentes de seguridad son poco mencionados en la literatura, y en su mayoría corresponden a aspectos técnicos de seguridad como violaciones a los sistemas de información y redes[254].

Como objetivo general, los autores que han tratado el tema, se han enfocado en mejorar el entendimiento de las amenazas a la seguridad de la información a fin

[254]KRAEMER, S., CARAYON, P. y CLEM, J.F. Characterizing violations in computer and information security systems.En: Proceedings of the 16th Triennial World Congress of the International Ergonomics Association (IEA). 2006.

de que los profesionales en el área puedan tomar mejores decisiones sobre cómo hacer frente a estas amenazas[255] [256] [257]. Algunos tipos de incidentes (o brechas) de seguridad de la información incluyen:

- Negación del servicio: El atacante envía un gran número de solicitudes de información a los servidores web de la compañía con el propósito de sobrecargarlos y hacer que no estén disponibles para uso legítimo. Su impacto es importante para compañías que dependen de su presencia en la web para generar ingreso. Sin embargo, raramente resultan en pérdida de información confidencial.
- Acceso desautorizado a información de clientes: En estos ataques, individuos desautorizados obtienen acceso a datos de los clientes. Estos ataques son en su mayoría considerados como violación de la confidencialidad y puede tener efectos negativos sobre la lealtad del cliente, independientemente del tipo de negocio o la pertenencia a la industria.
- Acceso desautorizado a información de empleados: Es similar al anterior; sin embargo, usualmente la escala de estos ataques es menor. Es decir, el número de empleados afectados es considerablemente menor que el de miles de clientes afectados por un acceso desautorizado.
- Alteración del sitio web: El atacante obtiene acceso a los servidores web de la compañía, y, altera su contenido con un mensaje, logo o material inapropiado, o eliminando todos los archivos, ocasionando el cierre completo del sitio web.
- Acceso desautorizado a información de la compañía: La información de la compañía puede ser un nuevo diseño de producto, un código fuente de un sistema operativo, la porción de una película que aún no ha sido estrenada, documentos de una adquisición de la compañía, etc. Dependiendo de la

[255] Ibid.
[256] WEI, June y LI, Yi. Computer information systems threat analysis on security. En: 2004 IRMA International Conference. 2004, p. 952.
[257] GOODALL, John, LUTTERS, Wayne y KOMLODI, Anita. Developing expertise for network intrusion detection. En: Information Technology & People. Vol. 22, No. 2 (2009); p. 7.

sensibilidad de la información, estas brechas de seguridad pueden afectar significativamente la ventaja competitiva de una empresa y, por consecuente, su existencia.

En cuanto a las causas que originan los incidentes de seguridad en las organizaciones. Beautement y Sasse[258] afirman que un gran número de incidentes ocurren como resultado de los fracasos de los empleados para cumplir con las políticas de seguridad. La causa más común son los errores no intencionales; pero, existe evidencia de que en algunos casos los empleados eligen no esforzarse por cumplir con las tareas de gestión de seguridad. Al indagar sobre las razones de este no cumplimiento, la mayoría lo justifica con el impacto que estas medidas tienen en la productividad personal y organizativa, la percepción de ausencia de riesgo y el hecho de que otros compañeros de trabajo tampoco las cumplan[259][260].

4. Sistemas de información y redes

Dentro de la investigación sobre seguridad de la información, los sistemas de información y las redes de telecomunicaciones hacen parte del común denominador en los análisis de riesgos. Son estos los principales objetivos de los ataques por parte de los criminales informáticos.

5. Recursos humanos

El rol de las personas es vital para el éxito de cualquier organización, sin embargo estas constituyen el eslabón más débil cuando se habla de seguridad de la

[258] BEAUTEMENT, Adam y SASSE, Angela. The economics of user effort in information security.En: Computer Fraud & Security. Vol. 2009, No. 10 (2009); p. 8
[259] WEIRICH, Dirk. Persuasive password security.Londres, 2005.Tesis para optar al título de doctor en filosofía. University of London.Department of Computer Science.p. 51.
[260] BEAUTEMENT, Adam, et al. Modelling human and technological costs and benefits of USB memory stick security. En: Workshop on economics in information security 2008. (2008); p. 1.

información[261] [262]. Esto explica porque gran parte de la literatura se ha dedicado a temáticas relacionadas con el comportamiento de los usuarios de la información. Thomson, von Solms y Louw[263], enfatizan que los empleados pueden volverse conscientes y estar entrenados en las habilidades correctas necesarias para proteger los activos de información, y estas habilidades pueden convertirse en parte de las prácticas diarias de los empleados.

Varios autores confirman la importancia de convertir las políticas de seguridad de la información en comportamientos cotidianos de los empleados, es decir, trabajar en la construcción de una cultura organizativa de seguridad de la información[264][265]. Además, la necesidad de cambiar el enfoque en tecnología por un enfoque en las personas[266] [267]. De los diferentes enfoques del cumplimiento de políticas de seguridad de la información, la formación es el más comúnmente sugerido en la literatura[268] [269].

Otro aspecto que se ha profundizado, es la relación entre la cultura de seguridad de la información y la cultura corporativa, resaltando que estas dos deberían estar alineadas y como se influencian mutuamente[270] [271].

---

[261]VROOM, Cheryl y VON SOLMS, Rossouw.Towards information security behaviouralcompliance.En: Computers & Security. Vol. 23, No. 3 (May. 2004); p. 193.
[262]BULGURCU, Burcu, CAVUSOGLU, Hasan y BENBASAT, Izak. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. En: Mis Quarterly. Vol. 34, No. 3 (Sep. 2010); p. 523.
[263]THOMSON, Kerry-Lynn, VON SOLMS, Rossouw y LOUW, Lynette.Cultivating an organizational information security culture.En: Computer Fraud & Security. Vol. 2006, No. 10 (Oct. 2006); p. 7.
[264] VON SOLMS, Rossouw y VON SOLMS, Bassie. From policies to culture.En: Computers & Security. Vol. 23, No. 4 (Jun. 2004); p. 279.
[265] VON SOLMS (2000), Op. cit., p. 618.
[266]KAYWORTH y WHITTEN. Op. cit., p. 164.
[267] JOHNSON, M. Eric y GOETZ, Eric. Embedding information security into the organization.En: IEEE Security & Privacy Magazine. Vol. 5, No. 3 (May. 2007); p. 16.
[268] PUHAKAINEN, Petri y SIPONEN, Mikko. Improving employees' compliance through information systems security training: an action research study.En: Mis Quarterly. Vol. 34, No. 4 (Dic. 2010); p. 758.
[269] VON SOLMS y VON SOLMS (2004), Op. cit., p. 279.
[270]CHANG, Shuchih y LIN, Chin-Shien.Exploring organizational culture for information security management.En: Industrial Management & Data Systems. Vol. 107, No. 3 (2007); p. 438.

6. Aspectos económicos

Bojanc y JermanJerman-Blažič[272], analizan varios enfoques que permitan evaluar las inversiones necesarias en tecnología de seguridad desde el punto de vista económico. Además presenta los métodos para la identificación de los activos, las amenazas, las vulnerabilidades de los sistemas de TIC y propone un procedimiento que permite la selección de la inversión óptima de tecnología de seguridad necesaria basada en la cuantificación de los valores de los sistemas protegidos.

Salmela[273] examina el uso de análisis de procesos de negocio como un método para asociar los riesgos de los sistemas de información con las pérdidas potenciales del negocio.

7. Gobernanza de seguridad de la información

La gobernanza como concepto aislado representa: "el proceso de toma de decisiones y el proceso por el que las decisiones son implementadas"[274]. Al hablar de gobernanza corporativa se hace referencia al compromiso de la dirección ejecutiva de una compañía y consiste en "un conjunto de políticas y controles internos por los cuales las organizaciones, sin importar su tamaño, son dirigidas y

---

[271] LIM, Joo, et al. Exploring the relationship between organizational culture and information security culture. En: Proceedings of the 7th Australian information security management conference. (2009); p. 8-9.

[272]BOJANC, Rok y JERMAN-BLAŽIČ, Borka. An economic modeling approach to information security risk management. En: International Journal of Information Management. Vol. 28, No. 5 (2008); p. 413.

[273]SALMELA, Hannu. Analysing business losses caused by information systems risk: a business process analysis approach.En: Journal of InformationTechnology. Vol. 23, No. 3 (2007); p. 185.

[274] COMISIÓN ECONÓMICA Y SOCIAL DE LAS NACIONES UNIDAS. ¿Qué es gobernanza? ¿y buen gobierno? [en línea]. [consultado el 8 de mayo de 2012]. Disponible en <http://www.casaasia.es/governasia/boletin2/3.pdf>

gestionadas"[275]. Del mismo modo, la gobernanza de seguridad de la información describe el proceso por el cual se aborda la seguridad de la información desde un nivel ejecutivo en la organización.

Al respecto, varios autores[276][277], muestran que la seguridad de la información debe ser una prioridad de la dirección ejecutiva, incluida la Junta Directiva, y por lo tanto, debe comenzar como una responsabilidad de gobierno corporativo. Esto establece la necesidad de integrar la seguridad de la información en la dirección corporativa a través del desarrollo de un marco de gobierno de la seguridad de la información.

De acuerdo con von Solms[278], la gobernanza de seguridad de la información hace parte integral de la gobernanza corporativa, y consiste en:

- El compromiso y conciencia de la alta dirección en cuanto a la gestión y liderazgo de una buena seguridad de la información.
- Las estructuras organizativas apropiadas para reforzar la buena seguridad de la información.
- Conocimiento de requisitos legales y reglamentarios, en cuanto a privacidad de los datos y la información se refiere.
- Óptimas implementaciones de políticas, procedimientos, procesos, tecnologías y mecanismos de cumplimiento necesarios, que mejoren falencias o eviten consecuencias nefastas debido a negligencia en una buena seguridad de la información.

[275]NATIONAL CYBER SECURITY SUMMIT TASK FORCE. Information security governance: a call to action. [en línea]. [consultado el 15 de septiembre de 2012]. Disponible en <http://www.cyberpartnership.org/InfoSecGov4_04.pdf>
[276] POSTHUMUS y VON SOLMS. Op. cit., p. 638.
[277] VON SOLMS, Bassie y VON SOLMS, Rossouw. From information security to… business security?En: Computers & Security. Vol. 24, No. 4 (Jun. 2005); p. 271.
[278] VON SOLMS (2006), Op. Cit., p. 167.

Por otra parte, Knapp et al.,[279]presenta la "gobernanza de seguridad de la información", como un componente general que afecta directamente a todas las etapas del proceso de gestión de política de seguridad de la información, insistiendo en que la gobernanza no es solamente un proceso interno de la organización, sino que también puede incluir la participación de entes externos tales como el comité directivo.

8. Políticas

En la literatura, hay amplio acuerdo en que una buena política de seguridad de información es la base de la seguridad de la información en las organizaciones[280][281][282][283]. Según David[284], "sin políticas de seguridad formales, la seguridad es arbitraria, sujeta a los caprichos de aquellos que la administran".

Los resultados de la evaluación y análisis de riesgos, deben conducir a la elaboración de la política de seguridad, la cual consiste en un documento que indica el compromiso y apoyo de la dirección, así como la definición del papel que debe jugar la seguridad de la información en la consecución de la misión y visión de la organización. En esencia, la política de seguridad se documenta para explicar la necesidad de seguridad de la información - y sus principios - a todos los usuarios de los recursos de información[285].

Algunas características de una política eficaz, son:

- Ser relevante, accesible, y comprensible para todos los usuarios previstos de la organización.

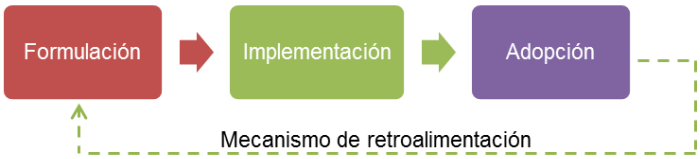
[279] KNAPP, Kenneth, et al. Information security policy: an organizational-level process model. En: Computers & Security. Vol. 28, No. 7 (Oct. 2009): p. 498.
[280] BASKERVILLE y SIPONEN. Op. cit., p. 337.
[281]KNAPP et al., Op. Cit., p.493.
[282]VON SOLMS y VON SOLMS (2004).
[283] DAVID, Op. Cit., p.506.
[284]Ibid. p. 506.
[285]HÖNE, y ELOFF, Op. Cit., p. 402.

- Especificar su frecuencia de revisión y las formas en que será comunicada a toda la organización.

Entre los aspectos que debería contener el documento sobre políticas de seguridad se encuentran[286][287][288]: definición de seguridad para los activos de información, responsabilidades, planes de contingencia, gestión de contraseñas, sistema de control de acceso, respaldo de datos, y manejo de virus e intrusos. Además se debe incluir el tema del reporte de incidentes de seguridad, sobre el cual se deben establecer lineamientos claros dentro de la política de seguridad de la compañía[289].

Para la creación de las políticas, se debe tener la participación activa de los colaboradores, o miembros de la organización, donde al mismo tiempo se involucran las actividades de éstos y el entorno de trabajo. Según Karyda, Kiiountouzis y Kokolakis[290], los tres procesos involucrados en la adopción de una política de seguridad son: formulación, implementación y adopción. Ver Figura 30.

Figura 30. Proceso de aplicación de una política de seguridad



Fuente. Autores del proyecto a partir de KARYDA, Maria, KIOUNTOUZIS, Evangelos y KOKOLAKIS, Spyros. Information systems security policies: a contextual perspective. En: Computers & Security. Vol. 24, No. 3 (2005); p. 248.

[286] DOHERTY, Neil y FULFORD, Heather. Aligning the information security policy with the strategic information systems.En: Computers & Security. Vol. 25, No.1 (2006); p. 57.
[287]HÖNE y ELOFF. Op. cit., p. 403-404.
[288] LINDUP, KENNETH. A new model for information security policies.En: Computers & Security. Vol. 14, No. 8 (1995); p. 694.
[289] WIANT, Terry. Information security policy's impact on reporting security incidents.En: Computers& Security. Vol. 24, No. 6 (Sep. 2005); p. 449.
[290]KARYDA, Maria, KIOUNTOUZIS, Evangelos y KOKOLAKIS, Spyros. Information systems security policies: a contextual perspective. En: Computers & Security. Vol. 24, No. 3 (2005); p. 248.

9. Buenas prácticas

Las buenas prácticas (*bestpractices)*"definen prácticas y procedimientos que permitan crear un ambiente consistente que sea seguro mientras siga siendo útil"[291]. En casi todas las áreas del conocimiento y del mundo económico se requieren estándares que permitan establecer bases y criterios para la excelencia. El campo de la seguridad de la información no ha sido la excepción.

Según Von Solms[292], las buenas prácticas internacionales, para la gestión de la seguridad de la información, son la compilación de experiencias combinadas de muchas compañías internacionales influyentes, acerca de la forma en que ellos gestionan la seguridad de la información. Estas prácticas reflejan la experiencia de dichas empresas sobre las medidas de control relevantes, procedimientos y técnicas, que proporcionan un nivel adecuado o aceptable de seguridad de la información.

Además, las buenas prácticas proveen un marco de trabajo como referencia para asegurar que las organizaciones cubran todas las bases de seguridad de la información. Uno de los documentos más conocidos de este tipo, es el código de buenas prácticas para la gestión de la seguridad, ISO/IEC 27002[293]. Este estándar establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de seguridad de la información en una organización. Además, tiene 133 medidas de control de alto nivel que abarcan tanto las amenazas externas como internas, las cuales se agrupan en 11 dimensiones (cláusulas). La consideración de otros controles de seguridad, no incluidos en ISO/IEC 27002, podría ser requerida para proveer mayor protección especialmente para activos de

[291] Information Security Best Practices. [En línea]. [Consultado 16 febrero 2012]. Disponible en: <http://networking.lamar.edu/files/LU%20Best%20Practices%20Final.pdf>
[292] VON SOLMS, (2000). Op. Cit., p. 616.
[293] VON SOLMS, Basie. Information security: a multidimensional discipline. En: Computers & Security. Vol. 20, No. 6 (2001); p. 505.

gran valor o para contrarrestar los niveles excepcionalmente altos de las amenazas de seguridad[294]. De igual forma, la norma ISO/IEC 27001, es el único esquema de aceptación internacional que permite certificación.

Finalmente, es importante mencionar el concepto de conformidad, que es el proceso práctico de comparar los controles aplicados en una organización con aquellos propuestos en ISO/IEC 27002. Es básicamente un análisis de brechas en el cual se descubren las diferencias entre la situación de la organización y el estándar. Al respecto, Karabacak y Sogukpinar[295], proponen un método cuantitativo basado en una encuesta que evalúa la conformidad de ISO/IEC 27002. Este tiene cualidades únicas como su facilidad de uso y flexibilidad. Se pueden cambiar fácilmente el número de preguntas, opciones de respuesta y ajustar los valores numéricos para las mismas.

[294] INTERNATIONAL STANDARDSORGANIZATION, Op. Cit.
*Sistemas de Gestión de la Seguridad de la Información (SGSI) – Requisitos
[295]KARABACAK, Bilge y SOGUKPINAR, Ibrahim. A quantitative method for ISO 17799 gap analysis. En: Computers& Security. Vol. 25 (2006); p. 419.

ANEXO 5. LISTADO INICIAL DE VARIABLES ANÁLISIS ESTRUCTURAL

ÁREA DE SI	DESCRIPCIÓN	#	NOMBRE VARIABLE
Política de seguridad de la información	Se refiere a la existencia de lineamientos claros establecidos por la dirección del grupo, entre los cuales se encuentra la política de seguridad de la información documentada y actualizada.	1	Políticas inadecuadas o pobres: Una política completa no existe, no ha sido comunicada o no es aplicada por los usuarios.
		2	No se ha establecido una metodología clara de análisis y evaluación de riesgos.
		3	Los controles implementados son débiles/ falta de nivel apropiado de controles de seguridad.
		4	No existe una política clara y en línea con los objetivos de la organización
		5	No se publica para todo el grupo de investigación ni se actualiza la política de seguridad
		6	No existen normas, procedimientos o directrices documentados en un manual
		7	No hay conocimiento de políticas, normas o procedimientos de control apropiados para el grupo
		8	No hay responsables de la revisión, actualización e implementación de la política.
Organización de la seguridad de la información	Se refiere a la existencia de una estructura de gestión interna que controle la seguridad de la información. Incluye: compromiso y apoyo de la alta dirección, asignación de responsabilidades, y procesos de control internos.	9	Entrenamiento inadecuado (Errores en el uso de software o hardware, eliminación de datos, documentos, reportes, discos, desconfiguración de la red-web)
		10	No se firman acuerdos de confidencialidad
		11	Las responsabilidades de seguridad de la información no son claras para los miembros del grupo
		12	Ausencia de objetivos de seguridad de la información
		13	No hay claridad en el concepto de confidencialidad de la información

ÁREA DE SI	DESCRIPCIÓN	#	NOMBRE VARIABLE
Gestión de activos	Alcanzar y mantener una protección adecuada de los activos del grupo de investigación. Incluye: justificación de activos, asignación de responsabilidad sobre los mismos y clasificación de la información (pública, restringida, crítica, etc.)	14	Siniestros: Sufrir Robo o perdida de portátiles u otros activos.
		15	Defectos del software o hardware
		16	Poca consciencia sobre la importancia de la información
		17	Ataque contra la confidencialidad. intercepción y alteración de datos
		18	Divulgar información confidencial
		19	Obsolescencia tecnológica
		20	No existe clasificación de la información
		21	Acceso sin autorización a una parte del sistema
		22	Modificación parcial o completa sin autorización del contenido o modo de funcionamiento del sistema
		23	Ausencia de inventario actualizado de equipos e información
Seguridad de recursos humanos	Se refiere a asegurarse que los miembros del grupo entiendan sus responsabilidades y roles desempeñados en la seguridad de la información. Incluye: verificación de antecedentes, programas de sensibilización y formación, y procesos disciplinarios.	24	No hay verificación de antecedentes de los integrantes del grupo
		25	Ausencia de programas de sensibilización y formación
		26	No existe claridad de roles y responsabilidades de cada integrante del grupo
Seguridad física y ambiental	Se refiere a la prevención del acceso físico no autorizado, daño o interferencia a la seguridad de la información. Incluye la protección de las instalaciones de procesamiento de información crítica a través de barreras físicas, controles de entrada y sistema de vigilancia por cámaras, entre otros.	27	Desastres naturales (tormenta eléctrica, inundación, terremoto, fuertes vientos, actividad sísmica)
		28	Seguridad física, o seguridad de infraestructuras materiales
		29	Colapso del edificio, incendio, fuga de gas, exposición a residuos peligrosos
		30	Vandalismo, desordenes civiles, ataques físicos que afectan la integridad de personas y conservación de bienes.
		31	Fluctuaciones o fallas en el suministro de energía
		32	Información confidencial/sensible se encuentra en activos eliminados o reasignados, y se puede acceder por un usuario no autorizado.

ÁREA DE SI	DESCRIPCIÓN	#	NOMBRE VARIABLE
Gestión de comunicaciones y operaciones	Se refiere a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información. Incluye: establecimiento de responsabilidades y procedimientos para la gestión y operación de todos los recursos para el tratamiento de la información; desarrollo de instrucciones apropiadas de operación; procedimientos de respuesta ante incidencias; y, segregación de tareas, cuando sea adecuado.	33	Delitos informáticos o programas maliciosos (troyanos, gusanos, virus, código malicioso, spyware, descifrado de claves)
		34	Fraude informático Hackers, crimen cibernético spoofing
		35	Pérdida o daño de las copias de resguardo
		36	Supervisión inadecuada del uso del sistema
		37	Seguridad en las telecomunicaciones (tecnologías de red, servidores, redes de acceso, etc.)
		38	Procedimientos no documentados (copias de seguridad, manejo de comunicaciones externas, gestión de incidentes)
		39	Se permite que un atacante reúna información sobre las actividades del sistema
		40	Penetración en el sistema a través de la red
Control de acceso	Se refiere a controlar los accesos a la red, sistema operativo, aplicaciones e información, con base en las necesidades de seguridad del grupo. Incluye: política de control de acceso, y los controles de acceso para cada uno de los aspectos mencionados anteriormente.	41	Amenaza contra la integridad de los datos, modifican los sistemas para que funcionen de una manera diferente, modifican el contenido de los mensajes transferidos en la red.
		42	Controles de acceso inadecuados (Desconfiguración de la red)
		43	Acceso desautorizado a sistemas.
		44	El acceso no es retirado inmediatamente o no es examinado antes de ser concedido.
		45	Cambio de acceso son informales o inadecuados. derechos de acceso no son consistentes con las funciones/roles del usuario.
		46	Intercepción de información, es un ataque contra la confidencialidad. Falta de ética, Espionaje corporativo y extorsiones (Acceso o exploraciones no autorizadas, suplantación de identidad, fraude) actos fraudulentos
		47	Posibilidad de añadir información o programas no autorizados en el sistema

ÁREA DE SI	DESCRIPCIÓN	#	NOMBRE VARIABLE
Adquisición, desarrollo y mantenimiento o de sistemas de información	Se refiere a garantizar que la seguridad es parte integral de los sistemas de información. Incluye: identificación de requisitos de seguridad para la implantación de sistemas de información, gestión de la vulnerabilidad técnica, controles criptográficos y seguridad de los archivos del sistema entre otros.	48	No existen criterios de aceptación para nuevas aplicaciones y sistemas
		49	Expansión del uso de ordenadores personales, lo cual dificulta los controles de seguridad
Gestión de incidentes de seguridad de la información	Se refiere a garantizar que los eventos y debilidades en la seguridad asociados a la información y conocimiento generado dentro del grupo se comuniquen de modo que se puedan realizar acciones correctivas oportunas. Incluye: notificación de eventos y puntos débiles de seguridad de la información.	50	Falta de registros sobre incidentes ocurridos en el pasado y las lecciones aprendidas
		51	No hay registro de incidentes de manera rápida y oportuna
Gestión de la continuidad	Se refiere a la inclusión de la seguridad de la información dentro del plan de continuidad del grupo. Este plan contiene los procedimientos que deben llevarse a cabo en el caso de ocurrir una interrupción de actividades del grupo con el fin de proteger sus procesos e información crítica.	52	Interrupción de la disponibilidad de la información (destrucción o daño del disco duro, cortan una línea de comunicación)
		53	Denegación de servicios para los usuarios, porque el ordenador está estropeado o la red de internet se ha caído, los ordenadores no tienen suficiente capacidad para ejecutar los programas.
Conformidad / cumplimiento legal	Se refiere a la prevención de incumplimientos de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requisito de seguridad. Incluye: cumplimiento de los requisitos legales, de las políticas y normas de seguridad y cumplimiento técnico.	54	Problemas legales, demandas, litigio
		55	No hay acuerdos de obligaciones legales para la relación con terceros.
		56	No se cuenta con asesoramiento legal competente.
		57	No se tienen identificados los requisitos reglamentarios, legales y contractuales.
		58	No está protegida la información personal de los integrantes y las partes interesadas del grupo de investigación.
		59	No hay un responsable de la protección de la privacidad de la información

ANEXO 6. ACTORES QUE PARTICIPARON EN LA PRIMERA ETAPA

NOMBRE	FACULTAD	ESCUELA	GRUPO DE INVESTIGACIÓN	CARGO	ACTIVIDAD
Juan Andrés Montoya Arguello	Facultad de Ciencias	N/A	N/A	Director de investigación y extensión - DIEF	· Matriz de impactos cruzados
José Horacio Rosales Cuevas	Facultad de Ciencias Humanas	N/A	N/A	Decano	· Matriz de impactos cruzados
Eduardo Serafín Guevara Melo	Facultad de Ingenierías Físicomecánicas	Escuela de Diseño Industrial	Biónica	Líder del grupo	· Cuestionario para la valoración en grupos de investigación UIS
Francisco Espinel	Facultad de Ingenierías Físicomecánicas	Escuela de Diseño Industrial	Ergonomía, producto y significado GEPS	Profesor asociado	· Cuestionario para la valoración en grupos de investigación UIS
John Faber Archila Díaz	Facultad de Ingenierías Físicomecánicas	Escuela de Diseño Industrial	Grupo de Investigación en Robótica de servicio y Diseño Industrial GIROD	Líder del grupo	· Cuestionario para la valoración en grupos de investigación UIS
José Miguel Enrique Higuera Marín	Facultad de Ingenierías Físicomecánicas	Escuela de Diseño Industrial	Interfaz	Líder del grupo, Director de escuela	· Cuestionario para la valoración en grupos de investigación UIS · Matriz de impactos cruzados
Edna Bravo Ibarra	Facultad de Ingenierías Físicomecánicas	Escuela de Estudios Industriales y Empresariales	INNOTEC	Profesora asociada	· Cuestionario para la valoración en grupos de investigación UIS · Matriz de impactos cruzados
Javier Arias Osorio	Facultad de Ingenierías Físicomecánicas	Escuela de Estudios Industriales y Empresariales	OPALO	Líder del grupo	· Cuestionario para la valoración en grupos de investigación UIS

NOMBRE	FACULTAD	ESCUELA	GRUPO DE INVESTIGACIÓN	CARGO	ACTIVIDAD
Aura Cecilia Pedraza Avella	Facultad de Ingenierías Físicomecánicas	Escuela de Estudios Industriales y Empresariales	FINANCE	Líder del grupo	· Cuestionario para la valoración en grupos de investigación UIS
Néstor Raúl Ortiz Pimiento	Facultad de Ingenierías Físicomecánicas	Escuela de Estudios Industriales y Empresariales	N/A	Director de escuela	· Matriz de impactos cruzados
Ricardo Alfredo Cruz Hernández	Facultad de Ingenierías Físicomecánicas	Escuela de Ingeniería Civil	Grupo de Investigación en Materiales y Estructuras de Construcción INME	Líder del grupo	· Cuestionario para la valoración en grupos de investigación UIS · Matriz de impactos cruzados
Vanessa Quiroga Arciniegas	Facultad de Ingenierías Físicomecánicas	Escuela de Ingeniería Civil	GEOMÁTICA, Gestión y optimización de sistemas	Profesional de apoyo	· Cuestionario para la valoración en grupos de investigación UIS
Eduardo Alberto Castañeda Pinzón	Facultad de Ingenierías Físicomecánicas	Escuela de Ingeniería Civil	Grupo de Investigación en Asfaltos - GIAS	Líder del grupo	· Cuestionario para la valoración en grupos de investigación UIS
Lola Xiomara Bautista Rozo	Facultad de Ingenierías Físicomecánicas	Escuela de Ingeniería de Sistemas e Informática.	Grupo de Investigación en Ingeniería Biomédica- GIIB	Líder del grupo	· Cuestionario para la valoración en grupos e investigación UIS
Hugo Andrade Sosa	Facultad de Ingenierías Físicomecánicas	Escuela de Ingeniería de Sistemas e Informática.	Grupo de Investigaciones en Modelamiento y Simulación - SIMON	Líder del grupo	· Cuestionario para la valoración en grupos de investigación UIS
Luis Carlos Gómez Flórez	Facultad de Ingenierías Físicomecánicas	Escuela de Ingeniería de Sistemas e Informática.	Grupo de Investigación en Sistemas y Tecnología de la Información - STI	Líder del grupo	· Cuestionario para la valoración en grupos de investigación UIS

NOMBRE	FACULTAD	ESCUELA	GRUPO DE INVESTIGACIÓN	CARGO	ACTIVIDAD
José Cárcamo Sepúlveda	Facultad de Ingenierías Físicomecánicas	Escuela de Ingeniería de Sistemas e Informática.	N/A	Director de escuela	· Matriz de impactos cruzados
Julián Ernesto Jaramillo Ibarra & David Alfredo Fuentes Díaz	Facultad de Ingenierías Físicomecánicas	Escuela de Ingeniería Mecánica	Grupo de Investigación en Energía y Medio Ambiente GIEMA	Profesores asociados	· Cuestionario para la valoración en grupos de investigación UIS
Jabid Eduardo Quiroga Mendez	Facultad de Ingenierías Físicomecánicas	Escuela de Ingeniería Mecánica	Centro de Investigaciones en Sistemas Dinámicos Multifísicos, Control y Robótica; Centro Investigaciones DICBOT	Profesor asociado	· Cuestionario para la valoración en grupos de investigación UIS
Heller Guillermo Sánchez Acevedo	Facultad de Ingenierías Físicomecánicas	Escuela de Ingeniería Mecánica	Grupo de investigación en diseño y procesos de manufactura	Profesor asociado	· Cuestionario para la valoración en grupos de investigación UIS
Alfonso García	Facultad de Ingenierías Físicomecánicas	Escuela de Ingeniería Mecánica	N/A	Director de escuela	· Matriz de impactos cruzados
Johann Farith Petit Suárez	Facultad de Ingenierías Físicomecánicas	Escuela de Ingenierías Eléctrica, Electrónica y de Telecomunicaciones	Grupo de Investigación en Sistemas de Energía Eléctrica GISEL	Líder del grupo	· Cuestionario para la valoración en grupos de investigación UIS
Daniel Alfonso Sierra Bueno	Facultad de Ingenierías Físicomecánicas	Escuela de Ingenierías Eléctrica, Electrónica y de Telecomunicaciones	Grupo de Investigación en Control, Electrónica, Modelado y Simulación CEMOS	Líder del grupo	· Cuestionario para la valoración en grupos de investigación UIS

NOMBRE	FACULTAD	ESCUELA	GRUPO DE INVESTIGACIÓN	CARGO	ACTIVIDAD
Oscar Gualdrón González	Facultad de Ingenierías Físicomecánicas	Escuela de Ingenierías Eléctrica, Electrónica y de Telecomunicaciones	Grupo de Investigación en Conectividad y Procesado de Señal CPS	Líder del grupo, Vicerrector de investigación y extensión	· Cuestionario para la valoración en grupos de investigación UIS · Matriz de impactos cruzados
Camilo Rodríguez	Facultad de Ingenierías Físicomecánicas	Escuela de Ingenierías Eléctrica, Electrónica y de Telecomunicaciones	Grupo de Investigación RadioGis	Responsable temporal	· Cuestionario para la valoración en grupos de investigación UIS
Gerardo Latorre Bayona	Facultad de Ingenierías Físicomecánicas	N/A	N/A	Decano	· Matriz de impactos cruzados
Carlos Alberto García Ramírez	Facultad de Ingenierías Fisicoquímicas	N/A	N/A	Director de investigación y extensión - DIEF	· Matriz de impactos cruzados

ANEXO 7. INSTRUCTIVO DE DILIGENCIAMIENTO DE LA MATRIZ DE IMPACTOS CRUZADOS

DESCRIPCIÓN DEL PROYECTO

El proyecto busca dar solución al problema de la desprotección e inseguridad de la información y del capital intelectual, los cuales son activos estratégicos de los grupos de investigación de la Universidad. Como resultado del mismo, se obtendrá un modelo de gestión de seguridad, que especifique las políticas, objetivos, principios y controles relevantes que permitan garantizar la protección y correcta manipulación de la información como recurso organizativo. Este modelo servirá de insumo para otros grupos y/o centros de investigación dentro y fuera de la Universidad Industrial de Santander, y para todo aquel interesado en tomar como base el modelo desarrollado en este proyecto para la aplicación a su contexto específico.

Algunas de las preguntas que se pretenden resolver son:
- Cómo crear una estrategia de seguridad de la información
- Cómo definir las políticas de seguridad
- Cuáles son los recursos que se deben proteger
- Qué procedimientos debe tener un grupo de investigación para cumplir los objetivos de seguridad.
- Qué personas están involucradas en el establecimiento de las políticas y quienes deben velar por hacerlas cumplir

ANÁLISIS ESTRUCTURAL

El análisis estructural es una herramienta de estructuración de una reflexión colectiva. Ofrece la posibilidad de describir un sistema con ayuda de una matriz que relaciona todos sus elementos constitutivos.

Tiene la ventaja de estimular la reflexión dentro del grupo, y hacer que las personas analicen ciertos aspectos que algunas veces son poco intuitivos. Se aplica al estudio cualitativo de sistemas extremadamente diferentes.

EVALUACIÓN DE LAS RELACIONES ENTRE DIMENSIONES

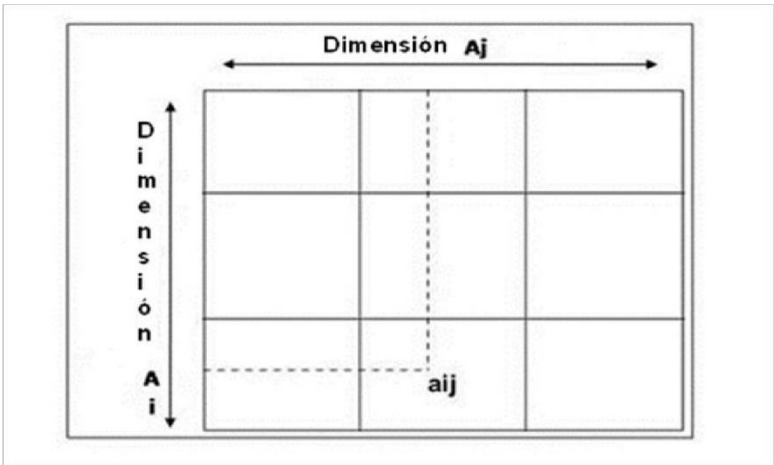
OBJETIVO: Identificar las principales dimensiones influyentes y dependientes y, por ello, esenciales para la evolución del sistema.

INSTRUCCIONES:

A continuación encontrará una matriz con las dimensiones a evaluar ordenadas en filas y columnas, determine la influencia que tiene cada uno de las dimensiones ubicadas en las filas sobre cada uno de las dimensiones ubicadas en las columnas.

Tenga en cuenta que se van evaluar influencias directas, con base en esto indique en la matriz relacional el valor que según su criterio puede tener cada factor sobre los demás siguiendo las siguientes convenciones:

1: la dimensión **Ai** tiene **influencia débil** sobre la dimensión **Aj**
2: la dimensión **Ai** tiene **influencia moderada** sobre la dimensión **Aj**
3: la dimensión **Ai** tiene **influencia fuerte** sobre la dimensión **Aj**
4: la dimensión **Ai** tiene **influencia potencial** sobre la dimensión **Aj**



IMPORTANTE:

- Evaluar siempre la influencia en una sola dirección (Ai sobre Aj).
- La diagonal principal no se llena, puesto que una dimensión no puede influir sobre sí misma.
- Si no hay influencia directa el cuadro queda vacío.

DIMENSIONES QUE AFECTAN LA SEGURIDAD DE LA INFORMACIÓN

A continuación encontrará el listado de las 11 dimensiones a evaluar con su respectiva descripción. Las palabras entre paréntesis corresponden a los nombres abreviados que aparecen en la matriz de impactos cruzados.

1. Política de Seguridad de la Información (Política)

Se refiere a la existencia de lineamientos claros establecidos por la dirección del grupo, entre los cuales se encuentra la política de seguridad de la información documentada y actualizada.

2. Organización de la Seguridad de la Información (Organización)

Se refiere a la existencia de una estructura de gestión interna que controle la seguridad de la información. Incluye: compromiso y apoyo de la alta dirección, asignación de responsabilidades, y procesos de control internos.

3. Gestión de Activos (Gestión activos)

Alcanzar y mantener una protección adecuada de los activos del grupo de investigación. Incluye: justificación de activos, asignación de responsabilidad sobre los mismos y clasificación de la información (pública, restringida, crítica, etc.)

4. Seguridad de Recursos Humanos (Seguridad RR.HH.)

Se refiere a asegurarse que los miembros del grupo entiendan sus responsabilidades y roles desempeñados en la seguridad de la información. Incluye: verificación de antecedentes, programas de sensibilización y formación, y procesos disciplinarios.

5. Seguridad Física y Ambiental (Segu fis amb)

Se refiere a la prevención del acceso físico no autorizado, daño o interferencia a la seguridad de la información. Incluye la protección de las instalaciones de procesamiento de información crítica a través de barreras físicas, controles de entrada y sistema de vigilancia por cámaras, entre otros.

6. Gestión de Comunicaciones y Operaciones (Gestión com&oper)

Se refiere a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información. Incluye: establecimiento de responsabilidades y procedimientos para la gestión y operación de todos los recursos para el tratamiento de la información; desarrollo de instrucciones apropiadas de operación; procedimientos de respuesta ante incidencias; y, segregación de tareas, cuando sea adecuado.

7. Control de Acceso (Control acceso)

Se refiere a controlar los accesos a la red, sistema operativo, aplicaciones e información, con base en las necesidades de seguridad del grupo. Incluye: política de control de acceso, y los controles de acceso para cada uno de los aspectos mencionados anteriormente.

8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información (sistemas de información)

Se refiere a garantizar que la seguridad es parte integral de los sistemas de información. Incluye: identificación de requisitos de seguridad para la implantación de sistemas de información (sistemas operativos, infraestructuras, aplicaciones, y software); gestión de la vulnerabilidad técnica, controles criptográficos y seguridad de los archivos del sistema entre otros.

9. Gestión de Incidentes de Seguridad de la Información (Gestión incidentes)

Se refiere a garantizar que los eventos y debilidades en la seguridad asociados a la información y conocimiento generado dentro del grupo se comuniquen de modo que se puedan realizar acciones correctivas oportunas. Incluye: notificación de eventos y puntos débiles de seguridad de la información.

10. Gestión de la Continuidad (Gestión continuidad)

Se refiere a la inclusión de la seguridad de la información dentro del plan de continuidad del grupo. Este plan contiene los procedimientos que deben llevarse a cabo en el caso de ocurrir una interrupción de actividades del grupo con el fin de proteger sus procesos e información crítica.

11. Conformidad (cumplimiento legal)

Se refiere a la prevención de incumplimientos de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requisito de seguridad. Incluye: cumplimiento de los requisitos legales, de las políticas y normas de seguridad y cumplimiento técnico.

MATRIZ DE IMPACTOS CRUZADOS

	Política	Organización	Gestión activos	Seguridad RR.HH.	Segu fis amb	Gestión com&oper	Control acceso	sistemas de información	Gestión incidentes	Gestión continuidad	Cumplimiento legal
Política											
Organización											
Gestión activos											
Seguridad RR.HH.											
Segu fis amb											
Gestión com&oper											
Control acceso											
sistemas de información											
Gestión incidentes											
Gestión continuidad											
Cumplimiento legal											

ANEXO 8. TRATAMIENTO ESTADÍSTICO PARA CONSOLIDACIÓN DE LA MATRIZ DE IMPACTOS CRUZADOS

La metodología utilizada para consolidar la matriz de influencias entre variables que fue ingresada al software MICMAC para su análisis consistió en los siguientes pasos (Ver también figura):

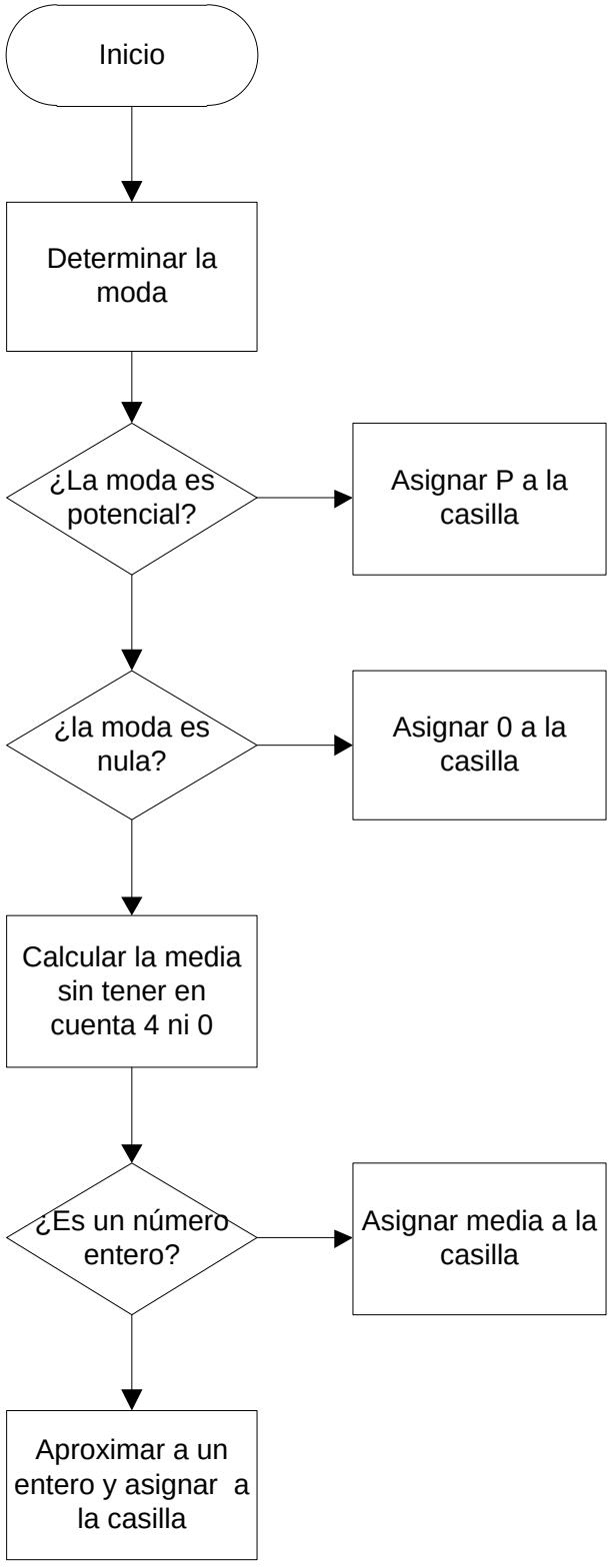
1. Por cada par de variables evaluado se calculó la moda teniendo en cuenta lo siguiente: los valores 1, 2 y 3 se agruparon bajo un mismo carácter numérico al indicar la existencia de una relación de influencia de tipo de real, sea de tipo directo o indirecto, y los "4" tomaron un valor numérico estándar para facilitar el cálculo e indicaban una relación de tipo potencial. El objetivo de este primer paso era establecer si la tendencia de las influencias era potencial o real.

2. Cuando la moda era una relación de tipo potencial se asignó una "P" en la casilla correspondiente al par de variables evaluadas.

3. Cuando la moda indicó que la influencia es real se calculó la mediana, la cual tomó un valor entre el intervalo cerrado de 1 y 3, de esta forma se evitó los inconvenientes que se pueden presentar al emplear la media como estadístico, a saber:
    - Obliga una mayor subjetividad al requerir un criterio adicional para aproximar el resultado obtenido por encima o por debajo.

    Para el cálculo de la mediana se omitieron los valores correspondientes a relaciones de tipo potencial al no ser un valor numérico y tratarse de conceptos distintos. Cuando la mediana se evalúa con datos pares el resultado es un número decimal, la aproximación hacia la unidad siguiente o una unidad anterior estuvo dada por el valor que tomó la media. De esta forma se consolidó una matriz final.

Figura 31. Tratamiento estadístico para consolidación de la matriz



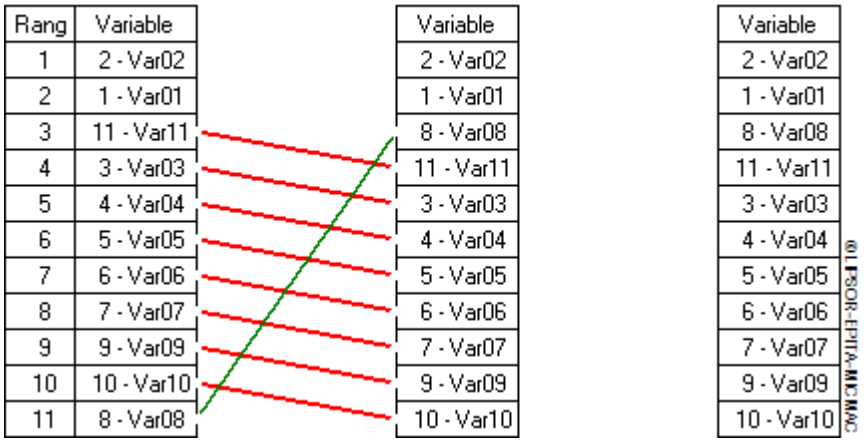
ANEXO 9. MATRIZ DE IMPACTOS CRUZADOS

	Política	Organización	Gestión activos	Seguridad RR.HH.	Segu fis amb	Gestión com & oper	Control acceso	sistemas de información	Gestión incidentes	Gestión continuidad	Cumplimiento legal
Política		3	2	3	2	3	2	2	2	2	2
Organización	2		3	3	3	3	3	3	2	2	2
Gestión activos	2	2		2	2	2	2	2	2	2	2
Seguridad RR.HH.	2	2	2		2	2	2	2	2	2	2
Segu fis amb	2	2	2	2		2	2	2	2	2	2
Gestión com & oper	2	2	2	2	2		2	2	2	2	2
Control acceso	2	2	2	2	2	2		2	2	2	2
sistemas de información	2	4	2	2	2	2	2		2	2	2
Gestión incidentes	2	2	2	2	2	2	2	2		2	2
Gestión continuidad	2	2	2	2	2	2	2	2	2		2
Cumplimiento legal	3	2	2	2	2	2	2	2	2	2	

ANEXO 10. PLANO DE DESPLAZAMIENTOS DIRECTO / INDIRECTO

ANEXO 11. CLASIFICACIÓN POR INFLUENCIAS Y DEPENDENCIAS

Clasificación por influencias: indirecta / directa potencial / indirecta potencial

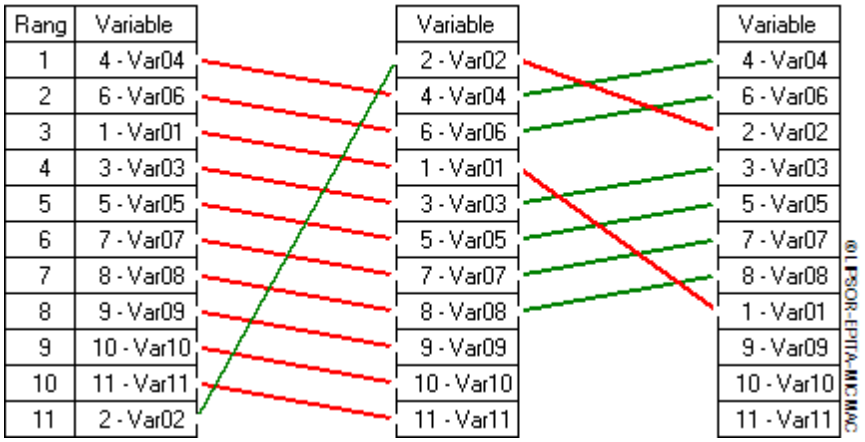


Rang	Variable
1	2 - Var02
2	1 - Var01
3	11 - Var11
4	3 - Var03
5	4 - Var04
6	5 - Var05
7	6 - Var06
8	7 - Var07
9	9 - Var09
10	10 - Var10
11	8 - Var08

Variable
2 - Var02
1 - Var01
8 - Var08
11 - Var11
3 - Var03
4 - Var04
5 - Var05
6 - Var06
7 - Var07
9 - Var09
10 - Var10

Variable
2 - Var02
1 - Var01
8 - Var08
11 - Var11
3 - Var03
4 - Var04
5 - Var05
6 - Var06
7 - Var07
9 - Var09
10 - Var10

Clasificación por dependencias: indirecta / directa potencial / indirecta potencial



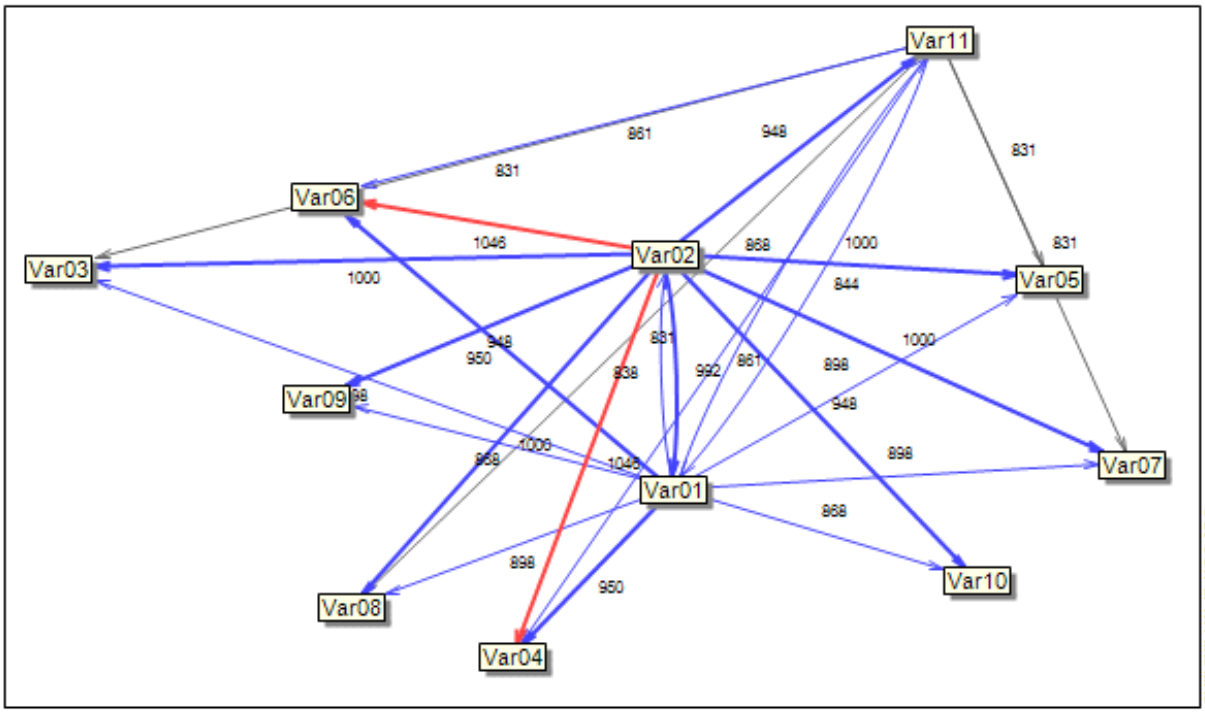
Rang	Variable
1	4 - Var04
2	6 - Var06
3	1 - Var01
4	3 - Var03
5	5 - Var05
6	7 - Var07
7	8 - Var08
8	9 - Var09
9	10 - Var10
10	11 - Var11
11	2 - Var02

Variable
2 - Var02
4 - Var04
6 - Var06
1 - Var01
3 - Var03
5 - Var05
7 - Var07
8 - Var08
9 - Var09
10 - Var10
11 - Var11

Variable
4 - Var04
6 - Var06
2 - Var02
3 - Var03
5 - Var05
7 - Var07
8 - Var08
1 - Var01
9 - Var09
10 - Var10
11 - Var11

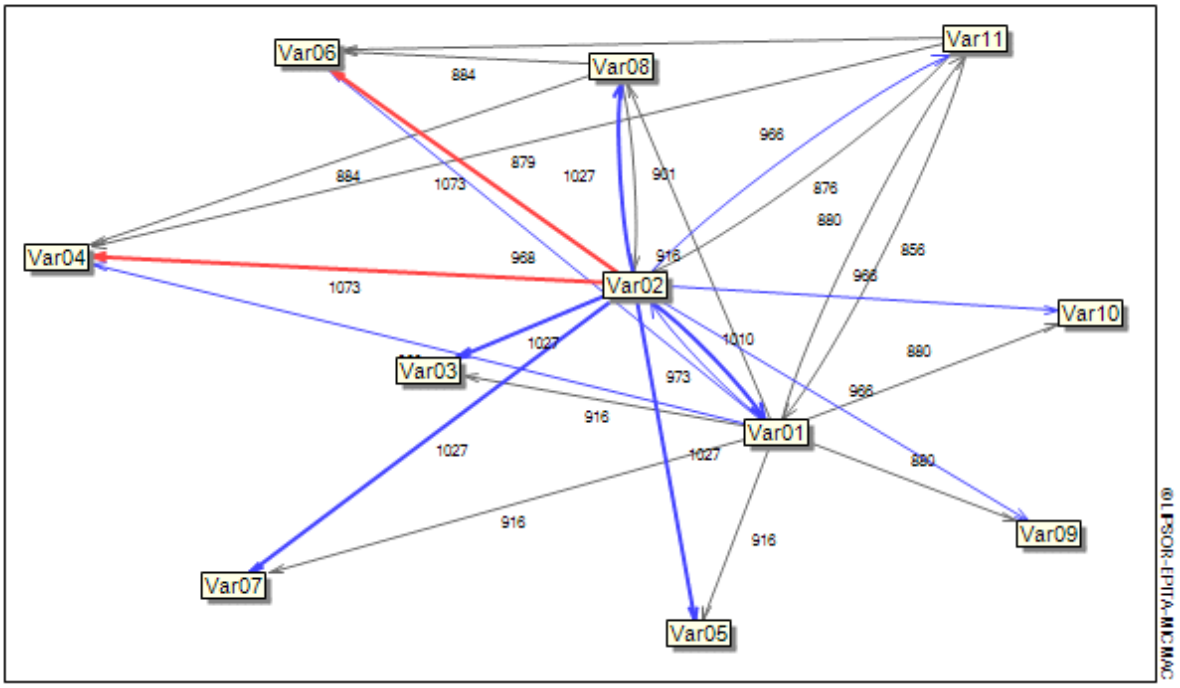
ANEXO 12. GRÁFICOS DE INFLUENCIAS

Gráfico de influencias indirectas



Influences les plus faibles
Influences faibles
Influences moyennes
Influences relativement importantes
Influences les plus importantes

Gráfico de influencias indirectas potenciales



Influences les plus faibles
Influences faibles
Influences moyennes
Influences relativement importantes
Influences les plus importantes

ANEXO 13. CUESTIONARIO PARA GRUPOS DE INVESTIGACIÓN DE LA FACULTAD

El propósito de este cuestionario es establecer las condiciones actuales en materia de seguridad de la información a nivel institucional, a fin de detectar fortalezas y debilidades que sirvan como base para la creación de un modelo de gestión de seguridad del capital intelectual, que fortalezca la actividad investigativa de la UIS, los centros y grupos de investigación y demás UAAs que lleven a cabo proyectos de generación y transformación de conocimiento. Por favor, lea detenidamente cada pregunta y seleccione la repuesta que más se ajuste a la realidad del grupo de investigación del cual usted hace parte. Sus repuestas son confidenciales y no serán evaluadas como buenas o malas. De antemano agradecemos su sincera participación.

Nombre completo *

Vinculación con el grupo de investigación *

Grupo de Investigación *

Escuela a la que pertenece el grupo de investigación *

Política de seguridad de la información

Documento de alto nivel que define los objetivos, intenciones y prioridades del grupo de investigación, relacionados con la protección del conocimiento creado, gestionado y transferido.

1. ¿Existe una política de seguridad de la información documentada y actualizada? *

- Si
- No

Conteste las preguntas 2, 3 y 4 solo si existe la política de seguridad de la información en el grupo de investigación

2. ¿Cómo se comunica la política de seguridad de la información a todas las partes interesadas en el grupo de investigación?

- Manual de Seguridad
- Sitio web del grupo
- Correo electrónico
- Actividades de capacitación (charlas, conferencias, seminarios...)
- Folletos
- No se comunica la política
- Other:

3. ¿Con qué frecuencia se comunica la política de seguridad de la información a todos los integrantes y las partes externas interesadas del grupo de investigación?

- Mensual
- Trimestral
- Semestral
- Anual
- Nunca
- Other:

4. Cuáles de los siguientes aspectos están incluídos en la política de seguridad de la información del grupo de investigación:

- Objetivos de seguridad de la información
- Clasificación de la información (pública, confidencial, restringida...)
- Asignación de responsabilidades en seguridad de la información
- Programas de sensibilización, formación o educación
- Asignación de activos
- Control de acceso a las instalaciones del grupo de investigación
- Procedimientos en caso de incumplimiento de las normas de seguridad de la información
- Estructura de la evaluación y gestión del riesgo
- Monitoreo de amenazas relacionadas con el entorno
- Requerimientos estatutarios, reguladores y contractuales relevantes
- No conozco los aspectos incluidos en la política de seguridad de la información
- Other:

Controles de seguridad de la información

Medios para manejar el riesgo, los cuales pueden ser administrativos, técnico, de gestión o legales.

5. Cuáles de los siguientes controles de seguridad de la información se encuentran implementados actualmente en el grupo de investigación: *

- Acuerdos de confidencialidad en seguridad de la información (con miembros y terceros)
- Reportes en caso de incidentes de seguridad de la información
- Copias de seguridad de la información (back up)
- Destrucción segura de información

- [ ] Seguridad de la red interna (intranet)
- [ ] Acceso a equipos (computadores), software e información
- [ ] Instalación de software
- [ ] Uso, publicación o divulgación de la información
- [ ] Protección de las instalaciones físicas donde opera el grupo de investigación
- [ ] Creación y eliminación de cuentas de usuario
- [ ] Procedimientos en caso de incumplimiento de las normas de seguridad de la información
- [ ] No existe ningún control implementado en el momento
- [ ] Other:

6. Evalúe la importancia dada en el grupo de investigación a cada uno de los siguientes ítems: *

	Nula	Poca	Media	Alta	Muy Alta
Seguridad de la información	○	○	○	○	○
Rol desempeñado por cada integrante en la seguridad de la información	○	○	○	○	○
Responsabilidad que usted tiene en la seguridad de la información	○	○	○	○	○
Clasificación de la información	○	○	○	○	○
Reporte de eventos que constituyan un incidente de seguridad de la información	○	○	○	○	○
Usos autorizados de los activos del grupo de investigación	○	○	○	○	○

7. Cuáles de los siguientes procedimientos se llevan a cabo cuando ingresa un nuevo integrante al grupo de investigación: *

- [ ] Programa de sensibilización, formación o educación
- [ ] Firma de acuerdo de confidencialidad
- [ ] Entrega de normatividad del grupo
- [ ] Presentación de los demás miembros
- [ ] Asignación de activos
- [ ] Asignación de responsabilidades
- [ ] Ninguna acción
- [ ] Other:

Sugerencias u observaciones que considere deben ser tenidos en cuenta para el diseño del modelo de gestión de seguridad del capital intelectual en grupos de investigación

Final del formulario

ANEXO 14. INFORMACIÓN GENERAL SOBRE LOS GRUPOS DE INVESTIGACIÓN ENCUESTADOS

	Antigüedad (años)	No investiga-dores	No estudian-tes	No. Líneas de investiga-ción
Escuela de Estudios Industriales y Empresariales				
Grupo de Optimización y Organización de sistemas Productivos, Administrativos y Logísticos – OPALO	6	11	13	10
Finance & Management	4	5	7	4
INNOTEC	16	12	32	3
Escuela de Ingeniería Civil				
GEOMÁTICA, Gestión y optimización de sistemas	13	12	14	4
Asfaltos (GIAS)	20	9	1	4
Materiales y estructuras - INME	21	5	21	4
Predicción y modelamiento hidroclimático – GPH	14	7	49	4
Escuela de Ingeniería Mecánica				
Diseño y procesos de manufactura	9	6	4	2
Energía y Medio Ambiente – GIEMA	9	10	5	6
Centro de Investigaciones DICBOT	10	3	3	5
Escuela de Diseño Industrial				
Interfaz	5	4	0	5
Biónica	6	2	5	5
Ergonomía, producto y significado - GEPS	6	7	10	3
Robótica de servicio y Diseño Industrial - GIROD	3	8	8	5
Escuela de Ingeniería de Sistemas e Informática				
Ingeniería Biomédica – GIIB	19	14	106	5
Sistemas y Tecnología de la Información - STI	10	9	40	6
Modelamiento y Simulación – SIMON	20	2	18	4
Escuela de Ingenierías Eléctrica, Electrónica y de Telecomunicaciones				
Control, Electrónica, Modelado y Simulación – CEMOS	10	18	40	4
Sistemas de Energía Eléctrica – GISEL	15	12	60	9

Fuente. GrupLAC

ANEXO 15. CARACTERIZACIÓN GRUPOS DE INVESTIGACIÓN

1. Definición de grupo de investigación científica y tecnológica[296]

"…Conjunto de personas que se reúnen para realizar investigación en una temática dada, formulan uno a varios problemas de su interés, trazan un plan estratégico de largo o mediano plazo para trabajar en él y producen unos resultados de conocimiento sobre el tema en cuestión. Un grupo existe siempre y cuando demuestre producción de resultados tangibles y verificables fruto de proyectos y de otras actividades de investigación convenientemente expresadas en un plan de acción (proyectos) debidamente formalizado".

Un grupo de investigación científica y tecnológica s define como un grupo de personas que interactúan para investigar y generar conjuntamente productos de conocimiento en uno o varios temas, de acuerdo con un plan de trabajo de mediano o largo plazo. Asimismo, un grupo es reconocido como tal, siempre y cuando demuestre continuamente resultados verificables fruto de proyectos y de otras actividades derivadas de su plan de trabajo, además de cumplir con los siguientes 8 requisitos:

- Estar registrado Plataforma ScienTI – Colombia en Colciencias
- Aval institucional
- Tener un mínimo de 2 integrantes
- Tener uno o más años de experiencia
- El líder del grupo deberá tener título de pregrado, maestría o doctorado
- Tener un proyecto de ID + I en ejecución
- Haber obtenido un (1) producto de nuevo conocimiento por año, durante los últimos tres años.

[296] Departamento Administrativo de Ciencia, Tecnología e Innovación - COLCIENCIAS

- Haber obtenido, durante los últimos tres años al menos dos productos que estén en las categorías de *Productos de Circulación e Impacto social o Productos de formación de recurso humano.*

2. Tipos de integrantes de un grupo de investigación

Tipo	Sub-tipo	Requisitos
INVESTIGADOR	Investigador Senior	Autor de al menos cinco productos de nuevo conocimiento en los últimos cinco años.
	Investigador Junior I	Con formación de doctorado finalizada. Asignación válida por dos años desde la obtención del grado de doctorado.
	Investigador Junior II	Con formación de maestría finalizada. Asignación válida por un año desde la obtención del grado de maestría.
INVESTIGADOR EN FORMACIÓN	Estudiante de Doctorado	En formación de Doctorado. Asignación válida durante máximo 8 años desde que inicia el proceso de formación.
	Estudiante de Maestría	En formación de maestría. Asignación válida durante máximo 4 años desde que inicia el proceso de formación.
	Jóvenes investigadores	Con formación de pregrado finalizada, integrante de un grupo de investigación y que hace parte de un proyecto de investigación del grupo. Asignación válida por dos años desde la obtención del grado de pregrado.
PERSONAL DE APOYO	Estudiante de Pregrado	En formación de pregrado. Asignación válida durante máximo 8 años desde que inicia el proceso de formación.
	Integrante Vinculado	Vinculado a un grupo de investigación y que no cumple con ninguna de las anteriores definiciones.

3. Tipología de Productos Resultados de Investigación e Innovación

***Producción intelectual*:** "Es el resultado de la actividad permanente de creación, innovación, comprobación de conocimientos y de las actividades que tengan como objetivo el desarrollo de la cultura, la ciencia, el arte y la

tecnología y que realiza el profesor de la Universidad Industrial de Santander, para cumplir con su misión, en beneficio de su crecimiento intelectual y del fortalecimiento académico de la institución."[297] En documentos como el Decreto 1279, los acuerdos 031, 093 y 065 es común la utilización del término *productividad académica* como sinónimo de *producción intelectual*, pero para la definición de datos del sistema se recomienda la utilización del término *producción intelectual*.

***Producto*:** un producto es el material resultado de una labor o actividad en cualquier área de conocimiento, es una recopilación de información que puede ser susceptible de reconocimiento monetario por parte de la Universidad. Los términos *trabajo* y *obra* suelen ser usados por los usuarios como sinónimos de producto, pero se recomienda usar *producto* con el propósito de estandarizar la terminología usada durante el proceso de evaluación. Los productos se definen en tres grandes tipos y 15 subtipos:

Productos de Nuevo Conocimiento: corresponden a los productos que aportan nuevos avances en ciencia, tecnología y que son resultado de las actividades de investigación de los grupos.

Productos de Circulación e Impacto: productos que surgen de las actividades de aplicación y circulación del conocimiento generado por los grupos de investigación y que generan un impacto en la sociedad.

Productos de formación de recurso humano para la investigación: productos resultado del apoyo a la formación de recurso humano, que se hace visible en la generación de tesis y trabajos de grado, en la participación del grupo en el desarrollo de programas de maestría o doctorado y en el desarrollo de proyectos con componentes de formación en empresas y otras instituciones.

[297] Acuerdo No. 065 de 1994, Reglamento de evaluación de la producción intelectual, Consejo Superior, Universidad Industrial de Santander.

Número del Tipo	Nombre del Tipo – Subtipo
PRODUCTOS DE NUEVO CONOCIMIENTO	
1	Artículos de investigación A
2	Artículos de investigación B
3	Libros de Investigación
4	Capítulos de libros de investigación
5	Productos tecnológicos patentados o en proceso de solicitud de patente
6	Productos tecnológicos certificados o validados
PRODUCTOS DE CIRCULACIÓN E IMPACTO SOCIAL	
7	Productos Empresariales
8	Productos de Innovación Social
9	Normas Técnicas
10	Productos de Apropiación Social del Conocimiento
11	Difusión de Conocimiento
PRODUCTOS DE FORMACIÓN DE RECURSO HUMANO PARA LA INVESTIGACIÓN	
12	Tesis de Doctorado
13	Tesis de Maestría
14	Trabajos de Grado y Proyectos de Formación en ID+i
15	Apoyo a Programas de Formación

ANEXO 16. CARACTERIZACIÓN GRUPO INNOTEC

INNOTEC, es un centro de investigación creado por el Consejo Superior de la Universidad Industrial de Santander por Acuerdo Nº 040 del 6 de junio de 1995, adscrito a la Escuela de Estudios Industriales y Empresariales. INNOTEC desarrolla una gama de actividades propias del quehacer universitario: docencia, investigación, prestación de servicios tecnológicos y difusión.

El grupo de investigación se encuentra liderado actualmente por el Doctor Jaime Alberto Camacho Pico, ex rector de la Universidad Industrial de Santander.

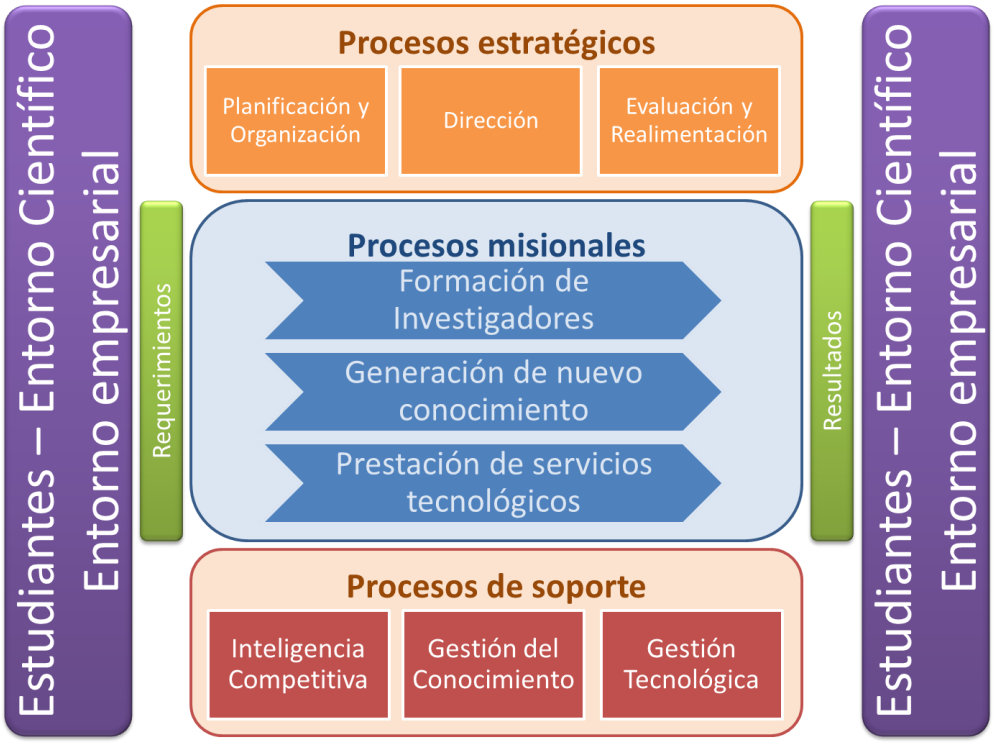
1. MISIÓN

INNOTEC tiene como misión realizar estudios y fomentar la gestión de la innovación tecnológica y la búsqueda de mecanismos de transferencia entre la Universidad con el sector productivo para reforzar el papel de la UIS como uno de los núcleos motores de la innovación regional y nacional; adicionalmente auxiliar el fortalecimiento de la investigación aplicada y la rápida estructuración de paquetes tecnológicos y su transferencia al sector productivo. En la Figura 32 se muestra el mapa de procesos del grupo.

2. VISIÓN

INNOTEC será líder en el impulso de la gestión de la innovación y la tecnología en la Universidad Industrial de Santander, mediante la coordinación de esfuerzos interdisciplinarios entre los diferentes grupos de la Universidad y de la región. Asimismo, será generador de nuevos conocimientos.

Figura 32. Mapa de procesos de INNOTEC 2011



Fuente. Msc. Gerardo Angulo

3. EXPERIENCIA Y TRAYECTORIA

Actualmente se están desarrollando los proyectos Plan maestro del parque tecnológico de Guatiguará: PTG, SUMA – ALFA3, Impactos de innovación, Definición de áreas estratégicas de investigación y una Red de buenas prácticas de innovación. El grupo tiene dentro de sus responsabilidades el manejo de las áreas de gestión tecnológica en los programas pregrado, maestría y doctorado.

En el tiempo de trayectoria del grupo se han dirigido más de 100 tesis de pregrado así como tesis de especialización, maestría y doctorado. El grupo cuenta con dos espacios físicos, el primero dedicado al observatorio de prospectiva tecnológica industrial y el segundo dedicado a consolidar las líneas de innovación y apropiación, y determinar la capacidad de absorción de las mismas. La primera

instalación se encuentra ubicada en el sótano de la perla, cuenta con un área total de 60m2, con 12 puestos de trabajo ocupados por estudiantes de maestría y doctorado dedicados al apoyo de la definición y seguimiento de las líneas estratégicas de investigación de la Universidad, como parte del proyecto del PTG, esta acción es continua en el tiempo.

4. OBJETIVOS

Objetivo principal

Realizar estudios y fomentar la gestión de la innovación tecnológica para reforzar el papel de la UIS como uno de los núcleos motores de la innovación regional y nacional; adicionalmente, auxiliar el fortalecimiento de la investigación aplicada y la rápida estructuración de paquetes tecnológicos y su transferencia al sector productivo.

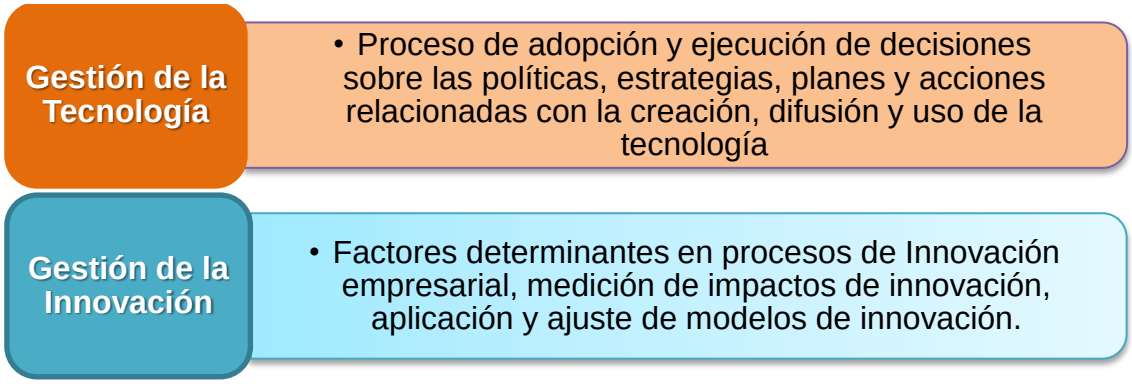
Objetivos específicos

- En el ámbito de la investigación sobre Política y Gestión de la Ciencia y la Tecnología: realizar actividades de investigación académica para generar y difundir conocimientos en el medio universitario, industrial y gubernamental, sobre política, prospectiva, economía, sociología y administración de la Ciencia y la Tecnología.
- En el ámbito del entrenamiento en Innovación Tecnológica: formar recursos humanos y capacitar personal ya formado, tanto a nivel de estudiantes como de investigadores, profesionales y funcionarios universitarios y gubernamentales, en distintos aspectos de política, prospectiva, economía y administración de la Ciencia y la Tecnología.
- En el ámbito de la Transferencia de Tecnología: agilizar la vinculación entre la capacidad tecnológica de las diversas dependencias UIS y el Sector Productivo, captando sus demandas, colaborando en la correcta estructuración

de paquetes de tecnología, adecuando la organización interna y difundiendo el potencial tecnológico de la UIS.

- En el ámbito de la Concertación de Proyectos y Programas: diagnóstico permanente de líneas estratégicas de investigación tecnológica e identificación, concertación y gestión de proyectos tecnológicos prioritarios para el país y la región, que involucren la participación de diversas dependencias universitarias y extrauniversitarias.
- En el ámbito de la Asesoría en Gestión de la Innovación: presta servicios a dependencias de la propia universidad, de otras universidades, al gobierno y al sector productivo, en materia de planeación estratégica, administración de la tecnología y organización de la investigación.
- En el ámbito de la normatividad: colabora con el Comité de Propiedad Intelectual de la UIS en la definición de políticas universitarias en materia de propiedad industrial y resolución de conflictos de intereses derivados de la interacción con el sector productivo, así como en materia de evaluación del trabajo tecnológico y la tramitación de patentes
- En el ámbito del financiamiento: obtención de recursos para la adecuada estructuración de paquetes de tecnología, con el fin de fomentar la interdisciplinariedad y poder lograr una transferencia al sector productivo.
- En el ámbito de la competitividad empresarial: Realización de estudios sectoriales alrededor de la gestión e innovación tecnológica y social.

5. LÍNEAS DE INVESTIGACIÓN



6. LÍNEAS DE INTERÉS

Gestión de la tecnología	Gestión de la Innovación
• Prospectiva y vigilancia tecnológica • Planificación del desarrollo tecnológico. • Valoración y negociación de tecnologías. • Gestión de proyectos de I+D.	• Triple Hélice • Políticas CTI • SRI • Propiedad Intelectual • Modelos de Gestión del conocimiento • Capacidades de Innovación

7. LÍNEAS DE INVESTIGACIÓN CONEXAS

8. FORTALEZAS

- Creación de modelos de gestión de conocimiento y gestión tecnológica.
- Medición de impactos en procesos innovativos.
- Desarrollo de estrategias de competitividad tecnológica e industrial.
- Dinámica de ingreso e interés de participación

- Creación de modelos de Transferencia Tecnológica.
- Creación y aplicación de modelos de Innovación Tecnológica.
- Asesoría para la Innovación y Desarrollo Tecnológico.
- Aplicación de la metodología de Prospectiva Tecnológica.
- Capacitación en procesos de gestión tecnológica y gestión de conocimiento.
- Grupo humano multidisciplinario especialistas en gestión tecnológica, vigilancia y prospectiva tecnológica, gestión de la innovación y minería de datos.
- Suscripción a las mejores bases de datos e internacionales
- Experiencia en cooperación internacional
- Altas capacidades técnicas y metodologías propias de investigación

9. INVESTIGADORES PRINCIPALES

Nombre del Investigador	UAA a la que pertenece	Modalidad de Vinculación	Formación Académica
Jaime Alberto Camacho Pico	Escuela de Estudios Industriales y Empresariales	Profesor Planta	Doctorado en Ingeniería Industrial de la Universidad Politécnica de Cataluña - UCP, España (2000)
Luis Eduardo Becerra Árdila	Vicerrectoría Administrativa	Profesor Planta	Magister en Administración con énfasis en Gestión del Conocimiento del Instituto Tecnológico de Estudios Superiores de Monterrey, México (2002)
Piedad Arenas Díaz	Escuela de Estudios Industriales y Empresariales	Profesor Planta	Magister en Política y Gestión de la Ciencia y la tecnología de la Universidad de Buenos Aires, Argentina (2011)
Edna Rocío Bravo Ibarra	Escuela de Estudios Industriales y Empresariales	Profesor Planta	Doctorado en Administración de Empresas (2010)
Mireya Astrid Jaime Arias	Vicerrectoría de Investigación y Extensión	Administrativo Planta	Doctorado en Ingeniería Industrial con énfasis en gestión de conocimientos (2005)

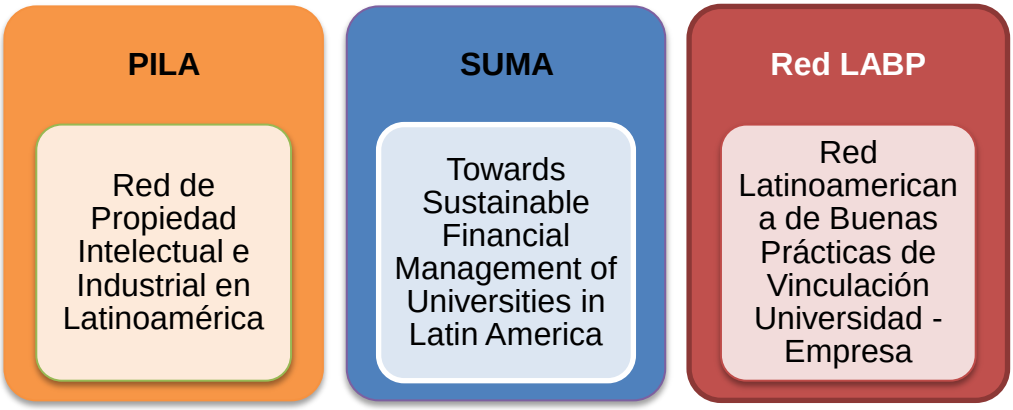
10. EQUIPO DE TRABAJO

Actualmente el equipo de trabajo está conformado por:

Tipo de Vinculación	No. de personas
Investigadores:	5
Estudiantes de Doctorado	4
Estudiantes de Maestría:	12
Estudiantes de pregrado:	13

11. INFRAESTRUCTURA TECNOLÓGICA INNOTEC

11.1 Membresías a sociedades científicas, redes científicas y tecnológicas y otras



11.2 Software especializado

NOMBRE	CARACTERÍSTICAS
SPSS	Statistical Package for the Social Sciences (SPSS) es un programa estadístico informático muy usado en las ciencias sociales y las empresas de investigación de mercado.
STATGRAPHICS	STATGRAPHICS es una potente herramienta de análisis de datos que combina una amplia gama de procedimientos analíticos con extraordinarios gráficos interactivos para proporcionar un entorno integrado de análisis que puede ser aplicado en cada una de las fases de un proyecto.

Office Profesional	Office Professional es un completo paquete de software y soporte que le ayude a poner en marcha y desarrollar los objetivos de negocio.
Matheo Patent	Matheo Patent es un software diseñado para buscar, recuperar y analizar los datos de patentes de la USPTO y servicios de la Oficina Europea de Patentes ESPACENET.
Matheo Analyzer	Matheo Analyzer a partir de datos estructurados en un campo relevante de la tecnología, crea información estratégica a partir de grandes volúmenes de datos. Es un mecanismo de apoyo para la fabricación de tableros de control, la cartografía, la síntesis y los indicadores generados a partir de grandes conjuntos de información.
Matheo Web	Herramientas de análisis estadístico y un motor de búsqueda interno, incluido por defecto en el software, permiten el análisis y la visualización de la información básica para la investigación.
GoldFire Innovator	Software para la gestión, optimización y aceleración del proceso de innovación : "un proceso Estructurado, Predecible y Reutilizable"
Vantagepoint	Herramienta de minería de datos para el descubrimiento de conocimiento en resultados de búsqueda en bases de datos de literatura y patentes
NVIVO	Es un software de análisis cualitativo de datos de QSR International que ayuda a explorar, analizar y comprender la información de documentos, archivos PDF, videos, encuestas, fotografías y archivos de audio. El programa ayuda a obtener rápidamente respuestas, justificar conclusiones y tomar decisiones fundamentadas.
MAXQDA	Es software diseñado para el análisis cualitativo de datos de texto y multimedia en el ámbito académico, científico y de negocios. Es también una herramienta para desarrollar teorías así como para probar conclusiones teóricas del análisis.
MIC MAC	Software para realizar análisis estructural de una reflexión colectiva, obteniendo como resultado las principales variables influyentes y dependientes.
Mactor	Herramienta para el Análisis del juego de actores.

Smic Prob-Expert	"Método de impactos cruzados" que intenta evaluar los cambios en las probabilidades de un conjunto de acontecimientos como consecuencia de la realización de uno de ellos.
Mulitpol	Pretende comparar diferentes acciones o soluciones a un problema en función de criterios y de políticas múltiples.
LIPSOR	Son herramientas utilizadas para prospectiva, gestión estratégica y organización.
3IE-EPITA	

11.3 Bases de datos especializadas

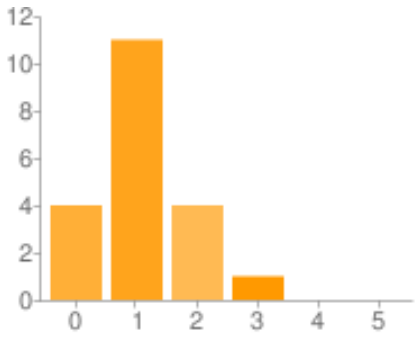
IEEE Cubre principalmente áreas del conocimiento en Ingeniería Eléctrica, Electrónica, Sistemas y Telecomunicaciones	**Zentralblat** Base de datos referencial en el área de matemáticas, que contiene alrededor de 1.800.000 referencias de más de 2300 trabajos
HW Wilson Ciencias Básicas e Ingeniería y Ciencias Sociales	**Economic and Business Report** Base de datos en línea especializada para el área de economía e información económica de países de América latina
ASTM Desarrolla normas aplicables a los materiales, productos, sistemas y servicios	**EbscoHost** Incluye: Library Information Science & Technology Abstracts, ERIC, MEDLINE, Economía y Negocios, GeoREF, DynaMed, Newspaper Source, MasterFILE Premier, Medic Latina, Business Source Premier, Academic Search
MathSciNet Base de datos referencial en el área de Matemáticas y afines	**E-Libro** Más de 20.000 libros en Texto Completo en todas las áreas

Web of SCIENCE Acceso referencial a información científica internacional	**SME SOURCE (Society of Manufacturing Engineers)** Base de datos sobre publicaciones en Ingeniería de manufacturación

ANEXO 17. ANÁLISIS DEL NIVEL DE EFECTIVIDAD DE CONTROLES

- **Documento de política de seguridad de la información**

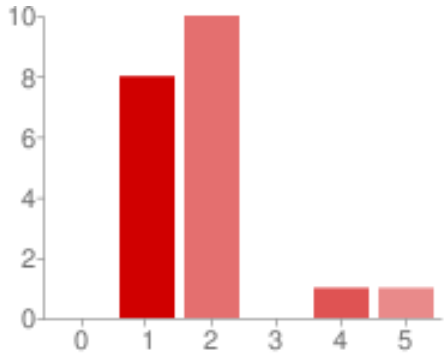
Nivel	Frecuencia	Porcentaje
0	**4**	20%
1	**11**	55%
2	**4**	20%
3	**1**	5%
4	**0**	0%
5	**0**	0%



Actualmente, en el grupo de investigación INNOTEC, no existe una política de seguridad de la información documentada y actualizada. En el cuestionario exploratorio, la mayoría de personas seleccionó el nivel 1 para este control, dicha respuesta podría estar influenciada por factores como el hecho de que ya se ha comentado en las reuniones del grupo la importancia de contar con unos lineamientos de seguridad de la información que sean comunicados a todos los integrantes. Por tanto, existe una conciencia de la necesidad del control, y hasta ahora se va a comenzar el esfuerzo formal de implementación. El presente proyecto hace parte del esfuerzo de la dirección por implementar la política de seguridad de la información en el grupo.

- **Compromiso de la dirección con la seguridad de la información**

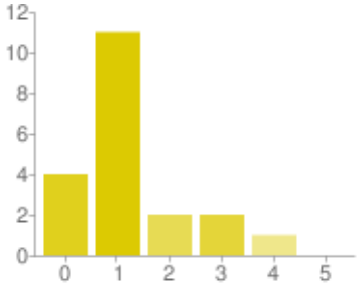
Nivel	Frecuencia	Porcentaje
0	**0**	0%
1	**8**	40%
2	**10**	50%
3	**0**	0%
4	**1**	5%
5	**1**	5%



El 50% de los encuestados percibe que se han hecho algunos esfuerzos por implementar el control. La media y la moda son iguales.

- **Asignación de responsabilidades**

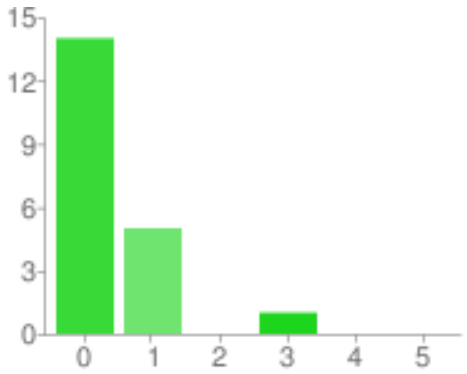
Nivel	Frecuencia	Porcentaje
0	**4**	20%
1	**11**	55%
2	**2**	10%
3	**2**	10%
4	**1**	5%
5	**0**	0%



La mayoría de las personas encuestadas percibió la asignación de responsabilidades como aplicable y necesaria, pero consideran que aún no se han hecho esfuerzos formales de aplicación del control. Generalmente la responsabilidad asignada a las personas radica en los compromisos relacionados con su proyecto de investigación, sea de pregrado o posgrado. Por otro lado, las responsabilidades relacionadas con la seguridad de la información no están claras, y por tanto las personas actúan de acuerdo a su criterio personal.

- **Revisión independiente**

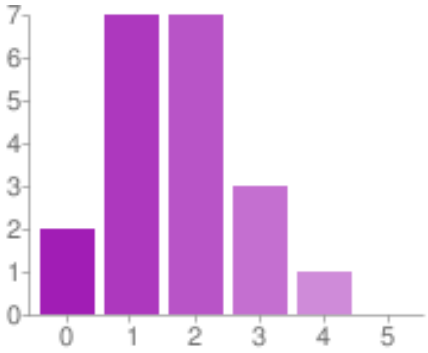
Nivel	Frecuencia	Porcentaje
0	**14**	70%
1	**5**	25%
2	**0**	0%
3	**1**	5%
4	**0**	0%
5	**0**	0%



Este es un control cuya necesidad aún o se ha detectado en el grupo. La razón es que una revisión independiente debería realizarse después de tener una política, controles y procedimientos implementados, de manera que se pudiera obtener retroalimentación de un experto sobre cómo mejorar la gestión del riesgo. Es posible que más adelante, cuando se tenga el modelo de gestión, sea evidente la necesidad de este control.

- **Identificación de los riesgos relacionados con las partes externas**

Nivel	Frecuencia	Porcentaje
0	**2**	10%
1	**7**	35%
2	**7**	35%
3	**3**	15%
4	**1**	5%
5	**0**	0%

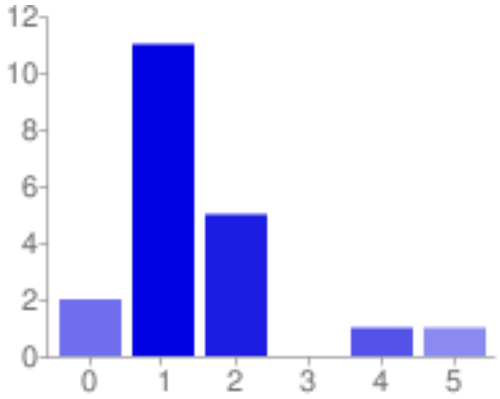


En el grupo se han trabajado varios proyectos con entidades externas a la universidad como la gobernación de Santander, la Unión Europea, el Ministerio de Educación, Colciencias, el Observatorio de Ciencia y Tecnología, y otras

universidades, por lo cual ya hay algunas prácticas implementadas para gestionar la seguridad de la información en proyectos interinstitucionales.

- **Directrices de clasificación**

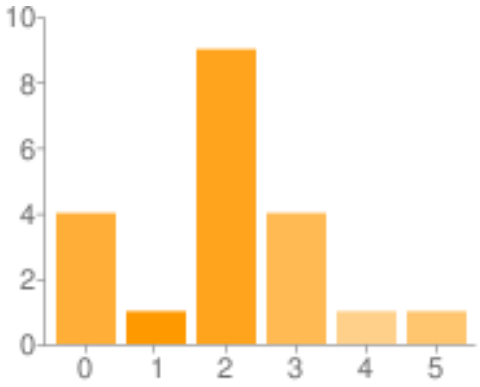
Nivel	Frecuencia	Porcentaje
0	**2**	10%
1	**11**	55%
2	**5**	25%
3	**0**	0%
4	**1**	5%
5	**1**	5%



Se ha detectado la necesidad de clasificar la información con el fin de controlar y de cierta manera restringir el acceso a la misma dependiendo del rol que desempeña cada persona y su vinculación con los diferentes proyectos de investigación. Solo unos pocos encuestados, 25%, perciben que se han hecho algunos esfuerzos para implementar este control.

- **Investigación de antecedentes**

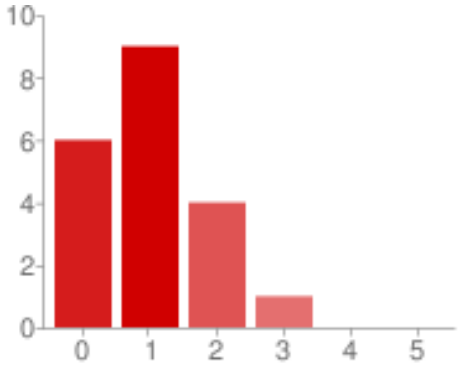
Nivel	Frecuencia	Porcentaje
0	**4**	20%
1	**1**	5%
2	**9**	45%
3	**4**	20%
4	**1**	5%
5	1	5%



Las respuestas se encuentran bastante fraccionadas, y no se podría hablar de una mayoría absoluta. Una posible razón para esta situación es que debido a la falta de lineamientos generales para el grupo, cada quien contesta de acuerdo a su experiencia, es decir, a quien se le haya realizado un chequeo de antecedentes (ya sea académicos o disciplinarios) en su proceso de ingreso al grupo, contestará que el control esta efectivamente implementado, mientras que la persona que no haya pasado por ese proceso contestará lo contrario.

- **Concienciación, formación y capacitación en seguridad de la información**

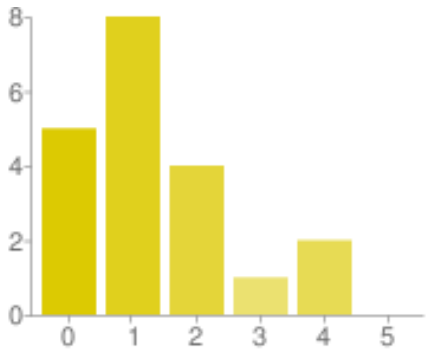
Nivel	Frecuencia	Porcentaje
0	**6**	30%
1	**9**	45%
2	**4**	20%
3	**1**	5%
4	**0**	0%
5	**0**	0%



De acuerdo con la gráfica se observa una clara inclinación de las respuestas hacia la zona izquierda donde las opciones corresponden a la poca conciencia, y a la falta de acción. La realidad es que no se ha realizado ningún programa de sensibilización, formación ni capacitación sobre temas de seguridad de la información en el grupo de investigación. La única capacitación grupal y virtual realizada el año anterior trato la temática de propiedad intelectual (derechos de autor, propiedad industrial y otras formas de propiedad intelectual)

- **Retiro de los derechos de acceso**

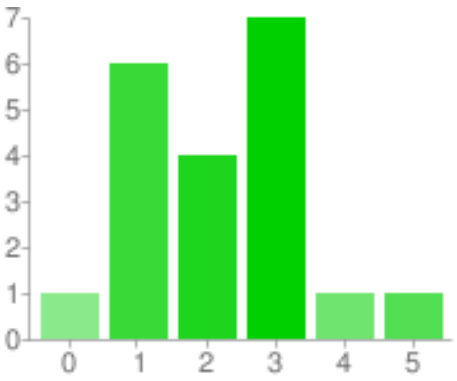
Nivel	Frecuencia	Porcentaje
0	**5**	25%
1	**8**	40%
2	**4**	20%
3	**1**	5%
4	**2**	10%
5	**0**	0%



En esta pregunta, las respuestas se distribuyeron en los 6 niveles de efectividad del control, con una inclinación hacia la izquierda, es decir, la percepción de las personas es que el control no esta implementado completamente. Por la variabilidad de las respuestas se observa la falta de claridad frente al asunto.

- **Protección contra las amenazas del entorno**

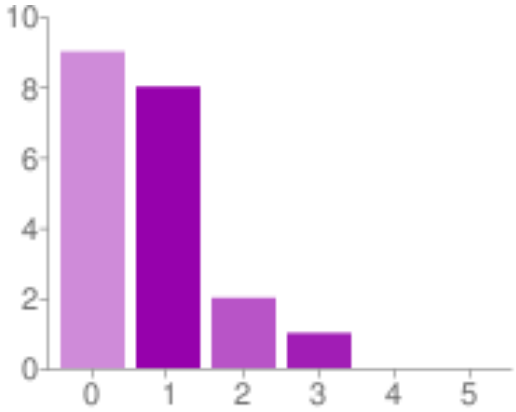
Nivel	Frecuencia	Porcentaje
0	**1**	5%
1	**6**	30%
2	**4**	20%
3	**7**	35%
4	**1**	5%
5	**1**	5%



En este caso, las respuestas pueden estar condicionadas a la ubicación de las instalaciones físicas. En este momento, el grupo de investigación trabaja en diferentes oficinas dentro de la universidad, y el nivel de protección varía en cada una de ellas.

- **Documentación de los procedimientos de operación**

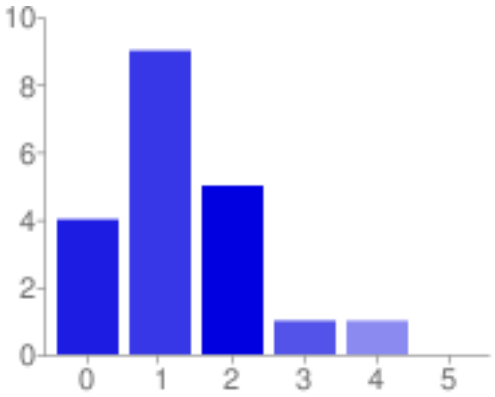
Nivel	Frecuencia	Porcentaje
0	**9**	45%
1	**8**	40%
2	**2**	10%
3	**1**	5%
4	**0**	0%
5	**0**	0%



El 85% de las personas reconocen que los procedimientos de operación relacionados con seguridad de la información no están documentados en el grupo.

- **Segregación de los deberes**

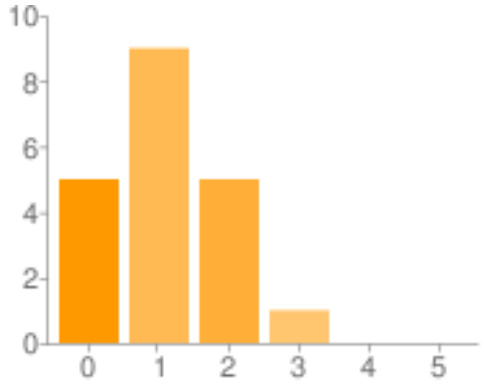
Nivel	Frecuencia	Porcentaje
0	**4**	20%
1	**9**	45%
2	**5**	25%
3	**1**	5%
4	**1**	5%
5	**0**	0%



La percepción del control se encuentra aprox. en el nivel 1, es decir se han hecho algunos esfuerzos por implementarlo.

- **Aceptación del sistema**

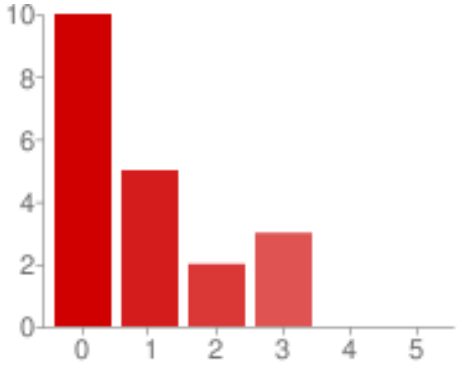
Nivel	Frecuencia	Porcentaje
0	**5**	25%
1	**9**	45%
2	**5**	25%
3	**1**	5%
4	**0**	0%
5	**0**	0%



Al igual que en el caso anterior, la percepción que tienen las personas que contestaron el cuestionario, es que se han hecho algunos esfuerzos por implementar el control, esto es coherente con la realidad puesto que la adquisición de nuevo software especializado requiere de un profundo análisis por parte de la dirección del grupo.

- **Controles contra el código malicioso**

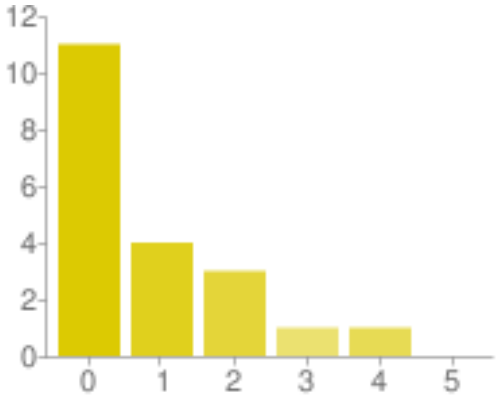
Este control se relaciona altamente con el uso de internet, el cual es indispensable para acceder a las bases de datos de publicaciones y patentes. La mitad de los encuestados perciben que no hay conciencia de la necesidad de este control en el grupo, a pesar de ser una amenaza latente para los sistemas de cómputo si estos no están adecuadamente protegidos.



Nivel	Frecuencia	Porcentaje
0	**10**	50%
1	**5**	25%
2	**2**	10%
3	**3**	15%
4	**0**	0%
5	**0**	0%

- **Gestión de los medios removibles**

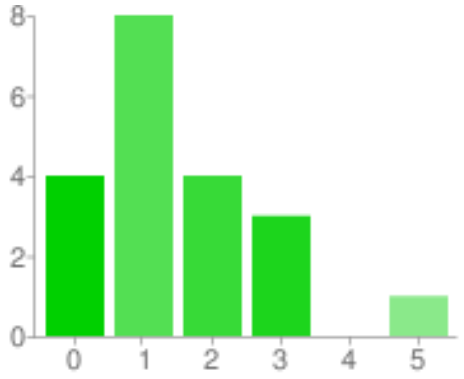
Nivel	Frecuencia	Porcentaje
0	**11**	55%
1	**4**	20%
2	**3**	15%
3	**1**	5%
4	**1**	5%
5	**0**	0%



Este control se refiere al manejo (gestión) de los medios de almacenamiento y transporte como USBs, CDs, DVDs y discos duros extraíbles. El nivel de efectividad del control está muy cercano al cero, pues cada quien hace uso de estos dispositivos de manera individual y no hay lineamientos sobre cómo gestionarlos.

- **Procedimientos para el manejo de información**

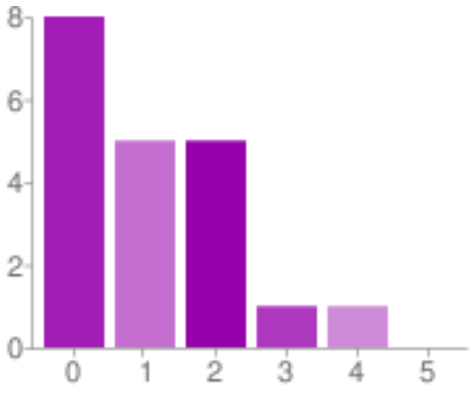
Nivel	Frecuencia	Porcentaje
0	**4**	20%
1	**8**	40%
2	**4**	20%
3	**3**	15%
4	**0**	0%
5	**1**	5%



Las respuestas se reparten entre los primeros cuatro niveles (0 al 3), por lo que se observa falta de claridad en cuanto a lo que se considera un procedimiento de manejo de información y si este existe o no en el grupo.

- **Política de control de acceso**

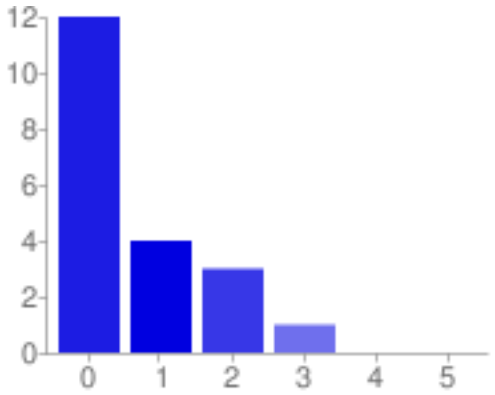
Nivel	Frecuencia	Porcentaje
0	**8**	40%
1	**5**	25%
2	**5**	25%
3	**1**	5%
4	**1**	5%
5	**0**	0%



Los resultados demuestran que no existe una política clara y documentada de acceso lógico a la información. Sin embargo algunos datos aislados indican la percepción de que el control si existe, puede ser que esto se deba a que en algún proyecto específico se haya aplicado pero no de manera general para el grupo.

- **Registro del usuario**

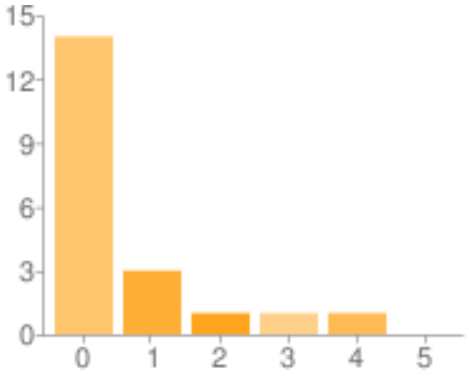
Nivel	Frecuencia	Porcentaje
0	**12**	60%
1	**4**	20%
2	**3**	15%
3	**1**	5%
4	**0**	0%
5	**0**	0%



El 60% de los encuestados coincide en que no se ha detectado la necesidad del control. Esto se explica en que cada investigador tiene su computador personal en el que se maneja la información. Los equipos utilizados en la sala grupal (bunker) cada uno tienen usuario administrador e invitado.

- **Teletrabajo**

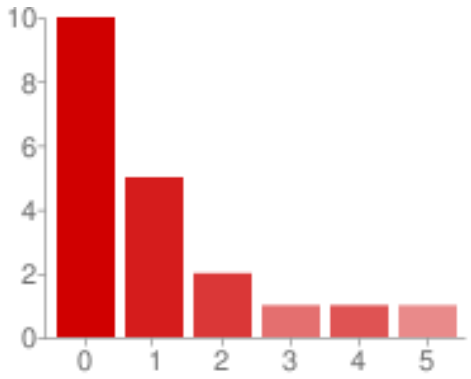
Nivel	Frecuencia	Porcentaje
0	**14**	70%
1	**3**	15%
2	**1**	5%
3	**1**	5%
4	**1**	5%
5	**0**	0%



Siendo el teletrabajo una de las características más relevantes del grupo INNOTEC, ya que sus miembros se encuentran ubicados en diferentes lugares de la universidad, aún no se controla la información que se maneja en este tipo de trabajo.

- **Análisis y especificación de los requerimientos de seguridad**

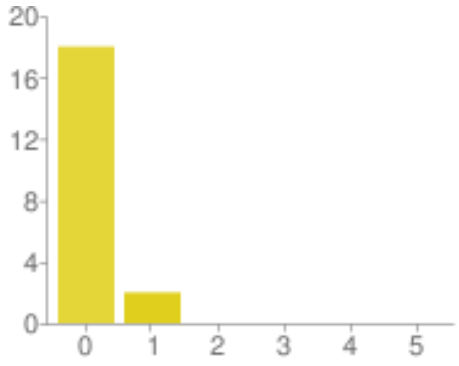
Nivel	Frecuencia	Porcentaje
0	**10**	50%
1	**5**	25%
2	**2**	10%
3	**1**	5%
4	**1**	5%
5	**1**	5%



El software utilizado por el grupo consiste en: Matheo Patent, Web y Analyzer, Vantage Point, Goldfire Innovator, Mic Mac, Mactor, SPSS, Statgraphics, Office Profesional, NVIVO, MAXQDA, Smic Prob- Expert, y Mulitpol. Según las observaciones de los miembros no se han tenido en cuenta consideraciones de seguridad de la información para su instalación y uso en el grupo.

- **Política sobre el uso de controles criptográficos**

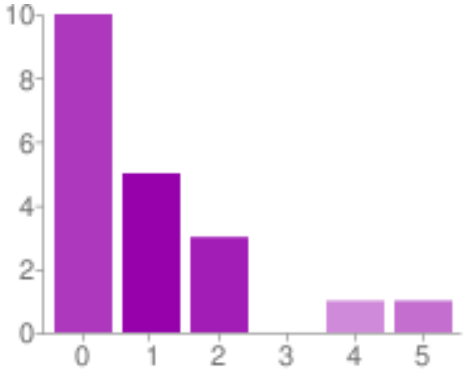
Nivel	Frecuencia	Porcentaje
0	**18**	90%
1	**2**	10%
2	**0**	0%
3	**0**	0%
4	**0**	0%
5	**0**	0%



Este control es netamente técnico por lo cual aún no se ha detectado su necesidad dentro del grupo. Se le da prioridad a los controles de gestión pues son aquellos que proporcionan direccionamiento en las actividades de los investigadores.

- **Control de vulnerabilidades técnicas**

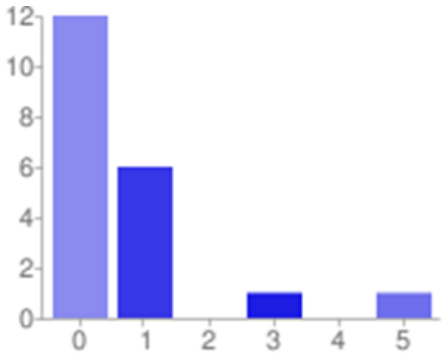
Nivel	Frecuencia	Porcentaje
0	**10**	50%
1	**5**	25%
2	**3**	15%
3	**0**	0%
4	**1**	5%
5	**1**	5%



Este control es de características técnicas, es posible que por esta razón no haya una clara identificación de su necesidad de implementación.

- **Reporte de eventualidades en la seguridad de la información**

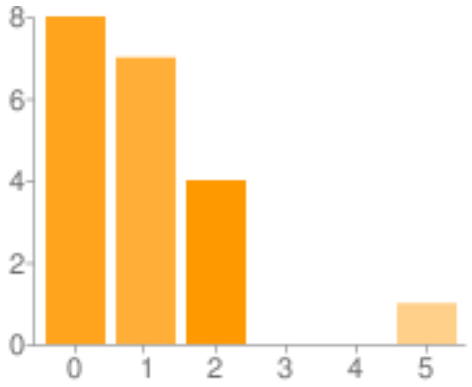
Nivel	Frecuencia	Porcentaje
0	**12**	60%
1	**6**	30%
2	**0**	0%
3	**1**	5%
4	**0**	0%
5	**1**	5%



No se tiene registro de eventos o brechas de seguridad de la información por lo cual los miembros perciben que no es necesario reportar eventualidades.

- **Seguridad de la información incluida en el plan continuidad de los procesos**

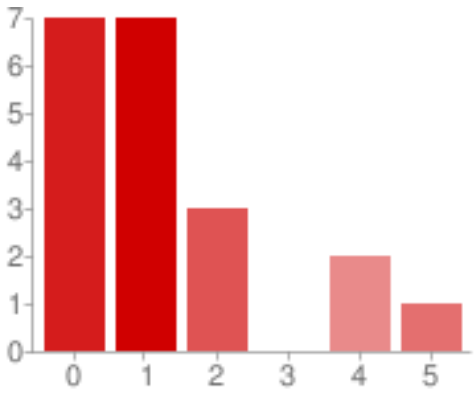
Nivel	Frecuencia	Porcentaje
0	**8**	40%
1	**7**	35%
2	**4**	20%
3	**0**	0%
4	**0**	0%
5	**1**	5%



Para que este control sea aplicable debe existir un plan de continuidad de los procesos de investigación.

- **Identificación de la legislación ajustable**

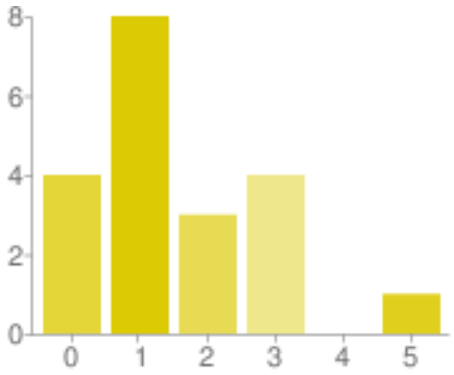
Nivel	Frecuencia	Porcentaje
0	**7**	35%
1	**7**	35%
2	**3**	15%
3	**0**	0%
4	**2**	10%
5	**1**	5%



En esta pregunta las respuestas estuvieron bastante divididas, posiblemente debido a que no se especifico que tipo de legislación es ajustable a un grupo de investigación. Algunos reglamentos aplicables son: Estatutos de investigación UIS, reglamento de propiedad intelectual UIS, reglamento académico de pregrado y posgrado, entre otros.

- **Protección de datos y privacidad de la información personal**

Nivel	Frecuencia	Porcentaje
0	**4**	20%
1	**8**	40%
2	**3**	15%
3	**4**	20%
4	**0**	0%
5	**1**	5%



De nuevo, las opiniones se encuentran divididas, entre los cuatro primeros niveles (0 al 3). Se podría decir que cada miembro tiene la responsabilidad de proteger su información personal, y la única información pública es la que aparece en la página GroupLac.

ANEXO 18. CUESTIONARIO NIVEL DE EFECTIVIDAD DE CONTROLES

El propósito de este cuestionario es establecer las condiciones actuales en materia de seguridad de la información dentro del grupo de investigación INNOTEC, a fin de detectar fortalezas y debilidades que sirvan como base para la creación de un modelo de gestión de seguridad del capital intelectual, que fortalezca la actividad investigativa de la UIS. Recuerde que sus repuestas son confidenciales y no serán evaluadas como buenas o malas. De antemano agradecemos su sincera participación.

* Required

INFORMACIÓN PERSONAL

Nombre completo *

Tipo de vinculación con el grupo *

Lea detenidamente la descripción de cada control y seleccione el nivel en el que se encuentra el grupo de investigación de acuerdo a la siguiente tabla

0 - El control es aplicable pero no ha se ha reconocido la necesidad de implementarlo. 1- Existe conciencia, pero no hay acción. No existe un esfuerzo formal de implementación. 2- Parcialmente implementado. Se reconoce la aplicabilidad de este control y se han hecho algunos intentos de implementación. 3- Control implementado. Se revisa por lo menos una vez al año, pero el proceso y los resultados no siempre se documentan. 4 - Control gestionado. Se tienen políticas y procedimientos documentados. El control se revisa de manera regular, y el proceso y los resultados se documentan adecuadamente. 5 - Comprensible. Alto nivel de consciencia sobre las responsabilidades con este control. Se revisa continuamente y los resultados se documentan completamente.

Documento de política de seguridad de la información *Es un documento de alto nivel, que define los objetivos, intenciones y prioridades de la organización

0	1	2	3	4	5
○	○	○	○	○	○

Compromiso de la dirección con la seguridad de la información *Apoyo de la dirección a través de una dirección clara, compromiso demostrado, asignación de recursos

0	1	2	3	4	5
○	○	○	○	○	○

Asignación de responsabilidades relativas a la seguridad de la información *Todas las responsabilidades de la seguridad de la información están claramente definidas.

0	1	2	3	4	5
○	○	○	○	○	○

Revisión independiente de la seguridad de la información *Un ente externo revisa periódicamente los controles y procedimientos para manejar la seguridad de la información.

0	1	2	3	4	5
○	○	○	○	○	○

Identificación de los riesgos relacionados con partes externas *Se identifican los riesgos para la información que se originan por la relación con partes externas; y se implementan controles adecuados.

0	1	2	3	4	5
○	○	○	○	○	○

Directrices de clasificación *La información está clasificada en términos de su valor, requerimientos legales, y confidencialidad

0	1	2	3	4	5
○	○	○	○	○	○

Investigación de antecedentes *Se verifican antecedentes de todos los candidatos, en concordancia con lo perfiles académicos requeridos, y las leyes, regulaciones y ética relevantes.

0	1	2	3	4	5
○	○	○	○	○	○

Concienciación, formación y capacitación en seguridad de la información *Todos los integrantes reciben una adecuada capacitación y actualizaciones regulares sobre las políticas y procedimientos de seguridad de la información

0	1	2	3	4	5
○	○	○	○	○	○

Retiro de los derechos de acceso *Los derechos de acceso a la información y los medios de procesamiento de información son retirados a la terminación de su vinculación con el grupo, o son reajustados según los cambios de roles

0	1	2	3	4	5
○	○	○	○	○	○

Protección contra las amenazas del entorno *Se aplica protección física contra daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de amenazas (naturales y humanas)

0	1	2	3	4	5
○	○	○	○	○	○

Documentación de los procedimientos de operación. *Los procedimientos de operación (relacionados con seguridad de la información) están documentados, y a disposición de todos los usuarios que los necesiten.

0	1	2	3	4	5
○	○	○	○	○	○

Segregación de los deberes *Los deberes y áreas de responsabilidad están segregados para reducir las oportunidades de una modificación no-autorizada o mal uso de los activos de información

0	1	2	3	4	5
○	○	○	○	○	○

Aceptación del sistema *Están establecidas criterios y pruebas para aceptar los sistemas de información nuevos, actualizaciones o versiones nuevas.

0	1	2	3	4	5
○	○	○	○	○	○

Controles contra el código malicioso *Existen controles y procedimientos de detección, prevención y recuperación para proteger contra códigos maliciosos.

0	1	2	3	4	5
○	○	○	○	○	○

Gestión de los medios removibles *Exixten procedimientos para la gestión de los medios removibles (usb, discos duros, cds, etc)

0	1	2	3	4	5

Procedimientos para el manejo de información *Existen procedimientos para el manejo y almacenamiento de información a fin de protegerla de una divulgación no-autorizada o mal uso

0 1 2 3 4 5

Política de control de acceso *Existe una política de control de acceso, documentada y revisada, con base en los requerimientos comerciales y de seguridad para el acceso a la información

0 1 2 3 4 5

Registro del usuario *Existe un procedimiento formal para la creación y eliminación de cuentas de usuario que otorguen y revoquen el acceso a todos los sistemas y servicios de información

0 1 2 3 4 5

Teletrabajo *Se ha desarrollado e implementado una política, planes operacionales y procedimientos para las actividades de tele-trabajo (trabajo a distancia)

0 1 2 3 4 5

Análisis y especificación de los requerimientos de seguridad *Los requerimientos (técnicos y comerciales) para los sistemas de información tienen en cuenta los controles de seguridad de la información

0 1 2 3 4 5

Política sobre el uso de controles criptográficos *Existe una política sobre el uso de controles criptográficos para proteger la información.

0 1 2 3 4 5

○	○	○	○	○	○

Control de las vulnerabilidades técnicas *Se obtiene oportunamente la información sobre las vulnerabilidades técnicas de los sistemas de información que se están utilizando

0	1	2	3	4	5
○	○	○	○	○	○

Reporte de eventualidades en la seguridad de la información *Es claro que constituye un incidente de seguridad de la información y los procedimientos formales para reportarlo o notificarlo cuando se sospeche o identifique el evento.

0	1	2	3	4	5
○	○	○	○	○	○

Seguridad de la Información Incluida en el proceso de gestión de la continuidad empresarial *Se garantiza que la seguridad de la información sea incluida en el plan de continuidad del grupo de investigación.

0	1	2	3	4	5
○	○	○	○	○	○

Identificación de la Legislación ajustable *Tienen identificados los requerimientos estatutarios, reguladores y contractuales relevantes ajustables al grupo de investigación

0	1	2	3	4	5
○	○	○	○	○	○

Protección de datos y privacidad de la información personal *La información personal de los integrantes y partes externas del grupo está debidamente protegida de acuerdo con las leyes y reglamentos pertinentes

0	1	2	3	4	5
○	○	○	○	○	○

ANEXO 19. ACTORES QUE PARTICIPARON EN LA SEGUNDA ETAPA

NOMBRE	TIPO DE VINCULACIÓN	ACTIVIDAD
Marcela Contreras Cruz	Estudiante de pregrado	- Cuestionario de nivel de efectividad de control - Cuestionario evaluación de riesgos - Cuestionario de policy capturing
Luis Gabriel Ordoñez Cárdenas	Estudiante de pregrado	- Cuestionario de policy capturing
Leiner Lache Salcedo	Estudiante de pregrado	- Cuestionario de nivel de efectividad de control - Cuestionario evaluación de riesgos - Cuestionario de policy capturing
Efrén Romero Riaño	Estudiante de maestría	- Cuestionario de nivel de efectividad de control - Cuestionario evaluación de riesgos - Cuestionario de policy capturing
María Isabela Villamizar Ariza	Estudiante de pregrado	- Cuestionario evaluación de riesgos - Cuestionario de policy capturing
Liseth Dayana Carballido Mier	Estudiante de pregrado	Cuestionario de policy capturing
María Lucia Lizarazo Rivero	Estudiante de pregrado	Cuestionario de policy capturing
Ximena Serrano	Estudiante de maestría	- Cuestionario evaluación de riesgos Cuestionario de policy capturing
Katia Fernanda Reyes Arias	Estudiante de pregrado	- Cuestionario de nivel de efectividad de control - Cuestionario evaluación de riesgos - Cuestionario de policy capturing
Piedad Arenas Díaz	Profesor planta	- Cuestionario evaluación de riesgos Cuestionario de policy capturing

NOMBRE	TIPO DE VINCULACIÓN	ACTIVIDAD
María Fernanda Díaz Delgado	Estudiante de maestría	- Cuestionario de nivel de efectividad de control - Cuestionario de policy capturing
Cinthya Carolina Arias Manjarrez	Estudiante de pregrado	- Cuestionario de policy capturing
Jaime Alberto Camacho Pico	Profesor planta	- Cuestionario de policy capturing
Luis Eduardo Becerra Ardila	Profesor planta	- Cuestionario de nivel de efectividad de control - Cuestionario evaluación de riesgos - Cuestionario de policy capturing
Carolina Sarmiento Delgado	Estudiante de maestría	- Cuestionario de nivel de efectividad de control - Cuestionario evaluación de riesgos - Cuestionario de policy capturing
Dayanna Paola Cárdenas Caicedo	Estudiante de pregrado	- Cuestionario evaluación de riesgos - Cuestionario de policy capturing
Edna Rocío Bravo Ibarra	Profesor planta	- Cuestionario de nivel de efectividad de control - Cuestionario evaluación de riesgos - Cuestionario de policy capturing
Adriana León Arenas	Estudiante de pregrado	- Cuestionario de nivel de efectividad de control - Cuestionario evaluación de riesgos - Cuestionario de policy capturing
Leidy Johanna Cárdenas Solano	Estudiante de pregrado	- Cuestionario de nivel de efectividad de control - Cuestionario evaluación de riesgos - Cuestionario de policy capturing
Hugo Martínez Ardila	Estudiante de doctorado	- Cuestionario de nivel de efectividad de control - Cuestionario evaluación de riesgos - Cuestionario de policy capturing
Lizeth Fernanda Serrano	Estudiante de pregrado	- Cuestionario de policy capturing

NOMBRE	TIPO DE VINCULACIÓN	ACTIVIDAD
Leidy Yohana Flórez Gómez	Estudiante de maestría	- Cuestionario de nivel de efectividad de control - Cuestionario evaluación de riesgos - Cuestionario de policy capturing
Jhuliana Paola Galvis Gómez	Estudiante de maestría	- Cuestionario de nivel de efectividad de control - Cuestionario evaluación de riesgos - Cuestionario de policy capturing
Yesith Valencia Galvan	Estudiante de maestría	- Cuestionario evaluación de riesgos - Cuestionario de policy capturing
Clara López	Estudiante de doctorado	- Cuestionario de policy capturing
Diana González Gelvez	Estudiante de maestría	- Cuestionario de nivel de efectividad de control - Cuestionario evaluación de riesgos - Cuestionario de policy capturing
Maryuris Charris Polo	Estudiante de maestría	- Cuestionario de policy capturing
Astrid Jaime Arias	Profesional de apoyo	- Cuestionario de nivel de efectividad de control - Cuestionario evaluación de riesgos - Cuestionario de policy capturing
Francy Castro Aponte	Estudiante de maestría	- Cuestionario de nivel de efectividad de control - Cuestionario evaluación de riesgos - Cuestionario de policy capturing
Laura Pinto Prieto	Estudiante de maestría	- Cuestionario de nivel de efectividad de control - Cuestionario evaluación de riesgos Cuestionario de policy capturing
Gerardo Angulo	Estudiante de doctorado	- Cuestionario de nivel de efectividad de contro - Cuestionario evaluación de riesgos
Luis Fernando Sierra Joya	Estudiante de maestría	- Cuestionario de nivel de efectividad de control - Cuestionario evaluación de riesgos
Diana Milena Cárdenas Herrera	Estudiante de pregrado	- Cuestionario de nivel de efectividad de control

ANEXO 20. LISTADO DE AMENAZAS

- Acceso desautorizado a información confidencial.
- Acceso desautorizado a software especializado o información con fines no académicos
- Actos deliberados de extorsión con la información: chantaje de la divulgación de información.
- Actos deliberados de robo: confiscación ilegal de los equipos o la información.
- Actos deliberados de sabotaje o vandalismo: destrucción de los sistemas o la información.
- Ataque contra la confidencialidad y/o integridad de la información: Intercepción y alteración de datos.
- Ataques de ingeniería social
- Ataques deliberados de software: Delito/fraude informático o programas maliciosos (malware).
- Divulgación de información confidencial.
- Expansión del uso de ordenadores personales (dispositivos móviles), lo cual dificulta los controles de seguridad.
- Fallas en el servicio de almacenamiento de información en la nube.
- Fallas técnicas o errores del hardware: fallas en los equipos.
- Fallas técnicas o errores del software: bugs, problemas de código, lagunas desconocidos.
- Falta de ética de los usuarios del sistema.
- Fluctuaciones o fallas en el suministro de energía.
- Fuerzas de la naturaleza: fuego, inundaciones, terremotos, rayos.
- Fuga de conocimiento
- Interrupción de la disponibilidad de la información: destrucción o daño del disco duro, cortan una línea de comunicación, se cae el internet.

- Modificación parcial o completa sin autorización del contenido o modo de funcionamiento del sistema
- Obsolescencia tecnológica: tecnologías anticuadas o no actualizados
- Ingreso desautorizado en el sistema a través de la red: hackers, descifrado de claves
- Pérdida o daño de las copias de resguardo
- Posibilidad de añadir o modificar información relevante.
- Problemas legales, demandas, litigio
- Robo o pérdida accidental de documentos o activos de información o equipos de procesamiento de información
- Siniestros: Colapso del edificio, incendio, fuga de gas, exposición a residuos peligrosos.
- Suplantación de identidad
- Vandalismo, desordenes civiles, ataques físicos que afectan la integridad de personas y conservación de bienes.
- Violación a la propiedad intelectual: piratería, violaciones a los derechos de autor.

ANEXO 21. LISTADO DE VULNERABILIDADES

- Ausencia de cláusulas de permanencia en el grupo de investigación
- Ausencia de inventario actualizado de equipos e información
- Ausencia de planta eléctrica.
- Ausencia de programas de capacitación y sensibilización.
- Ausencia de política de seguridad de la información
- Ausencia o desconocimientos de objetivos de la seguridad de la información
- Capacitación inadecuada de los integrantes del grupo.
- Controles de acceso lógico y/o físico inadecuados.
- Desconocimiento de las normas legales vigentes / aplicables al contexto del grupo de investigación.
- Descuidos en las políticas, procedimientos, capacitación y tecnología
- Descuidos, errores humanos (dejar la puerta abierta, dejar documentos sobre el escritorio... etc.)
- El acceso lógico no es retirado inmediatamente una vez se termina la vinculación del integrante con el grupo o no es examinado antes de ser concedido.
- Errores de software
- Falta de asesoramiento legal competente.
- Falta de controles de acceso lógico y/o físico
- Incapacidad financiera para ofrecer remuneración lo suficientemente atractiva para que el investigador decida permanecer en el grupo
- Información confidencial se encuentra en activos eliminados o reasignados, y se puede acceder por un usuario no autorizado.
- Integrantes del grupo manejan parte de la información mediante los servicios ofrecidos en la nube.
- Integrantes del grupo no entrenados / inconscientes

- La dirección no apoya los programas de capacitación y sensibilización para los integrantes del grupo.
- La dirección no exige el cumplimiento de la política de seguridad de la información.
- La dirección no apoya el desarrollo de una política de seguridad de la información.
- La información no está protegida de acuerdo a su grado de confidencialidad
- Las responsabilidades de seguridad de la información no son claras para los integrantes del grupo
- Los cambios de acceso son informales o inadecuados.
- Los controles implementados son débiles, es decir, no hay un nivel apropiado de controles de seguridad.
- Los derechos de acceso no son consistentes con las funciones/roles del usuario de información.
- Los integrantes del grupo no cumplen con la política de seguridad de manera deliberada.
- Los integrantes del grupo no son conscientes de los requerimientos de seguridad de la información.
- Los procedimientos de seguridad física que se siguen son inadecuados.
- Mantenimiento deficiente de las instalaciones físicas.
- Ningún responsable de la revisión, actualización e implementación de la política de seguridad de la información.
- No está protegida la información personal de los integrantes y los *stakeholders* del grupo de investigación.
- No existe autonomía suficiente en la toma de decisiones de los integrantes del grupo debido a discrepancias en el rol desempeñado al interior del grupo.
- No existe clasificación de la información
- No existe contacto estrecho entre los integrantes del grupo de investigación.
- No existen criterios de aceptación para nuevas aplicaciones y sistemas.

- No existen normas, procedimientos o directrices documentadas en un manual
- No existen políticas de mantenimiento de los equipos, o existen pero no se cumplen.
- No hay acuerdos de obligaciones legales para la relación con terceros.
- No hay compromiso de los integrantes del grupo
- No hay conocimiento sobre protección y comercialización de derechos de propiedad intelectual
- No hay políticas que exijan la transferencia de conocimiento
- No hay procesos de licitación
- No hay reporte de incidentes de forma oportuna y rápida.
- No hay un responsable de la protección de la privacidad de la información
- No hay retiro de los beneficios institucionales una vez el usuario se retira del grupo de investigación
- No hay verificación de antecedentes de los integrantes del grupo de investigación
- No se valúan las capacidades, habilidades y experiencia de los proveedores
- No se firman acuerdos de confidencialidad
- No se realizan copias de seguridad de la información.
- No se realizan las actualizaciones adecuadas.
- Poca claridad del concepto de confidencialidad de la información.
- Poca consciencia sobre la importancia de la información (discusión abierta de temas confidenciales, dejar la puerta abierta, dejar el computador sin bloqueo o documentos confidenciales sobre el escritorio)
- Procedimientos de copias de seguridad no documentados.
- Procedimientos de uso de la información no documentados en un manual de acceso libre para los integrantes del grupo.
- Procesos disciplinarios deficientes
- Seguridad física insuficiente.

- Seguridad insuficiente en los servidores, tecnologías de red y redes de acceso.
- Servicio de suministro deficiente.
- Sobreprivilegios de usuario
- Supervisión inadecuada del uso del sistema.
- Ubicación vulnerable de las instalaciones físicas.

ANEXO 22. LISTADO DE IMPACTOS

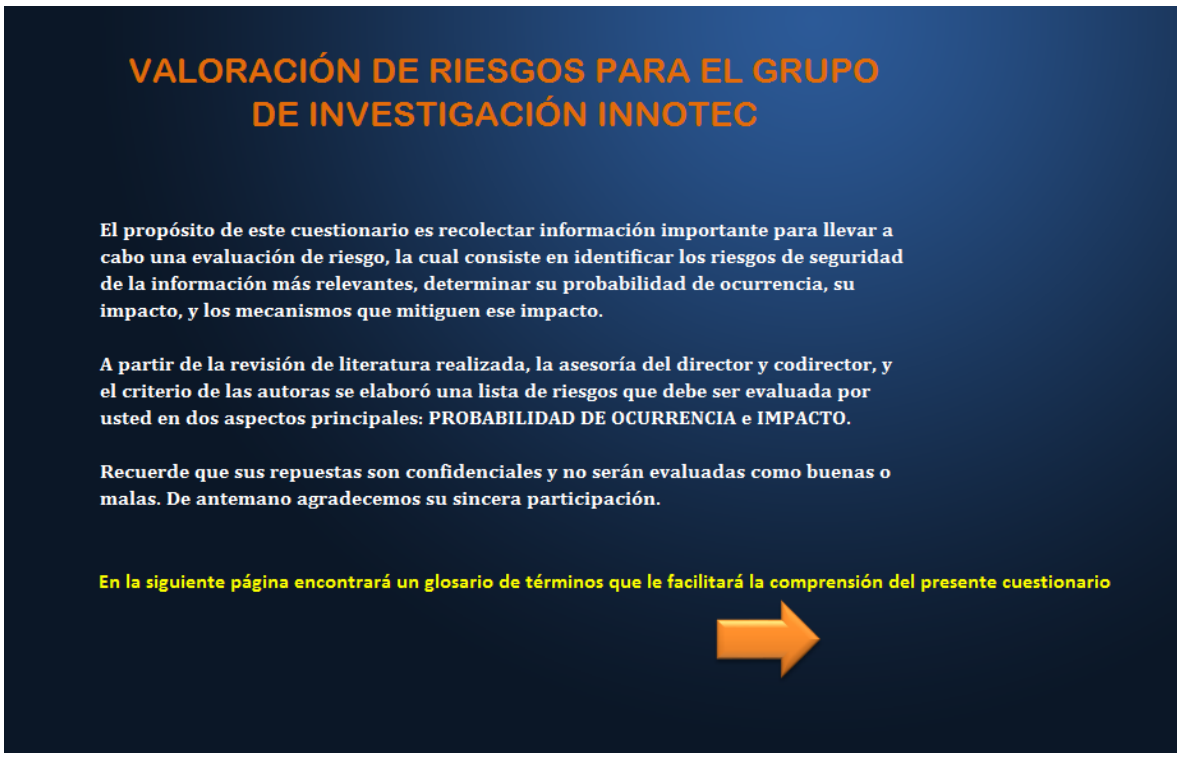
- Acceso remoto no autorizado a los sistemas internos de la organización
- Asimetrías en la información
- Consecuencias de las cláusulas contractuales del proveedor del servicio (software).
- Costo de oportunidad
- Costos de remplazo de equipos
- Daño de la reputación
- Daños del software
- Deterioro en las relaciones con los *stakeholders*
- Discontinuidad en los procesos organizativos
- Divulgación no autorizada de información
- Fuga de información
- Impedimento de la auditoría de información
- Inaccesibilidad de la información cuando se necesita
- Incapacidad de cumplir con los objetivos organizativos
- Incumplimiento de compromisos y responsabilidades adquiridas
- Interrupción de las actividades cotidianas
- Lesión o pérdida de la vida
- No acumulación de experiencia
- Pérdidas de tiempo significativo
- Sanciones civiles: multas, suspensión de licencias, entre otras.
- Pérdida de confianza
- Pérdida de diferenciación y crecimiento
- Pérdida de habilidades capacidades y talentos
- Pérdida de la privacidad
- Pérdida de nuevas alianzas o fuentes de financiamiento
- Pérdida de participación en procesos de licitación.

- Pérdida de ventajas competitivas
- Pérdidas financieras
- Reducción de la productividad
- Reducción de la rentabilidad
- Robo de equipos
- Violación de la integridad de la información

ANEXO 23. TABLA DE AMENAZAS, VULNERABILIDADES, IMPACTOS, RIESGOS Y CONTROLES

Amenaza	Vulnerabilidad Asociada	Impacto	Riesgo	Control que aplica
(1) Suplantación de identidad	Controles de acceso lógico y/o físico inadecuados.	Costo de oportunidad	Suplantación de identidad por baja efectividad de los controles de seguridad físicos y/o errores humanos, que conlleva a perdidas de información confidencial a un costo muy alto.	8.3.3 Retirada de los derechos de acceso
	Descuidos, errores humanos	Incapacidad de cumplir con los objetivos organizativos		10.1.1 Documentación de los procedimientos de operación
	Integrantes del grupo no cumplen con la política de seguridad de la información.	Pérdida de confianza		10.7.3 Procedimientos de manipulación de la información
	La dirección no exige el cumplimiento de la política de seguridad de la información.	Pérdida de diferenciación y crecimiento		11.1.1 Política de control de acceso
	La dirección no apoya el desarrollo de una política de seguridad de la información.	Fuga de información		11.2.1 Registro de usuario
	La dirección no apoya los programas de capacitación y sensibilización para los	Pérdida de la privacidad		12.3.1 Política de uso de los controles criptográficos
	Integrantes del grupo no capacitados / inconscientes	Pérdida de ventajas competitivas		6.1.6 Contacto con las autoridades
	Contacto poco estrecho entre los integrantes del grupo.	Pérdidas financieras		8.1.3 Términos y condiciones de contratación
	Ausencia de programas de capacitación y sensibilización			8.2.1 Responsabilidades de la Dirección
	Ausencia de política de seguridad de la información			8.2.3 Proceso disciplinario
	Falta de controles de acceso lógido y/o físico			9.1.1 Perímetro de seguridad física
				9.1.2 Controles fisicos de entrada
				9.1.3 Seguridad de oficinas, despachos e instalaciones
				9.2.1 Emplazamiento y protección de equipos
				9.2.7 Retirada de materiales propiedad de la empresa
				10.7.4 Seguridad de la documentación del sistema
				10.8.1 Políticas y procedimientos de intercambio de información
				10.8.2 Acuerdos de intercambio
				10.10.1 Registros de auditoría
				10.10.3 Protección de la información de los registros
				10.10.4 Registros de administración y operación
				11.2.2 Gestión de privilegios
				11.2.3 Gestión de contraseñas de usuario
				11.2.4 Revisión de los derechos de acceso de usuario
				11.3.1 Uso de contraseñas
				11.3.2 Equipo de usuario desatendido
				11.4.2 Autenticación de usuario para conexiones externas
				11.5.1 Procedimientos seguros de inicio de sesión
				11.5.2 Identificación y autenticación de usuario
				11.5.3 Sistema de Gestión de contraseñas
				11.5.5 Desconexión automática de sesión
				11.5.6 Limitación del tiempo de conexión
				12.3.2 Gestión de claves
				12.5.4 Fugas de información
				15.1.6 Regulación de los controles criptográficos

ANEXO 24. CUESTIONARIO NIVEL DE RIESGO INNOTEC



En la siguiente página encontrará las instrucciones para el diligenciamiento del cuestionario

GLOSARIO DE TÉRMINOS

Activo de información: se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para el grupo de investigación.

Amenaza: Aquello puede dañar o intentar dañar un activo de información. Suelen clasificarse por su origen: naturales, humanas (intencionales o no intencionales), accidentales.

Confidencialidad de la información: se refiere a asegurar que solo podrán acceder a la información (usarla, leerla o escucharla) las personas autorizadas

Controles de acceso lógico: Evita que programas o personal no autorizado usen recursos como bases de datos o sistemas de información del grupo

Disponibilidad (accesibilidad) de la información: implica garantizar que la información estará disponible siempre que cualquier persona autorizada necesita hacer uso de ella.

Dispositivos móviles: aparatos de pequeño tamaño, con algunas capacidades de procesamiento, con conexión permanente o intermitente a una red, memoria limitada, que ha sido diseñado específicamente para una función, pero que puede llevar a cabo otras funciones más generales. Ejemplos: reproductores de audio portátiles, navegadores GPS, teléfonos móviles, los PDAs, los Tablet PCs.

Fuga de conocimiento: es la emigración de investigadores ya formados (generalmente para no regresar) a otros grupos, en busca de mejores oportunidades de desarrollo, empleo y remuneración económica.

Fuga de información: incidente que pone en poder de una persona ajena al grupo, información confidencial y que sólo debería estar disponible para integrantes del mismo (tanto todos como un grupo reducido).

Grupo: Se refiere al grupo de investigación INNOTEC.

Información confidencial: Es toda información que por su naturaleza no puede ser revelada a terceros, y que por lo tanto no es pública. Ejemplos:avances o resultados de proyectos, datos recopilados en una investigación, información personal de los investigadores, propuestas o planes de proyectos . Pueden existir distintos niveles de confidencialidad.

Integridad de la información: busca asegurar que la información con la que se trabaja sea completa y precisa, poniéndole énfasis en la exactitud tanto en su contenido como en los procesos involucrados en su procesamiento.

Malware: es la abreviatura de ***"Malicious software"*** (software malicioso), término que engloba a todo tipo de programa o código de computadora cuya función es dañar un sistema o causar un mal funcionamiento. Ejemplos: virus, troyanos, gusanos, spyware, adware, keyloggers, etc.

Objetivo principal: Realizar estudios y fomentar la gestión de la innovación tecnológica para reforzar el papel de la UIS como uno de los núcleos motores de la innovación regional y nacional; adicionalmente, auxiliar el fortalecimiento de la investigación aplicada y la rápida estructuración de paquetes tecnológicos y su transferencia al sector productivo.

Obsolescencia tecnológica: término que se le otorga al hecho que las tecnologías quedan obsoletas. Puede ser de dos tipos: de software y formato de archivos o de hardware y soporte físico.

Política de seguridad de la información: documento que indica el compromiso y apoyo de la dirección, así como la definición del papel que debe jugar la seguridad de la información en la consecución de la misión y visión de la organización.

Proceso disciplinario: Según la norma ISO 27002, debiera existir un proceso disciplinario para los empleados que han cometido un incumplimiento de la seguridad.

Riesgo: Es la probabilidad de que una amenaza ataque un activo de información a través de una vulnerabilidad concreta

Sistema de información: Conjunto de componentes interrelacionados que recolectan (o recuperan), procesan, almacenan y distribuyen información para apoyar la toma de decisiones y el control de una organización.

TI: Se conoce como tecnología de información (TI) a la utilización de tecnología para el manejo y procesamiento de información – especificamente la captura, transformación, almacenamiento, protección, y recuperación de datos e información.

Ventaja competitiva: El grupo posee una ventaja competitiva cuando tiene alguna característica diferencial respecto de sus competidores, que le confiere la capacidad para alcanzar unos rendimientos superiores a ellos, de manera sostenible en el tiempo.

Verificación de antecedentes: Los chequeos de verificación de antecedentes de todos los nuevos integrantes y terceros debieran llevarse a cabo en concordancia con las leyes, regulaciones y ética relevantes; y debieran ser proporcionales a los requerimientos comerciales, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.

Vulnerabilidad: Defecto o debilidad en los procedimientos y controles de seguridad, que podrían ser aprovechados por una amenaza y resultar en un incidente de seguridad o violación de la política de seguridad de la información.

VALORACIÓN DE LA PROBABILIDAD DE OCURRENCIA

DEFINICIÓN
Se refiere a la probabilidad de que ocurra el riesgo

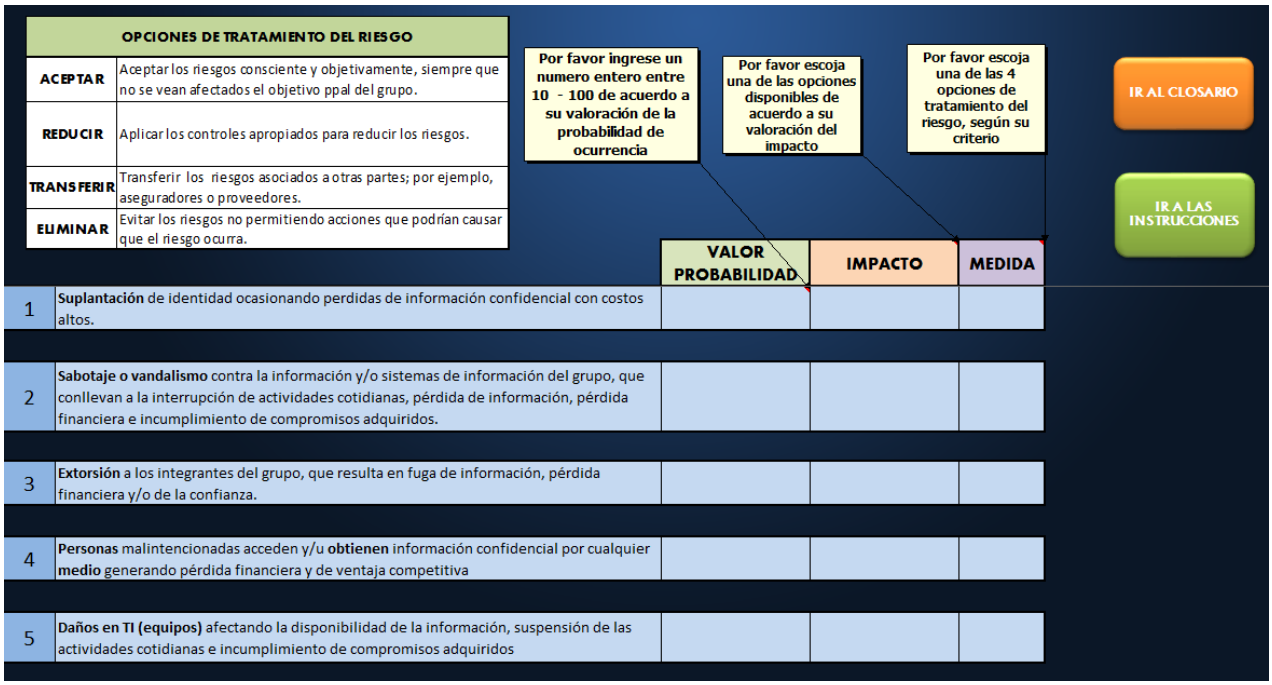
ESCALA DE VALORACIÓN	
70-100%	Pueden existir vulnerabilidades y amenazas y el nivel de efectividad del control es muy bajo o no es aceptable. Existen otras variables del entorno que pueden aumentar el rating de la probabilidad de ocurrencia. La fuente de la amenaza esta altamente motivada y es suficientemente capaz de hacerse efectiva.
40-69%	Existen amenazas y vulnerabilidades, pero el nivel de efectividad del control se considera que esta en el límite aceptable o las variables del entorno que existen causan que la probabilidad de ocurrencia sea menor que alta y mayor que la baja.La fuente de la amenaza tiene la motivación y la capacidad de hacerse efectiva.
10-39%	Existen amenazas y vulnerabilidades, el nivel de efectividad del control esta ranqueado en 4 o 5, es decir que puede impedir significativamente la ocurrencia de la amenaza sobre la vulnerabilidad. No existen variables del entorno que pudiesen incrementar la posibilidad de ser explotada y ejercida. La fuente de la amenaza le falta motivación o capacidad.

VALORACIÓN DEL IMPACTO

DEFINICIÓN
Se refiere al grado en que el riesgo afecta el grupo de investigación

ESCALA DE VALORACIÓN	
5	Incapacidad para recuperarse. Cierre permanente del grupo o pérdida permanente de las instalaciones. Es muy probable una pérdida total de los negocios y operaciones.
4	Posible daño a la reputación del grupo. Cese prolongado de las actividades del grupo. Requiere la activación de un plan de contingencia. Meses de refuerzo son necesarios para la reparación/recuperación. Pérdida temporal de las instalaciones.
3	Semanas de esfuerzo son necesarias para la reparación/recuperación. Hay gastos importantes y pérdidas de ingresos.
2	Días de esfuerzo son necesarios para la reparación / recuperación. Hay gastos significativos y/o cierta pérdida de ingresos
1	Se requiere de algunos esfuerzos para reparar el daño. Los costos de recuperación son mínimos. No hay pérdidas de ingresos.
0	Sin impacto medible en este momento

En la siguiente página se encuentra el listado de los riesgos que serán evaluados



OPCIONES DE TRATAMIENTO DEL RIESGO	
ACEPTAR	Aceptar los riesgos consciente y objetivamente, siempre que no se vean afectados el objetivo ppal del grupo.
REDUCIR	Aplicar los controles apropiados para reducir los riesgos.
TRANSFERIR	Transferir los riesgos asociados a otras partes; por ejemplo, aseguradores o proveedores.
ELIMINAR	Evitar los riesgos no permitiendo acciones que podrían causar que el riesgo ocurra.

Por favor ingrese un numero entero entre 10 - 100 de acuerdo a su valoración de la probabilidad de ocurrencia

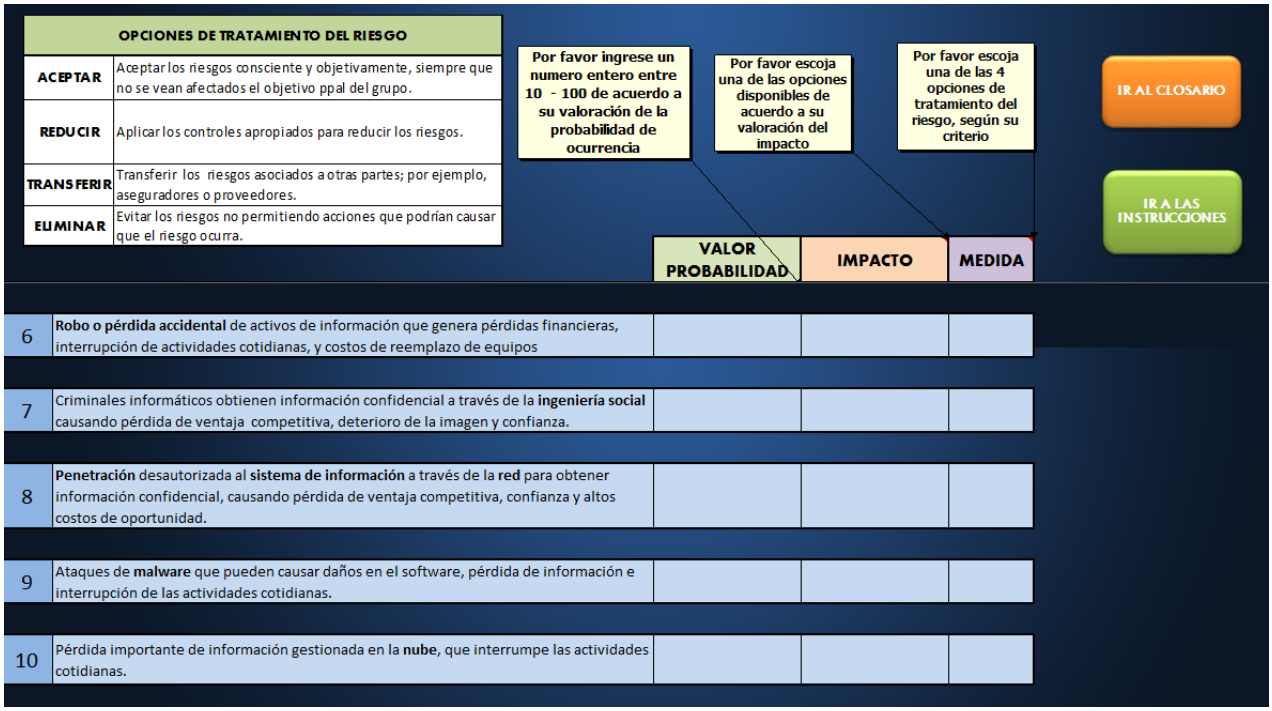
Por favor escoja una de las opciones disponibles de acuerdo a su valoración del impacto

Por favor escoja una de las 4 opciones de tratamiento del riesgo, según su criterio

IR AL CLOSARIO

IR A LAS INSTRUCCIONES

		VALOR PROBABILIDAD	IMPACTO	MEDIDA
1	**Suplantación** de identidad ocasionando perdidas de información confidencial con costos altos.			
2	**Sabotaje o vandalismo** contra la información y/o sistemas de información del grupo, que conllevan a la interrupción de actividades cotidianas, pérdida de información, pérdida financiera e incumplimiento de compromisos adquiridos.			
3	**Extorsión** a los integrantes del grupo, que resulta en fuga de información, pérdida financiera y/o de la confianza.			
4	**Personas** malintencionadas acceden y/u **obtienen** información confidencial por cualquier **medio** generando pérdida financiera y de ventaja competitiva			
5	**Daños en TI (equipos)** afectando la disponibilidad de la información, suspensión de las actividades cotidianas e incumplimiento de compromisos adquiridos			



OPCIONES DE TRATAMIENTO DEL RIESGO	
ACEPTAR	Aceptar los riesgos consciente y objetivamente, siempre que no se vean afectados el objetivo ppal del grupo.
REDUCIR	Aplicar los controles apropiados para reducir los riesgos.
TRANSFERIR	Transferir los riesgos asociados a otras partes; por ejemplo, aseguradores o proveedores.
ELIMINAR	Evitar los riesgos no permitiendo acciones que podrían causar que el riesgo ocurra.

Por favor ingrese un numero entero entre 10 - 100 de acuerdo a su valoración de la probabilidad de ocurrencia

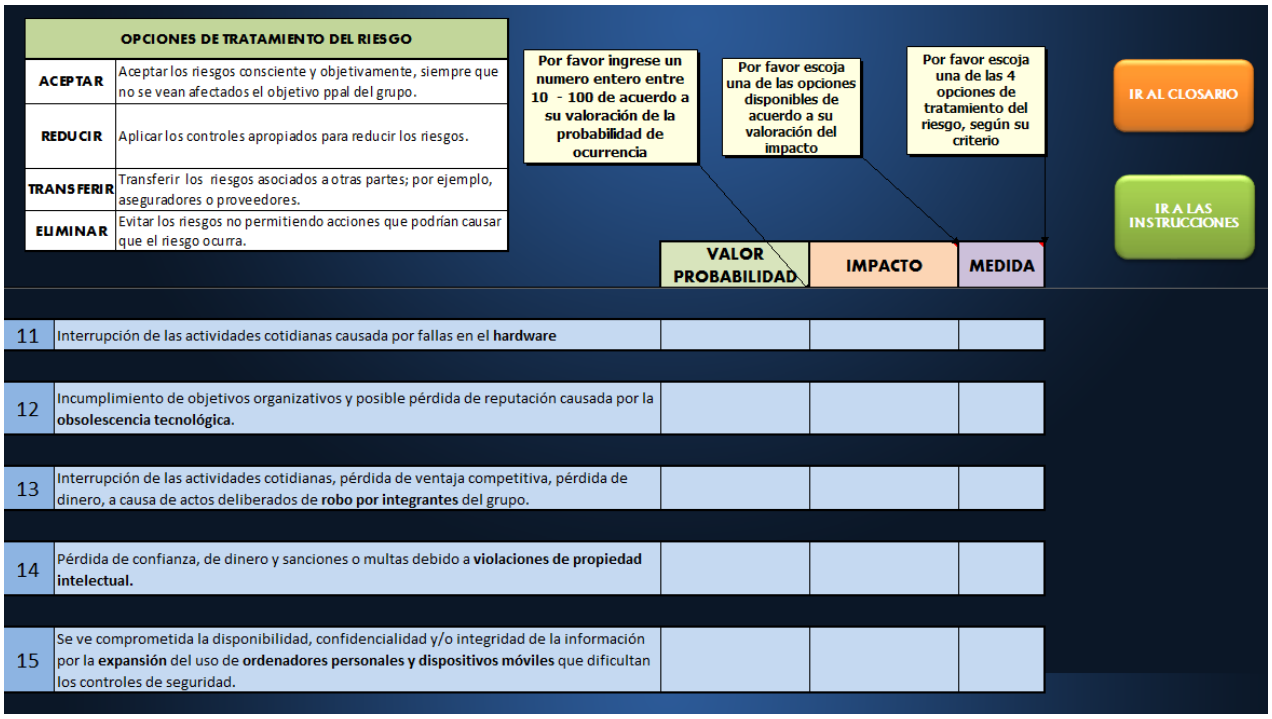
Por favor escoja una de las opciones disponibles de acuerdo a su valoración del impacto

Por favor escoja una de las 4 opciones de tratamiento del riesgo, según su criterio

IR AL CLOSARIO

IR A LAS INSTRUCCIONES

		VALOR PROBABILIDAD	IMPACTO	MEDIDA
6	**Robo o pérdida accidental** de activos de información que genera pérdidas financieras, interrupción de actividades cotidianas, y costos de reemplazo de equipos			
7	Criminales informáticos obtienen información confidencial a través de la **ingeniería social** causando pérdida de ventaja competitiva, deterioro de la imagen y confianza.			
8	**Penetración** desautorizada al **sistema de información** a través de la **red** para obtener información confidencial, causando pérdida de ventaja competitiva, confianza y altos costos de oportunidad.			
9	Ataques de **malware** que pueden causar daños en el software, pérdida de información e interrupción de las actividades cotidianas.			
10	Pérdida importante de información gestionada en la **nube**, que interrumpe las actividades cotidianas.			



OPCIONES DE TRATAMIENTO DEL RIESGO	
ACEPTAR	Aceptar los riesgos consciente y objetivamente, siempre que no se vean afectados el objetivo ppal del grupo.
REDUCIR	Aplicar los controles apropiados para reducir los riesgos.
TRANSFERIR	Transferir los riesgos asociados a otras partes; por ejemplo, aseguradores o proveedores.
ELIMINAR	Evitar los riesgos no permitiendo acciones que podrían causar que el riesgo ocurra.

Por favor ingrese un numero entero entre 10 - 100 de acuerdo a su valoración de la probabilidad de ocurrencia

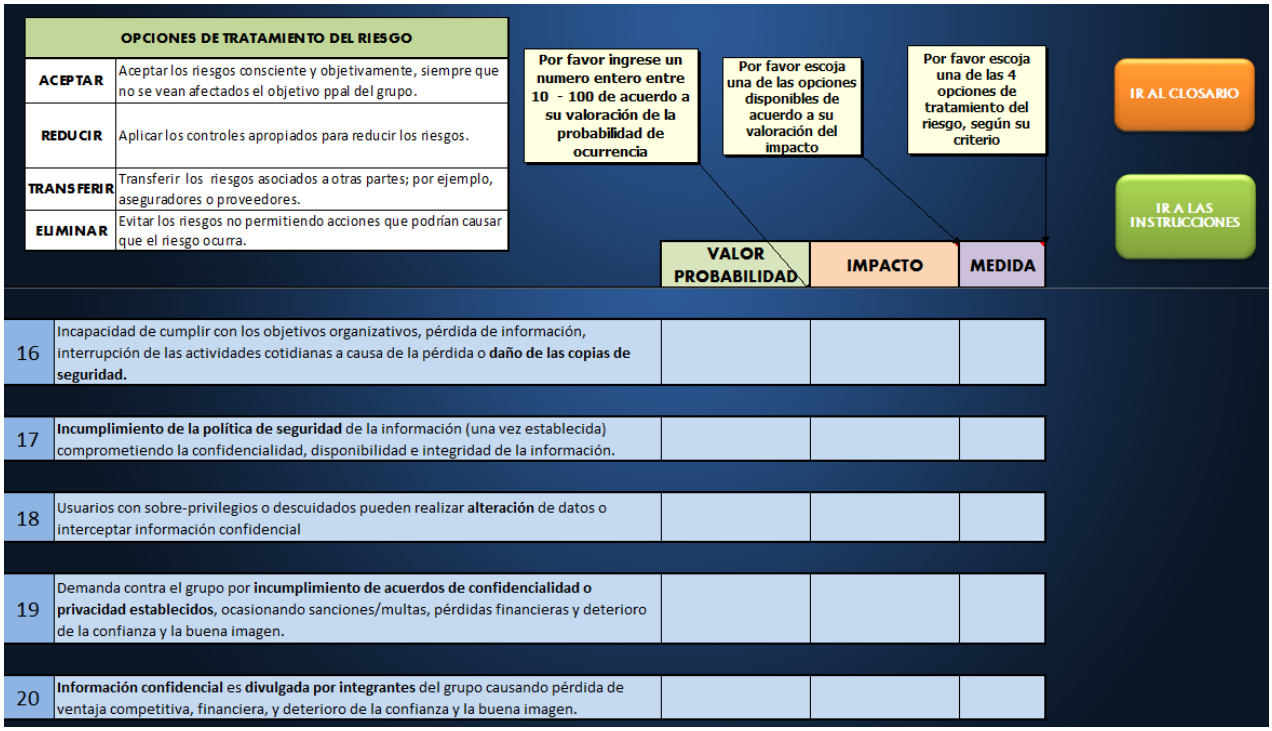
Por favor escoja una de las opciones disponibles de acuerdo a su valoración del impacto

Por favor escoja una de las 4 opciones de tratamiento del riesgo, según su criterio

IR AL CLOSARIO

IR A LAS INSTRUCCIONES

		VALOR PROBABILIDAD	IMPACTO	MEDIDA
11	Interrupción de las actividades cotidianas causada por fallas en el **hardware**			
12	Incumplimiento de objetivos organizativos y posible pérdida de reputación causada por la **obsolescencia tecnológica**.			
13	Interrupción de las actividades cotidianas, pérdida de ventaja competitiva, pérdida de dinero, a causa de actos deliberados de **robo por integrantes** del grupo.			
14	Pérdida de confianza, de dinero y sanciones o multas debido a **violaciones de propiedad intelectual.**			
15	Se ve comprometida la disponibilidad, confidencialidad y/o integridad de la información por la **expansión** del uso de **ordenadores personales y dispositivos móviles** que dificultan los controles de seguridad.			



OPCIONES DE TRATAMIENTO DEL RIESGO	
ACEPTAR	Aceptar los riesgos consciente y objetivamente, siempre que no se vean afectados el objetivo ppal del grupo.
REDUCIR	Aplicar los controles apropiados para reducir los riesgos.
TRANSFERIR	Transferir los riesgos asociados a otras partes; por ejemplo, aseguradores o proveedores.
ELIMINAR	Evitar los riesgos no permitiendo acciones que podrían causar que el riesgo ocurra.

Por favor ingrese un numero entero entre 10 - 100 de acuerdo a su valoración de la probabilidad de ocurrencia

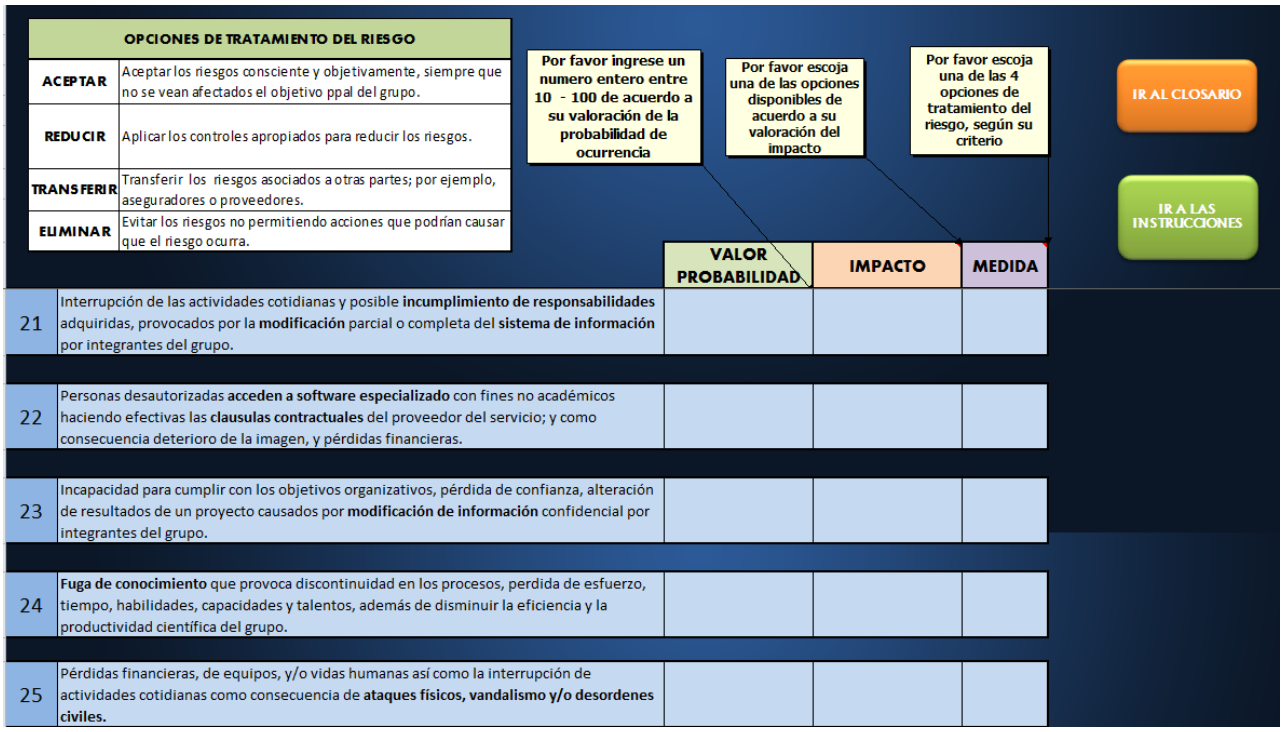
Por favor escoja una de las opciones disponibles de acuerdo a su valoración del impacto

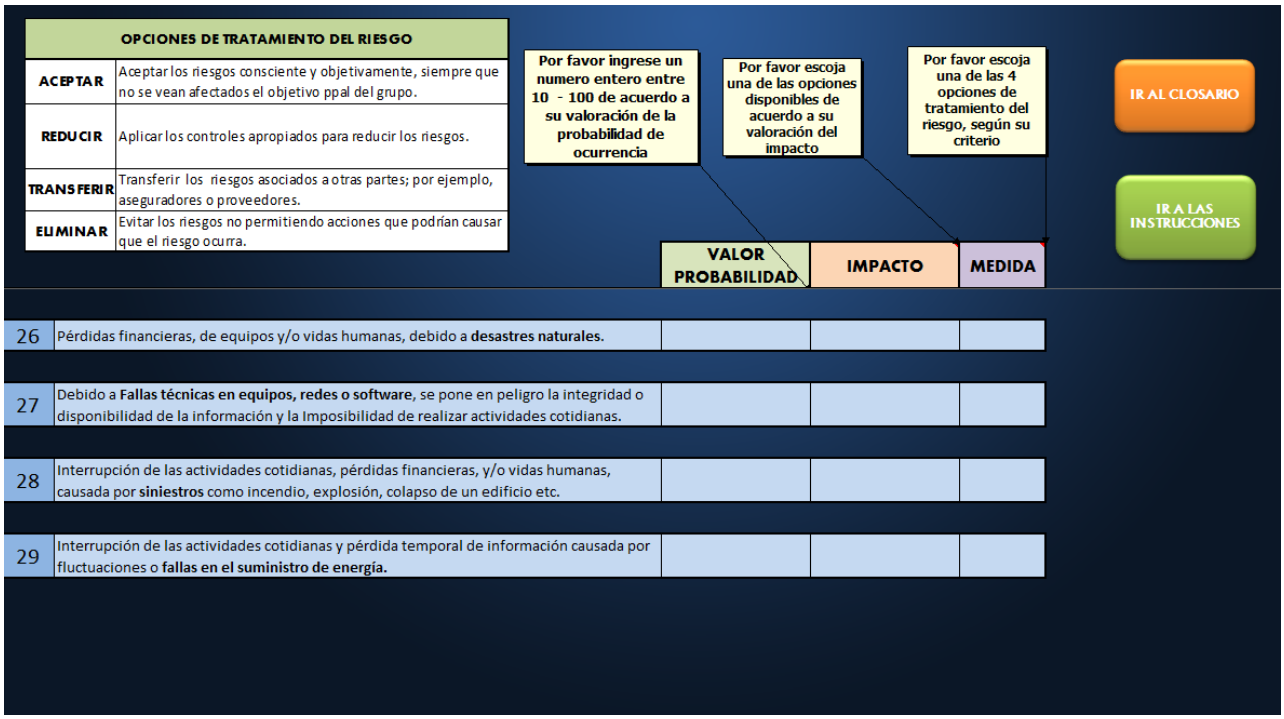
Por favor escoja una de las 4 opciones de tratamiento del riesgo, según su criterio

IR AL CLOSARIO

IR A LAS INSTRUCCIONES

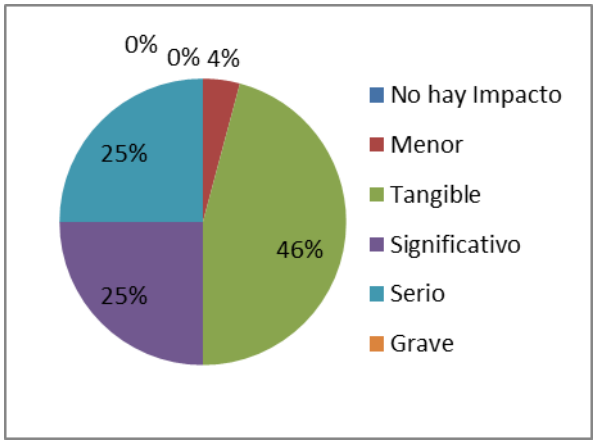
		VALOR PROBABILIDAD	IMPACTO	MEDIDA
16	Incapacidad de cumplir con los objetivos organizativos, pérdida de información, interrupción de las actividades cotidianas a causa de la pérdida o **daño de las copias de seguridad.**			
17	**Incumplimiento de la política de seguridad** de la información (una vez establecida) comprometiendo la confidencialidad, disponibilidad e integridad de la información.			
18	Usuarios con sobre-privilegios o descuidados pueden realizar **alteración** de datos o interceptar información confidencial			
19	Demanda contra el grupo por **incumplimiento de acuerdos de confidencialidad o privacidad establecidos**, ocasionando sanciones/multas, pérdidas financieras y deterioro de la confianza y la buena imagen.			
20	**Información confidencial** es **divulgada por integrantes** del grupo causando pérdida de ventaja competitiva, financiera, y deterioro de la confianza y la buena imagen.			


OPCIONES DE TRATAMIENTO DEL RIESGO
ACEPTAR
Aceptar los riesgos consciente y objetivamente, siempre que no se vean afectados el objetivo ppal del grupo.
REDUCIR
Aplicar los controles apropiados para reducir los riesgos.
TRANSFERIR
Transferir los riesgos asociados a otras partes; por ejemplo, aseguradores o proveedores.
ELIMINAR
Evitar los riesgos no permitiendo acciones que podrían causar que el riesgo ocurra.
Por favor ingrese un numero entero entre 10 - 100 de acuerdo a su valoración de la probabilidad de ocurrencia
Por favor escoja una de las opciones disponibles de acuerdo a su valoración del impacto
Por favor escoja una de las 4 opciones de tratamiento del riesgo, según su criterio
IR AL CLOSARIO
IR A LAS INSTRUCCIONES
VALOR PROBABILIDAD
IMPACTO
MEDIDA
21 Interrupción de las actividades cotidianas y posible incumplimiento de responsabilidades adquiridas, provocados por la modificación parcial o completa del sistema de información por integrantes del grupo.
22 Personas desautorizadas acceden a software especializado con fines no académicos haciendo efectivas las clausulas contractuales del proveedor del servicio; y como consecuencia deterioro de la imagen, y pérdidas financieras.
23 Incapacidad para cumplir con los objetivos organizativos, pérdida de confianza, alteración de resultados de un proyecto causados por modificación de información confidencial por integrantes del grupo.
24 Fuga de conocimiento que provoca discontinuidad en los procesos, perdida de esfuerzo, tiempo, habilidades, capacidades y talentos, además de disminuir la eficiencia y la productividad científica del grupo.
25 Pérdidas financieras, de equipos, y/o vidas humanas así como la interrupción de actividades cotidianas como consecuencia de ataques físicos, vandalismo y/o desordenes civiles.

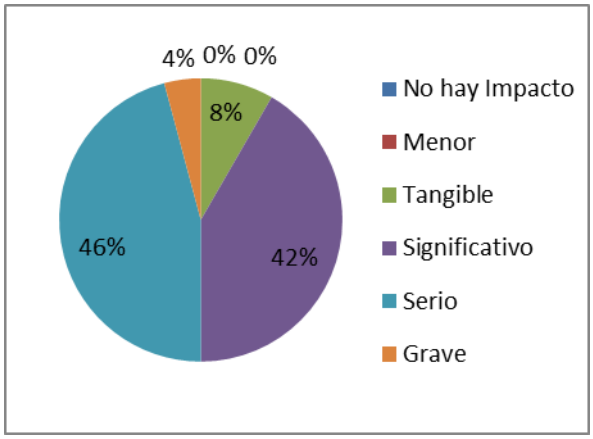

OPCIONES DE TRATAMIENTO DEL RIESGO
ACEPTAR
Aceptar los riesgos consciente y objetivamente, siempre que no se vean afectados el objetivo ppal del grupo.
REDUCIR
Aplicar los controles apropiados para reducir los riesgos.
TRANSFERIR
Transferir los riesgos asociados a otras partes; por ejemplo, aseguradores o proveedores.
ELIMINAR
Evitar los riesgos no permitiendo acciones que podrían causar que el riesgo ocurra.
Por favor ingrese un numero entero entre 10 - 100 de acuerdo a su valoración de la probabilidad de ocurrencia
Por favor escoja una de las opciones disponibles de acuerdo a su valoración del impacto
Por favor escoja una de las 4 opciones de tratamiento del riesgo, según su criterio
IR AL CLOSARIO
IR A LAS INSTRUCCIONES
VALOR PROBABILIDAD
IMPACTO
MEDIDA
26 Pérdidas financieras, de equipos y/o vidas humanas, debido a desastres naturales.
27 Debido a Fallas técnicas en equipos, redes o software, se pone en peligro la integridad o disponibilidad de la información y la Imposibilidad de realizar actividades cotidianas.
28 Interrupción de las actividades cotidianas, pérdidas financieras, y/o vidas humanas, causada por siniestros como incendio, explosión, colapso de un edificio etc.
29 Interrupción de las actividades cotidianas y pérdida temporal de información causada por fluctuaciones o fallas en el suministro de energía.

ANEXO 25. GRÁFICOS DEL NIVEL DE IMPACTO

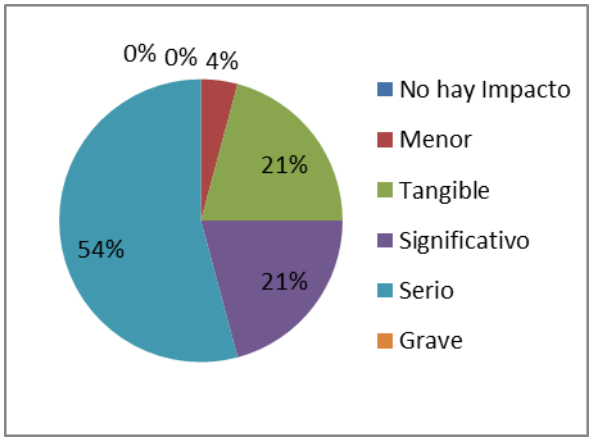
1. Suplantación de identidad



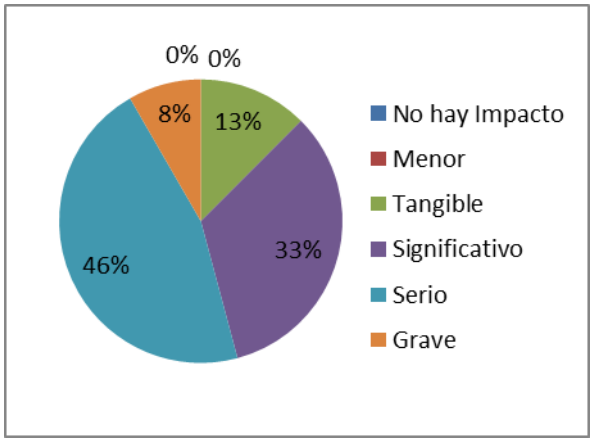
2. Sabotaje o vandalismo contra la información y/o sistemas de información del grupo



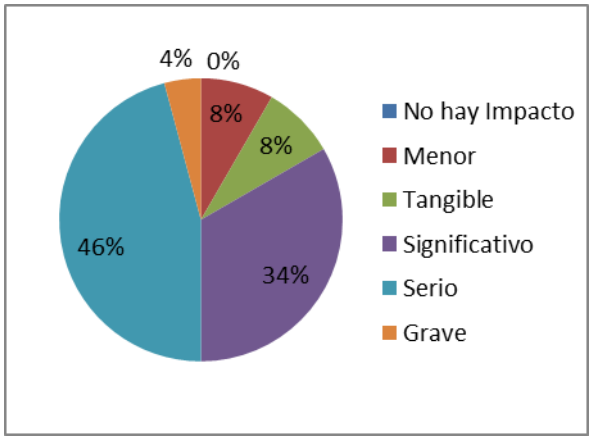
3. Extorsión a los integrantes del grupo



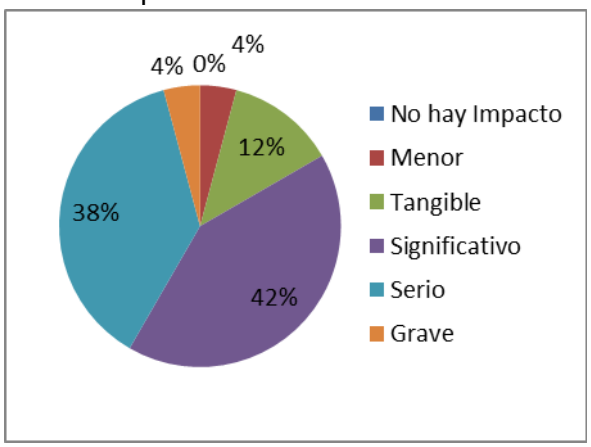
4. Personas malintencionadas acceden y/u obtienen información confidencial



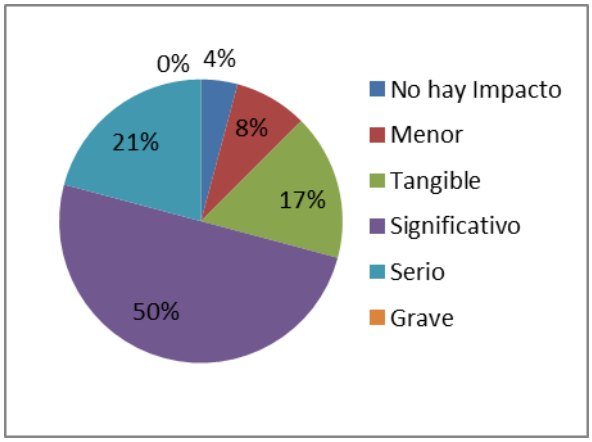
5. Daños en TI (equipos)



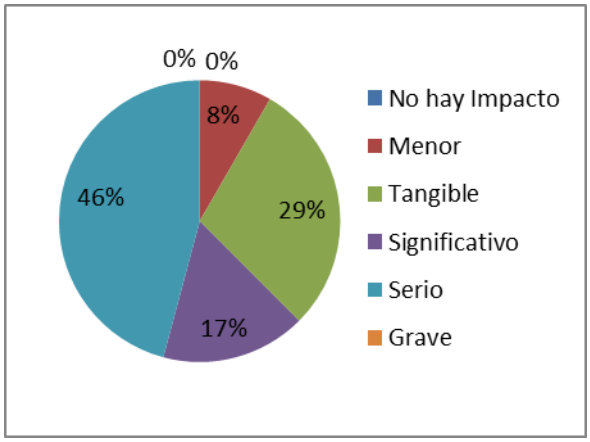
6. Robo o pérdida accidental



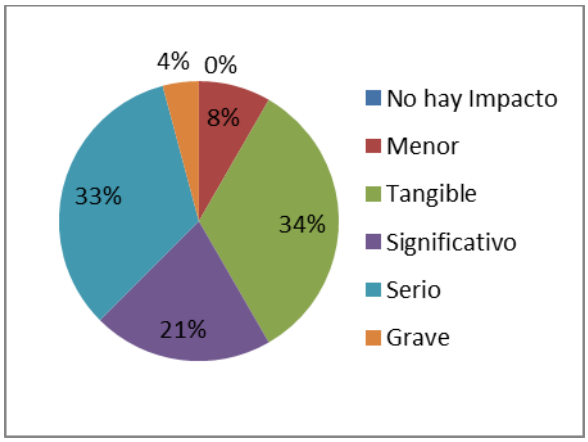
7. Ingeniería social



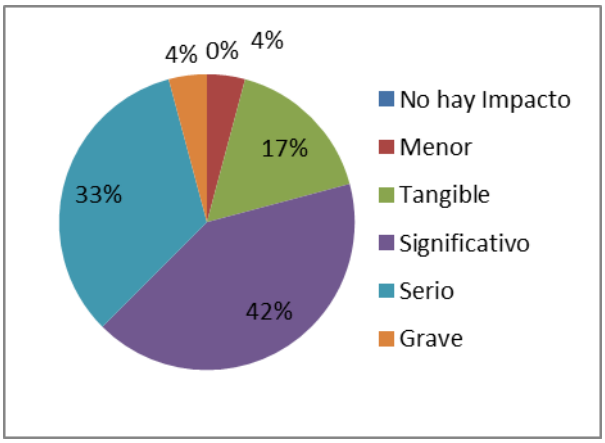
8. Penetración desautorizada al sistema de información a través de la red



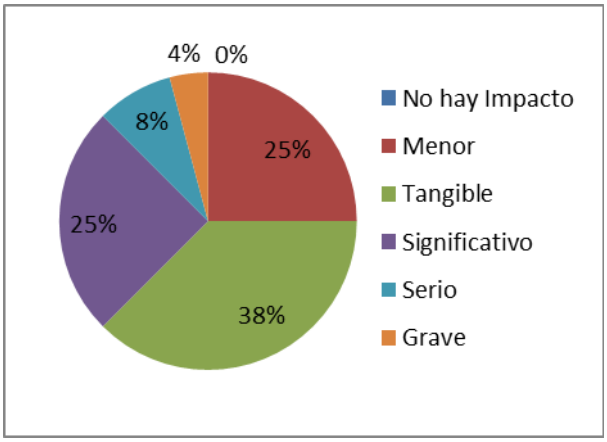
9. Ataques de malware



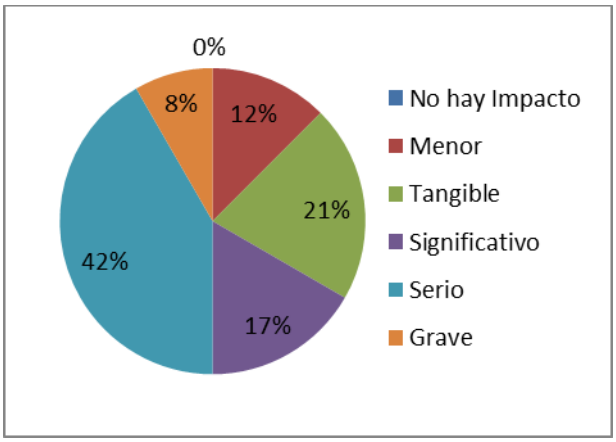
10. Pérdida de información gestionada en la nube



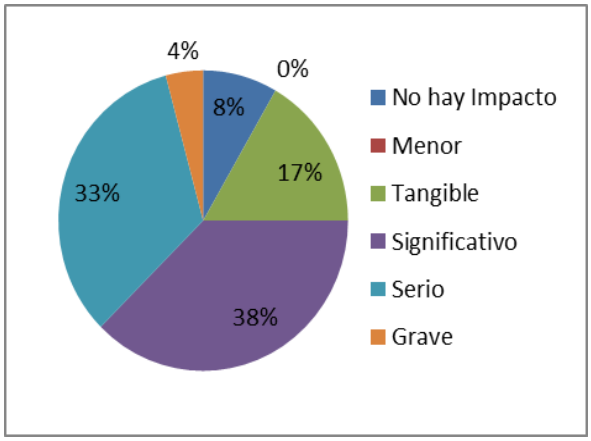
11. Fallas en el hardware



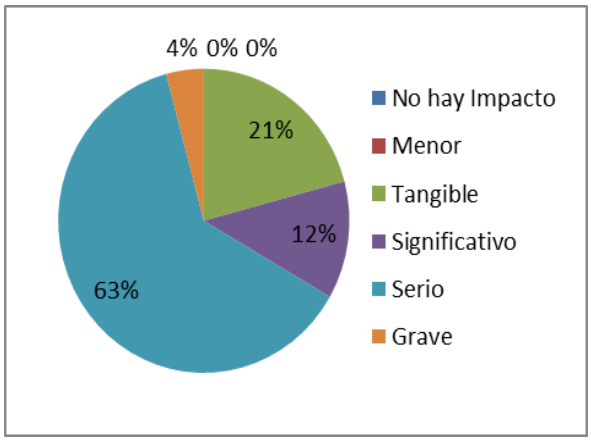
12. Obsolescencia tecnológica



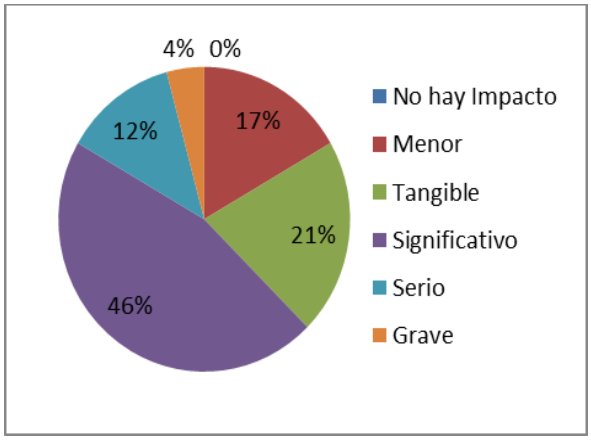
13. Robo por integrantes del grupo



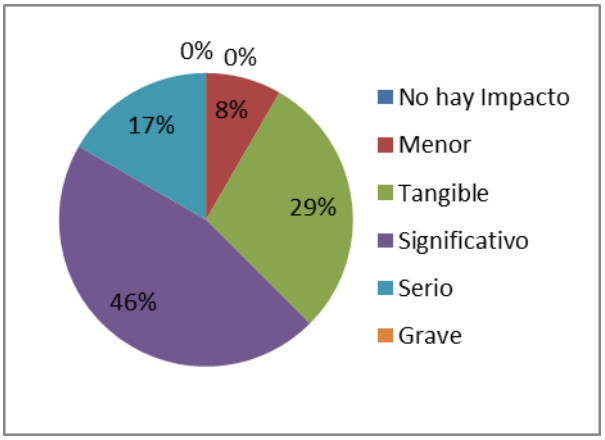
14. Violaciones de propiedad intelectual



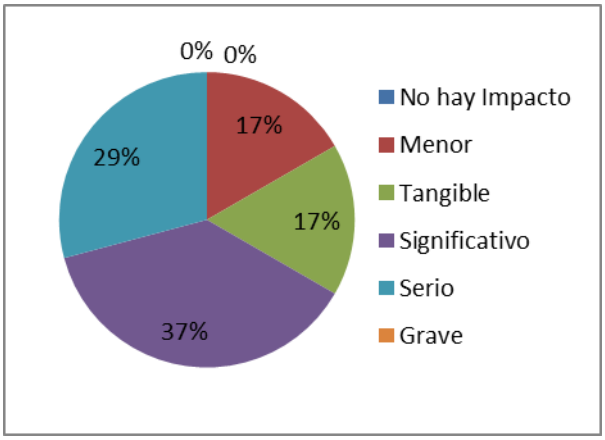
15. Expansión del uso de ordenadores personales y dispositivos móviles



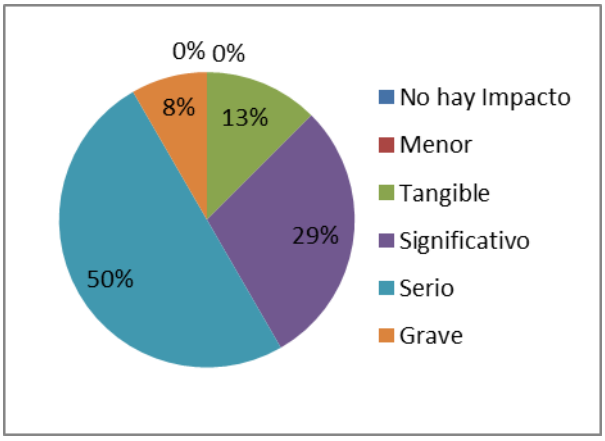
16. Daño de las copias de seguridad



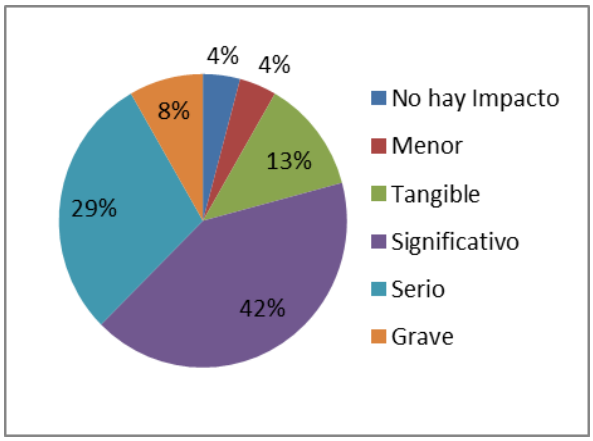
17. Usuarios con sobre-privilegios alteran los datos o interceptan información



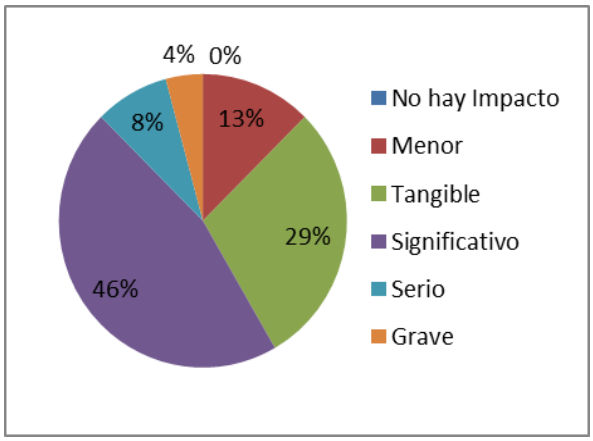
18. Incumplimiento de acuerdos de confidencialidad o privacidad establecidos



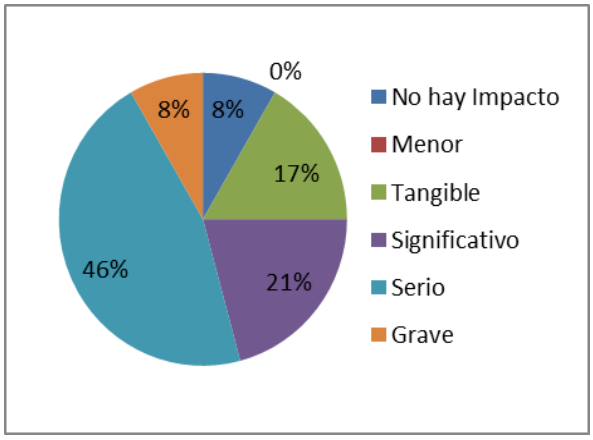
19. Información confidencial es divulgada por integrantes del grupo



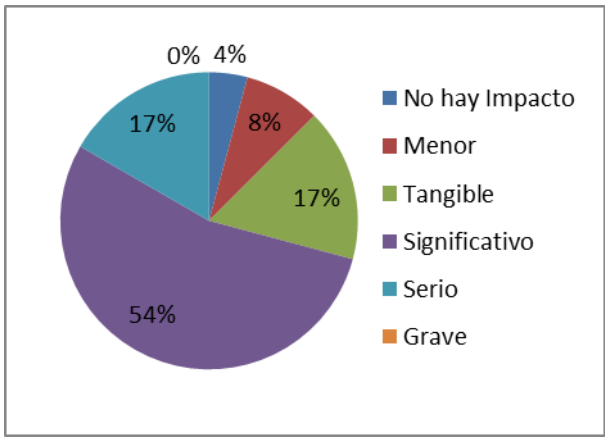
20. Incumplimiento de responsabilidades por modificaciones en los sistemas de información



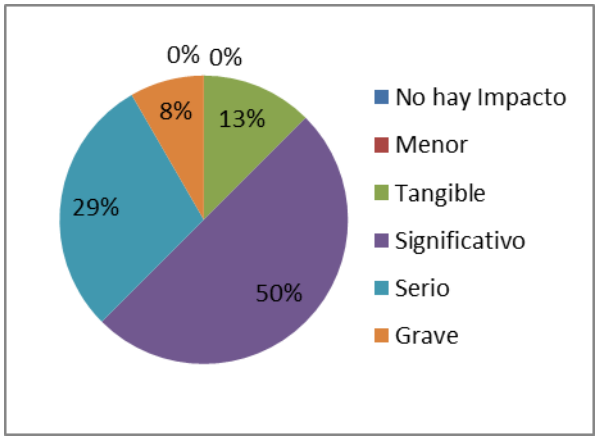
21. Acceso a software especializado con fines no académicos



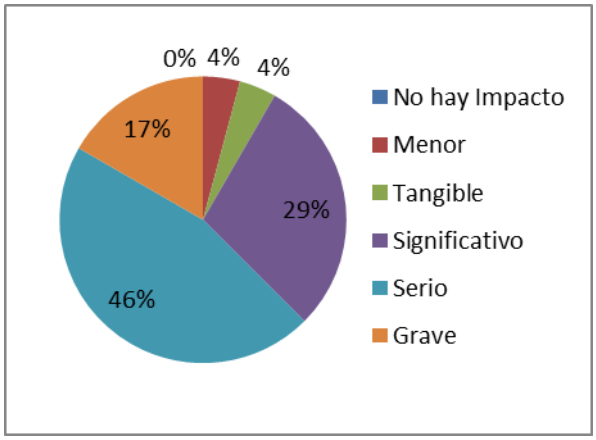
22. Modificación de información confidencial por integrantes del grupo.



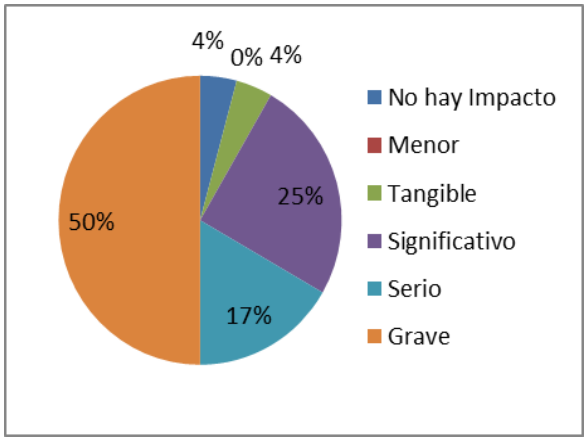
23. Fuga de conocimiento



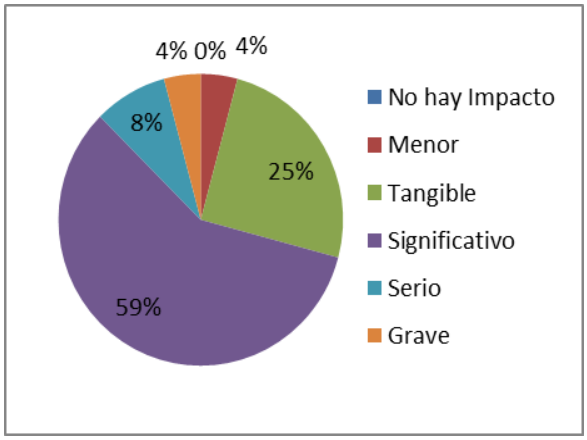
24. Ataques físicos, vandalismo y/o desordenes civiles.



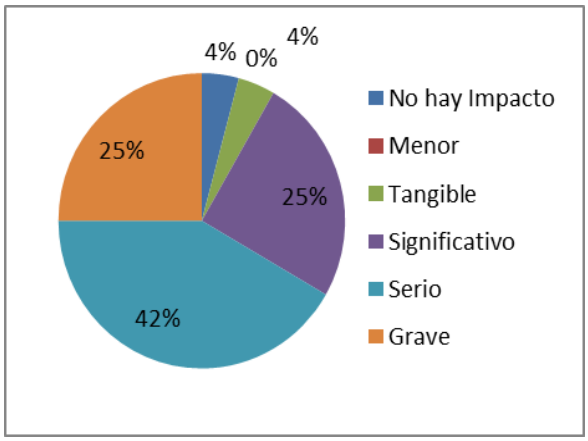
25. Desastres naturales



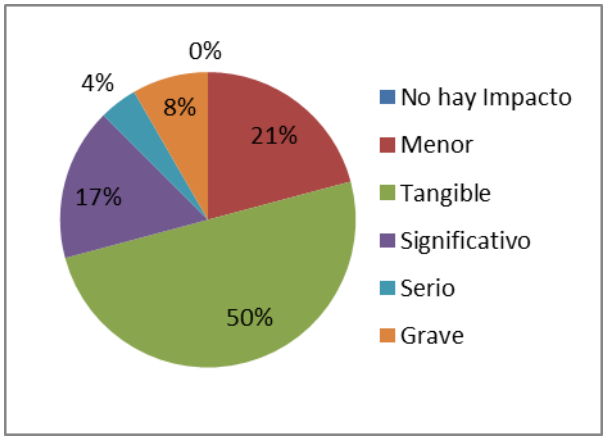
26. Fallas técnicas en equipos, redes o software



27. Interrupción de las actividades cotidianas por siniestros

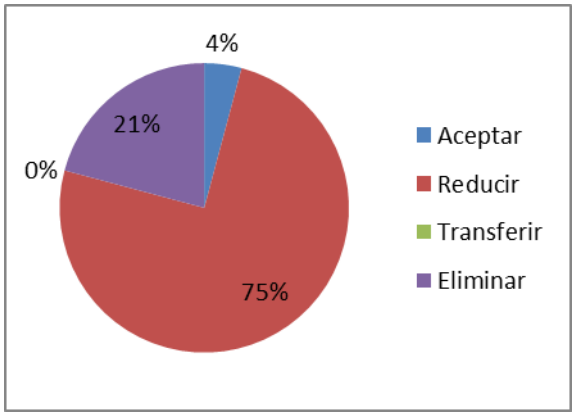


28. Fallas en el suministro de energía

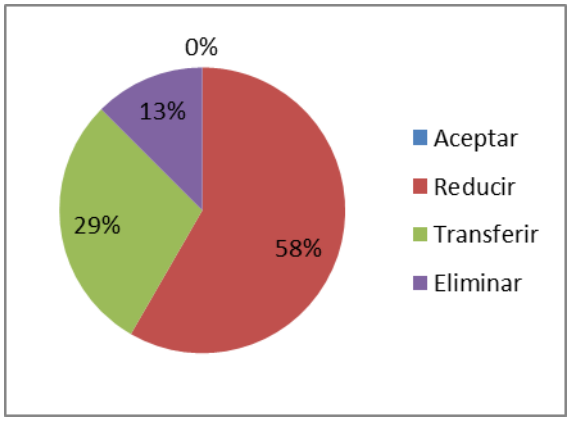


ANEXO 26. GRÁFICOS DE LA MEDIDA DE TRATAMIENTO DE RIESGOS

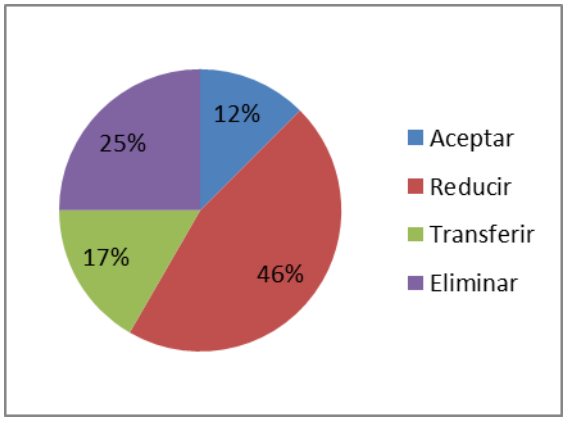
1. Suplantación de identidad



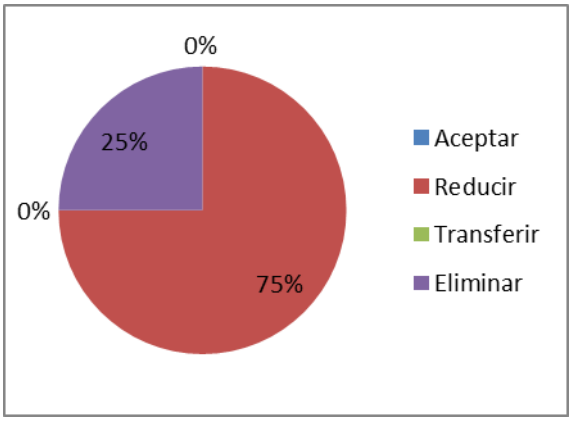
2. Sabotaje o vandalismo contra la información y/o sistemas de información del grupo



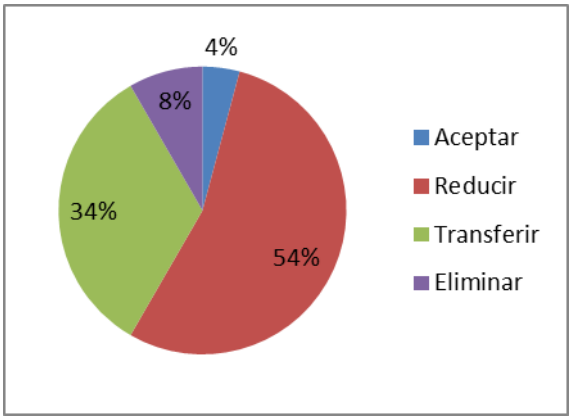
3. Extorsión a los integrantes del grupo



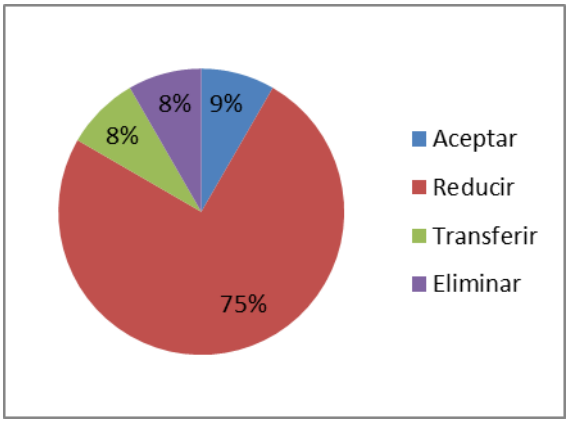
4. Personas malintencionadas acceden y/u obtienen información confidencial



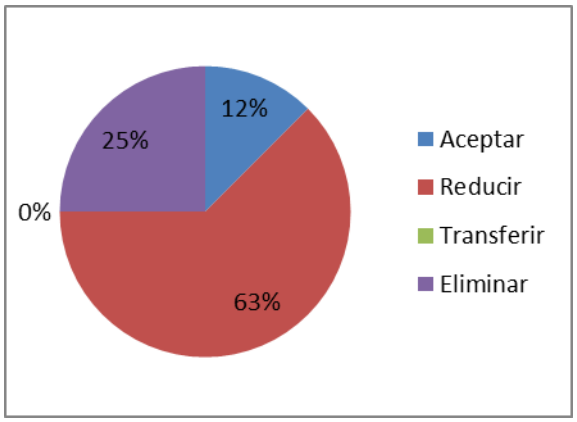
5. Daños en TI (equipos)



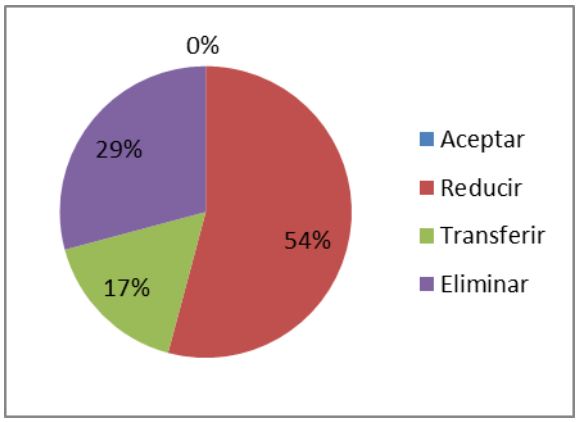
6. Robo o pérdida accidental



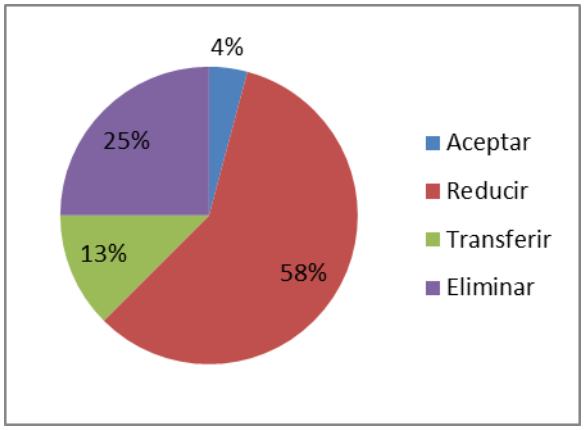
7. Ingeniería social



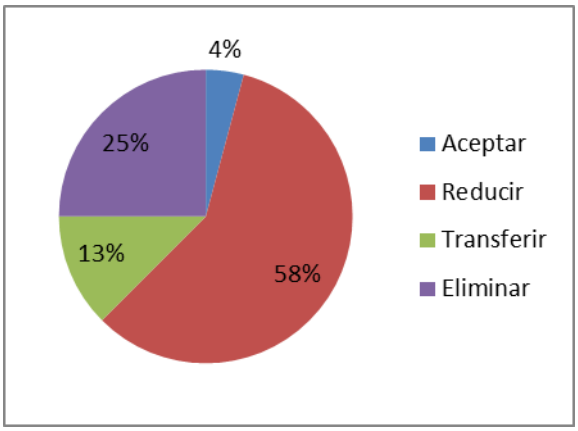
8. Penetración desautorizada al sistema de información a través de la red



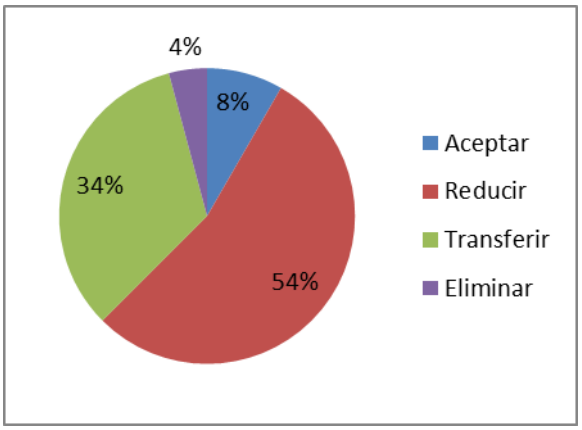
9. Ataques de malware



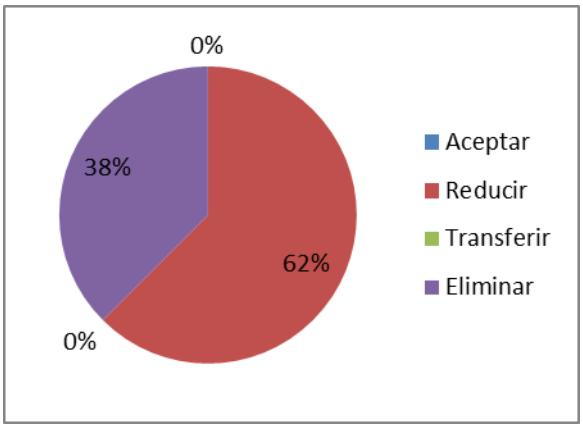
10. Pérdida de información gestionada en la nube



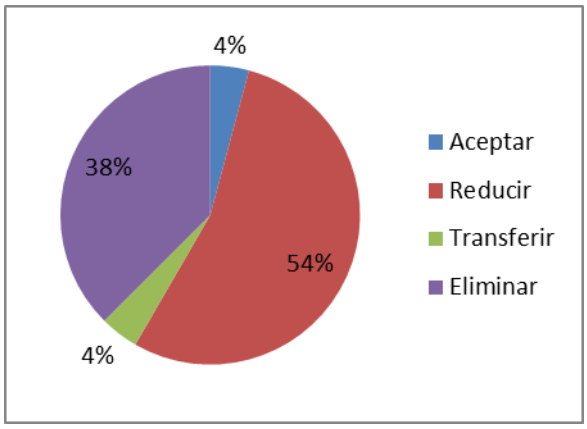
11. Fallas en el hardware



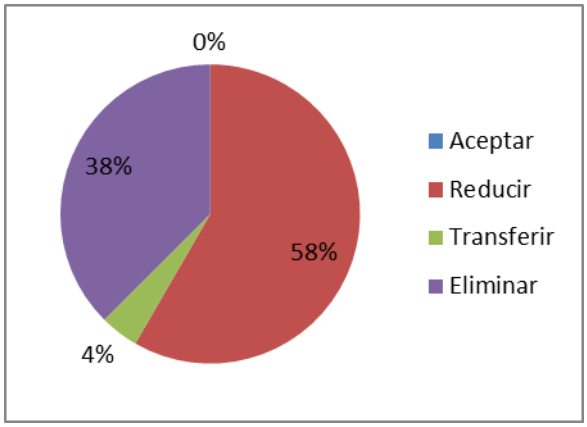
12. Obsolescencia tecnológica



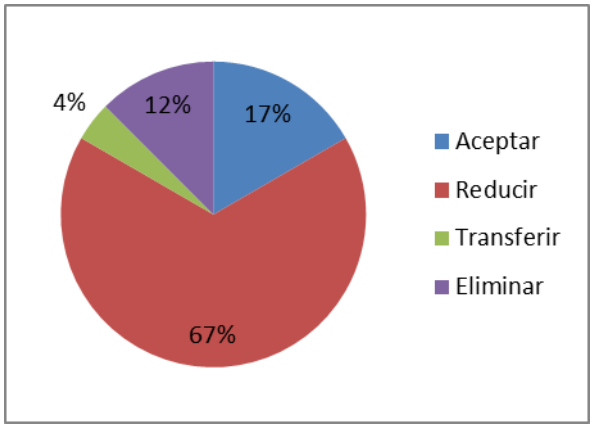
13. Robo por integrantes del grupo



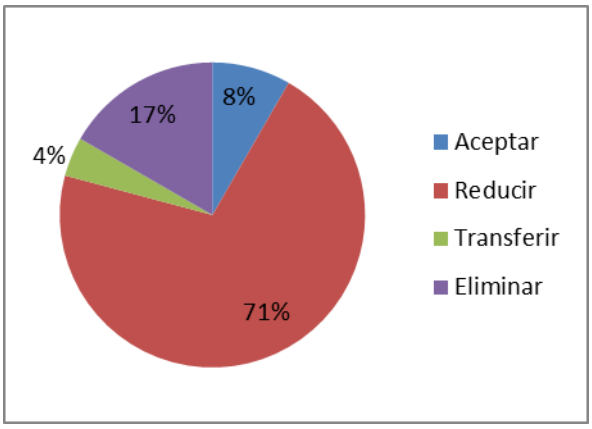
14. Violaciones de propiedad intelectual



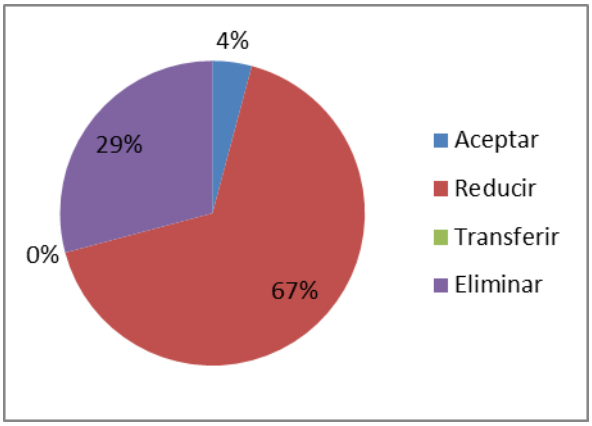
15. Expansión del uso de ordenadores personales y dispositivos móviles



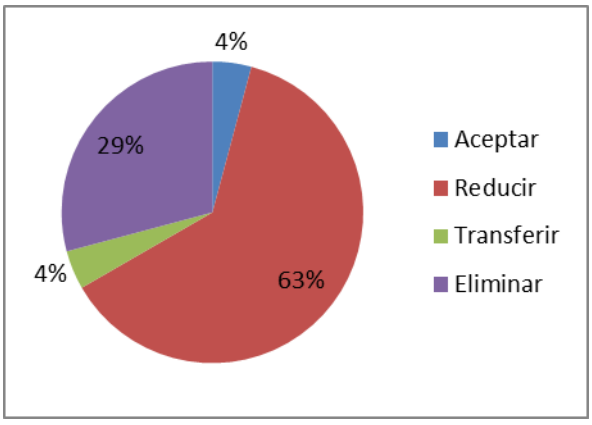
16. Daño de las copias de seguridad



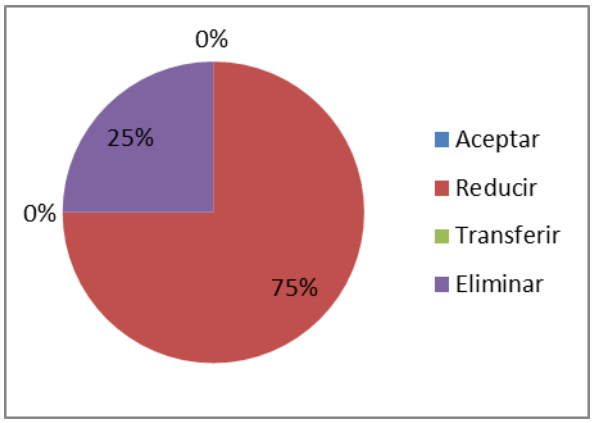
17. Usuarios con sobre-privilegios alteran los datos o interceptan información



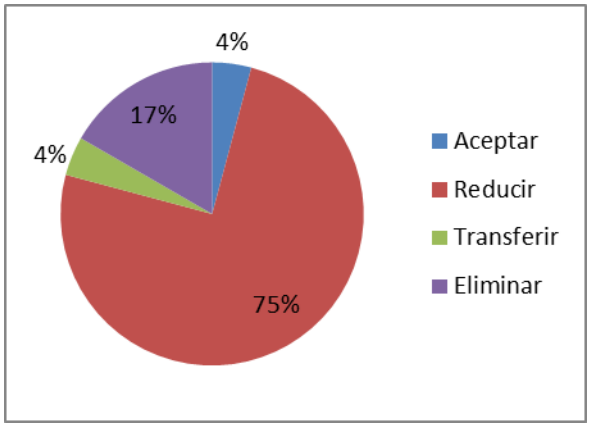
18. Incumplimiento de acuerdos de confidencialidad o privacidad establecidos



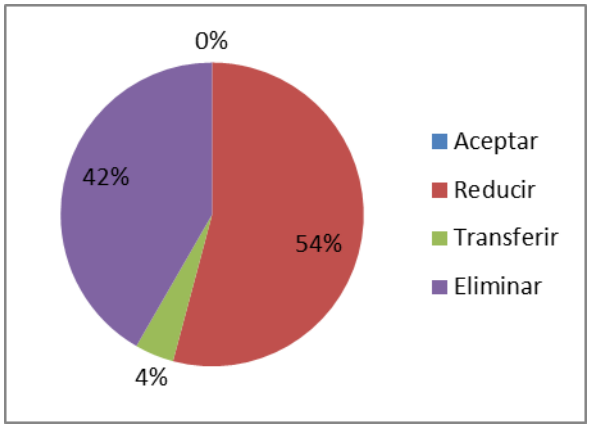
19. Información confidencial es divulgada por integrantes del grupo



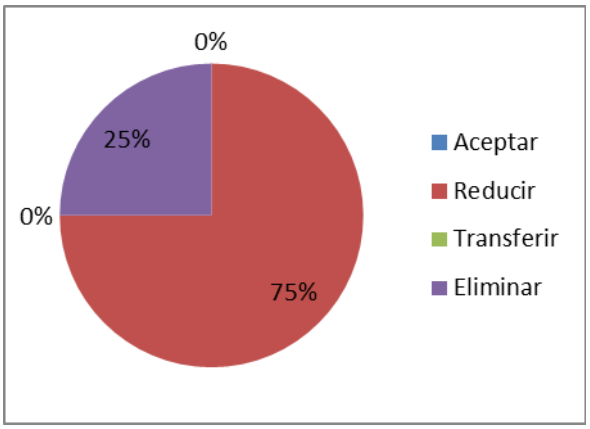
20. Incumplimiento de responsabilidades por modificaciones en los sistemas de información



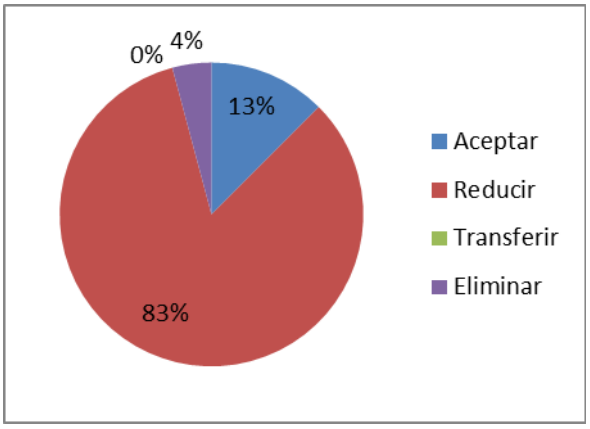
21. Acceso a software especializado con fines no académicos



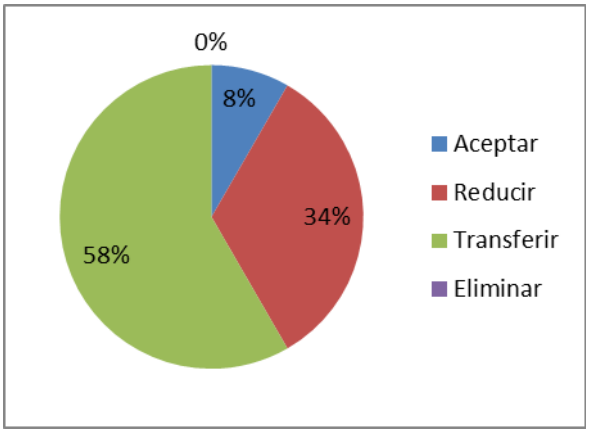
22. Modificación de información confidencial por integrantes del grupo.



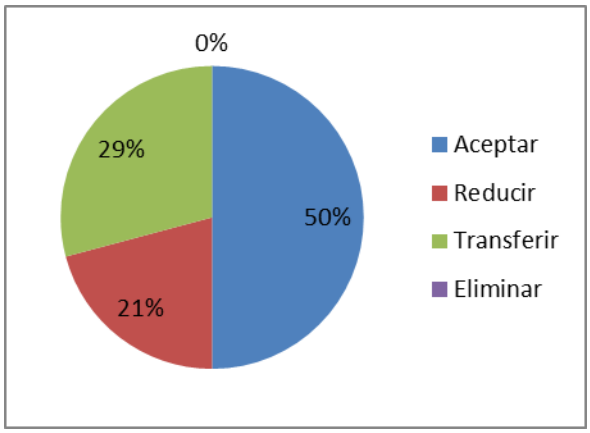
23. Fuga de conocimiento



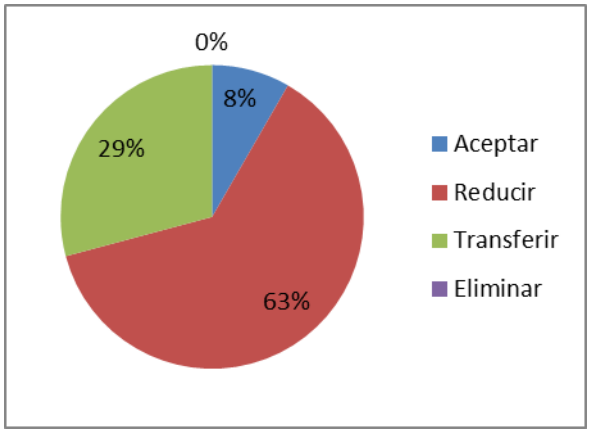
24. Ataques físicos, vandalismo y/o desordenes civiles.



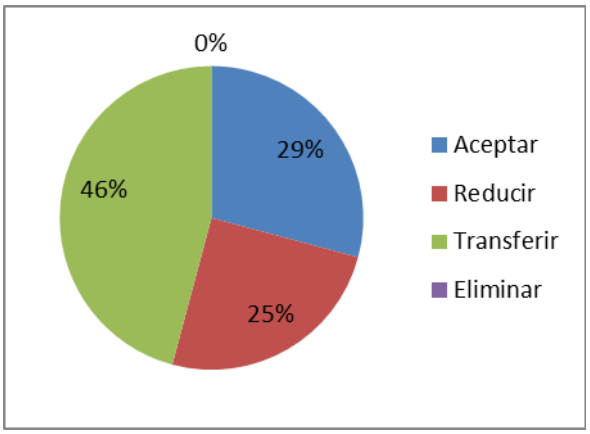
25. Desastres naturales



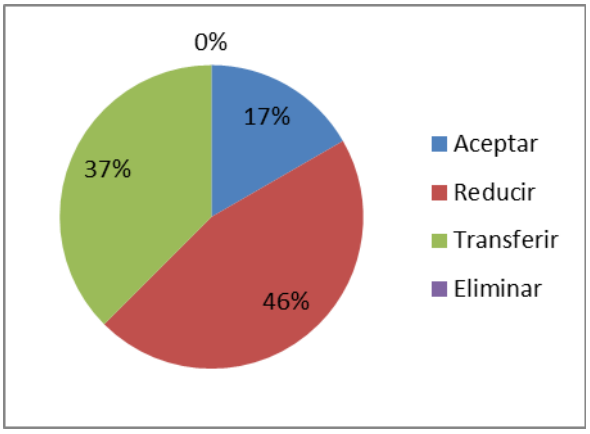
26. Fallas técnicas en equipos, redes o software



27. Interrupción de las actividades cotidianas por siniestros



28. Fallas en el suministro de energía



ANEXO 27. MATRIZ DE NIVEL DE RIESGO COMPLETA

	PROBABILIDAD BAJA	PROBABILIDAD MEDIA	PROBABILIDAD ALTA
IMPACTO ALTO	(3) Extorsión (12) Obsolescencia tecnológica (17) Incumplimiento política (19) Incumplimiento acuerdos confidencialidad (26) Desastres naturales (28) Siniestros	(2) Sabotaje o vandalismo (4) Personas malintencionadas (5) Daños en TI (8) Penetración desautorizada (14) Violaciones de propiedad intelectual (25) Ataques físicos, vandalismo (22) Acceso a softare académico	
IMPACTO MEDIO	(7) Ingeniería social (13) Robo por integrantes del grupo (18) usuarios con sobre privilegios alteran datos (21) Modificaciones en los sistemas de información (23) Modificación información confidencial	(1) Suplantación de identidad (6) Robo o pérdida accidental (10) Pérdida de información gestionada en la nube (11) Fallas en el hardware (16) Daño backups (20) Divulgación de información confidencial (27) Fallas técnicas en equipos, redes o software (29) Fallas suministro de energía	(9) Ataques de malware (15) Expansión del uso de ordenadores personales (24) Fuga de conocimiento
IMPACTO BAJO			

ANEXO 28. TABLA DE ASIGNACIÓN DE CONTROLES

Amenaza	Vulnerabilidad Asociada	Impacto	Riesgo	Control que aplica
(1) Suplantación de identidad	Controles de acceso lógico y/o físico inadecuados.	Costo de oportunidad	Suplantación de identidad por baja efectividad de los controles de seguridad físicos y/o errores humanos, que conlleva a perdidas de información confidencial a un costo muy alto.	8.3.3 Retirada de los derechos de acceso
	Descuidos, errores humanos	Incapacidad de cumplir con los objetivos organizativos		10.1.1 Documentación de los procedimientos de operación
	Integrantes del grupo no cumplen con la política de seguridad de la información.	Pérdida de confianza		10.7.3 Procedimientos de manipulación de la información
	La dirección no exige el cumplimiento de la política de seguridad de la información.	Pérdida de diferenciación y crecimiento		11.1.1 Política de control de acceso
	La dirección no apoya el desarrollo de una política de seguridad de la información.	Fuga de información		11.2.1 Registro de usuario
	La dirección no apoya los programas de capacitación y sensibilización para los	Pérdida de la privacidad		12.3.1 Política de uso de los controles criptográficos
	Integrantes del grupo no capacitados / inconscientes	Pérdida de ventajas competitivas		6.1.6 Contacto con las autoridades
	Contacto poco estrecho entre los integrantes del grupo.	Pérdidas financieras		8.1.3 Términos y condiciones de contratación
	Ausencia de programas de capacitación y sensibilización			8.2.1 Responsabilidades de la Dirección
	Ausencia de política de seguridad de la información			8.2.3 Proceso disciplinario
	Falta de controles de acceso lógido y/o físico			9.1.1 Perímetro de seguridad física
				9.1.2 Controles fisicos de entrada
				9.1.3 Seguridad de oficinas, despachos e instalaciones
				9.2.1 Emplazamiento y protección de equipos
				9.2.7 Retirada de materiales propiedad de la empresa
				10.7.4 Seguridad de la documentación del sistema
				10.8.1 Políticas y procedimientos de intercambio de información
				10.8.2 Acuerdos de intercambio
				10.10.1 Registros de auditoría
				10.10.3 Protección de la información de los registros
				10.10.4 Registros de administración y operación
				11.2.2 Gestión de privilegios
				11.2.3 Gestión de contraseñas de usuario
				11.2.4 Revisión de los derechos de acceso de usuario
				11.3.1 Uso de contraseñas
				11.3.2 Equipo de usuario desatendido
				11.4.2 Autenticación de usuario para conexiones externas
				11.5.1 Procedimientos seguros de inicio de sesión
				11.5.2 Identificación y autenticación de usuario
				11.5.3 Sistema de Gestión de contraseñas
				11.5.5 Desconexión automática de sesión
				11.5.6 Limitación del tiempo de conexión
				12.3.2 Gestión de claves
				12.5.4 Fugas de información
				15.1.6 Regulación de los controles criptográficos

ANEXO 29. TABLA DE CÁLCULO DE RIESGO RESIDUAL

	Valoración del impacto	Probabilidad de Ocurrencia	Nombre del control que debería estar implementado	Nivel de Efectividad del Control	Puntaje Control vs. Impacto	Score * Probabilidad de Ocurrencia	Riesgo Residual
Suplantación de identidad por baja efectividad de los controles de seguridad físicos y/o errores humanos, que conlleva a perdidas de información confidencial a un costo muy alto	2	40,0%	5.1.1 Documento de política de seguridad de la información	1	6	2,4	**2,50**
			6.1.1 Compromiso de la Dirección con la seguridad de la información	2	3	1,2	
			6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	1	6	2,4	
			8.2.2 Concienciación, formación y capacitación en seguridad de la información	1	6	2,4	
			8.3.3 Retirada de los derechos de acceso	1	6	2,4	
			10.1.1 Documentación de los procedimientos de operación	0	7	2,8	
			10.7.3 Procedimientos de manipulación de la información	1	6	2,4	
			11.1.1 Política de control de acceso	0	7	2,8	
			11.2.1 Registro de usuario	0	7	2,8	
			12.3.1 Política de uso de los controles criptográficos	0	7	2,8	
			13.1.1 Notificación de los eventos de seguridad de la información	0	7	2,8	
			14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	0	7	2,8	
Actos deliberados de sabotaje o vandalismo contra la información y/o TI del grupo, causados por supervisión inadecuada, controles de acceso inexistentes o insuficientes, falta de copias de seguridad y/o descuidos humanos, que conllevan a la interrupción de actividades cotidianas, pérdida de información, pérdida financiera e incumplimiento de compromisos adquiridos	4	50,0%	5.1.1 Documento de política de seguridad de la información	1	8	4	**4,18**
			6.1.1 Compromiso de la Dirección con la seguridad de la información	2	7	3,5	
			6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	1	8	4	
			6.2.1 Identificación de los riesgos derivados del acceso de terceros	1	8	4	
			8.2.2 Concienciación, formación y capacitación en seguridad de la información	1	8	4	
			8.3.3 Retirada de los derechos de acceso	1	8	4	
			10.1.3 Segregación de tareas	1	8	4	
			10.7.3 Procedimientos de manipulación de la información	1	8	4	
			11.1.1 Política de control de acceso	0	9	4,5	
			11.2.1 Registro de usuario	0	9	4,5	
			12.3.1 Política de uso de los controles criptográficos	0	9	4,5	
			12.6.1 Control de las vulnerabilidades técnicas	0	9	4,5	
			13.1.1 Notificación de los eventos de seguridad de la información	0	9	4,5	

	Valoración del impacto	Probabilidad de Ocurrencia	Nombre del control que debería estar implementado	Nivel de Efectividad del Control	Puntaje Control vs. Impacto	Score * Probabilidad de Ocurrencia	Riesgo Residual
			14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	0	9	4,5	
Actos deliberados de extorsión a los integrantes del grupo cuándo estos no son conscientes/capacitados, falta asesoramiento legal competente, faltan programas de concienciación, capacitación y formación, la administración no apoya dichos programas o no hay reporte de incidentes de forma oportuna y rápida	4	20,0%	5.1.1 Documento de política de seguridad de la información	1	8	1,6	**1,66**
			6.1.1 Compromiso de la Dirección con la seguridad de la información	2	7	1,4	
			6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	1	8	1,6	
			8.2.2 Concienciación, formación y capacitación en seguridad de la información	1	8	1,6	
			11.1.1 Política de control de acceso	0	9	1,8	
			13.1.1 Notificación de los eventos de seguridad de la información	0	9	1,8	
			14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	0	9	1,8	
Una persona malintencionada obtiene acceso a información confidencial del grupo de investigación por falta de políticas de seguridad, procedimientos definidos, controles de acceso lógico y físico, descuidos o errores humanos, o poca consciencia, lo cual puede generar pérdidas financieras, de la confianza, y/o de la ventaja competitiva	4	50,0%	5.1.1 Documento de política de seguridad de la información	1	8	4	**4,15**
			6.1.1 Compromiso de la Dirección con la seguridad de la información	2	7	3,5	
			6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	1	8	4	
			7.2.1 Directrices de clasificación	1	8	4	
			8.2.2 Concienciación, formación y capacitación en seguridad de la información	1	8	4	
			8.3.3 Retirada de los derechos de acceso	1	8	4	
			10.1.3 Segregación de tareas	1	8	4	
			10.7.3 Procedimientos de manipulación de la información	1	8	4	
			11.1.1 Política de control de acceso	0	9	4,5	
			11.2.1 Registro de usuario	0	9	4,5	
			12.3.1 Política de uso de los controles criptográficos	0	9	4,5	
			13.1.1 Notificación de los eventos de seguridad de la información	0	9	4,5	
			14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	0	9	4,5	
Interrupción de la disponibilidad de la información debido a un mantenimiento	4	49,5%	5.1.1 Documento de política de seguridad de la información	1	8	3,96	**4,07**
			6.1.1 Compromiso de la Dirección con la seguridad de la información	2	7	3,465	
			6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	1	8	3,96	

	Valoración del impacto	Probabilidad de Ocurrencia	Nombre del control que debería estar implementado	Nivel de Efectividad del Control	Puntaje Control vs. Impacto	Score * Probabilidad de Ocurrencia	Riesgo Residual
inadecuado de equipos de procesamiento de información y redes de comunicación, descuidos o errores humanos			6.2.1 Identificación de los riesgos derivados del acceso de terceros	1	8	3,96	
			8.2.2 Concienciación, formación y capacitación en seguridad de la información	1	8	3,96	
			10.1.3 Segregación de tareas	1	8	3,96	
			11.1.1 Política de control de acceso	0	9	4,455	
			13.1.1 Notificación de los eventos de seguridad de la información	0	9	4,455	
			14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	0	9	4,455	
Pérdida de activos de información como consecuencia de descuidos o errores humanos y controles inadecuados de seguridad	3	50,0%	5.1.1 Documento de política de seguridad de la información	1	7	3,5	**3,68**
			6.1.1 Compromiso de la Dirección con la seguridad de la información	2	6	3	
			6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	1	7	3,5	
			8.2.2 Concienciación, formación y capacitación en seguridad de la información	1	7	3,5	
			8.3.3 Retirada de los derechos de acceso	1	7	3,5	
			10.1.3 Segregación de tareas	1	7	3,5	
			11.1.1 Política de control de acceso	0	8	4	
			11.2.1 Registro de usuario	0	8	4	
			12.3.1 Política de uso de los controles criptográficos	0	8	4	
			13.1.1 Notificación de los eventos de seguridad de la información	0	8	4	
			14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	0	8	4	
Obtención de información confidencial por parte de personas no autorizadas y malintencionadas que se aprovechan del descuido o ingenuidad de los integrantes del grupo de la información	3	35,0%	5.1.1 Documento de política de seguridad de la información	1	7	2,45	**2,52**
			6.1.1 Compromiso de la Dirección con la seguridad de la información	2	6	2,1	
			6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	1	7	2,45	
			7.2.1 Directrices de clasificación	1	7	2,45	
			8.2.2 Concienciación, formación y capacitación en seguridad de la información	1	7	2,45	
			10.1.3 Segregación de tareas	1	7	2,45	
			10.7.3 Procedimientos de manipulación de la información	1	7	2,45	
			11.1.1 Política de control de acceso	0	8	2,8	
			13.1.1 Notificación de los eventos de seguridad de la información	0	8	2,8	

	Valoración del impacto	Probabilidad de Ocurrencia	Nombre del control que debería estar implementado	Nivel de Efectividad del Control	Puntaje Control vs. Impacto	Score * Probabilidad de Ocurrencia	Riesgo Residual
			14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	0	8	2,8	
Acceso o penetración desautorizada al sistema de información a través de la red debido a violaciones de los mecanismos de seguridad resultando en perdidas de información confidencial/estratégica, ventaja competitiva, dinero, confianza e imagen del grupo	4	45,0%	5.1.1 Documento de política de seguridad de la información	1	8	3,6	**3,78**
			6.1.1 Compromiso de la Dirección con la seguridad de la información	2	7	3,15	
			6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	1	8	3,6	
			8.2.2 Concienciación, formación y capacitación en seguridad de la información	1	8	3,6	
			10.1.3 Segregación de tareas	1	8	3,6	
			11.1.1 Política de control de acceso	0	9	4,05	
			12.3.1 Política de uso de los controles criptográficos	0	9	4,05	
			12.6.1 Control de las vulnerabilidades técnicas	0	9	4,05	
			13.1.1 Notificación de los eventos de seguridad de la información	0	9	4,05	
			14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	0	9	4,05	
Sufrir ataques de malware debido a falta de entrenamiento de los empleados, controles de acceso lógico inadecuados, o sobreprivilegios de integrantes del grupo que pueden causar daños en el software, pérdida de información e interrupción de las actividades cotidianas	2	70,0%	5.1.1 Documento de política de seguridad de la información	1	6	4,2	**4,28**
			6.1.1 Compromiso de la Dirección con la seguridad de la información	2	3	2,1	
			6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	1	6	4,2	
			8.2.2 Concienciación, formación y capacitación en seguridad de la información	1	6	4,2	
			10.1.3 Segregación de tareas	1	6	4,2	
			10.4.1 Controles contra el código malicioso	0	7	4,9	
			12.6.1 Control de las vulnerabilidades técnicas	0	7	4,9	
			13.1.1 Notificación de los eventos de seguridad de la información	0	7	4,9	
			14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	0	7	4,9	
Pérdida importante de la información confidencial/estratégica gestionada en la nube, e interrupción de las actividades cotidianas por descuidos de los integrantes del grupo,	3	50,0%	5.1.1 Documento de política de seguridad de la información	1	7	3,5	**3,61**
			6.1.1 Compromiso de la Dirección con la seguridad de la información	2	6	3	
			6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	1	7	3,5	
			7.2.1 Directrices de clasificación	1	7	3,5	
			8.2.2 Concienciación, formación y capacitación en seguridad de la información	1	7	3,5	

	Valoración del impacto	Probabilidad de Ocurrencia	Nombre del control que debería estar implementado	Nivel de Efectividad del Control	Puntaje Control vs. Impacto	Score * Probabilidad de Ocurrencia	Riesgo Residual
falta de seguridad o errores del software			10.1.1 Documentación de los procedimientos de operación	0	8	4	
			10.7.3 Procedimientos de manipulación de la información	1	7	3,5	
			13.1.1 Notificación de los eventos de seguridad de la información	0	8	4	
			14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	0	8	4	
Interrupción de las actividades cotidianas causada por fallas en el hardware cuando no existen políticas de mantenimiento de los equipos, o existen pero no se cumplen	2	40,0%	5.1.1 Documento de política de seguridad de la información	1	6	2,4	**2,40**
			6.1.1 Compromiso de la Dirección con la seguridad de la información	2	3	1,2	
			6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	1	6	2,4	
			8.2.2 Concienciación, formación y capacitación en seguridad de la información	1	6	2,4	
			10.1.1 Documentación de los procedimientos de operación	0	7	2,8	
			10.1.3 Segregación de tareas	1	6	2,4	
			13.1.1 Notificación de los eventos de seguridad de la información	0	7	2,8	
			14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	0	7	2,8	
Falta de capacidad para cumplir con los objetivos organizativos y posible pérdida de reputación causada por la obsolescencia tecnológica cuando no se realizan las actualizaciones adecuadas.	4	25,0%	5.1.1 Documento de política de seguridad de la información	1	8	2	**2,04**
			6.1.1 Compromiso de la Dirección con la seguridad de la información	2	7	1,75	
			6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	1	8	2	
			8.2.2 Concienciación, formación y capacitación en seguridad de la información	1	8	2	
			10.3.2 Aceptación del sistema	1	8	2	
			13.1.1 Notificación de los eventos de seguridad de la información	0	9	2,25	
			14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	0	9	2,25	
Interrupción de las actividades cotidianas, pérdida de ventaja competitiva, pérdida de dinaro, a causa de actos deliberados de robo cuando no existe verificación de antecedentes de los	3	20,0%	5.1.1 Documento de política de seguridad de la información	1	7	1,4	**1,42**
			6.1.1 Compromiso de la Dirección con la seguridad de la información	2	6	1,2	
			6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	1	7	1,4	
			7.2.1 Directrices de clasificación	1	7	1,4	
			8.1.2 Investigación de antecedentes	2	6	1,2	
			8.2.2 Concienciación, formación y capacitación en seguridad de la información	1	7	1,4	

	Valoración del impacto	Probabilidad de Ocurrencia	Nombre del control que debería estar implementado	Nivel de Efectividad del Control	Puntaje Control vs. Impacto	Score * Probabilidad de Ocurrencia	Riesgo Residual
miembros del grupo o los procesos disciplinarios son deficientes			10.1.3 Segregación de tareas	1	7	1,4	
			10.7.3 Procedimientos de manipulación de la información	1	7	1,4	
			11.1.1 Política de control de acceso	0	8	1,6	
			13.1.1 Notificación de los eventos de seguridad de la información	0	8	1,6	
			14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	0	8	1,6	
Pérdida de confianza, de dinero y sanciones o multas debido a violaciones de propiedad intelectual, por falta de normas, procedimientos o directrices en el tema, y personal inconsciente o no entrenado	4	40,0%	5.1.1 Documento de política de seguridad de la información	1	8	3,2	**3,29**
			6.1.1 Compromiso de la Dirección con la seguridad de la información	2	7	2,8	
			6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	1	8	3,2	
			7.2.1 Directrices de clasificación	1	8	3,2	
			8.2.2 Concienciación, formación y capacitación en seguridad de la información	1	8	3,2	
			10.7.3 Procedimientos de manipulación de la información	1	8	3,2	
			11.1.1 Política de control de acceso	0	9	3,6	
			13.1.1 Notificación de los eventos de seguridad de la información	0	9	3,6	
			14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	0	9	3,6	
Inaccesibilidad de la información cuando esta se necesita originada por la expansión del uso de ordenadores personales y dispositivos móviles que dificultan los controles de seguridad cuando no existe un inventario actualizado y los integrantes del grupo son inconscientes de los requerimientos de seguridad	3	70,0%	5.1.1 Documento de política de seguridad de la información	1	7	4,9	**5,16**
			6.1.1 Compromiso de la Dirección con la seguridad de la información	2	6	4,2	
			6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	1	7	4,9	
			8.2.2 Concienciación, formación y capacitación en seguridad de la información	1	7	4,9	
			11.7.2 Teletrabajo	0	8	5,6	
			12.3.1 Política de uso de los controles criptográficos	0	8	5,6	
			13.1.1 Notificación de los eventos de seguridad de la información	0	8	5,6	
			14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	0	8	5,6	
Incapacidad de cumplir con los objetivos	3	42,5%	5.1.1 Documento de política de seguridad de la información	1	7	2,975	**3,08**
			6.1.1 Compromiso de la Dirección con la seguridad de la información	2	6	2,55	

	Valoración del impacto	Probabilidad de Ocurrencia	Nombre del control que debería estar implementado	Nivel de Efectividad del Control	Puntaje Control vs. Impacto	Score * Probabilidad de Ocurrencia	Riesgo Residual
organizativos, pérdida de información, interrupción de las actividades cotidianas a causa de la pérdida o daño de las copias de seguridad cuando los procedimientos no están documentados, la dirección no organiza actividades capacitación y los integrantes del grupo son inconscientes de los requerimientos de seguridad de la información			6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	1	7	2,975	
			8.2.2 Concienciación, formación y capacitación en seguridad de la información	1	7	2,975	
			10.1.1 Documentación de los procedimientos de operación	0	8	3,4	
			10.1.3 Segregación de tareas	1	7	2,975	
			13.1.1 Notificación de los eventos de seguridad de la información	0	8	3,4	
			14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	0	8	3,4	
Integrantes del grupo con sobre-privilegios o descuidados pueden realizar alteración de datos o interceptar información confidencial	3	30,0%	5.1.1 Documento de política de seguridad de la información	1	7	2,1	**2,17**
			6.1.1 Compromiso de la Dirección con la seguridad de la información	2	6	1,8	
			6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	1	7	2,1	
			7.2.1 Directrices de clasificación	1	7	2,1	
			8.1.2 Investigación de antecedentes	2	6	1,8	
			8.2.2 Concienciación, formación y capacitación en seguridad de la información	1	7	2,1	
			10.1.3 Segregación de tareas	1	7	2,1	
			10.7.3 Procedimientos de manipulación de la información	1	7	2,1	
			11.1.1 Política de control de acceso	0	8	2,4	
			11.2.1 Registro de usuario	0	8	2,4	
			12.3.1 Política de uso de los controles criptográficos	0	8	2,4	
			13.1.1 Notificación de los eventos de seguridad de la información	0	8	2,4	
			14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	0	8	2,4	
Un trabajador o un tercero presenta una demanda o litigio contra el grupo de investigación por violación de derechos	4	30,0%	5.1.1 Documento de política de seguridad de la información	1	8	2,4	**2,46**
			6.1.1 Compromiso de la Dirección con la seguridad de la información	2	7	2,1	
			6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	1	8	2,4	
			8.1.2 Investigación de antecedentes	2	7	2,1	

	Valoración del impacto	Probabilidad de Ocurrencia	Nombre del control que debería estar implementado	Nivel de Efectividad del Control	Puntaje Control vs. Impacto	Score * Probabilidad de Ocurrencia	Riesgo Residual
de privacidad, divulgación de información confidencial, o incumplimiento de acuerdos establecidos de intercambio de información o conocimiento			8.2.2 Concienciación, formación y capacitación en seguridad de la información	1	8	2,4	
			12.3.1 Política de uso de los controles criptográficos	0	9	2,7	
			13.1.1 Notificación de los eventos de seguridad de la información	0	9	2,7	
			14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	0	9	2,7	
			15.1.1 Identificación de la legislación aplicable	0	9	2,7	
			15.1.4 Protección de datos y privacidad de la información de carácter personal	1	8	2,4	
Información confidencial (como avances o resultados de proyectos, datos recopilados en una investigación, información personal de los investigadores, propuestas o planes de proyectos) es divulgada debido a vulnerabilidades humanas y técnicas causadas por insuficientes controles de seguridad	3	40,0%	5.1.1 Documento de política de seguridad de la información	1	7	2,8	**2,89**
			6.1.1 Compromiso de la Dirección con la seguridad de la información	2	6	2,4	
			6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	1	7	2,8	
			8.1.2 Investigación de antecedentes	2	6	2,4	
			8.2.2 Concienciación, formación y capacitación en seguridad de la información	1	7	2,8	
			8.3.3 Retirada de los derechos de acceso	1	7	2,8	
			10.1.3 Segregación de tareas	1	7	2,8	
			10.7.3 Procedimientos de manipulación de la información	1	7	2,8	
			11.1.1 Política de control de acceso	0	8	3,2	
			11.2.1 Registro de usuario	0	8	3,2	
			12.3.1 Política de uso de los controles criptográficos	0	8	3,2	
			13.1.1 Notificación de los eventos de seguridad de la información	0	8	3,2	
			14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	0	8	3,2	
Interrupción de las rutinas organizativas causada por la modificación parcial o completa del contenido o modo de funcionamiento del sistema operativo sin autorización cuando no existe claridad en los roles y	3	30,0%	5.1.1 Documento de política de seguridad de la información	1	7	2,1	**2,19**
			6.1.1 Compromiso de la Dirección con la seguridad de la información	2	6	1,8	
			6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	1	7	2,1	
			8.1.2 Investigación de antecedentes	2	6	1,8	
			8.2.2 Concienciación, formación y capacitación en seguridad de la información	1	7	2,1	
			8.3.3 Retirada de los derechos de acceso	1	7	2,1	
			10.1.1 Documentación de los procedimientos de operación	0	8	2,4	

	Valoración del impacto	Probabilidad de Ocurrencia	Nombre del control que debería estar implementado	Nivel de Efectividad del Control	Puntaje Control vs. Impacto	Score * Probabilidad de Ocurrencia	Riesgo Residual
responsabilidades de los integrantes del grupo ni verificación de antecedentes de los mismos			10.1.3 Segregación de tareas	1	7	2,1	
			10.7.3 Procedimientos de manipulación de la información	1	7	2,1	
			11.1.1 Política de control de acceso	0	8	2,4	
			11.2.1 Registro de usuario	0	8	2,4	
			12.3.1 Política de uso de los controles criptográficos	0	8	2,4	
			13.1.1 Notificación de los eventos de seguridad de la información	0	8	2,4	
			14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	0	8	2,4	
Personas desautorizadas acceden a software especializado o información para fines comerciales y no académicos lo cual haría efectivas clausulas contractuales del proveedor del servicio; esto se causa por los cambios de acceso informal, derechos de acceso no consistentes con las funciones/roles del usuario, entre otras vulnerabilidades	4	40,0%	5.1.1 Documento de política de seguridad de la información	1	8	3,2	**3,32**
			6.1.1 Compromiso de la Dirección con la seguridad de la información	2	7	2,8	
			6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	1	8	3,2	
			8.2.2 Concienciación, formación y capacitación en seguridad de la información	1	8	3,2	
			8.3.3 Retirada de los derechos de acceso	1	8	3,2	
			10.1.3 Segregación de tareas	1	8	3,2	
			11.1.1 Política de control de acceso	0	9	3,6	
			11.2.1 Registro de usuario	0	9	3,6	
			13.1.1 Notificación de los eventos de seguridad de la información	0	9	3,6	
			14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	0	9	3,6	
Incapacidad para cumplir con los objetivos organizativos, pérdida de confianza, alteración de resultados de un proyecto causados por adición de información o modificación de información relevante debido a que los controles de seguridad implementados son débiles, no hay verificación de	3	25,0%	5.1.1 Documento de política de seguridad de la información	1	7	1,75	**1,80**
			6.1.1 Compromiso de la Dirección con la seguridad de la información	2	6	1,5	
			6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	1	7	1,75	
			7.2.1 Directrices de clasificación	1	7	1,75	
			8.1.2 Investigación de antecedentes	2	6	1,5	
			8.2.2 Concienciación, formación y capacitación en seguridad de la información	1	7	1,75	
			8.3.3 Retirada de los derechos de acceso	1	7	1,75	
			10.1.3 Segregación de tareas	1	7	1,75	
			10.7.3 Procedimientos de manipulación de la información	1	7	1,75	
			11.1.1 Política de control de acceso	0	8	2	

	Valoración del impacto	Probabilidad de Ocurrencia	Nombre del control que debería estar implementado	Nivel de Efectividad del Control	Puntaje Control vs. Impacto	Score * Probabilidad de Ocurrencia	Riesgo Residual
antecedentes de los integrantes del grupo o no hay procedimientos de uso de la información documentados			11.2.1 Registro de usuario	0	8	2	
			12.3.1 Política de uso de los controles criptográficos	0	8	2	
			13.1.1 Notificación de los eventos de seguridad de la información	0	8	2	
			14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	0	8	2	
La ausencia de clausulas de permanencia, junto con la incapacidad financiera para ofrecer remuneración lo suficientemente atractiva, permiten que haya fuga de conocimiento hacia otras organizaciones lo cual ocasiona discontinuidad en los procesos, perdida de esfuerzo, tiempo, habilidades, capacidades y talentos, además de disminuir la eficiencia y la productividad	3	70,0%	5.1.1 Documento de política de seguridad de la información	1	7	4,9	**5,00**
			6.1.1 Compromiso de la Dirección con la seguridad de la información	2	6	4,2	
			6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	1	7	4,9	
			8.2.2 Concienciación, formación y capacitación en seguridad de la información	1	7	4,9	
			8.3.3 Retirada de los derechos de acceso	1	7	4,9	
			13.1.1 Notificación de los eventos de seguridad de la información	0	8	5,6	
			14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	0	8	5,6	
Sufrir pérdidas financieras, de equipos, y/o vidas humanas así como la interrupción de actividades cotidianas causadas por insuficiente seguridad frente a ataques físicos, vandalismo y desordenes civiles	4	40,0%	5.1.1 Documento de política de seguridad de la información	1	8	3,2	**3,25**
			6.1.1 Compromiso de la Dirección con la seguridad de la información	2	7	2,8	
			6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	1	8	3,2	
			8.2.2 Concienciación, formación y capacitación en seguridad de la información	1	8	3,2	
			9.1.4 Protección contra las amenazas externas y de origen ambiental	1	8	3,2	
			10.1.3 Segregación de tareas	1	8	3,2	
			13.1.1 Notificación de los eventos de seguridad de la información	0	9	3,6	
			14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	0	9	3,6	
Sufrir pérdidas financieras, de equipos o vidas humanas, debido a desastres naturales y a la falta de preparación para reaccionar ante su ocurrencia	5	20,0%	5.1.1 Documento de política de seguridad de la información	1	9	1,8	**1,83**
			6.1.1 Compromiso de la Dirección con la seguridad de la información	2	8	1,6	
			6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	1	9	1,8	
			8.2.2 Concienciación, formación y capacitación en seguridad de la información	1	9	1,8	
			9.1.4 Protección contra las amenazas externas y de origen ambiental	1	9	1,8	

	Valoración del impacto	Probabilidad de Ocurrencia	Nombre del control que debería estar implementado	Nivel de Efectividad del Control	Puntaje Control vs. Impacto	Score * Probabilidad de Ocurrencia	Riesgo Residual
(mantenimiento y seguridad insuficientes)			13.1.1 Notificación de los eventos de seguridad de la información	0	10	2	
			14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	0	10	2	
Debido a daños inesperados en las TI, se pone en peligro la integridad o disponibilidad de la información	3	40,0%	5.1.1 Documento de política de seguridad de la información	1	7	2,8	**2,87**
			6.1.1 Compromiso de la Dirección con la seguridad de la información	2	6	2,4	
			6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	1	7	2,8	
			8.1.2 Investigación de antecedentes	2	6	2,4	
			8.2.2 Concienciación, formación y capacitación en seguridad de la información	1	7	2,8	
			10.1.1 Documentación de los procedimientos de operación	0	8	3,2	
			10.1.3 Segregación de tareas	1	7	2,8	
			10.3.2 Aceptación del sistema	1	7	2,8	
			12.6.1 Control de las vulnerabilidades técnicas	0	8	3,2	
			13.1.1 Notificación de los eventos de seguridad de la información	0	8	3,2	
			14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	0	8	3,2	
Interrupción de las actividades cotidianas, pérdidas financieras o pérdida de vidas humanas, a causa de siniestros como incendio, explosión, colapso de las edificaciones, etc., cuando el mantenimiento de las instalaciones físicas es deficiente	4	22,5%	5.1.1 Documento de política de seguridad de la información	1	8	1,8	**1,83**
			6.1.1 Compromiso de la Dirección con la seguridad de la información	2	7	1,575	
			6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	1	8	1,8	
			8.2.2 Concienciación, formación y capacitación en seguridad de la información	1	8	1,8	
			9.1.4 Protección contra las amenazas externas y de origen ambiental	1	8	1,8	
			13.1.1 Notificación de los eventos de seguridad de la información	0	9	2,025	
			14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	0	9	2,025	
Interrupción de las actividades cotidianas y pérdida temporal de información causada por fluctuaciones o fallas en el suministro de energía cuando hay ausencia de planta	2	40,0%	5.1.1 Documento de política de seguridad de la información	1	6	2,4	**2,33**
			6.1.1 Compromiso de la Dirección con la seguridad de la información	2	3	1,2	
			6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	1	6	2,4	
			8.2.2 Concienciación, formación y capacitación en seguridad de la información	1	6	2,4	
			13.1.1 Notificación de los eventos de	0	7	2,8	

	Valoración del impacto	Probabilidad de Ocurrencia	Nombre del control que debería estar implementado	Nivel de Efectividad del Control	Puntaje Control vs. Impacto	Score * Probabilidad de Ocurrencia	Riesgo Residual
eléctrica o el servicio de suministro es deficiente.			seguridad de la información				
			14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	0	7	2,8	

ANEXO 30. FICHAS DE RIESGO

Formato de Riesgo					
No:	001		**Fecha:**	02-mar-12	
Impacto	MEDIO	**Probabilidad**	MEDIA	**Prioridad**	MEDIA
Declaración de riesgo (con contexto)					
Suplantación de identidad ocasionando pérdidas de información confidencial con costos altos. **Causado por:** - Controles de acceso físico inadecuados. - Descuidos, errores humanos. - Integrantes del grupo no capacitados / inconscientes. - Contacto poco estrecho entre los integrantes del grupo. - Ausencia de programas de capacitación y sensibilización. - Ausencia de política de seguridad de la información.					
	Requiere atención inmediata de la dirección				
Recomendaciones para tratar el riesgo (opcional): Mitigar el riesgo					

Formato de Riesgo					
No:	002		**Fecha:**	02-mar-12	
Impacto	ALTO	**Probabilidad**	MEDIA	**Prioridad**	ALTA
Declaración de riesgo (con contexto)					
Sabotaje o vandalismo contra la información y/o sistemas de información del grupo, que conllevan a la interrupción de actividades cotidianas, pérdida de información, pérdida financiera e incumplimiento de compromisos adquiridos. **Causado por:** - Descuidos, errores humanos - Ausencia de programas de capacitación y sensibilización - Ausencia de política de seguridad de la información - No hay controles de acceso lógico y físico - Supervisión inadecuada del uso del sistema de información - Seguridad insuficiente en los servidores, tecnologías de red, redes de acceso - No se realizan copias de seguridad de la información confidencial					
X	Requiere atención inmediata de la dirección				
Recomendaciones para tratar el riesgo (opcional): Mitigar el riesgo					

Formato de Riesgo					
No:	003		**Fecha:**	02-mar-12	
Impacto	ALTO	**Probabilidad**	BAJA	**Prioridad**	MEDIA
Declaración de riesgo (con contexto)					
Extorsión a los integrantes del grupo, que resulta en fuga de información, pérdida financiera y/o de la confianza. **Causado por:** - Falta de asesoramiento legal competente - Integrantes del grupo no capacitados / inconscientes - Ausencia de programas de capacitación y sensibilización - No hay reporte de incidentes de forma oportuna y rápida - No hay conocimiento sobre protección y comercialización de derechos de propiedad intelectual - No existen normas, procedimientos o directrices documentadas en un manual - No hay un responsable de la protección de la privacidad de la información. - Ausencia de política de seguridad de la información					
	Requiere atención inmediata de la dirección				
Recomendaciones para tratar el riesgo (opcional):					
Clasificación:					

Formato de Riesgo					
No:	004		**Fecha:**	02-mar-12	
Impacto	ALTO	**Probabilidad**	MEDIA	**Prioridad**	ALTA
Declaración de riesgo (con contexto)					
Personas malintencionadas acceden y/u obtienen información confidencial por cualquier medio generando pérdida financiera y de ventaja competitiva. **Causado por:** - Ausencia de política de seguridad de la información - No hay controles de acceso lógico y físico - Descuidos, errores humanos - Las responsabilidades de seguridad de la información no son claras para los integrantes del grupo - No esta protegida adecuadamente la información de acuerdo a su grado de confidencialidad y tampoco se tiene delegada esa responsabilidad en el grupo con claridad. - Poca consciencia sobre la importancia de la información					
X	Requiere atención inmediata de la dirección				
Recomendaciones para tratar el riesgo (opcional):					
Clasificación:					

Formato de Riesgo					
No:	005		**Fecha:**	02-mar-12	
Impacto	ALTO	**Probabilidad**	MEDIA	**Prioridad**	ALTA
Declaración de riesgo (con contexto)					
Daños en TI (equipos) afectando la disponibilidad de la información, suspensión de las actividades cotidianas e incumplimiento de compromisos adquiridos. **Causados por:** - Descuidos o errores humanos - Ausencia de controles de acceso físico - Ausencia de política de seguridad de la información - Las responsabilidades de seguridad de la información, TI e instalaciones físicas no son claras para los miembros del grupo - No hay reporte de incidentes de forma oportuna y rápida - Ausencia de programas de capacitación y sensibilización					
X	Requiere atención inmediata de la dirección				
Recomendaciones para tratar el riesgo (opcional):					
Clasificación:					

Formato de Riesgo					
No:	006		**Fecha:**	02-mar-12	
Impacto	MEDIO	**Probabilidad**	MEDIA	**Prioridad**	MEDIA
Declaración de riesgo (con contexto)					
Robo o pérdida accidental de activos de información que genera pérdidas financieras, interrupción de actividades cotidianas, y costos de reemplazo de equipos. **Causado por:** - Controles de acceso físico inadecuados - Descuidos, errores humanos -Ausencia de política de seguridad de la información - Procedimientos de seguridad física inadecuados - Mantenimiento deficiente de las instalaciones físicas - Las responsabilidades de seguridad de la información, TI e instalaciones físicas no son claras para los miembros del grupo - Seguridad física insuficiente - Ausencia de programas de capacitación y sensibilización					
	Requiere atención inmediata de la dirección				
Recomendaciones para tratar el riesgo (opcional):					
Clasificación:					

Formato de Riesgo					
No:	007		**Fecha:**	02-mar-12	
Impacto	MEDIO	**Probabilidad**	BAJA	**Prioridad**	BAJA
Declaración de riesgo (con contexto)					
Criminales informáticos obtienen información confidencial a través de la ingeniería social causando pérdida de ventaja competitiva, deterioro de la imagen y confianza. **Causado por:** - Ausencia de política de seguridad de la información - Ausencia de programas de capacitación y sensibilización - Integrantes del grupo no entrenados/ inconscientes - Descuidos o errores humanos. - Poca consciencia sobre la importancia de la información - No esta protegida adecuadamente la información de acuerdo a su grado de confidencialidad y tampoco se tiene delegada esa responsabilidad en el grupo con claridad.					
	Requiere atención inmediata de la dirección				
Recomendaciones para tratar el riesgo (opcional):					
Clasificación:					

Formato de Riesgo					
No:	008		**Fecha:**	02-mar-12	
Impacto	ALTO	**Probabilidad**	MEDIA	**Prioridad**	ALTA
Declaración de riesgo (con contexto)					
Ingreso desautorizado al sistema de información a través de la red para obtener información confidencial, causando pérdida de ventaja competitiva, confianza y altos costos de oportunidad. **Causado por:** - No existen criterios de aceptación para nuevas aplicaciones y sistemas - Los controles implementados son débiles / falta nivel apropiado de controles de seguridad - Seguridad insuficiente en los servidores, tecnologías de red - Ausencia de programas de capacitación y sensibilización - Ausencia de política de seguridad de la información - No hay reporte de incidentes de manera oportuna y rápida - No esta protegida adecuadamente la información de acuerdo a su grado de confidencialidad y tampoco se tiene delegada esta responsabilidad en el grupo con claridad.					
X	Requiere atención inmediata de la dirección				
Recomendaciones para tratar el riesgo (opcional):					
Clasificación:					

Formato de Riesgo					
No:	009		**Fecha:**	02-mar-12	
Impacto	MEDIO	**Probabilidad**	ALTA	**Prioridad**	ALTA
Declaración de riesgo (con contexto)					
Ataques de malware que pueden causar daños en el software, pérdida de información e interrupción de las actividades cotidianas. **Causados por:** - Errores de software - Sobreprivilegios de usuario - Descuidos o errores humanos - integrantes del grupo no entrenados / inconscientes - Falta de controles de acceso lógico - Ausencia de programas de capacitación y sensibilización - Ausencia de política de seguridad de la información					
X	Requiere atención inmediata de la dirección				
Recomendaciones para tratar el riesgo (opcional):					
Clasificación:					

Formato de Riesgo					
No:	010		**Fecha:**	02-mar-12	
Impacto	MEDIO	**Probabilidad**	MEDIA	**Prioridad**	MEDIA
Declaración de riesgo (con contexto)					
Pérdida importante de información gestionada en la nube, que interrumpe las actividades cotidianas. **Causada por:** - Poca seguridad en los servidores, tecnologías de red, redes de acceso... - Descuidos o errores humanos - No se realizan copias de seguridad - Integrantes del grupo manejan parte de la información mediante servicios ofrecidos en la nube. - Ausencia de programas de capacitación y sensibilización - Ausencia de política de seguridad de la información					
	Requiere atención inmediata de la dirección				
Recomendaciones para tratar el riesgo (opcional):					
Clasificación:					

Formato de Riesgo					
No:	011		**Fecha:**	02-mar-12	
Impacto	MEDIO	**Probabilidad**	MEDIA	**Prioridad**	MEDIA
Declaración de riesgo (con contexto)					
Interrupción de las actividades cotidianas causada por fallas en el hardware. (Interrupción de la disponibilidad de la información) **Causada por:** - No existen políticas de mantenimiento de los equipos - Ausencia de política de seguridad de la información - Ausencia de programas de capacitación y sensibilización - Descuidos o errores humanos - No hay reporte de incidentes de forma oportuna y rápida					
	Requiere atención inmediata de la dirección				
Recomendaciones para tratar el riesgo (opcional):					
Clasificación:					

Formato de Riesgo					
No:	012		**Fecha:**	02-mar-12	
Impacto	ALTO	**Probabilidad**	BAJA	**Prioridad**	MEDIA
Declaración de riesgo (con contexto)					
Incumplimiento de objetivos organizativos y posible pérdida de reputación causada por la obsolescencia tecnológica. **Causado por:** - No se realizan las actualizaciones adecuadas. - Descuidos o errores humanos - Ausencia de programas de capacitación y sensibilización					
	Requiere atención inmediata de la dirección				
Recomendaciones para tratar el riesgo (opcional):					
Clasificación:					

Formato de Riesgo					
No:	013		**Fecha:**	02-mar-12	
Impacto	MEDIO	**Probabilidad**	BAJA	**Prioridad**	BAJA
Declaración de riesgo (con contexto)					
Interrupción de las actividades cotidianas, pérdida de ventaja competitiva, pérdida de dinero, a causa de actos deliberados de robo por integrantes del grupo. **Causada por:** - No hay verificación de antecedentes de los integrantes del grupo de investigación - Procesos disciplinarios deficientes - Ausencia de política de seguridad de la información - No hay reporte de incidentes de forma oportuna y rápida					
	Requiere atención inmediata de la dirección				
Recomendaciones para tratar el riesgo (opcional):					
Clasificación:					

Formato de Riesgo					
No:	014		**Fecha:**	02-mar-12	
Impacto	ALTO	**Probabilidad**	MEDIA	**Prioridad**	ALTA
Declaración de riesgo (con contexto)					
Pérdida de confianza, de dinero y sanciones o multas debido a violaciones de propiedad intelectual. **Causada por:** **-** Integrantes no entrenados / inconscientes - No existen normas, procedimientos o directrices documentadas en un manual - No hay conocimiento sobre protección y comercialización de derechos de propiedad intelectual - Ausencia de política de seguridad de la información - Ausencia de programas de capacitación y sensibilización					
X	Requiere atención inmediata de la dirección				
Recomendaciones para tratar el riesgo (opcional):					
Clasificación:					

Formato de Riesgo					
No:	015		**Fecha:**	02-mar-12	
Impacto	MEDIO	**Probabilidad**	ALTA	**Prioridad**	ALTA
Declaración de riesgo (con contexto)					
Se ve comprometida la disponibilidad, confidencialidad y/o integridad de la información por la expansión del uso de ordenadores personales y dispositivos móviles que dificultan los controles de seguridad. **Causado por:** - Ausencia de inventario actualizado de equipos e información - Conexiones inseguras a servicios de red no autorizados - Los integrantes del grupo no son conscientes de los requerimientos de seguridad de la información - Integrantes del grupo no entrenados - Ausencia de programas de capacitación y sensibilización - Ausencia de política de seguridad de la información					
X	Requiere atención inmediata de la dirección				
Recomendaciones para tratar el riesgo (opcional):					
Clasificación:					

Formato de Riesgo					
No:	016		**Fecha:**	02-mar-12	
Impacto	MEDIO	**Probabilidad**	MEDIA	**Prioridad**	MEDIA
Declaración de riesgo (con contexto)					
Incapacidad de cumplir con los objetivos organizativos, pérdida de información, interrupción de las actividades cotidianas a causa de la pérdida o daño de las copias de seguridad. **Causado por:** - Procedimientos de copias de seguridad no documentados - Los integrantes del grupo no son conscientes de los requerimientos de seguridad de la información - Integrantes del grupo no entrenados - Ausencia de política de seguridad de la información - Ausencia de programas de capacitación y sensibilización					
	Requiere atención inmediata de la dirección				
Recomendaciones para tratar el riesgo (opcional):					
Clasificación:					

Formato de Riesgo					
No:	017		**Fecha:**	02-mar-12	
Impacto	MEDIO	**Probabilidad**	BAJA	**Prioridad**	BAJA
Declaración de riesgo (con contexto)					
Usuarios con sobre-privilegios o descuidados pueden realizar alteración de datos o interceptar información confidencial **Causado por:** - Sobreprivilegios de usuario - Descuidos o errores humanos - Ausencia de política de seguridad de la información - Los derechos de acceso no son consistentes con las funciones o roles de usuario - Ausencia de programas de capacitación y sensibilización					
	Requiere atención inmediata de la dirección				
Recomendaciones para tratar el riesgo (opcional):					
Clasificación:					

Formato de Riesgo					
No:	018		**Fecha:**	02-mar-12	
Impacto	ALTO	**Probabilidad**	BAJA	**Prioridad**	MEDIA
Declaración de riesgo (con contexto)					
Demanda contra el grupo por incumplimiento de acuerdos de confidencialidad o privacidad establecidos, ocasionando sanciones/multas, pérdidas financieras y deterioro de la confianza y la buena imagen. **Causado por:** - No hay acuerdos de obligaciones legales para la relación con terceros - Desconocimiento de las normas legales vigentes/aplicables al contexto del grupo de investigación - Falta de asesoramiento legal competente - No esta protegida la información personal de los integrantes y las partes interesadas del grupo - No hay un responsable de la protección de la privacidad de la información - No se firman acuerdos de confidencialidad - Ausencia de programas de capacitación y sensibilización - Ausencia de política de seguridad de la información					
	Requiere atención inmediata de la dirección				
Recomendaciones para tratar el riesgo (opcional):					
Clasificación:					

Formato de Riesgo					
No:	019		**Fecha:**	02-mar-12	
Impacto	MEDIO	**Probabilidad**	MEDIA	**Prioridad**	MEDIA
Declaración de riesgo (con contexto)					
Información confidencial es divulgada por integrantes del grupo causando pérdida de ventaja competitiva, financiera, y deterioro de la confianza y la buena imagen. **Causado por:** - Poca consciencia sobre la importancia de la información - Ausencia de objetivos de seguridad de la información - Descuidos o errores humanos - El acceso lógico no es retirado inmediatamente o no es examinado antes de ser concedido - Información confidencial se encuentra en activos eliminados o reasignados y se puede acceder por un usuario no autorizado - No existe claridad de roles y responsabilidades de seguridad de la información - No existe clasificación de la información - No se firman acuerdos de confidencialidad - Poca claridad del concepto de confidencialidad de la información					
	Requiere atención inmediata de la dirección				
Recomendaciones para tratar el riesgo (opcional):					
Clasificación:					

Formato de Riesgo					
No:	020		**Fecha:**	02-mar-12	
Impacto	MEDIO	**Probabilidad**	BAJA	**Prioridad**	BAJA
Declaración de riesgo (con contexto)					
Interrupción de las actividades cotidianas y posible incumplimiento de responsabilidades adquiridas, provocados por la modificación parcial o completa del sistema de información por integrantes del grupo. **Causado por:** - No existe claridad de roles y responsabilidades de cada integrante del grupo - No hay verificación de antecedentes de los integrantes del grupo de investigación - Ausencia de programas de capacitación y sensibilización					
	Requiere atención inmediata de la dirección				
Recomendaciones para tratar el riesgo (opcional):					
Clasificación:					

Formato de Riesgo					
No:	021		**Fecha:**	02-mar-12	
Impacto	ALTO	**Probabilidad**	MEDIA	**Prioridad**	ALTA
Declaración de riesgo (con contexto)					
Personas desautorizadas acceden a software especializado con fines no académicos haciendo efectivas las clausulas contractuales del proveedor del servicio; y como consecuencia deterioro de la imagen, y pérdidas financieras. **Causado por:** - El acceso no es retirado inmediatamente o no es examinado antes de ser concedido - Los cambios de acceso son informales o inadecuados - Los derechos de acceso no son consistentes con los roles de usuario - No hay retiro de los beneficios institucionales una vez el usuario se retira del grupo de investigación - No hay claridad de roles y responsabilidades de cada integrante del grupo - Ausencia de programas de capacitación y sensibilización - Ausencia de política de seguridad de la información					
X	Requiere atención inmediata de la dirección				
Recomendaciones para tratar el riesgo (opcional):					
Clasificación:					

Formato de Riesgo					
No:	022		**Fecha:**	02-mar-12	
Impacto	MEDIO	**Probabilidad**	BAJA	**Prioridad**	BAJA
Declaración de riesgo (con contexto)					
Incapacidad para cumplir con los objetivos organizativos, pérdida de confianza, alteración de resultados de un proyecto causados por modificación de información confidencial por integrantes del grupo. **Causado por:** - Los controles implementados son débiles - No existe claridad de roles y responsabilidades para cada integrante del grupo - No hay verificación de antecedentes de los integrantes del grupo de investigación - Procedimientos de uso no documentados en un manual de acceso libre para los integrantes - Ausencia de política de seguridad de la información - Ausencia de programas de capacitación y sensibilización					
	Requiere atención inmediata de la dirección				
Recomendaciones para tratar el riesgo (opcional):					
Clasificación:					

Formato de Riesgo					
No:	023		**Fecha:**	02-mar-12	
Impacto	MEDIO	**Probabilidad**	ALTA	**Prioridad**	ALTA
Declaración de riesgo (con contexto)					
Fuga de conocimiento que provoca discontinuidad en los procesos; pérdida de esfuerzo, tiempo, habilidades, capacidades y talentos; disminución la eficiencia y la productividad científica del grupo. **Causado por:** - Ausencia de cláusulas de permanencia en el grupo de investigación - Incapacidad financiera para ofrecer remuneración lo suficientemente atractiva para que el investigador decida permanecer en el grupo - No hay compromiso de los integrantes del grupo - No hay políticas que exijan la transferencia de conocimiento - Ausencia de programas de capacitación y sensibilización - Ausencia de política de seguridad de la información					
X	Requiere atención inmediata de la dirección				
Recomendaciones para tratar el riesgo (opcional):					
Clasificación:					

Formato de Riesgo					
No:	024		**Fecha:**	02-mar-12	
Impacto	ALTO	**Probabilidad**	MEDIA	**Prioridad**	ALTA
Declaración de riesgo (con contexto)					
Pérdidas financieras, de equipos, y/o vidas humanas así como la interrupción de actividades cotidianas como consecuencia de ataques físicos, vandalismo y/o desórdenes civiles. **Causado por:** - Seguridad física insuficiente - Ubicación vulnerable de las instalaciones					
X	Requiere atención inmediata de la dirección				
Recomendaciones para tratar el riesgo (opcional):					
Clasificación:					

Formato de Riesgo					
No:	025		**Fecha:**	02-mar-12	
Impacto	ALTO	**Probabilidad**	BAJA	**Prioridad**	MEDIA
Declaración de riesgo (con contexto)					
Pérdidas financieras, de equipos y/o vidas humanas, debido a desastres naturales. **Causado por:** - Seguridad física insuficiente - Mantenimiento deficiente de las instalaciones físicas					
	Requiere atención inmediata de la dirección				
Recomendaciones para tratar el riesgo (opcional):					
Clasificación:					

Formato de Riesgo					
No:	026		**Fecha:**	02-mar-12	
Impacto	MEDIO	**Probabilidad**	MEDIA	**Prioridad**	MEDIA
Declaración de riesgo (con contexto)					
Debido a Fallas técnicas en equipos, redes o software, se pone en peligro la integridad o disponibilidad de la información y la Imposibilidad de realizar actividades cotidianas. **Causado por:** - Capacitación inadecuada de los integrantes del grupo del sistema - Ausencia de programas de capacitación y sensibilización - Supervisión inadecuada del uso del sistema - No existe política de mantenimiento de los equipos					
	Requiere atención inmediata de la dirección				
Recomendaciones para tratar el riesgo (opcional):					
Clasificación:					

Formato de Riesgo					
No:	027		**Fecha:**	02-mar-12	
Impacto	ALTO	**Probabilidad**	BAJA	**Prioridad**	MEDIA
Declaración de riesgo (con contexto)					
Interrupción de las actividades cotidianas, pérdidas financieras, y/o vidas humanas, causada por siniestros como incendio, explosión, colapso de un edificio etc. **Causada por:** - Mantenimiento deficiente de las instalaciones - Seguridad física insuficiente - Descuidos o errores humanos					
	Requiere atención inmediata de la dirección				
Recomendaciones para tratar el riesgo (opcional):					
Clasificación:					

Formato de Riesgo					
No:	028		**Fecha:**	02-mar-12	
Impacto	MEDIO	**Probabilidad**	MEDIA	**Prioridad**	MEDIA
Declaración de riesgo (con contexto)					
Interrupción de las actividades cotidianas y pérdida temporal de información causada por fluctuaciones o fallas en el suministro de energía. **Causado por:** - Ausencia de planta eléctrica - Servicio de suministro deficiente					
	Requiere atención inmediata de la dirección				
Recomendaciones para tratar el riesgo (opcional):					
Clasificación:					

ANEXO 31. HOJAS DE INFORMACIÓN DE RIESGOS CRÍTICOS

Hoja de información de riesgos			
ID 002	**Fecha de identificación**	2-mar-2012	
Prioridad ALTA	**Declaración**	Actos deliberados de sabotaje o vandalismo	
Probabilidad MEDIA	**Origen**	Personas externas	
Impacto ALTO	**Asignado a**		
Contexto: Sabotaje o vandalismo contra la información y/o sistemas de información del grupo, que conllevan a la interrupción de actividades cotidianas, pérdida de información, pérdida financiera e incumplimiento de compromisos adquiridos. **Causado por:** - Descuidos o errores humanos - integrantes del grupo no entrenados / inconscientes - Ausencia de programas de capacitación y sensibilización - Ausencia de política de seguridad de la información - No hay controles de acceso lógico y físico - Supervisión inadecuada del uso del sistema de información - Seguridad insuficiente en los servidores, tecnologías de red, redes de acceso - No se realizan copias de seguridad de la información confidencial - No hay reporte de incidentes de forma oportuna y rápida - Las responsabilidades de seguridad de la información no son claras para los integrantes del grupo - El acceso no es retirado inmediatamente o no es examinado antes de ser concedido			
Estrategia de mitigación: - Documento de política de seguridad de la información - Compromiso de la dirección con la seguridad de la información - Asignación de responsabilidades relativas a la seguridad de la información - Concienciación, formación y capacitación en seguridad de la información - Control de las vulnerabilidades técnicas - Notificación de los eventos de seguridad de la información - Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio - Identificación de los riesgos derivados del acceso de terceros - Retirada de los derechos de acceso - Segregación de tareas - Procedimientos de manipulación de la información - Política de control de acceso - Registro de usuario - Políticas de uso de los controles criptográficos			
Estado:			
Aprobación:	**Fecha de cierre:**	**Justificación de cierre:**	

Hoja de información de riesgos			
ID 004		**Fecha de identificación**	2-mar-2012
Prioridad ALTA		**Declaración**	Acceso desautorizado a información confidencial
Probabilidad MEDIA		**Origen**	Personas externas
Impacto ALTO		**Asignado a**	

Contexto:

Personas malintencionadas acceden y/u obtienen información confidencial por cualquier medio generando pérdida financiera y de ventaja competitiva.

Causado por:

- Descuidos o errores humanos
- integrantes del grupo no entrenados / inconscientes
- Ausencia de programas de capacitación y sensibilización
- Ausencia de política de seguridad de la información
- No hay controles de acceso lógico y físico
- Las responsabilidades de seguridad de la información no son claras para los integrantes del grupo
- No esta protegida adecuadamente la información de acuerdo a su grado de confidencialidad.
- Poca consciencia sobre la importancia de la información
- No hay reporte de incidentes de forma oportuna y rápida
- Las responsabilidades de seguridad de la información no son claras para los integrantes del grupo
- El acceso no es retirado inmediatamente o no es examinado antes de ser concedido

Estrategia de mitigación:

- Documento de política de seguridad de la información
- Compromiso de la dirección con la seguridad de la información
- Asignación de responsabilidades relativas a la seguridad de la información
- Concienciación, formación y capacitación en seguridad de la información
- Directrices de clasificación
- Segregación de tareas
- Retirada de los derechos de acceso
- Procedimientos de manipulación de la información
- Política de control de acceso
- Registro de usuario
- Política de uso de los controles criptográficos
- Notificación de los eventos de seguridad de la información
- Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio

Estado:

Aprobación:	**Fecha de cierre:**	**Justificación de cierre:**

Hoja de información de riesgos			
ID 005	**Fecha de identificación**	2-mar-2012	
Prioridad ALTA	**Declaración**	Interrupción de la disponiblidad de la información por la destrucción o daño de las TICs	
Probabilidad MEDIA	**Origen**		
Impacto ALTA	**Asignado a**		

Contexto:
Daños en TICs (equipos) afectando la disponibilidad de la información, suspensión de las actividades cotidianas e incumplimiento de compromisos adquiridos.

Causados por:
- Descuidos o errores humanos
- integrantes del grupo no entrenados / inconscientes
- Ausencia de programas de capacitación y sensibilización
- Ausencia de controles de acceso físico
- Ausencia de política de seguridad de la información
- Las responsabilidades de seguridad de la información no son claras para los integrantes del grupo
- No hay reporte de incidentes de forma oportuna y rápida

Estrategia de mitigación:
- Documento de política de seguridad de la información
- Compromiso de la dirección con la seguridad de la información
- Asignación de responsabilidades relativas a la seguridad de la información
- Concienciación, formación y capacitación en seguridad de la información
- Identificación de los riesgos derivados del acceso de terceros
- Segregación de tareas
- Política de control de acceso
- Notificación de los eventos de seguridad de la información
- Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio

Estado:

Aprobación:	**Fecha de cierre:**	**Justificación de cierre:**

Hoja de información de riesgos			
ID 008	**Fecha de identificación:**	2-mar-2012	
Prioridad ALTA	**Declaración**	Ingreso desautorizado al sistema de información a través de la red	
Probabilidad MEDIA	**Origen**		
Impacto ALTO	**Asignado a**		

Contexto:
Ingreso desautorizado al sistema de información a través de la red para obtener información confidencial, causando pérdida de ventaja competitiva, confianza y altos costos de oportunidad.

Causado por:
- Descuidos o errores humanos
- integrantes del grupo no entrenados / inconscientes
- Ausencia de programas de capacitación y sensibilización
- No existen criterios de aceptación para nuevas aplicaciones y sistemas
- Los controles implementados son débiles / falta nivel apropiado de controles de seguridad
- Seguridad insuficiente en los servidores, tecnologías de red
- Ausencia de política de seguridad de la información
- No hay reporte de incidentes de manera oportuna y rápida
- No esta protegida adecuadamente la información de acuerdo a su grado de confidencialidad
- Las responsabilidades de seguridad de la información no son claras para los integrantes del grupo

Estrategia de mitigación:
- Documento de política de seguridad de la información
- Compromiso de la dirección con la seguridad de la información
- Asignación de responsabilidades relativas a la seguridad de la información
- Concienciación, formación y capacitación en seguridad de la información
- Segregación de tareas
- Política de control de acceso
- Política de uso de los controles criptográficos
- Control de las vulnerabilidades técnicas
- Notificación de los eventos de seguridad de la información
- Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio

Estado:

Aprobación:	**Fecha de cierre:**	**Justificación de cierre:**

Hoja de información de riesgos			
ID 009	**Fecha de identificación:**	2-mar-2012	
Prioridad ALTA	**Declaración**	Ataques deliberados de malware	
Probabilidad ALTA	**Origen**	Criminal informático	
Impacto MEDIO	**Asignado a**		
Contexto: Ataques de malware que pueden causar daños en el software, pérdida de información e interrupción de las actividades cotidianas. **Causados por:** - Descuidos o errores humanos - integrantes del grupo no entrenados / inconscientes - Ausencia de programas de capacitación y sensibilización - Errores de software - Sobreprivilegios de usuario - Falta de controles de acceso lógico - Ausencia de política de seguridad de la información - No hay reporte de incidentes de forma oportuna y rápida - Las responsabilidades de seguridad de la información no son claras para los integrantes del grupo			
Estrategia de mitigación: - Documento de política de seguridad de la información - Compromiso de la dirección con la seguridad de la información - Asignación de responsabilidades relativas a la seguridad de la información - Concienciación, formación y capacitación en seguridad de la información - Segregación de tareas - Controles contra el código malicioso - Control de las vulnerabilidades técnicas - Notificación de los eventos de seguridad de la información - Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio			
Estado:			
Aprobación:	**Fecha de cierre:**	**Justificación de cierre:**	

Hoja de información de riesgos			
ID 014	**Fecha de identificación:**	2-mar-2012	
Prioridad ALTA	**Declaración**	Violación a la propiedad intelectual	
Probabilidad MEDIA	**Origen**	Personas internas	
Impacto ALTO	**Asignado a**		

Contexto:

Pérdida de confianza, de dinero y sanciones o multas debido a violaciones de propiedad intelectual.

Causada por:

- Descuidos o errores humanos
- Integrantes no entrenados / inconscientes
- No existen normas, procedimientos o directrices documentadas en un manual
- No hay conocimiento sobre protección y comercialización de derechos de propiedad intelectual
- Ausencia de política de seguridad de la información
- Ausencia de programas de capacitación y sensibilización
- No hay reporte de incidentes de forma oportuna y rápida
- Las responsabilidades de seguridad de la información no son claras para los integrantes del grupo
- No esta protegida adecuadamente la información de acuerdo a su grado de confidencialidad

Estrategia de mitigación:

- Documento de política de seguridad de la información
- Compromiso de la dirección con la seguridad de la información
- Asignación de responsabilidades relativas a la seguridad de la información
- Concienciación, formación y capacitación en seguridad de la información
- Directrices de clasificación
- Procedimientos de manipulación de la información
- Política de control de acceso
- Notificación de los eventos de seguridad de la información
- Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio

Estado:

Aprobación:	**Fecha de cierre:**	**Justificación de cierre:**

Hoja de información de riesgos			
ID 015	**Fecha de identificación:**	2-mar-2012	
Prioridad ALTA	**Declaración**	Expansión del uso de ordenadores personales (dispositivos móviles), lo cual dificulta los controles de seguridad	
Probabilidad ALTA	**Origen**	Personas internas	
Impacto MEDIO	**Asignado a**		

Contexto:

Se ve comprometida la disponibilidad, confidencialidad y/o integridad de la información por la expansión del uso de ordenadores personales y dispositivos móviles que dificultan los controles de seguridad.

Causado por:

- Descuidos o errores humanos
- Ausencia de inventario actualizado de equipos e información
- Conexiones inseguras a servicios de red no autorizados
- Integrantes no entrenados / inconscientes
- Ausencia de programas de capacitación y sensibilización
- Ausencia de política de seguridad de la información
- No hay reporte de incidentes de forma oportuna y rápida
- Las responsabilidades de seguridad de la información no son claras para los integrantes del grupo

Estrategia de mitigación:

- Documento de política de seguridad de la información
- Compromiso de la dirección con la seguridad de la información
- Asignación de responsabilidades relativas a la seguridad de la información
- Concienciación, formación y capacitación en seguridad de la información
- Teletrabajo
- Política de uso de los controles criptográficos
- Notificación de los eventos de seguridad de la información
- Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio

Estado:

Aprobación:	**Fecha de cierre:**	**Justificación de cierre:**

Hoja de información de riesgos			
ID 021		**Fecha de identificación:**	2-mar-2012
Prioridad ALTA		**Declaración**	Acceso desautorizado a software especializado o información con fines no académicos
Probabilidad MEDIA		**Origen**	Personas internas
Impacto ALTO		**Asignado a**	

Contexto:

Personas desautorizadas acceden a software especializado con fines no académicos haciendo efectivas las clausulas contractuales del proveedor del servicio; y como consecuencia deterioro de la imagen, y pérdidas financieras.

Causado por:

- Descuidos o errores humanos
- integrantes del grupo no entrenados / inconscientes
- Ausencia de programas de capacitación y sensibilización
- El acceso no es retirado inmediatamente o no es examinado antes de ser concedido
- Los cambios de acceso son informales o inadecuados
- Los derechos de acceso no son consistentes con los roles de usuario
- No hay retiro de los beneficios institucionales una vez el usuario se retira del grupo de investigación
- Las responsabilidades de seguridad de la información no son claras para los integrantes del grupo
- Ausencia de política de seguridad de la información
- No hay reporte de incidentes de forma oportuna y rápida

Estrategia de mitigación:

- Documento de política de seguridad de la información
- Compromiso de la dirección con la seguridad de la información
- Asignación de responsabilidades relativas a la seguridad de la información
- Concienciación, formación y capacitación en seguridad de la información
- Retirada de los derechos de acceso
- Segregación de tareas
- Política de control de acceso
- Registro de usuario
- Notificación de los eventos de seguridad de la información
- Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio

Estado:

Aprobación:	**Fecha de cierre:**	**Justificación de cierre:**

Hoja de información de riesgos			
ID 023	**Fecha de identificación:**	2-mar-2012	
Prioridad ALTA	**Declaración**	Fuga de conocimiento	
Probabilidad ALTA	**Origen**	Personas internas	
Impacto MEDIO	**Asignado a**		

Contexto:

Fuga de conocimiento que provoca discontinuidad en los procesos; pérdida de esfuerzo, tiempo, habilidades, capacidades y talentos; disminución la eficiencia y la productividad científica del grupo.

Causado por:

- Descuidos o errores humanos
- Integrantes del grupo no entrenados / inconscientes
- Ausencia de programas de capacitación y sensibilización
- Ausencia de cláusulas de permanencia en el grupo de investigación
- Incapacidad financiera para ofrecer remuneración lo suficientemente atractiva para que el investigador decida permanecer en el grupo
- No hay compromiso de los integrantes del grupo
- No hay políticas que exijan la transferencia de conocimiento
- Ausencia de política de seguridad de la información
- No hay reporte de incidentes de forma oportuna y rápida
- Las responsabilidades de seguridad de la información no son claras para los integrantes del grupo
-El acceso no es retirado inmediatamente o no es examinado antes de ser concedido

Estrategia de mitigación:

- Documento de política de seguridad de la información
- Compromiso de la dirección con la seguridad de la información
- Asignación de responsabilidades relativas a la seguridad de la información
- Concienciación, formación y capacitación en seguridad de la información
- Retirada de los derechos de acceso
- Notificación de los eventos de seguridad de la información
- Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio

Estado:

Aprobación:	**Fecha de cierre:**	**Justificación de cierre:**

Hoja de información de riesgos			
ID 024	**Fecha de identificación:**	2-mar-2012	
Prioridad ALTA	**Declaración**	Ataques físicos, vandalismo y/o desórdenes civiles	
Probabilidad MEDIA	**Origen**	Vándalo	
Impacto ALTO	**Asignado a**		

Contexto:

Pérdidas financieras, de equipos, y/o vidas humanas así como la interrupción de actividades cotidianas como consecuencia de ataques físicos, vandalismo y/o desórdenes civiles.

Causado por:

- Descuidos o errores humanos
- Integrantes del grupo no entrenados / inconscientes
- Ausencia de programas de capacitación y sensibilización
- Seguridad física insuficiente
- Ubicación vulnerable de las instalaciones
- No hay reporte de incidentes de forma oportuna y rápida
- Ausencia de política de seguridad de la información
- Las responsabilidades de seguridad de la información no son claras para los integrantes del grupo

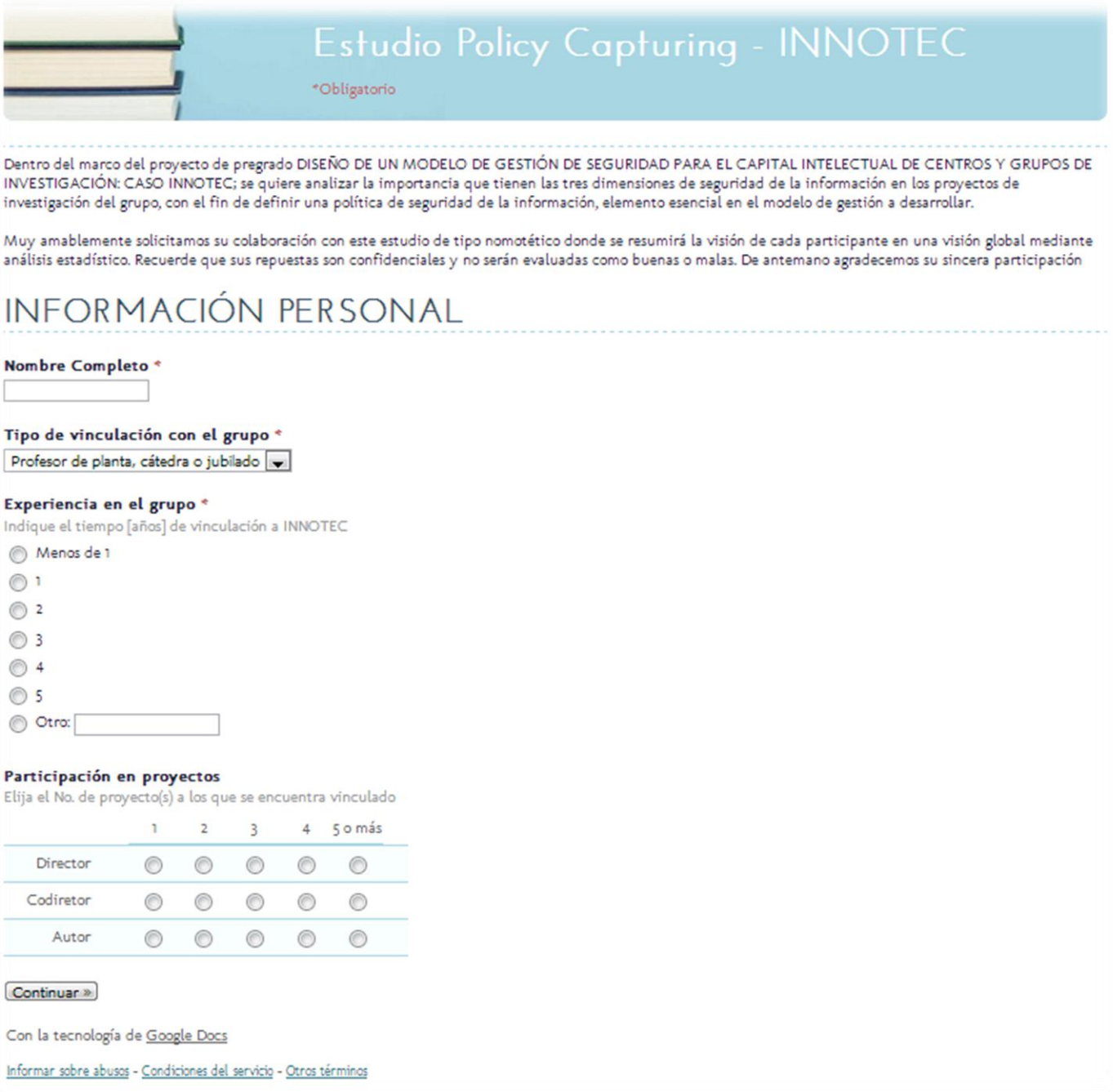
Estrategia de mitigación:

- Documento de política de seguridad de la información
- Compromiso de la dirección con la seguridad de la información
- Asignación de responsabilidades relativas a la seguridad de la información
- Concienciación, formación y capacitación en seguridad de la información
- Protección contra las amenazas externas y de origen ambiental
- Segregación de tareas
- Notificación de los eventos de seguridad de la información
- Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio

Estado:

Aprobación:	**Fecha de cierre:**	**Justificación de cierre:**

ANEXO 32. CUESTIONARIO POLICY CAPTURING



Estudio Policy Capturing - INNOTEC

*Obligatorio

Dentro del marco del proyecto de pregrado DISEÑO DE UN MODELO DE GESTIÓN DE SEGURIDAD PARA EL CAPITAL INTELECTUAL DE CENTROS Y GRUPOS DE INVESTIGACIÓN: CASO INNOTEC; se quiere analizar la importancia que tienen las tres dimensiones de seguridad de la información en los proyectos de investigación del grupo, con el fin de definir una política de seguridad de la información, elemento esencial en el modelo de gestión a desarrollar.

Muy amablemente solicitamos su colaboración con este estudio de tipo nomotético donde se resumirá la visión de cada participante en una visión global mediante análisis estadístico. Recuerde que sus repuestas son confidenciales y no serán evaluadas como buenas o malas. De antemano agradecemos su sincera participación

INFORMACIÓN PERSONAL

Nombre Completo *

Tipo de vinculación con el grupo *

Profesor de planta, cátedra o jubilado

Experiencia en el grupo *

Indique el tiempo [años] de vinculación a INNOTEC

- Menos de 1
- 1
- 2
- 3
- 4
- 5
- Otro:

Participación en proyectos

Elija el No. de proyecto(s) a los que se encuentra vinculado

	1	2	3	4	5 o más
Director					
Codirector					
Autor					

Continuar »

Con la tecnología de Google Docs

Informar sobre abusos - Condiciones del servicio - Otros términos

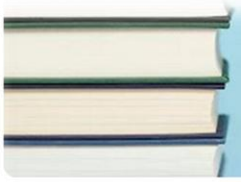
Estudio Policy Capturing - INNOTEC

ANTES DE COMENZAR TENGA EN CUENTA LAS SIGUIENTES DEFINICIONES

- CONFIDENCIALIDAD: Es la necesidad de que la información sensible de los proyectos desarrollados en INNOTEC sólo sea conocida por personas autorizadas
- INTEGRIDAD: Es la característica que hace que el contenido de la información permanezca inalterado, a menos que sea modificado o eliminado por personal autorizado
- DISPONIBILIDAD: Es la característica que hace que la información esté siempre disponible en el momento que la necesiten, para ser procesada por las personas autorizadas.

- MEDIDA DE CONTROL: medidas para eliminar la causa de una no conformidad detectada u otra situación indeseable (Acciones correctivas).

« Atrás | Continuar »



Estudio Policy Capturing - INNOTEC

INSTRUCCIONES

Teniendo en cuenta el CONTEXTO GENERAL, lea cuidadosamente cada una de las situaciones que se le presentan, y asuma que usted está realmente en el escenario descrito. Por favor, NO subestime NI exagere sus respuestas; sea honesto. Conteste con base en el escenario correspondiente SIN tener en cuenta el anterior.

CONTEXTO GENERAL

Usted está participando como coordinador en un proyecto de cooperación internacional, donde se esta realizando una investigación que debe terminar (según cronograma) en 6 meses. Como parte de los compromisos adquiridos, se debe entregar: 1 artículo publicable en una revista internacional, 1 manual de buenas prácticas, 3 ponencias, y la documentación de la experiencia. Para ello, usted cuenta con el siguiente equipo de trabajo: 2 profesionales de apoyo, 2 auxiliares administrativos, 2 estudiantes de maestría en pasantía de investigación.

Por favor suponga que este proyecto es de gran impacto para la proyección del grupo y de la universidad en el mundo. Y la información que se está manejando en los productos y resultados es crítica, por tanto, su gestión debe ser cuidadosa, de tal manera que se conserve la ventaja competitiva.

« Atrás | Continuar »

Estudio Policy Capturing - INNOTEC

*Obligatorio

Escenario 1

Recientemente, usted envió copia de varios informes de la primera etapa del proyecto; la persona encargada de recibir el sobre con los documentos acaba de confirmar que están completos y en perfecto estado. Además, usted esta trabajando en un artículo publicable, accediendo a la información necesaria en el sistema de información del grupo. Sin embargo, usted ha descubierto que información clasificada como confidencial en el proyecto esta siendo divulgada sin autorización.

¿Aplicaría medidas de control en este caso? *

	Ningún control	Control leve	Control moderado	Control fuerte	Control muy fuerte
Indique si aplicaría medidas de control y de qué magnitud	○	○	○	○	○

Aclaración de las opciones de respuesta

- NINGÚN CONTROL: Las condiciones no ameritan la implementación de medidas de control, usted se siente tranquilo.
- LEVE: Se requieren algunos controles, con un costo mínimo y de rápida implementación, con tan sólo horas para que usted solucione la situación.
- MODERADO: Se requieren controles que implican costos significativos y algunos días para su implementación. Usted puede hacerse cargo de la situación.
- FUERTE: La situación causa daños en la calidad del proyecto, pero se pueden reparar, incurriendo en costos altos, intervención de la dirección del grupo y algunos meses para implementar controles.
- MUY FUERTE: Se requiere completo compromiso de la dirección, costos altos, e incluso pueden existir daños irreparables. Se necesitarán meses para implementar controles.

« Atrás | Continuar »

Estudio Policy Capturing - INNOTEC

*Obligatorio

Escenario 2

Usted y su equipo de trabajo mantienen la confidencialidad respecto a los resultados del proyecto. Como apoyo a la etapa actual, han consultado información de proyectos anteriores. Sin embargo, realizando una revisión detallada, notaron que existen datos desactualizados y otros incompletos. Después de indagar, descubre que uno de los auxiliares del grupo que NO es parte del proyecto, modificó los archivos sin que nadie notara los cambios.

¿Aplicaría medidas de control en este caso? *

	Ningún control	Control leve	Control moderado	Control fuerte	Control muy fuerte
Indique si aplicaría medidas de control y de qué magnitud	○	○	○	○	○

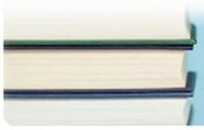
Aclaración de las opciones de respuesta

- NINGÚN CONTROL: Las condiciones no ameritan la implementación de medidas de control, usted se siente tranquilo.
- LEVE: Se requieren algunos controles, con un costo mínimo y de rápida implementación, con tan sólo horas para que usted solucione la situación.
- MODERADO: Se requieren controles que implican costos significativos y algunos días para su implementación. Usted puede hacerse cargo de la situación.
- FUERTE: La situación causa daños en la calidad del proyecto, pero se pueden reparar, incurriendo en costos altos, intervención de la dirección del grupo y algunos meses para implementar controles.
- MUY FUERTE: Se requiere completo compromiso de la dirección, costos altos, e incluso pueden existir daños irreparables. Se necesitarán meses para implementar controles.

« Atrás | Continuar »

Con la tecnología de Google Docs

Informar sobre abusos - Condiciones del servicio - Otros términos



Estudio Policy Capturing - INNOTEC

*Obligatorio

Escenario 3

Mientras usted trabajaba en la redacción del informe final, el suministro de energía fue interrumpido, y perdió los datos que se estaban procesando en un software especializado desde hace dos días, los cuales eran parte de los análisis del informe. Además, en la sala de investigación donde estaba trabajando, el ingreso de personas es libre, y un estudiante utilizó accidentalmente algunos de sus documentos (impresos) como papel de reciclaje; esta situación permitió que personal no autorizado conociera información exclusiva del proyecto.

¿Aplicaría medidas de control en este caso? *

	Ningún control	Control leve	Control moderado	Control fuerte	Control muy fuerte
Indique si aplicaría medidas de control y de qué magnitud	○	○	○	○	○

Aclaración de las opciones de respuesta

- NINGÚN CONTROL: Las condiciones no ameritan la implementación de medidas de control, usted se siente tranquilo.
- LEVE: Se requieren algunos controles, con un costo mínimo y de rápida implementación, con tan sólo horas para que usted solucione la situación.
- MODERADO: Se requieren controles que implican costos significativos y algunos días para su implementación. Usted puede hacerse cargo de la situación.
- FUERTE: La situación causa daños en la calidad del proyecto, pero se pueden reparar, incurriendo en costos altos, intervención de la dirección del grupo y algunos meses para implementar controles.
- MUY FUERTE: Se requiere completo compromiso de la dirección, costos altos, e incluso pueden existir daños irreparables. Se necesitarán meses para implementar controles.

« Atrás | Continuar »

Estudio Policy Capturing - INNOTEC

*Obligatorio

Escenario 4

Usted necesita continuamente consultar datos sobre otros proyectos que ha realizado el grupo; por tanto, tiene acceso completo al sistema de información del grupo, donde a su vez puede cargar versiones de los documentos de avance del proyecto. El día de ayer uno de los estudiantes eliminó accidentalmente la versión del informe que usted estaba redactando. Aparte de esto, usted olvidó accidentalmente el portátil en la oficina, y personas ajenas al proyecto conocieron información NO sólo del proyecto sino de los demás archivos guardados en el equipo.

¿Aplicaría medidas de control en este caso? *

	Ningún control	Control leve	Control moderado	Control fuerte	Control muy fuerte
Indique si aplicaría medidas de control y de qué magnitud	○	○	○	○	○

Aclaración de las opciones de respuesta

- NINGÚN CONTROL: Las condiciones no ameritan la implementación de medidas de control, usted se siente tranquilo.
- LEVE: Se requieren algunos controles, con un costo mínimo y de rápida implementación, con tan sólo horas para que usted solucione la situación.
- MODERADO: Se requieren controles que implican costos significativos y algunos días para su implementación. Usted puede hacerse cargo de la situación.
- FUERTE: La situación causa daños en la calidad del proyecto, pero se pueden reparar, incurriendo en costos altos, intervención de la dirección del grupo y algunos meses para implementar controles.
- MUY FUERTE: Se requiere completo compromiso de la dirección, costos altos, e incluso pueden existir daños irreparables. Se necesitarán meses para implementar controles.

« Atrás | Continuar »

Con la tecnología de Google Docs

Informar sobre abusos - Condiciones del servicio - Otros términos

Estudio Policy Capturing - INNOTEC

*Obligatorio

Escenario 5

Usted y su equipo de trabajo mantienen en secreto, información clave de los socios recolectada en varias reuniones, y sólo usted realiza los cambios necesarios sobre estos documentos.
Debido a que esta información es importante en el proyecto, nadie puede consultarla sin previa autorización suya, por lo que en algunas ocasiones esto ha demorado el trabajo del profesional de apoyo.

¿Aplicaría medidas de control en este caso? *

	Ningún control	Control leve	Control moderado	Control fuerte	Control muy fuerte
Indique si aplicaría medidas de control y de qué magnitud	○	○	○	○	○

Aclaración de las opciones de respuesta

- NINGÚN CONTROL: Las condiciones no ameritan la implementación de medidas de control, usted se siente tranquilo.
- LEVE: Se requieren algunos controles, con un costo mínimo y de rápida implementación, con tan sólo horas para que usted solucione la situación.
- MODERADO: Se requieren controles que implican costos significativos y algunos días para su implementación. Usted puede hacerse cargo de la situación.
- FUERTE: La situación causa daños en la calidad del proyecto, pero se pueden reparar, incurriendo en costos altos, intervención de la dirección del grupo y algunos meses para implementar controles.
- MUY FUERTE: Se requiere completo compromiso de la dirección, costos altos, e incluso pueden existir daños irreparables. Se necesitarán meses para implementar controles.

« Atrás | Continuar »

Con la tecnología de Google Docs

Informar sobre abusos - Condiciones del servicio - Otros términos

Estudio Policy Capturing - INNOTEC

*Obligatorio

Escenario 6

Los resultados del procesamiento de información en software especializado fueron guardados en el computador del profesional de apoyo, y solo él los edita. No obstante, esta persona se encuentra fuera de la ciudad; por lo cual, usted no podrá utilizar dichos informes por dos semanas. Por otra parte, ayer usted envió un documento confidencial a uno de los profesionales de apoyo, y para su sorpresa, al pasar por su oficina escuchó a dos personas externas al proyecto comentando el contenido del mismo.

¿Aplicaría medidas de control en este caso? *

	Ningún control	Control leve	Control moderado	Control fuerte	Control muy fuerte
Indique si aplicaría medidas de control y de qué magnitud	○	○	○	○	○

Aclaración de las opciones de respuesta

- NINGÚN CONTROL: Las condiciones no ameritan la implementación de medidas de control, usted se siente tranquilo.
- LEVE: Se requieren algunos controles, con un costo mínimo y de rápida implementación, con tan sólo horas para que usted solucione la situación.
- MODERADO: Se requieren controles que implican costos significativos y algunos días para su implementación. Usted puede hacerse cargo de la situación.
- FUERTE: La situación causa daños en la calidad del proyecto, pero se pueden reparar, incurriendo en costos altos, intervención de la dirección del grupo y algunos meses para implementar controles.
- MUY FUERTE: Se requiere completo compromiso de la dirección, costos altos, e incluso pueden existir daños irreparables. Se necesitarán meses para implementar controles.

« Atrás | Continuar »

Con la tecnología de Google Docs

Informar sobre abusos - Condiciones del servicio - Otros términos

Estudio Policy Capturing - INNOTEC

*Obligatorio

Escenario 7

Usted y su equipo de trabajo mantienen la confidencialidad respecto a los resultados del proyecto. Como apoyo a la etapa actual, han consultado información de proyectos anteriores. Sin embargo, realizando una revisión detallada, notaron que existen datos desactualizados y otros incompletos. Después de indagar, descubre que uno de los auxiliares del grupo que NO es parte del proyecto, modificó los archivos sin que nadie notara los cambios.

¿Aplicaría medidas de control en este caso? *

	Ningún control	Control leve	Control moderado	Control fuerte	Control muy fuerte
Indique si aplicaría medidas de control y de qué magnitud	○	○	○	○	○

Aclaración de las opciones de respuesta

- NINGÚN CONTROL: Las condiciones no ameritan la implementación de medidas de control, usted se siente tranquilo.
- LEVE: Se requieren algunos controles, con un costo mínimo y de rápida implementación, con tan sólo horas para que usted solucione la situación.
- MODERADO: Se requieren controles que implican costos significativos y algunos días para su implementación. Usted puede hacerse cargo de la situación.
- FUERTE: La situación causa daños en la calidad del proyecto, pero se pueden reparar, incurriendo en costos altos, intervención de la dirección del grupo y algunos meses para implementar controles.
- MUY FUERTE: Se requiere completo compromiso de la dirección, costos altos, e incluso pueden existir daños irreparables. Se necesitarán meses para implementar controles.

« Atrás | Continuar »

Con la tecnología de Google Docs

Informar sobre abusos - Condiciones del servicio - Otros términos

Estudio Policy Capturing - INNOTEC

*Obligatorio

Escenario 8

Usted y su equipo de trabajo mantienen la confidencialidad respecto a los análisis de información del proyecto. Para llevarlos a cabo, usted necesita información que está compartida en dropbox con el resto del equipo; pero, nota que han sido eliminadas permanentemente varias carpetas y necesita recuperar estos datos con urgencia para seguir cumpliendo con lo planeado. Afortunadamente, hay guardada una copia de seguridad de estos datos en la oficina de uno de los profesionales, sólo que él está fuera de la ciudad y tardará en regresar.

¿Aplicaría medidas de control en este caso? *

	Ningún control	Control leve	Control moderado	Control fuerte	Control muy fuerte
Indique si aplicaría medidas de control y de qué magnitud	○	○	○	○	○

Aclaración de las opciones de respuesta

- NINGÚN CONTROL: Las condiciones no ameritan la implementación de medidas de control, usted se siente tranquilo.
- LEVE: Se requieren algunos controles, con un costo mínimo y de rápida implementación, con tan sólo horas para que usted solucione la situación.
- MODERADO: Se requieren controles que implican costos significativos y algunos días para su implementación. Usted puede hacerse cargo de la situación.
- FUERTE: La situación causa daños en la calidad del proyecto, pero se pueden reparar, incurriendo en costos altos, intervención de la dirección del grupo y algunos meses para implementar controles.
- MUY FUERTE: Se requiere completo compromiso de la dirección, costos altos, e incluso pueden existir daños irreparables. Se necesitarán meses para implementar controles.

« Atrás | Continuar »

Con la tecnología de Google Docs

Informar sobre abusos - Condiciones del servicio - Otros términos

Estudio Policy Capturing - INNOTEC

*Obligatorio

Escenario 9

Durante la documentación de los resultados del proyecto, usted y su equipo de trabajo han podido consultar oportunamente archivos con información de etapas anteriores, los cuales han sido editados únicamente por usted. Además, sólo el equipo de trabajo tiene pleno conocimiento de los resultados antes de su publicación.

¿Aplicaría medidas de control en este caso? *

	Ningún control	Control leve	Control moderado	Control fuerte	Control muy fuerte
Indique si aplicaría medidas de control y de qué magnitud	○	○	○	○	○

Aclaración de las opciones de respuesta

- NINGÚN CONTROL: Las condiciones no ameritan la implementación de medidas de control, usted se siente tranquilo.
- LEVE: Se requieren algunos controles, con un costo mínimo y de rápida implementación, con tan sólo horas para que usted solucione la situación.
- MODERADO: Se requieren controles que implican costos significativos y algunos días para su implementación. Usted puede hacerse cargo de la situación.
- FUERTE: La situación causa daños en la calidad del proyecto, pero se pueden reparar, incurriendo en costos altos, intervención de la dirección del grupo y algunos meses para implementar controles.
- MUY FUERTE: Se requiere completo compromiso de la dirección, costos altos, e incluso pueden existir daños irreparables. Se necesitarán meses para implementar controles.

« Atrás | Continuar »

Estudio Policy Capturing - INNOTEC

*Obligatorio

Escenario 10

Usted necesita continuamente consultar datos sobre otros proyectos que ha realizado el grupo; por tanto, tiene acceso completo al sistema de información del grupo, donde a su vez puede cargar versiones de los documentos de avance del proyecto. El día de ayer uno de los estudiantes eliminó accidentalmente la versión del informe que usted estaba redactando. Aparte de esto, usted olvidó accidentalmente el portátil en la oficina, y personas ajenas al proyecto conocieron información NO sólo del proyecto sino de los demás archivos guardados en el equipo.

¿Aplicaría medidas de control en este caso? *

	Ningún control	Control leve	Control moderado	Control fuerte	Control muy fuerte
Indique si aplicaría medidas de control y de qué magnitud	○	○	○	○	○

Aclaración de las opciones de respuesta

- NINGÚN CONTROL: Las condiciones no ameritan la implementación de medidas de control, usted se siente tranquilo.
- LEVE: Se requieren algunos controles, con un costo mínimo y de rápida implementación, con tan sólo horas para que usted solucione la situación.
- MODERADO: Se requieren controles que implican costos significativos y algunos días para su implementación. Usted puede hacerse cargo de la situación.
- FUERTE: La situación causa daños en la calidad del proyecto, pero se pueden reparar, incurriendo en costos altos, intervención de la dirección del grupo y algunos meses para implementar controles.
- MUY FUERTE: Se requiere completo compromiso de la dirección, costos altos, e incluso pueden existir daños irreparables. Se necesitarán meses para implementar controles.

« Atrás | Enviar

Con la tecnología de Google Docs

Informar sobre abusos - Condiciones del servicio - Otros términos

ANEXO 33. POLÍTICA DE SEGURIDAD

Fecha de emisión: Octubre 2012

Historial de las versiones

Versión	Fecha de emisión	Resumen de cambios	Propietario
V 1.0	28/10/2012		

Para más información sobre el estado de este documento, por favor contactar a:	**Luis Eduardo Becerra Ardila** Responsable de seguridad de la información **GRUPO DE INVESTIGACIÓN EN GESTIÓN DE LA INNOVACIÓN TECNOLÓGICA Y DEL CONOCIMIENTO - INNOTEC** Carrera 27 Calle 9 Universidad Industrial de Santander Tel: (577) 6344000 E-mail: innotec@uis.edu.co http://faisan.uis.edu.co/webUIS/es/investigacionExtension/grupos/innotec/

Título de la política:	Política de Seguridad de la Información para el grupo de investigación INNOTEC

Fecha de emisión:	Octubre 28 de 2012	**Fecha de revisión:**	Octubre 26 de 2012

Versión:	1.0	**Emitida por:**	Leidy Johanna Cárdenas Solano Marcela Contreras Cruz

Objetivo:	

Alcance:	Las disposiciones contenidas en la presente política son aplicables a profesores, estudiantes, auxiliares y personal que preste sus servicios al grupo de investigación INNOTEC bajo cualquier modalidad, que participen en forma directa e indirecta en actividades misionales y de apoyo.

Documentación asociada:	• Reglamento de propiedad intelectual de la UIS [Acuerdo 093 de 2010] • Estatuto de investigación de la UIS [Acuerdo 043 de 2011] • Guía de propiedad intelectual UIS
Apéndices:	Glosario de términos
Aprobado por:	Luis Eduardo Becerra Ardila
Fecha:	Octubre 28 de 2012

Proceso de revisión:	Revisión anual a partir de la fecha de aprobación
Responsabilidad de implementación y entrenamiento:	Luis Eduardo Becerra Ardila

---

HISTORIAL

Revisiones:		
Fecha:	**Autor:**	**Descripción:**

Métodos de Distribución:	Publicación en el sitio web del proyecto de grado y del grupo de investigación, distribución del documento vía correo electrónico a todos los investigadores y estudiantes.

1. Introducción

Las políticas de seguridad de la información "proporcionan la fuente de instrucciones más importante y más frecuentemente referenciada"[298], que describe cómo, se puede proteger tanto la información como los sistemas que la contienen. Las políticas deben estar adecuadas a las circunstancias particulares de cada organización.

El presente documento consiste en una versión inicial de una política de seguridad de la información para un grupo de investigación, y por tanto, debe ser considerada como un punto de partida, que le permitirá a los investigadores conocer los diferentes lineamientos generales acerca de seguridad de la información para el desarrollo de las actividades misionales del grupo.

Asimismo, vale la pena resaltar que este documento se encuentra sujeto a las modificaciones que sean pertinentes de acuerdo a las circunstancias del grupo de investigación.

[298] ROBLES, Luis C. Modelos de seguridad. [Diapositivas]. [20 Agosto de 2012]. Disponible en: http://www.slideshare.net/luisrobles17/modelos-de-seguridad-de-la-informacin

2. Objetivos, Propósito y Alcance

2.1. Objetivos.

Los objetivos de la presente política de seguridad de la información son preservar la:

2.1.1. **Confidencialidad** – Necesidad de que la información sensible sólo sea conocida por personas autorizadas.
2.1.2. **Integridad** – Característica que hace que el contenido de la información permanezca inalterado, a menos que sea modificado o eliminado por personal autorizado.
2.1.3. **Disponibilidad** – Característica que hace que la información esté siempre disponible en el momento que la necesitan para ser procesada por las personas autorizadas.

2.2. Propósito

El propósito de esta política es establecer y mantener la confidencialidad de la información manejada en los proyectos de investigación y extensión llevados a cabo por el grupo de investigación, mediante la aplicación de las siguientes directrices:

2.2.1. Asegurar que todos los integrantes del grupo sean conscientes de, y cumplan con los lineamientos descritos en esta política.
2.2.2. Describir los principios de seguridad y explicar como estos son implementados en el grupo de investigación.
2.2.3. Introducir un enfoque consistente a la seguridad, asegurando que todos los integrantes del grupo entiendan a cabalidad sus propias responsabilidades.
2.2.4. Crear y mantener un nivel de consciencia de la necesidad de seguridad de la información dentro del grupo como parte integral de sus actividades cotidianas.
2.2.5. Proteger los activos de información y conocimiento que se generan gestionan y transfieren en el grupo.

2.3. Alcance

Las disposiciones contenidas en la presente política son aplicables a toda la información y conocimiento, que se gestiona, genera y transfiere, como producto de las actividades de profesores, estudiantes, auxiliares y personal que preste sus

servicios al grupo de investigación bajo cualquier modalidad, que participen en forma directa e indirecta en actividades misionales y de apoyo.

3. Responsabilidades de Seguridad

3.1. Es claro que la responsabilidad final de seguridad de la información recae sobre el representante legal de la Universidad Industrial de Santander; no obstante, en el desarrollo de las actividades cotidianas del quehacer universitario, el director del grupo de investigación será responsable por gestionar e implementar la política y los procedimientos relacionados.

3.2. Los directores de proyecto serán responsables de generar los mecanismos y herramientas necesarios para asegurar que su equipo de trabajo sea consciente de:

3.2.1. Las políticas de seguridad de la información aplicable en sus actividades.

3.2.2. Su responsabilidad personal en material de seguridad de la información.

3.2.3. Cómo acceder a asesoramiento en material de seguridad de la información.

3.3. Todos los integrantes del grupo deben cumplir con los procedimientos de seguridad incluyendo la conservación de la confidencialidad, integridad y disponibilidad de la información, evitando así que se apliquen medidas correctivas de carácter disciplinario.

3.4. La política de seguridad de la información deberá ser conservada, revisada y actualizada por un líder encargado de esta labor. Esta revisión deberá realizarse anualmente.

3.5. Los directores de proyecto serán responsables individualmente por la seguridad de las instalaciones físicas usadas por ellos y su equipo de trabajo.

3.6. Cada usuario persona que utilice o maneje información, y conocimiento en general, será responsable por la protección y conservación de los sistemas de información y del conocimiento que utilicen.

3.7. Cada usuario del sistema debe cumplir con los requisitos de seguridad que se encuentran actualmente establecidos, y también debe garantizar que la confidencialidad, integridad y disponibilidad de la información y conocimiento se mantengan al más alto nivel.

3.8. Los contratos con partes externas que permiten acceder a sistemas de información del grupo se harán efectivos antes de que se permita el acceso. Estos contratos aseguraran que el personal o los subcontratistas de la organización externa cumpla con todas las normas de seguridad adecuadas.

4. Legislación

4.1. El grupo de investigación está obligado a cumplir con todos los estatutos pertinentes de la Universidad Industrial de Santander y de Colombia. La obligación de cumplir con esta legislación se transferirá a todos los integrantes del grupo de investigación, a quienes se les podría pedir rendición de cuentas por cualquier violación de seguridad de la cual puedan ser considerados responsables. Se deberá cumplir con las siguientes guías y normas, según sea apropiado:

- Estatuto de investigación de la UIS [Acuerdo 043 de 2011]
- Guía de propiedad intelectual UIS
- Reglamento de propiedad intelectual de la UIS [Acuerdo 093 de 2010]
- Reglamento de pregrado [Acuerdo 072 de 1982]
- Reglamento de posgrado [Acuerdo 090 del 2010]
- Acuerdos de confidencialidad

5. Gestión del riesgo

5.1. Un análisis exhaustivo de los activos de información del grupo será realizado en forma periódica (anualmente antes de la revisión de la política) para documentar las amenazas y vulnerabilidades del grupo de investigación con respecto a la seguridad de la información.

5.2. En el análisis de riesgos se examinarán siete fuentes de amenaza a saber: personas externas, criminal informático, personas internas, vándalos, naturaleza, proveedor de servicios y entorno.

5.3. Se deberán identificar los impactos asociados a la explotación de cada vulnerabilidad por parte de las amenazas. De la combinación de amenazas, vulnerabilidades e impactos, se determinará el nivel de riesgo para la confidencialidad, integridad y disponibilidad de la información.

5.4. Sobre la base de la evaluación periódica, se aplicarán medidas que reduzcan el impacto de las amenazas al reducir la cantidad y alcance de las vulnerabilidades.

6. Clasificación de la información

Se usa para promover los controles apropiados que protejan la confidencialidad de la información. Sin importar su clasificación, la integridad de toda la información debe conservarse. La información registrada en diferentes formatos (por ejemplo, registro electrónico, versión impresa, reporte) debe tener la misma clasificación

independientemente del formato en el que se encuentre. Los siguientes niveles se usarán para clasificar la información.

6.1. La **información confidencial** está constituida por material muy importante y altamente sensible, cuyo uso está restringido para necesidades legítimas y estratégicas del grupo de investigación.

6.2. **Ejemplos de información confidencial** son: Información personal, información financiera (presupuesto de proyectos), contraseñas de acceso a sistemas de información, procesos realizados en el grupo, procedimientos, ecuaciones de búsqueda, documentos de proyectos de investigación, resultados de proyectos (su confidencialidad se mantiene por 5 años después de su publicación)

6.3. La **divulgación desautorizada** de información confidencial a personas que no requieran acceso a la misma para el desarrollo de sus actividades de investigación podría violar reglamentos o causar problemas significativos para el grupo, o sus *stakeholders*. Las decisiones acerca de la provisión de acceso a esta información siempre deben ser aprobadas por el propietario de la información.

6.4. La **información privada** es para uso sin restricciones dentro del grupo de investigación, y en algunos casos dentro de las UAAs relacionadas con sus actividades principales. Este tipo de información ya está ampliamente distribuida dentro del grupo, o podría distribuirse dentro del mismo sin permiso previo del director.

6.5. **Ejemplos de información interna** pueden incluir: Directorios de personal, políticas y procedimientos internos, mensajes electrónicos internos, metodologías de investigación. Cualquier información que no esté explícitamente clasificada como confidencial o pública, de forma predeterminada, se clasificará como información interna.

6.6. La **divulgación no autorizada** de información interna a personas externas no es apropiada debido a provisiones legales o contractuales.

6.7. La Información Pública será específicamente aprobada para divulgación pública por la autoridad designada.

6.8. Ejemplos de información pública incluyen: Folletos de mercadeo, material publicado en la página web del grupo o en la página web de la UIS, artículos aprobados para publicación en revista, material publicado en posters. Esta información puede ser conocida fuera del grupo de investigación.

7. Acuerdos de confidencialidad

Los usuarios de información clasificada como confidencial deberán firmar, como condición de vinculación al grupo, un acuerdo de confidencialidad apropiado. El acuerdo deberá incluir el siguiente enunciado, o uno similar (parafraseo):

> *"Entiendo que cualquier uso o divulgación no autorizado de la información relacionada con _____, incluida en _____, puede ocasionar acciones disciplinarias consistentes con las políticas y procedimientos del grupo de investigación, y de la Universidad Industrial de Santander".*

Los acuerdos de confidencialidad deben ser revisados cuando haya cambios en los contratos u otros términos de trabajo, particularmente cuando los contratos finalicen o los empleados partan de la organización.

8. Almacenamiento y eliminación de la información

La información y sus registros, ya sean conservados en archivos electrónicos o en papel, deben ser almacenados y eliminados de manera segura.

8.1. Electrónica

- Información confidencial. Debe ser protegida por contraseña. En la medida de los posible, no debería almacenarse en dispositivos móviles (portátiles, tabletas, memorias usb, cds, dvds, etc.). En casos en que no se pueda evitar el almacenamiento de esta información en dichos dispositivos, debe ser conservada en lugares seguros.
- Información interna. Se puede seguir la política de información confidencial o las prácticas de cuidado prudente, en función de los requisitos del responsable de seguridad de la información
- Información pública. Esta información debe ser protegida contra modificaciones no autorizadas solamente

8.2. Copias físicas (papel)

- Información confidencial. Los documentos deben ser almacenados en espacios con acceso autorizado y destruidos cuando ya no sean necesarios.

- Información interna. Se puede seguir la política de información confidencial o las prácticas de cuidado prudente, en función de los requisitos del responsable de seguridad de la información
- Información pública. Los documentos deberían ser reciclados cuando ya no sean necesarios.

9. Capacitación en seguridad de la información

9.1. Será incluida en el proceso de inducción cada vez que ingrese un Nuevo miembro al grupo de investigación.

9.2. Un programa continuo de sensibilización será establecido con el fin de asegurar que la consciencia de seguridad sea actualizada y renovada en caso necesario.

10. Mayor información

Mayor información y guía sobre está política puede ser obtenida escribiendo al correo electrónico: innotec@uis.edu.co.

11.Política aprobada por:

Firma _____ Fecha _____

ANEXO 34. GRÁFICO DE PUBLICACIONES POR AÑO EN ISI WOS

ANEXO 35. DIAGRAMA DE PARETO