PROPUESTA DE DISEÑO, DOCUMENTACIÓN E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EL PROCESO SERVICIOS INFORMÁTICOS Y DE TELECOMUNICACIONES DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER BASADO EN LA NORMA NTC-ISO/IEC 27001:2005

JORGE ELIÉCER VIDAL RODRÍGUEZ
LADY PATRICIA BARON CONSUEGRA

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FÍSICOMECÁNICAS
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y DE TELECOMUNICACIONES
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2010

PROPUESTA DE DISEÑO, DOCUMENTACIÓN E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EL PROCESO SERVICIOS INFORMÁTICOS Y DE TELECOMUNICACIONES DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER BASADO EN LA NORMA NTC-ISO/IEC 27001:2005

JORGE ELIÉCER VIDAL RODRÍGUEZ
LADY PATRICIA BARON CONSUEGRA

Monografía para optar al título de
Especialista en Telecomunicaciones

Director
JORGE HERNANDO RAMÓN SUÁREZ
Ingeniero Electricista, MsC

Codirector
JAIME ENRIQUE SARMIENTO SUÁREZ
Ingeniero de Sistemas

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FÍSICOMECÁNICAS
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y DE TELECOMUNICACIONES
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2010

A ti Dios padre, Todo poderoso, que eres mi fuente de amor y apoyo. Eres ese gran amigo que nunca falla, que nos recuerda que tan valiosos somos. Gracias por no dejarme desfallecer dándome esa fortaleza y empuje que me caracteriza. Gracias por enseñarme a seguir adelante, por mostrarme luz en este gran camino "La vida".

A mis padres por brindarme su confianza, cariño y esfuerzo. Sé que han hecho de mí un ejemplo de mujer. Gracias por creer en mí.

A mis hermanos por acogerme en sus brazos.

A mi futuro esposo Juan Carlos, Gracias por compartir este gran triunfo.

Un agradecimiento especial a un hombre muy sabio: Jorge Vidal "Inge" por su colaboración, paciencia, apoyo brindados desde siempre y sobre todo por esa gran amistad que me brindó y me brinda, por escucharme y aconsejarme. Gracias e infinitas gracias por todos los bellos momentos compartidos, por haberme acogido en su vida y por haberme dado el gusto de trabajar con usted.

Lady Patricia

Deseo expresar mis agradecimientos a:

A Dios quien me sostuvo a pesar de todas las dificultades en el camino. Eres un gran maestro, guía y luz de mi existencia.

La Universidad Industrial de Santander, Institución que ha contribuido significativamente en mi proyecto de vida y a mejorar mi formación profesional.

Al Doctor Jaime Alberto Camacho Pico, Rector de Nuestra Universidad, por su impulso para iniciar esta nueva etapa, la cual, ha contribuido fundamentalmente en el fortalecimiento de mi formación profesional.

Al Ingeniero Jorge Hernando Ramón Suárez, por su dirección y colaboración en la realización de este proyecto.

A mi esposa Martha Isabel, por su apoyo incondicional, sus aportes profesionales y el impulso dado para el logro de esta meta.

Jorge Eliécer

TABLA DE CONTENIDO

Pág.

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

GLOSARIO

ACEPTACIÓN DE RIESGO: decisión de aceptar un riesgo.

ACTIVO (*Asset*): cualquier cosa que tenga valor para la organización.

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

ANÁLISIS DE RIESGO: uso sistemático de la información para identificar fuentes y estimar riesgos.

ANÁLISIS CUALITATIVO DE RIESGO: evaluación del impacto y la probabilidad de ocurrencia de los riesgos sobre las salidas del proyecto utilizando métodos cualitativos.

ANÁLISIS CUANTITATIVO DE RIESGO: evaluación matemática de la probabilidad de ocurrencia de cada riesgo y sus consecuencias en las salidas del proyecto.

CONFIDENCIALIDAD: (*confidentiality*): propiedad que la información no esté disponible o pueda ser descubierta por usuarios no autorizados, entidades o procesos.

DECLARACIÓN DE APLICABILIDAD: documento que describe los objetivos de control, y los controles que son relevantes y aplicables a la organización del SGSI.

NOTA: Estos controles están basados en los resultados y conclusiones de la valoración y los procesos de tratamiento de riesgos, los requerimientos y regulaciones legales, las obligaciones contractuales y los requerimientos de negocio para la seguridad de la información que defina la organización.

DISPONIBILIDAD (*availability*): propiedad de ser accesible y utilizable bajo demanda por una entidad autorizada.

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.

IMPACTO: el impacto es la materialización de un riesgo; una medida del grado de daño o cambio sobre un activo, entendiendo como riesgo la probabilidad de que un evento desfavorable ocurra y que tendría un impacto negativo si se llegase a materializar.

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.

INTEGRIDAD: propiedad de salvaguardar la precisión y completitud de los recursos.

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.

RIESGO RESIDUAL: el riesgo remanente luego de aplicar un control.

PLAN DE GESTIÓN DE RIESGOS: documento que describe la estrategia que se va a seguir en el proyecto, y cómo las actividades de gestión de riesgos van a ser organizadas y llevadas a cabo durante la vida del proyecto, es decir, a las actividades relacionadas con la reducción, previsión y control de riesgos, la preparación ante riesgos y la recuperación en caso de desastre. El plan de gestión de riesgos es la salida resultante de la fase de planificación de gestión de riesgos.

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

RIESGO RESIDUAL: un riesgo que permanece después de que las respuestas de riesgos hayan sido implementadas.

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.

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SGSI: parte de los sistemas de la organización, basado en el análisis de riesgo de negocio, cuya finalidad es establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información.

NOTA: el SGSI incluye las políticas, planes, actividades, responsabilidades, prácticas, procedimientos, procesos y recursos.

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

NOTA: el término “control” en esta norma es empleado como sinónimo de “Medida o medición”.

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

VULNERABILIDAD: una vulnerabilidad es una debilidad que puede ser “activada” de forma accidental o intencionadamente. Es un factor de riesgo interno de un elemento expuesto a una amenaza de ser susceptible a sufrir un daño y de encontrar dificultades en recuperarse posteriormente.

RESUMEN

TÍTULO: *PROPUESTA DE DISEÑO, DOCUMENTACIÓN E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EL PROCESO SERVICIOS INFORMÁTICOS Y DE TELECOMUNICACIONES DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER BASADO EN LA NORMA NTC-ISO/IEC 27001:2005*.[*]

AUTORES: JORGE ELIÉCER VIDAL RODRÍGUEZ
LADY PATRICIA BARÓN CONSUEGRA[**]

PALABRAS CLAVES: Información - Integridad, confidencialidad y disponibilidad; Activos de información - amenazas, análisis de riesgos; Información - riesgos lógicos, físicos y controles de seguridad; Sistemas de información – NORMA NTC-ISO/IEC 27001:2005, SGSI, PHVA.

DESCRIPCION:

La información es un valioso activo del que depende el buen funcionamiento de una organización, por lo que es fundamental mantener su integridad, confidencialidad y disponibilidad para alcanzar los objetivos de toda Organización.

En la actualidad las organizaciones, sus sistemas de información y redes se enfrentan con las amenazas a la seguridad, como son: riesgos lógicos, fraude ayudado por computador, espionaje, virus informáticos, ataques de instrucción, denegación de servicios, y riesgos físicos como sabotaje, vandalismo, fuego, inundaciones, entre otros, que afectan la disponibilidad de la información y recursos, haciendo inviable la continuidad de las actividades de las organizaciones no preparadas para afrontarlos.

Proteger a organizaciones de estas amenazas implica conocerlas y afrontarlas de una manera adecuada, implementando controles de seguridad idóneos, una evaluación de riesgos y medición de su eficacia.

En la Universidad Industrial de Santander, la información es un recurso, que como el resto de los activos, debe ser debidamente protegida, para garantizar la funcionalidad de sus sistemas de información y el valor de los activos de información asociados. Con la minimización de riesgos de daño, se contribuye a una mejor gestión, integridad, confidencialidad y disponibilidad para alcanzar los objetivos institucionales.

Para cumplir este objetivo, se realizó una recolección de información relacionada con la seguridad de la información con el estudio y análisis de la norma **NTC-ISO/IEC 27001:2005** relativa a la GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, esencial para esta Propuesta, presentada al proceso Servicios Informáticos y de Telecomunicaciones de la UIS, y para la posterior implementación del Sistema de Gestión de la Seguridad de la Información (SGSI), bajo el enfoque de la norma y basado en el modelo PHVA (Planificar-Hacer-Verificar-Actuar),utilizando la metodología “Magerit” para el análisis y gestión de riesgos de los activos de información críticos, incluidos dentro del alcance definido por la UIS.

---

[*] *Monografía*

[**] *Facultad de Ingenierías Físico-Mecánicas. Escuela de Ingenierías Eléctrica, Electrónica y Telecomunicaciones. Especialización en Telecomunicaciones. Director: Jorge Hernando Ramón Suárez, M.Sc. Codirector: Ing. Jaime Enrique Sarmiento Suárez.*

SUMMARY

TITLE: PROPOSAL FOR THE DESIGN, DOCUMENTATION AND IMPLEMENTATION OF AN INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) FOR THE COMPUTER AND TELECOMUNICATION PROCESSES OF UNIVERSIDAD INDUSTRIAL DE SANTANDER *BASED ON THE REGULATION NTC-ISO/IEC 27001:2005*.*

AUTHORS: JORGE ELIÉCER VIDAL RODRÍGUEZ
LADY PATRICIA BARÓN CONSUEGRA**

KEY WORDS: information – integrity – confidentiality – and availability; information assets - threats, risk assessment; Information - logic and physical hazards, and security controls; information systems – REGULATION NTC-ISO/IEC 27001:2005, SGSI, PHVA.

DESCRIPTION:

Information is a valuable asset that the proper functioning of an organization depends of. Therefore it is fundamental to maintain its integrity, confidentiality and availability in order to reach the objectives of any given organization.

Currently, organizations, along with their respective information systems and networking, face security threats such as: logical hazards, computer-assisted fraud, espionage, computer viruses, instruction attacks, service denials and actual physical perils such as: sabotage, vandalism, fire, and flooding among others. The aforementioned may affect the availability of information and resources, hampering the activity continuity of unready organizations.

Protecting organizations implies knowing the threats and facing them in an appropriate matter by implementing the right security protocols, risk assessments and effectiveness measurements. For Universidad Industrial de Santander, information is a resource, which alongside the rest of assets, should be properly secured. All this in order to guarantee the functionality of its information systems and the worth of any related information asset. By means of vulnerability reduction, a better management, integrity, confidentiality and availability is provided to reach institutional goals.

With the purpose of achieve this objective; information security related data was gathered under the analysis of directive NTC-ISO/IEC 27001 related to INFORMATION SECURITY MANAGEMENT, essential to this proposal, presented to the computer and telecommunication services division at Universidad Industrial de Santander, aiming to the further implementation of the Information Security Management System (ISMS). This will be carried out under the directive focal point while founded on the PHVA (Plan- Do- Verify- Act) model. Moreover the “Magerit” methodology will be implemented for risk assessment and analysis of critical information assets included within the UIS defined range.

---

* *Monograph*

** *Faculty of Physical-Mechanical Engineerings.School of Electrical Engineering, Electronic and Telecommunication. Specialization in Telecommunications. Director: Jorge Hernando Ramon Suarez, M.Sc. Codirector: Jaime Enrique Sarmiento Suárez*

INTRODUCCION

Históricamente la segunda guerra mundial marco la línea divisoria, en más de un sentido, para la seguridad de la información. Las técnicas de ocultamiento no sólo se aplicaron al ámbito estrictamente militar sino también a las relaciones diplomáticas con los gobiernos, a la información sobre secretos comerciales e industriales, a la información científica y técnica y, sobre todo, a mantener la información almacenada en los grandes computadores que surgieron en esa época, oculta de accesos no autorizados, entre otras aplicaciones.

La protección que la información guardada en los computadores requería en ese entonces pudiera parecer sencilla a la luz de la época actual, puesto que los equipos estaban centralizados y los computadores eran de propósito específico. Pero el hecho de que esos computadores empezaran a ser multiusuario y multitarea, inició el camino sin retorno de las preocupaciones de seguridad informática y computacional actuales.

Luego de esa época, cuando los computadores se concibieron para propósito general y multiusuario, el panorama de la seguridad de la información empezó a cambiar de manera compleja. La información que se procesaba ya no era sólo de tipo militar, de estado o científica. Se trataba con información tan diversa, dependiendo de las aplicaciones.

La situación se tornó aún más compleja con el surgimiento de los microcomputadores y las redes de computadores y con ello la necesidad de proteger la información particular en distintos y numerosos ámbitos y lugares y durante su viaje por canales públicos y abiertos.

En el ámbito universitario, la información es un recurso que, como el resto de los activos, tiene valor para la comunidad universitaria y por consiguiente debe ser debidamente protegida, garantizando la continuidad de los sistemas de información y los activos asociados, minimizando los riesgos de daño y contribuyendo de esta manera, a una mejor gestión de la Universidad. Mantener su integridad, confidencialidad y disponibilidad es esencial para alcanzar los objetivos institucionales.

Para que estos principios sean efectivos, se hace necesaria la implementación de Políticas de Seguridad de la Información, que formen parte de la cultura organizacional de la Universidad, lo que implica un compromiso real de todos los funcionarios de una manera u otra vinculados a la gestión, para contribuir a la difusión, consolidación y su cumplimiento.

Es así como se realizó una búsqueda y recolección de información relacionada con la seguridad de la información y se efectuó un estudio y análisis de las normas ISO/IEC 27000, relativas a la seguridad de la información, con el fin de tener las bases fundamentales para proponer al proceso de Servicios Informáticos y de Telecomunicaciones (SI) de la Universidad Industrial de Santander (UIS) el diseño y posterior implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI),utilizando el modelo de procesos PHVA (Planificar-Hacer-Verificar-Actuar) y una metodología comercial denominada “Magerit” para el análisis y gestión de riesgos de los sistemas de información, administrados de manera directa por dicho proceso, en concordancia con el alcance definido por la UIS.

1. PLANTEAMIENTO DEL PROBLEMA

1.1 DESCRIPCIÓN DEL PROBLEMA

Para Implementar Sistemas de Seguridad de la Información en plataformas informáticas, tanto en el ámbito público como privado, es indispensable ubicarnos en un espacio y tiempo específicos dentro de las dinámicas y cambiantes tecnologías de la información y comunicación.

Aunque en el mundo de las TICs se viene tocando este tema desde hace algunas décadas, en Colombia este concepto es incipiente para algunas organizaciones, que cobra importancia y se vislumbra como un problema una vez se han detectado las vulnerabilidades en los activos de información, o cuando ya han ocurrido los problemas, incluso en las más sofisticadas plataformas.

La investigación y puesta en marcha de los sistemas de seguridad de la información efectivos que cumplan con los parámetros establecidos en los estándares ya definidos, que en otros países de la Unión Europea y Norteamérica ya hacen parte de los presupuestos en las organizaciones y en planes de desarrollo nacional, en el Estado Colombiano es rudimentario, y tal vez uno de los grandes obstáculos, ha sido, no solo la brecha digital, sino también, en gran parte la falta de una formación adecuada y concienciación de los usuarios finales; sumado a esto el presupuesto destinado para este propósito es mínimo, lo que desencadena otras limitaciones tales como adquisición de tecnología de punta, disposición de personal idóneo en el manejo de la información, el mal disfrazado “costo-beneficio” que para algunas organizaciones en su escala administrativa no es asumido como una prioridad, lo que termina en la decisión de tomar riesgos que tarde o temprano terminan materializándose.

En el peor de los casos, grandes y pequeñas corporaciones se escudan en fenómenos tales como el acelerado crecimiento y desbordamiento de la información para sustentar que ninguna política será suficiente a la hora de asumir el compromiso de seguridad de la información.

No obstante, es necesario tener presente a ese vasto número de empresas que no ahorran esfuerzos y cuantiosas sumas de dinero en la realización del *in fashion ethical hacking*, en compra de software que desarrollan funciones de seguridad específica como antivirus, firewalls, entre otros[1], que luego justifican como la panacea para la seguridad y tranquilidad de las organizaciones. Igualmente, contratan consultorías y estudios de clima organizacionales; estas empresas una vez se presenta un daño que compromete directamente la seguridad de su información, encuentran la solución despidiendo e indemnizando al empleado encargado, directamente relacionado con el daño ocurrido, ya que esto le representa menos costos[2].

Los fenómenos transformadores, como las redes de nueva generación, las tecnologías convergentes, la movilidad, perímetros porosos y un fenómeno que se ha subestimado pero que puede llegar a romper estructuras en nuestra sociedad, "enemigos poderosos" como son las Redes sociales, los teléfonos inteligentes entre otros grandes flagelos de las nuevas tecnologías, son la pesadilla para las organizaciones que requerirán día a día más sistemas de seguridad y profesionales expertos en seguridad de la información que desarrollen destrezas, que transmitan conocimiento y sobre todo enfrenten los riesgos y peligros de esos valiosos activos que cada organización ubica en una escala de valores de acuerdo a sus necesidades.

[1] *ÁLVAREZ CABRERA, Carlos S. Aspectos legales prácticos de la seguridad de la información. Bogotá: Alfa-Redi, 2003.*
[2] *Ídems, pág. 7, tercer párrafo.*

Entonces, ¿a qué peligros y riesgos se enfrentan las diferentes organizaciones de orden público y privado? Se pueden mencionar algunas de tantas amenazas:

- Virus Informáticos, uno de los más grandes problemas de seguridad de la información.
- Robo de hardware.
- Plagio de información.
- Vandalismo.
- Fallas en los equipos.
- Equivocaciones.
- Accesos no autorizados de intrusos.
- Cracker, defacer, viruxer, Hackers, etc.
- Fraude.
- Siniestro (robo, incendio, inundación, terremoto).
- Ataques en redes sociales y correos electrónicos.
- Phishing de una cuenta.
- Ataques de malware y spam.
- Ataques a equipos con Backdoor.
- Amenazas internas (manejo fraudulento inapropiado e ilegal por parte de los conocedores de la red).
- La Web 3.0: modifica el significado del contenido digital, provocando confusión en el usuario, se permite el modo de intrusión en los sistemas.
- Abuso emocional que trae consigo el fácil acceso a la pornografía, juegos, videos sexuales en red, entre otros.
- Violación a la intimidad, (acceso indiscriminado de personas, apología de delitos sexuales, robos, estafas, secuestros, delitos económicos).
- Utilización frecuente de programas no autorizados.

En consecuencia, es necesario en cualquier organización grande o pequeña y sobre todo en instituciones como la Universidad Industrial de Santander, que cuenta con una muy buena infraestructura para los Sistemas de Información, crear lo que serán los cimientos de Seguridad de la información y Seguridad Informática de puerta abierta a los cambios e innovación permanentes en información, pero con una postura visionaria, futurista que vaya más allá de los planes locales y nacionales y que permita de cara al futuro, mantener la protección de la información, controlada con estándares, con un Sistema de Gestión de Seguridad estructurado y tecnologías modernas, todo ello contenido dentro de un marco legal, que permita que tanto políticas como normas vayan unidas sin que se desliguen de la órbita académica y científica, claro, teniendo siempre como premisa que la última verdad en materia de seguridad de la información y seguridad informática aún no se conoce.

1.2 FORMULACIÓN DEL PROBLEMA

En el siglo XXI, cuando la gestión del conocimiento es una característica vital en las empresas, se debiera tener formas de poder minimizar el riesgo de que la información se fugue, se altere o simplemente no esté disponible cuando se requiera. ¿Qué se debería hacer en las empresas para proteger su información?[3]

De acuerdo al entorno digital en que giran todos y a las necesidades y exigencias de los usuarios, cada vez más conectados a sistemas seguros e inseguros, es necesario como lo plantea C.F Borghello[4], formularse las siguientes preguntas:

---

[3] *ALEXANDER, Alberto G. Diseño de un sistema de gestión de seguridad de información, Óptica ISO 27001:2005. Bogotá: Alfaomega, 2007.*

[4] *BORGHELLO, Cristian F. Escribiendo Políticas de Seguridad – (online) [Buenos Aires, Argentina] SEGU-INFO: Seguridad de la información, Cristian Borghello, 2000 [Citado: 14 Ene, 2007]Disponible en Internet: http://www.segu-info.com.ar*

- ¿qué se desea proteger? Se definen los activos.

- ¿de qué o de quién se desea proteger? Se definen las amenazas, el riesgo y su ocurrencia probable.

- ¿cómo se protege? Se desarrollan estrategias adecuadas teniendo en cuenta la política, manejo, administración, tecnología y otros temas organizacionales para formarnos una idea clara del estado de la seguridad dentro de la organización.

Una vez analizados estos interrogantes en detalle, de los que obviamente surgirán otros no menos importantes, se debe dar el primer paso para ubicarse en el contexto y naturaleza de un Sistema de Gestión de la Seguridad de la Información (SGSI), que se cristaliza con la puesta en marcha e implementación de la NORMA NTC-ISO/IEC 27001: 2005, teniendo claros los conceptos de protección de activos de información de la Universidad, su identificación, alcance, evaluación y análisis de riesgo y la relación causa – efecto.

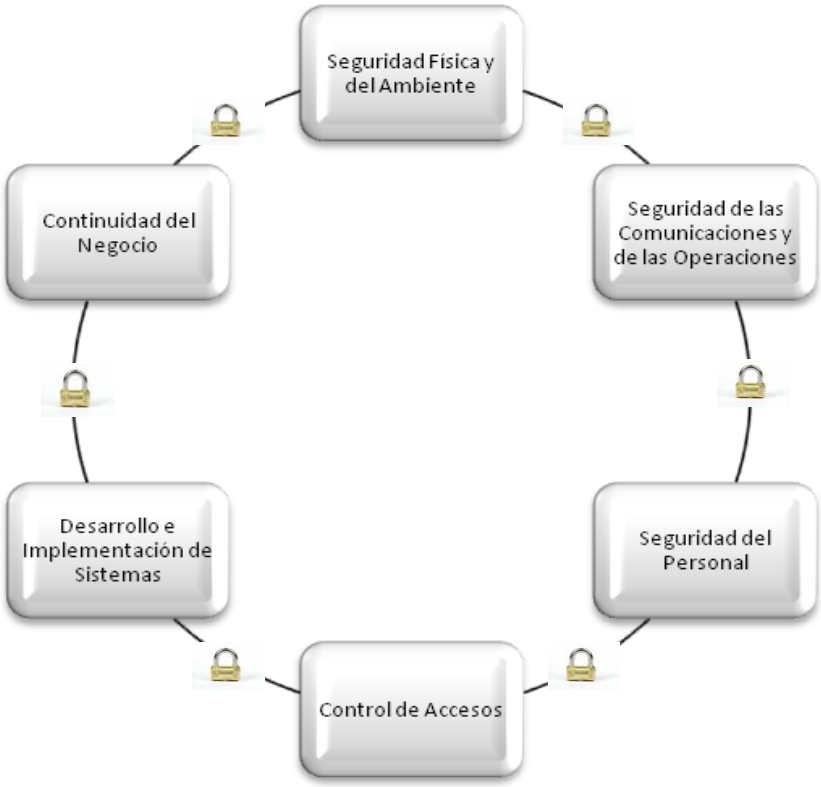
Es necesario entonces determinar, para el SGSI, su alcance, la política de seguridad, objetivos de control y controles y requisitos documentados para su exitosa implementación.

Desde luego, es importante tener claro que las vulnerabilidades no recaen únicamente sobre los sistemas de información, también se encuentran en el Recurso Humano como directo administrador de éstos, y en este sentido los sistemas de seguridad de la información deben referirse tanto a las vulnerabilidades de los activos tecnológicos como a las relacionadas con el

personal; esto no solo disminuirá los riesgos, sino que se creará una *cultura de la seguridad*[5] como elemento fundamental en la organización.

En el siguiente esquema se muestran las formas más importantes de seguridad acogidas por algunas organizaciones:

Figura 1. Formas importantes de seguridad.



Desarrollar las anteriores formas de seguridad obliga también a la implementación de políticas que en forma autónoma cada Organización creará de acuerdo a sus necesidades y requerimientos.

[5] *ÁLVAREZ CABRERA, Carlos S. Aspectos legales prácticos de la seguridad de la información. Bogotá: Alfa-Redi, 2003*

En el siguiente esquema se observan, de manera general, algunas de las políticas estándar acogidas por las Empresas, que para el tema que nos ocupa en esta monografía se hace necesario tener en cuenta:

Figura 2. Diversas políticas acogidas en empresas.

Otro elemento fundamental sin lugar a dudas del que se desprenden grandes males es la nula o escasa capacitación al interior de las organizaciones que impide que se hable un lenguaje igual, que guarde equilibrio entre el ser y el hacer. En un primer paso en la Implementación de la Familia ISO IEC 27000, la capacitación es el eje fundamental no solo en el sistema de seguridad sino en todos los sistemas de la organización, que no resulten en un fracaso por no haberse manejado un lenguaje comprensible a todos y cada uno de los usuarios, ameno, alejado de tecnicismos y anglicismos clásicos.

Al mismo tiempo que se diseña hoy un sistema de gestión de la seguridad de la información con sus políticas a seguir, es necesario repensar la política que

surgirá en el futuro, esto es, estar preparados para el cambio y para reconocer que la política de hoy, ya será obsoleta mañana.

¿Cuáles son entonces las políticas más importantes hoy por hoy?

Siempre surgirán nuevos esquemas de protección, nuevas formas, nuevos mecanismos, que coexistirán con las innovaciones tecnológicas (el remedio para muchos), para esto se hace necesaria la seguridad de la información, pero no solo para gestionarla, para implementarla, sino certificarla con el sello de calidad. Los indicadores sin lugar a dudas son una herramienta, que garantizan el monitoreo, rastreo y depuración de los sistemas de información. Tomarla seguridad como un elemento superficial en la cultura de la organización, es no acogerse al eje fundamental o norma establecida para salvaguardar patrimonios y bienes basados en la información.

Para concluir esta formulación del problema, se trae a colación la siguiente reflexión de (J.J.CANO, 2010)[6] sobre los signos y señales de la inseguridad de la información:

> *"Las señales en sí mismas, no son DIOS, sino elementos que deben ser revisados en el contexto de lo que ocurre, para revelar aspectos del camino que se sigue en el contexto de la vida. Por lo tanto, pueden seguirte muchas señales particulares que pueden ser ignoradas o analizadas, y es tu deber dedicarte a revisarlas o ignorarlas según tu cosmovisión del mundo y acercamiento a tu Creador.*
>
> *Considerando lo anterior como inspiración base para nuestra reflexión ante la pérdida y/o fuga de la información, se hace necesario monitorear y*

[6] *Jeimy J. Cano, Ph.D, CFE. Ingeniero y Magíster en Ingeniería de Sistemas y Computación de la Universidad de los Andes*

revisar de manera permanente los signos reportados de las fallas de seguridad, los comportamientos inadecuados con el uso de la información y las diferentes tendencias que la industria revela frente a las vulnerabilidades que se presentan con frecuencia tanto en procesos organizacionales como en las tecnologías de información disponibles.

Cuando las organizaciones no se encuentran atentas a los "signos de los tiempos", las sorpresas se hacen evidentes, los riesgos se materializan y los pronósticos se comprometen. En este sentido, las empresas deben "sensar" y responder a su entorno, de tal manera que capitalicen los referentes que marcan las "señales del camino" con relación a la información, como esa nueva moneda que circula de manera restringida o libre, según se establezca por sus dueños o propietarios".

2. JUSTIFICACIÓN

Seguridad de información es mucho más que establecer firewalls*, aplicar parches para corregir nuevas vulnerabilidades en el sistema de* software*, o guardar en la bóveda los* backup*.*

Seguridad de información es determinar qué hay que proteger y por qué, de qué se debe proteger y cómo protegerlo[7]

La información y los procesos, sistemas y redes que la soportan son activos importantes para el buen funcionamiento de una organización, y deben protegerse al máximo usando los estándares de seguridad de la información que sean pertinentes para alcanzar los objetivos de negocio de las instituciones.

Desafortunadamente, es relativamente fácil tener acceso a las herramientas que permiten a personas no autorizadas llegar hasta la información protegida, con poco esfuerzo y conocimientos, causando graves perjuicios para las empresas.

El escenario que se tenía anteriormente, en el cual los sistemas operaban de manera aislada o en redes privadas, ha sido sustituido por computadores personales que cada vez tienen mayor capacidad de procesamiento y almacenamiento de información, englobados dentro de lo que se conoce como sistemas de información; de la misma manera, las tecnologías convergentes y la difusión masiva del uso de internet han incrementado los riesgos.

Hoy en día el mundo se encuentra cada vez más interconectado, y esta interconexión se extiende a mayor escala a ritmos acelerados. Al mismo tiempo,

[7] *G.A., Alberto. Sistema de Seguridad de Información". Lima: Pontificia Universidad Católica del Perú, Centro de Negocios Centrum, 2005. Implantación del ISO 27001:2005*.

internet forma parte de la infraestructura operativa del sector estratégico de la educación, y desempeña un papel fundamental de modo tal que las instituciones de educación superior montan sus plataformas operativas e intercambian información académica y científica a través de dicha red internacional; igualmente, el uso de este de medio de comunicación para el intercambio de información de manera individual por parte de los beneficiarios de las instituciones de educación, también contribuye a la generación de riesgos reales y latentes.

La naturaleza y el tipo de tecnologías que constituyen la infraestructura de la información y comunicaciones también ha cambiado de manera significativa; el número y el tipo de dispositivos que integran la infraestructura de acceso se han multiplicado, incluyendo elementos de tecnología fija, inalámbrica y móvil, así como también una proporción creciente de accesos que están conectados permanentemente. A consecuencia de todos estos cambios, la naturaleza, el volumen y la sensibilidad de la información que se intercambia a través de esta infraestructura han incrementado de modo significativo la forma de pensar, en cuanto a la gestión de riesgos se refiere.

Los riesgos de pérdidas, hurtos o uso inadecuado de los datos pueden ocasionar daños representativos; dichos riesgos son latentes no sólo desde medios externos sino que internamente pueden ser aún más vulnerables. Para esto se han definido estándares que ayudan a la seguridad, minimizan el riesgo de fugas, fraudes, uso indebido de información, etc. Según la CITEL[8], el 35% de las empresas mencionan que el principal fraude detectado es el interno, el cual está directamente relacionado con la fuga de información.

Por todo lo anterior, se hace necesario el surgimiento de nuevos retos en materia de seguridad, motivo por el cual, en esta monografía se propone que la Universidad Industrial de Santander, a través de su proceso de Servicios

[8] *CITEL: Comisión Interamericana de las Telecomunicaciones.*

Informáticos y de Telecomunicaciones, debe comenzar a aplicar estándares de Seguridad de la Información, orientados a todos los participantes de la comunidad universitaria, que forman parte de la sociedad de la información, donde es inminente tener una mayor conciencia y entendimiento de los aspectos de seguridad, así como de la necesidad de desarrollar una cultura en torno a ésta.
Las siguientes razones han dado muestra a las empresas de la necesidad de contar con un estándar de seguridad:

- Establecer un reglamento de prácticas favorables para la gestión de la seguridad.

- Establecer las especificaciones para la adopción de un Sistema de Gestión de la Seguridad de la Información.

- Establecer un estándar de facto a nivel global, que se implemente en las entidades que administran la seguridad de la información.

- Establecer un conjunto de normas, procedimientos y controles que se apliquen en cualquier entorno y sector, y que utilicen tecnologías de la información para lograr los objetivos propuestos.

- Mejorar los niveles de competitividad, optimizando la seguridad y el funcionamiento de la empresa.

- Promover servicios para que la empresa se incorpore más fácil y eficientemente a la sociedad de la información.

Todas estas razones hacen indispensable contar con un Sistema de Gestión estandarizado para garantizar la Seguridad de la Información en la Universidad Industrial de Santander, en su proceso de Servicios Informáticos y de

Telecomunicaciones dentro de su Sistema de Gestión de la Calidad, que le permita a la Institución alcanzar sus objetivos y ser más competitiva en el mercado.
Los beneficiarios de los servicios que ofrece la Universidad demandan cada vez más que sus datos estén en un lugar seguro y, a su vez, que sean transferidos o difundidos por medios que garanticen el uso correcto para el cual están hechos.

El Sistema de Gestión permitirá identificar y afrontar de una manera adecuada las situaciones de inseguridad (amenazas) a las que están sometidos los sistemas de información y sus activos asociados, evitando llevar a la Institución a problemas de falta de confiablidad entre sus clientes, falta de integridad y disponibilidad de sus sistemas de información críticos, con la consecuente pérdida económica y pérdida de imagen en el mercado. Para ello se deben establecer unos procedimientos adecuados e implementar controles de seguridad basados en la evaluación de los riesgos y en una medición de su eficacia.

Los estándares de seguridad de la información, como las Normas Técnicas Colombianas NTC-ISO/IEC 27001:2005 y la NTC-ISO/IEC 27002:2005[9] y la normatividad legal aplicable, no son mecanismos coactivos sino de prevención, que permiten proporcionar un marco de Gestión de la Seguridad de la Información para facilitar entre otros el uso correcto la información disponible en las instituciones.

Los estándares mencionados anteriormente, están diseñados para que sus requisitos sean complementarios con los de cualquier otro sistema de gestión implantado, tal como el de gestión de la calidad NTC-ISO 9001:2008, lo que facilita su integración e implementación en la UIS, Institución que ya cuenta con un Sistema de Gestión de la Calidad certificado con esta norma y se proyecta hacia

[9] *Adoptadas por el Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, en Colombia.*

un Sistema Integrado de Gestión de la Calidad que incluya la norma de gestión ambiental NTC-ISO 14001:2004.

La implementación de estas normas permite de forma significativa disminuir el impacto de los riesgos sin necesidad de realizar grandes inversiones en software y sin contar con una gran estructura de personal.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Proponer, diseñar y documentar la implementación de un Sistema de Gestión de la Seguridad de la Información para el Proceso Servicios Informáticos y de Telecomunicaciones de la Universidad Industrial de Santander con base en los lineamientos de la Norma NTC-ISO/IEC 27001:2005.

3.2 OBJETIVOS ESPECÍFICOS

- Analizar los criterios de gestión de seguridad de la información desde la perspectiva del enfoque basado en procesos.

- Comprender y documentar la naturaleza y dinámica del estándar ISO 27001:2005 e interpretar cada una de sus respectivas cláusulas de naturaleza global.

- Identificar los activos de información más relevantes en el proceso Servicios Informáticos y de Telecomunicaciones de la UIS y seleccionar los más críticos.

- Seleccionar y analizar una metodología de gestión de riesgos, y aplicarla a los activos que impactan la seguridad de la información en la UIS-SI.

- Diseñar, documentar y proponer la implementación a futuro de un Sistema de Gestión de la Seguridad de la Información, que garantice controles de seguridad suficientes y proporcionales que protejan los activos de información de la UIS-SI.

- Compilar en un documento los resultados de la investigación realizada.

4. MARCO CONCEPTUAL

La información y los procesos de apoyo, sistemas y redes son uno de los recursos más importantes de las organizaciones. Definir, lograr, mantener y mejorar la seguridad de la información puede ser esencial para mantener la línea de competitividad, obtener rentabilidad, cumplimiento legal y sostenimiento de la imagen comercial.

Actualmente, las organizaciones y sus sistemas de información y redes se enfrentan con un amplio rango de fuentes de amenazas a la seguridad de la información, desde riesgos lógicos como fraude ayudado por computador, espionaje, virus informáticos, ataques de instrucción, denegación de servicios, hasta riesgos físicos como sabotaje, vandalismo, fuego, inundaciones[10], etc.

Ante estas circunstancias es imprescindible que las organizaciones evalúen los riesgos asociados y establezcan las estrategias y controles adecuados que aseguren una permanente protección y salvaguarda de la información.

4.1 CARACTERÍSTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

Las características o propiedades que enmarcan la seguridad de la información son básicamente tres: confidencialidad, Integridad y disponibilidad, como ya se mencionó en un apartado anterior en esta monografía.

La confidencialidad es la propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

[10] *RUBIO RINCON, Jaime Hernando, Introducción a los Conceptos de Seguridad, Escuela Colombiana de Ingeniería Julio Garavito, Bogotá, 2005.*

La integridad es la característica de salvaguardar la exactitud y estado completo de los activos.

La disponibilidad es la propiedad que determina que la información sea accesible y utilizable en el momento que sea requerida.

No todas las características deben estar presentes simultáneamente, ni tienen la misma importancia en todas las circunstancias. Hay circunstancias en la que la confidencialidad es fundamental, como en los casos cuando se maneja información personal. Otras circunstancias requieren que la información sea autentica, como en el caso cuando se dan instrucciones para realizar inversiones en una entidad financiera. Hay que determinar en cada caso cuáles de las propiedades son necesarias o importantes.

La seguridad de la información como disciplina, trata precisamente de establecer metodologías para determinar cuáles de las tres características son deseables en alguna circunstancia y de encontrar la forma que se apliquen.

4.2 CONCEPTOS BÁSICOS

Con el fin de precisar el alcance de los principales conceptos utilizados en esta monografía, se trascriben los más significativos que están incluidos en el Modelo de Sistemas de Gestión de la Seguridad de la Información (SGSI) recomendado por las Normas NTC ISO/IEC 27001:2005 y NTC ISO/IEC 27002:2005.

4.2.1 Definición de Seguridad de la Información

La norma NTC-ISO/IEC 27001:2005 la define como:

La "*Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad".*

Según la norma NTC ISO/IEC 27002:2005:
"La seguridad de la información es la protección de la información contra una gran variedad de amenazas con el fin de asegurar la continuidad del negocio, minimizar el riesgo para el negocio y maximizar el retorno de inversiones y oportunidades de negocio".

4.2.2 ¿Porqué es necesaria la seguridad de la información?.

Según la Norma Técnica Colombiana NTC-ISO/IEC 27002 (ICONTEC, 2010):

"La seguridad de la información es importante tanto para los negocios del sector público como del privado y para proteger la infraestructura crítica. En ambos sectores, la seguridad de la información actuará como un elemento facilitador para lograr, por ejemplo, gobierno en línea (e-government) o negocios electrónicos (e-business) y evitar o reducir los riesgos pertinentes. La interconexión de las redes públicas y privadas y compartir los recursos de información incrementan la dificultad para lograr el control del acceso. La tendencia hacia la computación distribuida también ha debilitado la eficacia del control central y especializado."

4.2.3 Seguridad proactiva de la información.

Para definir este concepto, se ha tomado una de las investigaciones realizadas por el Director de Iniciativas de Seguridad de Microsoft, Eduardo Núñez Parodi, quien en su Artículo "*Seguridad Proactiva para Proteger la Información*",[11] nos ilustra magistralmente sobre el tema argumentando:

> "*la información es uno de los activos más importantes de las empresas, y mantenerlo tiene unos riesgos asociados que aumentan cada día. Por ello es clave que la práctica para proteger la información empresarial sea proactiva, de forma que se convierta en un habilitador estratégico de negocios.*
>
> *La práctica proactiva para la seguridad de la información se basa en mantener tres principios fundamentales, que garantizan: a) la confiabilidad de los datos, b) su rápida disponibilidad y c) su integridad.*
>
> *En las empresas es importante contar con información accesible, pero también lo es protegerla de cualquier intento de robo, ya que la pérdida de información puede revelar secretos empresariales o exponer información confidencial a terceros.*
>
> *Dentro de los desafíos de la práctica proactiva para la seguridad de la información está la optimización de los recursos. Como estos siempre son limitados, algunas veces la decisión de dónde invertir puede no ser clara o no alinearse con los requerimientos de la organización. Sin embargo, la forma de determinar dónde invertir y cómo priorizar se puede basar en*

[11] *NUÑEZ PARODI, Eduardo. Seguridad Proactiva para Proteger la Información. En: Revista Actualización Gerencial de Microsoft, Edición No. 25, Octubre – Diciembre de 2010,*

diversas prácticas, siendo la más utilizada el análisis de riesgos asociados con el manejo de la información.

Esta práctica permite a las empresas analizar los riesgos con base en el estado actual de la organización, y establecer prioridades para determinar de manera ejecutiva dónde invertir los recursos".

4.3 SEGURIDAD FÍSICA

Es fundamental tomar conciencia que por más que la organización sea la más segura desde el punto de vista de ataques externos, Hackers, virus, etc., la seguridad de la misma será ineficaz si no se ha previsto como combatir un incendio o enfrentar cualquier otra amenaza de la naturaleza.

La seguridad física es uno de los aspectos más olvidados cuando se seleccionan y diseñan centros de procesamiento de datos y sistemas de información. Hay aspectos que no se prevén, como la detección de un atacante interno dentro de la organización que intenta ingresar físicamente a una sala de operaciones de la misma. Esto puede derivar en que para un atacante sea más fácil tomar y copiar la información de una cinta de un centro de procesamiento de datos, que intentar acceder a la información a través de procedimientos lógicos.

De esta manera, como lo menciona Borghello (2001) (citado en Huerta, 2000), la Seguridad Física "consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo, implementados para proteger el hardware y medios de almacenamiento de datos".

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro de cómputo. Las principales amenazas que se deben prever en la seguridad física son:

- Desastres naturales, incendios accidentales, tormentas e inundaciones;
- Amenazas hostiles ocasionadas por el hombre (vandalismo, robo, fraude);
- Disturbios, sabotajes internos y externos deliberados;
- Instalaciones eléctricas (picos y ruidos electromagnéticos, emisiones electromagnéticas, cableado, sistema de aire acondicionado).

4.3.1 Incendios. Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas.

El fuego es una de las principales amenazas contra la seguridad. Es considerado el enemigo número uno de los computadores ya que puede destruir fácilmente los archivos de información y programas.

4.3.2 Inundaciones. Se las define como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial. Esta es una de las causas de mayores desastres en centros de cómputo.

Además de las causas naturales de inundaciones, puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior.

4.4 SEGURIDAD LÓGICA

Se refiere a la seguridad en el uso de software y los sistemas, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información. La “seguridad lógica” involucra todas aquellas medidas establecidas por la Dirección, usuarios y administradores de activos de información para minimizar los riesgos de seguridad asociados con sus operaciones cotidianas llevadas a cabo utilizando las tecnologías de información.

Los principales objetivos que persigue la seguridad lógica son:

- Restringir el acceso a los programas y archivos

- Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.

- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.

- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.

- Que la información recibida sea la misma que ha sido transmitida.

- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.

- Que disponga de pasos alternativos de emergencia para la transmisión de información.

5. MARCO LEGAL

Siempre que se desea implementar un Sistema de Gestión, toda organización debe obligatoriamente cumplir con todas las leyes, normas, decretos, etc. que sean aplicables en el desarrollo de sus actividades. De manera general se puede mencionar el tema de seguridad social, cumplir con la Cámara de Comercio, permisos, licencias de construcción, etc.; pero en lo que se refiere específicamente a **Seguridad de la Información**, estas son las Leyes vigentes al día de hoy:

TABLA 1. MARCO LEGAL DE LA SEGURIDAD DE LA INFORMACION: COMUNIDAD ANDINA Y COLOMBIA

DERECHOS DE AUTOR	PROPIEDAD INDUSTRIAL
•Decisión 351 de la C.A.N. •Régimen Común sobre Derechos de Autor y Derechos Conexos. •Las disposiciones de la presente Decisión tienen por finalidad reconocer una adecuada y efectiva protección a los autores y demás titulares de derechos, sobre las obras del ingenio, en el campo literario, artístico o científico, cualquiera que sea el género o forma de expresión y sin importar el mérito literario o artístico ni su destino. •Asimismo, se protegen los Derechos Conexos a que hace referencia el Capítulo X de la presente Decisión.	•Decisión 486 de la C.A.N. •Trata del Régimen Común sobre Propiedad Industrial, entre otros temas. •Con respecto a la protección de la propiedad industrial, cada País Miembro concederá a los nacionales de los demás miembros de la Comunidad Andina, de la Organización Mundial del Comercio y del Convenio de París para la Protección de la Propiedad Industrial, un trato no menos favorable que el que otorgue a sus propios nacionales, a reserva de lo previsto en los artículos 3 y 5 del Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC), y en el artículo 2 del Convenio de París para la Protección de la Propiedad Industrial.

NORMATIVIDAD NACIONAL

DERECHOS DE AUTOR	PROPIEDAD INDUSTRIAL	COMERCIO ELECTRÓNICO Y FIRMAS DIGITALES
Ley 23 de 1982		
Decreto 1360 de 1989		
Ley 44 de 1993	Decreto 2591 de 2000	Ley 527 de 1999
Decreto 460 de 1995	Ley 463 de 1998	Decreto 1747 de 2000
Decreto 162 de 1996	Ley 170 de 1994	Resolución 26930 de 2000
Ley 545 de 1999	Ley 178 de 1994	
Ley 565 de 2000		
Ley 603 de 2000		
Ley 719 de 2001		

LEY 1273 DE 2009

- Esta Ley añade dos nuevos capítulos al Código Penal Colombiano
- Capítulo Primero: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos;
- Capitulo Segundo: De los atentados informáticos y otras infracciones.
- El primer capítulo, esta Ley está muy ligada a la ISO27000, lo cual coloca al País a la vanguardia en legislación de seguridad de la información, abriendo así la posibilidad de nuevas entradas con este tema.

6. NATURALEZA Y DINÁMICA DE LA NORMA ISO/IEC 27001:2005

6.1 ORIGEN Y POSICIONAMIENTO DE LA FAMILIA ISO/IEC 27000

Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution) es responsable de la publicación de importantes normas como:

1979. Publica BS 5750 - ahora ISO 9001
1992. Publica BS 7750 - ahora ISO 14001
1996. Publica BS 8800 - ahora OHSAS 18001

La norma BS 7799 de BSI apareció por primera vez en 1995, con objeto de proporcionar a cualquier empresa, británica o no, un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) fue una guía de buenas prácticas, para la que no se establecía un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que estableció los requisitos de un sistema de gestión de la seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En 2005, con más de 1700 empresas certificadas en BS 7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO

17799. Esta última norma se renombró como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

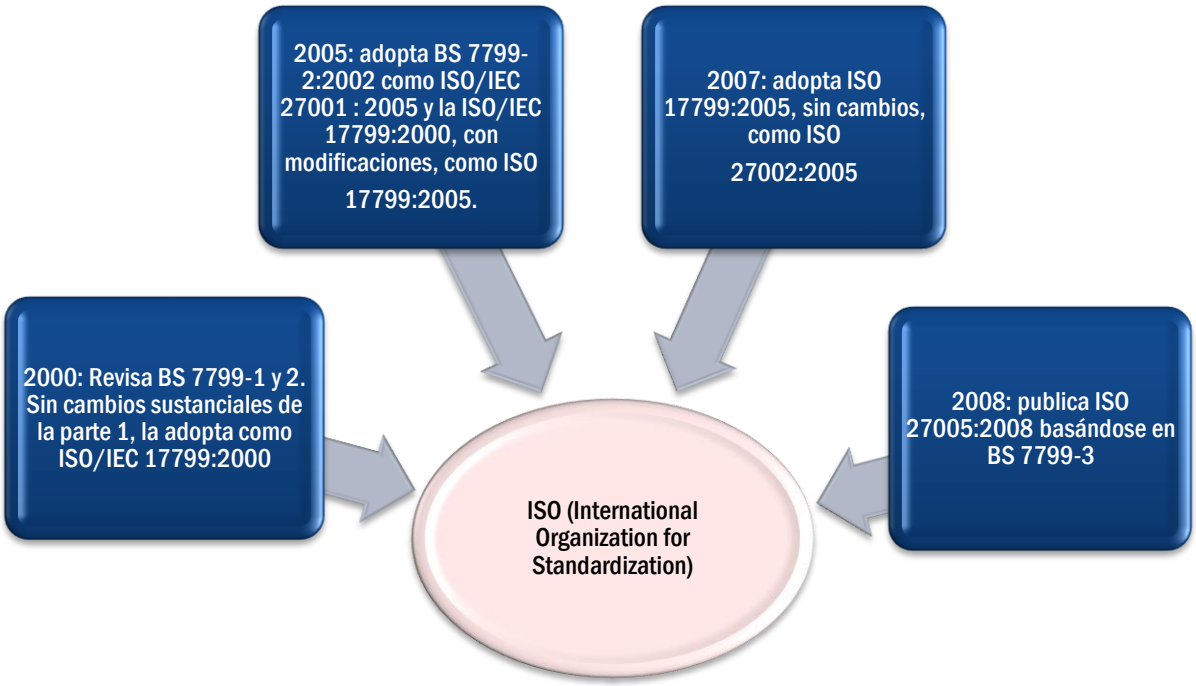
En Marzo de 2006, posteriormente a la publicación de ISO 27001:2005, BSI publicó la BS 7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.

Así mismo, ISO ha continuado, y continúa aún, desarrollando otras normas dentro de la serie 27000 que sirvan de apoyo a las organizaciones en la interpretación e implementación de ISO/IEC 27001, que es la norma principal y única certificable dentro de la serie.

La ISO (Organización Internacional de Estándares) y la IEC (Comisión Internacional de Electrotecnia) conforman un sistema especializado para los estándares mundiales. Los organismos nacionales en cada país que son miembros de ISO o IEC, participan en el desarrollo de Normas Internacionales a través de comités técnicos establecidos por la organización respectiva para tratar con los campos particulares de la actividad técnica.

En el campo de las tecnologías de la información, ISO ha establecido, dentro de su estructura organizacional, un comité técnico en unión con IEC, denominado ISO/IECJTC 1 (*Join Technical Committee* 1), al cual le reporta el subcomité 27 y luego al grupo de trabajo 1. El grupo de trabajo 1, cada cinco años, revisa las normas para decidir las posibles modificaciones. Los borradores de estas Normas Internacionales adoptados por este comité técnico son enviados a los organismos de las diferentes naciones para su votación. La publicación, ya como una Norma Internacional, requiere la aprobación de por lo menos el 75% de los organismos nacionales que emiten su voto.

Figura 3. Origen de los componentes más importantes de la familia ISO 27000.



A continuación se hace una breve descripción del conjunto de estándares que aportan información a la familia de normas ISO 27000:

6.2. La serie ISO 27000. A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares. Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044.

- **ISO/IEC 27000**: Publicada el 1 de Mayo de 2009. Esta norma proporciona una visión general de las normas que componen la serie 27000, una introducción a los Sistemas de Gestión de la Seguridad de la Información, una breve descripción del proceso Planificar-Hacer-Verificar-Actuar y términos y definiciones que se emplean en toda la serie 27000.

- **ISO/IEC 27001:** Publicada el 15 de Octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de la seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de su SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

- **ISO/IEC 27002**: Desde el 1 de Julio de 2007, es el nuevo nombre de la Norma ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a la seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de la Norma ISO 27002:2005.

- **ISO/IEC 27003**: Publicada el 01 de Febrero de 2010. No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001:2005. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la Dirección para implementar un SGSI. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

- **ISO/IEC 27004:** Publicada el 7 de Diciembre de 2009. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según la Norma ISO/IEC 27001.

- **ISO/IEC 27005**: Publicada el 4 de Junio de 2008. No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la Norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

- **ISO/IEC 27006**: Publicada el 1 de Marzo de 2007. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de la seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSI) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSI. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma.

- **ISO/IEC 27007**: En fase de desarrollo, con publicación prevista en 2011. Consistirá en una guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011.

- **ISO/IEC 27008**: En fase de desarrollo, con publicación prevista en 2011. Consistirá en una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI.

- **ISO/IEC 27010:** En fase de desarrollo, con publicación prevista en 2012. Es una norma en 2 partes, que consistirá en una guía para la gestión de la seguridad de la información en comunicaciones inter-sectoriales.

- **ISO/IEC 27011:** Publicada el 15 de Diciembre de 2008. Es una guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002. Está publicada también como norma ITU-TX.1051.

- **ISO/IEC 27012:** En fase de desarrollo, con publicación prevista en 2011. Consistirá en un conjunto de requisitos (complementarios a ISO/IEC 27001) y directrices (complementarias a ISO/IEC 27002) de gestión de seguridad de la información en organizaciones que proporcionen servicios de e-Administración.

- **ISO/IEC 27013**: En fase de desarrollo, con publicación prevista en 2012. Consistirá en una guía de implementación integrada de ISO/IEC 27001 (gestión de la seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI).

- **ISO/IEC 27014**: En fase de desarrollo, con publicación prevista en 2012. Consistirá en una guía de gobierno corporativo de la seguridad de la información.

- **ISO/IEC 27015:** En fase de desarrollo, con publicación prevista en 2012. Consistirá en una guía de SGSI para organizaciones del sector financiero y de seguros.

- **ISO/IEC 27031:** En fase de desarrollo, con publicación prevista en 2011. Consistirá en una guía de continuidad del negocio en cuanto a tecnologías de la información y comunicaciones.

- **ISO/IEC 27032:** En fase de desarrollo, con publicación prevista en 2011. Consistirá en una guía relativa a la ciberseguridad.

- **ISO/IEC 27033:** Norma dedicada a la seguridad en redes, consistente en 7 partes: 27033-1, conceptos generales (publicada el 10 de Diciembre de 2009); 27033-2, directrices de diseño e implementación de seguridad en redes (prevista para 2011); 27033-3, escenarios de redes de referencia (prevista para 2011); 27033-4, aseguramiento de las comunicaciones entre redes mediante Gateway de seguridad (prevista para 2012); 27033-5, aseguramiento de comunicaciones mediante VPNs (prevista para 2012); 27033-6, convergencia IP (prevista para 2012); 27033-7, redes inalámbricas (prevista para 2012).

- **ISO/IEC 27034:** En fase de desarrollo, con publicación prevista en 2010. Consistirá en una guía de seguridad en aplicaciones informáticas.

- **ISO/IEC 27035:** En fase de desarrollo, con publicación prevista en 2011. Consistirá en una guía de gestión de incidentes de seguridad de la información.

- **ISO/IEC 27036:** En fase de desarrollo, con publicación prevista en 2012. Consistirá en una guía de seguridad de outsourcing (externalización de servicios).

- **ISO/IEC 27037**: En fase de desarrollo, con publicación prevista en 2012. Consistirá en una guía de identificación, recopilación y preservación de evidencias digitales.

- **ISO 27799:** Publicada el 12 de Junio de 2008. Es una norma que proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de ISO/IEC 27002, en cuanto a la seguridad de la información sobre los datos de

salud de los pacientes. Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215.

Actualmente la Norma ISO/IEC 27001:2005 es el único estándar aceptado internacionalmente, y adoptado nacionalmente como Norma Técnica Colombiana NTC-ISO/IEC 27001:2005, para la gestión de la seguridad de la información y aplica a todo tipo de organizaciones, independientemente de su tipo, tamaño y naturaleza, a los efectos de la certificación.

6.3 ANÁLISIS DE LA NORMA NTC-ISO/IEC 27001:2005

El Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, que es el organismo nacional de normalización, adoptó el estándar ISO/IEC 27001:2005 como la Norma Técnica Colombiana NTC-ISO/IEC 27001:2005, "*para brindar un modelo para el establecimiento, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI)*".

La NTC-ISO/IEC 27001:2005 menciona que la adopción de un SGSI debe ser una decisión tomada a nivel estratégico. Así mismo, enfatiza en que el diseño y la implementación de un Sistema de Gestión de la Seguridad de la Información en una organización dependerán de sus necesidades, objetivos estratégicos, requerimientos de seguridad, procesos sustantivos, tamaño y estructura orgánica. Cada SGSI se confecciona de la manera más adecuada para cada empresa. Eso sí, debe permitir evaluar la conformidad, con cada uno de los requisitos de la norma.

6.3.1 Consideraciones claves del estándar. La propuesta de esta norma, no está orientada a despliegues tecnológicos o de infraestructura, sino a aspectos netamente organizativos, es decir, la frase que podría definir su propósito es "Organizar la seguridad de la información".

Por ello, propone toda una secuencia de acciones tendientes al *"establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del Sistema de Gestión de la Seguridad de la Información (SGSI)"*. El SGSI, es el punto fuerte de este estándar.

Los detalles que conforman el cuerpo de esta norma, se podrían agrupar en tres grandes líneas:

- Sistema de Gestión de la Seguridad de la Información (SGSI);
- Valoración de riegos, y
- Controles

Es importante entender la redacción de los requerimientos de esta norma. Cuando en las cláusulas del estándar aparece el vocablo "DEBE", eso significa que es una exigencia. Es decir, lo estipulado debe cumplirse.

A continuación, se hace una breve interpretación de la naturaleza de la norma y de las exigencias de las cláusulas o numerales de naturaleza global que se consideran de interés fundamental para la aplicación de esta norma.

Se consideró importante mantener los numerales que emplea el Estándar Internacional, para que, si es necesario, se pueda acceder directamente al mismo, para ampliar cualquier aspecto, por lo tanto, la numeración que sigue a continuación, no respeta la de esta monografía, pero sí la de la norma.

0.1 GENERALIDADES

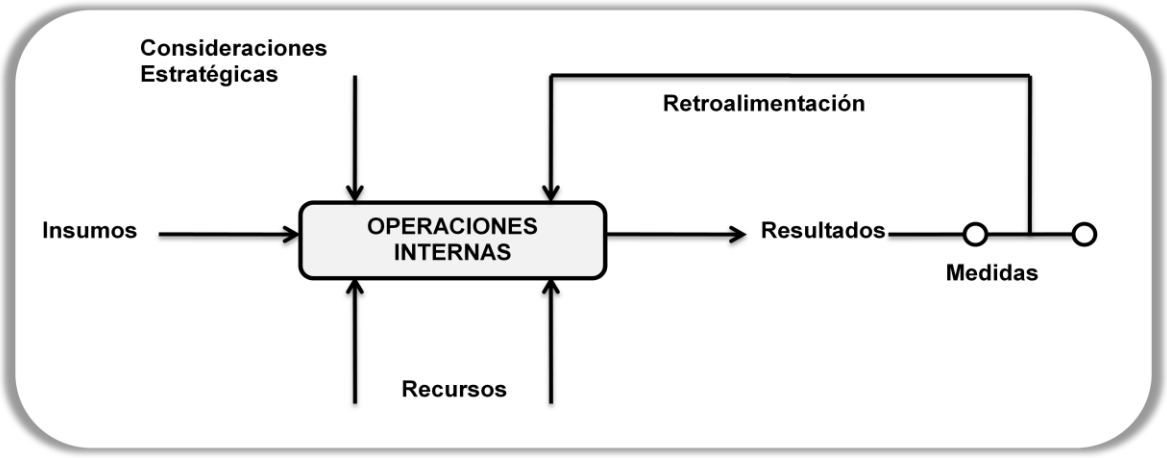
El estándar ISO/IEC 27001:2005 fue diseñado para proveer un modelo para el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI. La adopción del SGSI debe ser una decisión

estratégica de la organización, pues el mismo está influenciado por las necesidades y objetivos de la misma, los requerimientos de seguridad, los procesos, el tamaño y la estructura de la empresa; la dinámica que implica su aplicación, producirá en muchos casos el crecimiento del mismo, necesitando la misma dinámica para las soluciones.

0.2 ENFOQUE BASADO EN PROCESOS

El modelo ISO/IEC 27001.2005 está diseñado bajo una óptica de enfoque a procesos. El SGSI está contextualizado para funcionar en cualquier tipo de organización, operando bajo el enfoque de procesos. La Figura 5, ilustra los distintos componentes del modelo, bajo la perspectiva de procesos.

Figura 4. Enfoque a procesos de la Norma ISO/IEC 27001:2005



Fuente: ALEXANDER, Alberto, Diseño de un sistema de seguridad de información.

Una organización necesita identificar y administrar cualquier tipo de actividad para funcionar eficientemente. Cualquier actividad que emplea recursos, para que las operaciones internas funcionen adecuadamente, y es administrada para transformar entradas en salidas, puede ser considerada como un "proceso". A

menudo, estas salidas son aprovechadas nuevamente como entradas, generando una realimentación de los mismos.

La aplicación de un sistema de procesos dentro de una organización, junto con la identificación e interacciones entre estos procesos, y su gestión, se puede denominar como un "enfoque basado en procesos[12].

Una ventaja del enfoque basado en procesos es el control continuo que proporciona sobre los vínculos entre los procesos individuales dentro del sistema, así como sobre su combinación e interacción.

Cuando se utiliza un enfoque de este tipo para la Gestión de la Seguridad de la Información, enfatiza a sus usuarios la importancia de:

a) La comprensión por parte de la organización de sus requerimientos de Seguridad de la Información y su necesidad de establecer una política y objetivos para garantizar la Seguridad de la Información.

b) La implementación y operación de controles para administrar los riesgos inherentes a la Seguridad de la Información de la empresa en concordancia con los riesgos del negocio.

c) El monitoreo y revisión del desempeño y la efectividad del sistema.

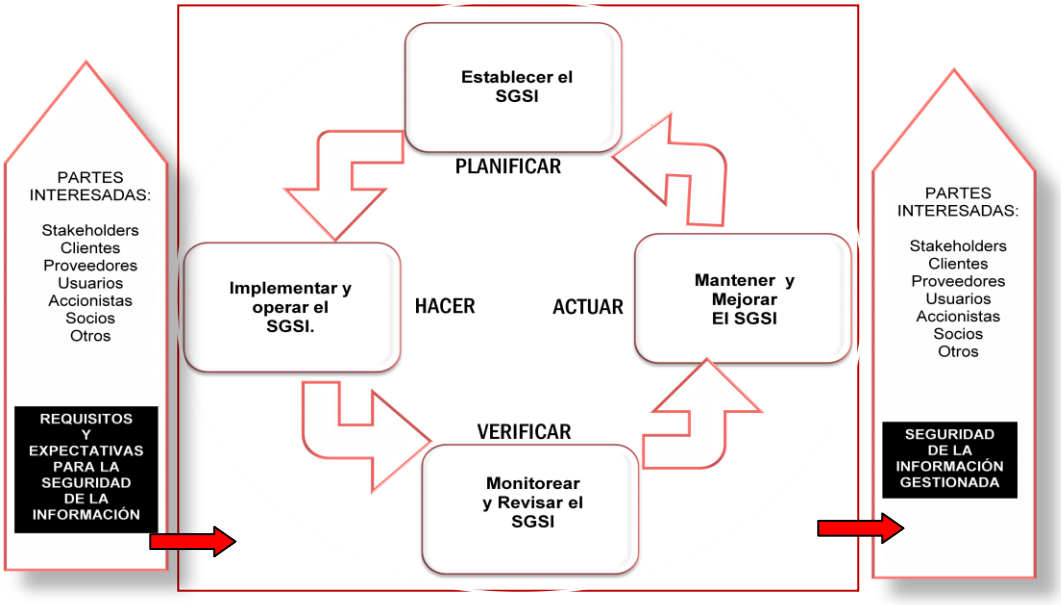
d) La mejora continua de los procesos con base en mediciones objetivas.

Esta norma también adopta el modelo "Planificar-Hacer-Verificar-Actuar" (PHVA) o fases del ciclo Deming, el cual es aplicado a toda la estructura de procesos del SGSI. La Figura 6 Ilustra cómo el SGSI toma como elementos de entrada los

[12]*Norma Técnica Colombiana, NTC-ISO/IEC 27001:2005*

requisitos de seguridad de la información y las expectativas de las partes interesadas, y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que cumplen estos requisitos y expectativas[13].

Figura 5. Modelo PHVA aplicado a los procesos del SGSI



En esencia, cada fase contempla las siguientes acciones:

- **Planificar** (Establecer el SGSI): Implica, determinar el alcance, establecer la política del SGSI, sus objetivos, procesos, identificar los activos de información, procedimientos relevantes para la administración de riesgos y mejoras para la seguridad de la información, entregando resultados acordes a las políticas y objetivos de toda la organización.

- **Hacer** (Implementar y operar el SGSI): Representa la forma en que se debe operar e implementar la política, controles, procesos y procedimientos.

[13] *Norma Técnica Colombiana, NTC-ISO/IEC 27001:2005, ICONTEC, Bogotá, 2010.*

- **Verificar** (Monitorizar y revisar el SGSI): Analizar y medir donde sea aplicable, los procesos ejecutados con relación a la política del SGSI, evaluar objetivos, experiencias e informar los resultados a la Dirección para su revisión.

- **Actuar** (Mantener y mejorar el SGSI): Realizar las acciones preventivas y correctivas, basados en las auditorías internas y revisiones del SGSI o cualquier otra información relevante para permitir la continua mejora del SGSI.

1.2 APLICACIÓN

Los requerimientos de este estándar internacional, son genéricos y aplicables a la totalidad de las organizaciones. La exclusión de los requerimientos especificados en las cláusulas 4, 5, 6, 7 y 8, no son aceptables cuando una organización solicite su conformidad con esta norma.

Estas cláusulas son:

4. SGSI
5. Responsabilidad de la Dirección
6. Auditoría Interna del SGSI
7. Revisión del SGSI por la Dirección
8. Mejora del SGSI

Estas cláusulas realmente conforman el cuerpo principal de esta norma.

Cualquier exclusión a los controles detallados por la norma y denominados como "necesarios" para satisfacer los criterios de aceptación de riesgos, debe ser justificada y se debe poner de manifiesto, o evidenciar claramente los criterios por los cuales este riesgo es asumido y aceptado. En cualquier caso en el que un control sea excluido, la conformidad con este estándar internacional, no será

aceptable, a menos que dicha exclusión no afecte a la capacidad y/o responsabilidad de proveer seguridad a los requerimientos de información que se hayan determinado a través de la evaluación de riesgos, y sea a su vez aplicable a las regulaciones y legislación vigente.

2. REFERENCIA NORMATIVA

Para la aplicación de esta norma, es indispensable tener en cuenta la última versión de ISO/IEC 17799:2005, Tecnología de la información. Técnicas de seguridad. Código de práctica para la gestión de la seguridad de la información.

4. SGSI

4.1 REQUERIMIENTOS GENERALES

La organización establecerá, implementará, operará, monitorizará, revisará, mantendrá y mejorará un SGSI documentado en el contexto de su propia organización, para las actividades globales de su negocio y de cara a los riesgos.

Para el propósito de esta norma el proceso está basado en el modelo PHVA comentado en el numeral 0.2.

Figura 6. Ciclo modelo del PHVA.

4.3.2 Control de documentos

Todos los documentos requeridos por el SGSI serán protegidos y controlados. Un procedimiento documentado deberá establecer las acciones de gestión necesarias para:

a) aprobar documentos en cuanto a su suficiencia antes de su publicación;

b) revisiones, actualizaciones y reaprobación de documentos;

c) asegurar que los cambios y las revisiones de documentos sean identificados;

d) asegurar que las últimas versiones de los documentos aplicables estén disponibles y listas para ser usadas;
e) asegurar que los documentos permanezcan legibles y fácilmente identificables;

f) asegurar que los documentos estén disponibles para quien los necesite y sean transferidos, guardados y finalmente dispuestos acorde a los procedimientos aplicables a su clasificación;

g) asegurar que los documentos de origen externo sean identificados;

h) asegurar el control de la distribución de documentos;

i) prevenir el empleo no deseado de documentos obsoletos, y

j) aplicar una clara identificación para poder acceder a ellos y que queden almacenados para cualquier propósito.

5. RESPONSABILIDAD DE LA DIRECCIÓN

5.1 COMPROMISO DE LA DIRECCIÓN

La Dirección proveerá evidencias de su compromiso para el establecimiento, implementación, operación, monitorización, mantenimiento y mejora del SGSI:

a) estableciendo la política del SGSI;

b) asegurando el establecimiento de los objetivos y planes del SGSI;

c) estableciendo roles y responsabilidades para la seguridad de la información;

d) comunicando y concientizando a la organización sobre la importancia y apoyo necesario a los objetivos propuestos por la política de seguridad, sus responsabilidades legales y la necesidad de una continua mejora en este aspecto;

e) brindando los recursos suficientes para establecer, operar, implementar, monitorizar, revisar, mantener y mejorar el SGSI (…Véase el numeral 5.2.1… de la norma ISO 27001);

f) decidiendo los criterios de aceptación de riesgos y los niveles del mismo;

g) asegurando que las auditorías internas del SGSI, se realizan (Véase el numeral 6 de la norma ISO 27001), y

h) que a su vez conduzcan a la Dirección para la revisión del SGSI (Véase el numeral 7 de la norma ISO 27001).

5.2.2 Formación, toma de conciencia y competencia

La organización asegurará que todo el personal a quien le sean asignadas responsabilidades definidas en el SGSI sea competente y esté en capacidad de ejecutar las tareas requeridas, para ello deberá proveer las herramientas y capacitación necesaria.

En esta cláusula la norma tiene cuatro exigencias específicas[14]:

[14] *ALEXANDER, Alberto G., Diseño de un sistema de gestión de seguridad de información, Bogotá, Alfaomega, 2007.*

a) *Se deben determinar los perfiles requeridos del personal al que se le asignan responsabilidades en el SGSI y diagnosticar sus necesidades de entrenamiento.*

b) *Capacitar y seleccionar al personal para satisfacer los perfiles requeridos.*

c) *Efectuar una evaluación de la eficacia del entrenamiento efectuado.*

d) *Mantener expedientes del personal, donde se detallen: educación recibida, capacitación realizada, capacidades desarrolladas, experiencias profesionales y calificaciones obtenidas.*

La cláusula 5.2.2 es un complemento a la cláusula de control A.8.2.2 del Anexo A.

Este numeral de la norma tiene un requerimiento bastante particular. Exige que la organización implemente un mecanismo que le permita medir la eficacia de la capacitación realizada. La organización debe mostrar la evidencia de que a toda persona que ha sido entrenada se le mide si ha adquirido las competencias deseadas.

6. AUDITORÍAS INTERNAS DEL SGSI

Esta cláusula exige que la organización realice auditorías internas al SGSI a intervalos planeados para determinar si los controles, sus objetivos, los procesos y procedimientos continúan de conformidad a esta norma, y para analizar y planificar acciones de mejora.

Ninguna persona podrá auditar su propio trabajo, ni cualquier otro que guarde relación con él. De esta manera se evita que haya conflictos de intereses.

La responsabilidad y requerimientos para el planeamiento y la conducción de las actividades de auditoría, los informes resultantes y el mantenimiento de los registros serán definidos en un procedimiento (aplica el Procedimiento de Auditorías Internas del SGC de la UIS).

7. REVISIÓN DEL SGSI POR LA DIRECCIÓN

Las revisiones mencionadas en el punto anterior deberán llevarse a cabo al menos una vez al año para asegurar su vigencia, adecuación y efectividad. Estas revisiones incluirán valoración de oportunidades para mejorar o cambiar el SGSI incluyendo la política de seguridad de la información y sus objetivos. Los resultados de estas revisiones, como se mencionó en el punto anterior serán claramente documentados y los mismos darán origen a esta actividad.

Esta actividad está constituida por la verificación de los aspectos que deben contemplarse en las revisiones …Véase el numeral 7.2… de la norma, y los aspectos que deben alcanzarse como resultado de las revisiones …Véase el numeral 7.3… lo cual dará como resultado el documento correspondiente (Actas de Revisión del SGSI por la Dirección).

8. MEJORAMIENTO DEL SGSI

8.1 MEJORAMIENTO CONTINUO

La mejora continua es visualizada como el conjunto de acciones emprendidas por la organización, para aumentar la probabilidad de incrementar la satisfacción de las partes interesadas.

En esta cláusula la norma especifica que la organización debe tomar como fuentes de datos, para iniciar la mejora continua:

- *La política de seguridad de la información;*
- *Los objetivos de seguridad;*
- *Los resultados de auditoría;*
- *El análisis de los eventos monitoreados;*
- *Las acciones correctivas y preventivas*
- *La revisión por la Dirección.*

La organización debe tener un mecanismo que propicie las acciones continuas de mejora del SGSI en el tiempo.

8.2. ACCIONES CORRECTIVAS

La organización llevará a cabo acciones para eliminar las causas que no estén en conformidad con los requerimientos del SGSI, con el objetivo de minimizar y evitar la recurrencia de las mismas. Cada una de estas acciones correctivas deberá documentarse (Ver Anexo 1: Procedimiento de Acciones Correctivas)

8.3 ACCIONES PREVENTIVAS

La *acción preventiva* se entiende como la "acción tomada para eliminar la causa de una no conformidad potencial u otra situación potencialmente indeseable" (ISO 9000:2000).

La cláusula exige también la existencia de un procedimiento documentado, y menciona que la evaluación del riesgo determina la prioridad de las acciones preventivas a tomarse (Ver Anexo 1)

El anexo A de esta norma propone una tabla detallada de los controles, los cuales quedan agrupados y enumerados de la siguiente forma:

A.5 Política de seguridad
A.6 Organización de la información de seguridad
A.7 Administración de recursos
A.8 Seguridad de los recursos humanos
A.9 Seguridad física y del entorno
A.10 Administración de las comunicaciones y operaciones
A.11 Control de accesos
A.12 Adquisición de sistemas de información, desarrollo y mantenimiento
A.13 Administración de los incidentes de seguridad
A.14 Administración de la continuidad de negocio
A.15 Cumplimiento (legales, de estándares, técnicas y auditorías)

El anexo B, que es informativo, a su vez proporciona los principios presentados en las directrices de la OECD (Organización para la Cooperación y el Desarrollo Económico) (Directrices para la Seguridad de Sistemas y Redes de Información) y su correspondencia con el modelo PHVA.

Por último el Anexo C, también informativo, resume la correspondencia entre esta norma y los estándares ISO/IEC 9001:2000 (ahora ISO/IEC 9001:2008) e ISO 14001:2004.

7. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

El Sistema de Gestión de la Seguridad de la Información (SGSI) es la base fundamental sobre la que se construye la Norma Internacional ISO/IEC 27001:2005.

Garantizar un nivel de protección total es virtualmente imposible. El propósito de un SGSI es, por lo tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

7.1 ¿QUÉ ES UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN?

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información, ISMS (por sus siglas en inglés: "*Information Security Management System*").

En el contexto del SGSI propuesto en esta monografía, el término "información" es todo aquel conjunto de datos organizados en poder de una organización que poseen valor para la misma, independientemente:

- de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.);

- de su origen (de la propia organización o de fuentes externas), o

❖ de la fecha de elaboración.

Figura 7. Proceso general que origina la "Información".

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como la ISO 9001, como el sistema de calidad para la seguridad de la información, el cual, garantiza que la seguridad de la información sea gestionada correctamente, desde un enfoque de riesgo empresarial.

7.2 PARA QUÉ SIRVE UN SGSI

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de la información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen institucional necesarios para lograr los objetivos de la organización y asegurar los beneficios económicos.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, el apoyo adecuado a los objetivos institucionales para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades empresariales, son algunos de los aspectos fundamentales que hacen que un SGSI se convierta en una herramienta de gran utilidad y de ayuda para la gestión de las organizaciones.

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la alta Dirección al frente, tomando en consideración también a clientes y proveedores de bienes y servicios.

El modelo de gestión de la seguridad debe contemplar procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer políticas y procedimientos en concordancia con los objetivos institucionales de la organización, con el fin de mantener un nivel de exposición siempre menor al nivel de riesgo que la misma Institución decida asumir.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o los controla mediante una Política sistemática, definida, documentada y conocida por todos, que se revisa y mejora constantemente.

7.3 DOCUMENTACIÓN DEL SGSI

En el ambiente de gestión de la calidad según la ISO 9001, siempre se ha mostrado gráficamente la documentación del sistema como una pirámide de cuatro niveles. Es posible trasladar ese modelo a un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001 de la siguiente forma:

Figura 8. Pirámide documental de un SGSI.

7.3.1 Documentos de Nivel 1.

Manual de seguridad: por analogía con el manual de calidad, aunque el término se usa también en otros ámbitos. Sería el documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI.

7.3.2 Documentos de Nivel 2.

Procedimientos: documentos en el nivel operativo, que aseguran que se realice de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.

7.3.3 Documentos de Nivel 3.

Instrucciones, *checklists* y formularios: documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

7.3.4 Documentos de Nivel 4.

Registros: documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como salidas que demuestran que se ha cumplido lo indicado en los mismos.

En la cláusula 4.3.1, de manera específica, la Norma NTC-ISO/IEC 27001:2005 indica que un SGSI debe contar con los siguientes documentos, en cualquier formato o tipo de medio:

Alcance del SGSI: ámbito de la organización que queda cubierto por el SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y las partes que no hayan sido consideradas en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como sedes, divisiones, áreas, procesos, sistemas o tareas concretas.

Política y objetivos de seguridad: documento de contenido genérico que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Procedimientos y mecanismos de control que soportan al SGSI: aquellos procedimientos que regulan el propio funcionamiento del SGSI.

Enfoque de evaluación de riesgos: descripción de la metodología a emplear. Cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación con los activos de información contenidos dentro del alcance establecido. Desarrollo de criterios de aceptación de riesgos y fijación del nivel de riesgo aceptable.

Informe de evaluación de riesgos: estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.

Plan de tratamiento de riesgos: documento que identifica las acciones de la Dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.

Procedimientos documentados: todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.

Registros: documentos que proporcionan evidencia de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.

Declaración de Aplicabilidad (SOA, por sus siglas en inglés "*Statement of Applicability*"): documento referenciado en la cláusula 4.2.1 j) del estándar ISO/IEC 27001:2005. Contiene la lista de los objetivos de control y los controles contemplados por el SGSI. Para establecer este listado, se requiere de una identificación de riesgos, definición de controles, identificación de requisitos legales, regulatorios, contractuales, etc., y por supuesto, de revisar las necesidades de la Organización, justificando inclusiones y exclusiones.

Esta identificación se conoce como un *GAP ANALYSIS*, el cual identifica la diferencia entre lo que debería tenerse implementado en la organización y lo que se tiene realmente disponible. Para el caso especifico de la UIS, este tipo de análisis se debe hacer evaluando el cumplimiento de la norma NTC-ISO/IEC 27002:2005, para cada uno de los controles establecidos en los 11 dominios o temas relacionados con la gestión de la seguridad de la información que este estándar especifica.

Normalmente los controles incluidos se basan en la Norma ISO 27002, pero es válido establecer controles adicionales a los incluidos en dicha Norma, informando la inclusión de tales controles en una sección propia del documento. Ahora, para los controles que no se vayan a implementar se debe incluir una justificación individual para cada uno de ellos explicando el porqué no se implementaron.

7.3.5 Documentos del SGC Institucional que aplican al SGSI. Una vez revisada la documentación del SGC de la UIS, se pudo confirmar que los siguientes documentos de dicho sistema, ya certificado en la Universidad, aplican en su totalidad para los documentos obligatorios exigidos por la norma ISO 27001, en el numeral 4.3.1:

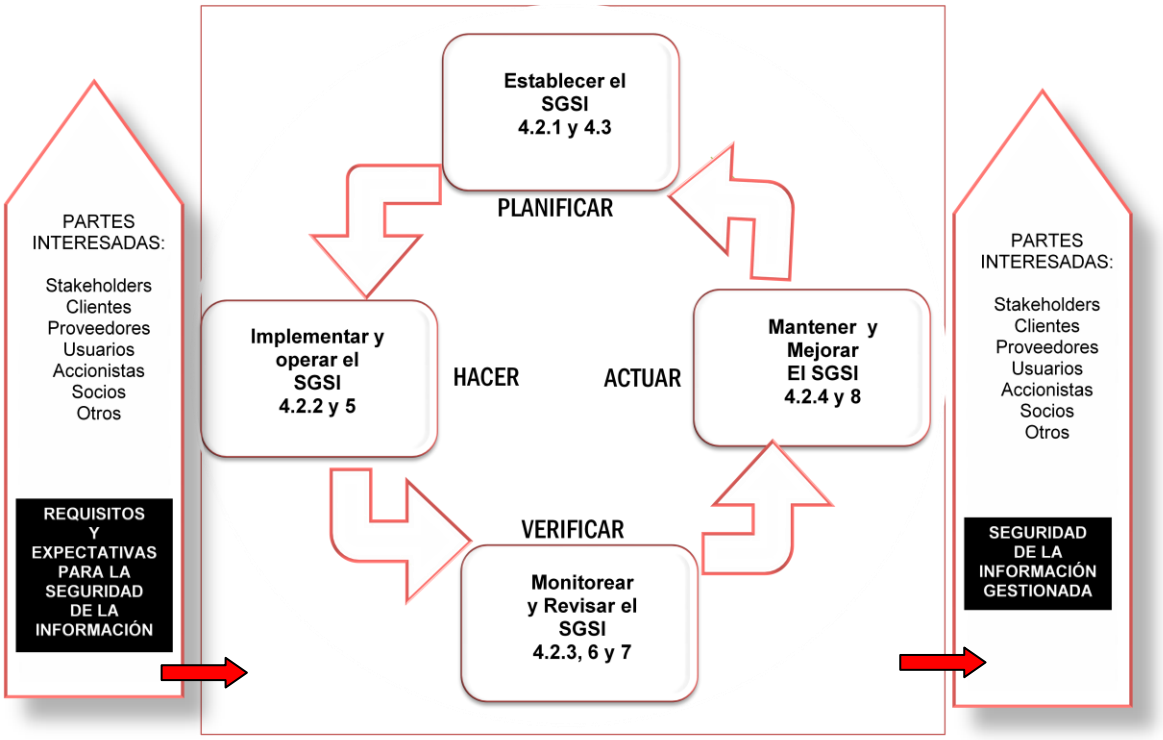
- PGD.01. CONTROL DE DOCUMENTOS INTERNOS
- PGD.09. CONTROL DE DOCUMENTOS EXTERNOS
- PGD.02. CONTROL DE REGISTROS
- PSE.01. AUDITORÍAS INTERNAS DE CALIDAD, y

la mayoría de los formatos que son transversales para los procesos, como son: Listados Maestros de Documentos Internos, Externos y de Registros, donde se pueden incluir los documentos legales y normas internas que apliquen al SGSI, al igual que los registros que se generen en el sistema mismo. La documentación adicional que se identifique como requerida durante la proyección de la implementación del SGSI se tiene que diseñar.

7.4 ¿CÓMO SE IMPLEMENTA UN SGSI?

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información con base en la Norma NTC-ISO/IEC 27001:2005, se utiliza el ciclo de mejora continua PHVA (PDCA por sus siglas en inglés), tradicional en los sistemas de gestión de la calidad.

Figura 9. PHVA del SGSI con la norma ISO/IEC 27001:2005.

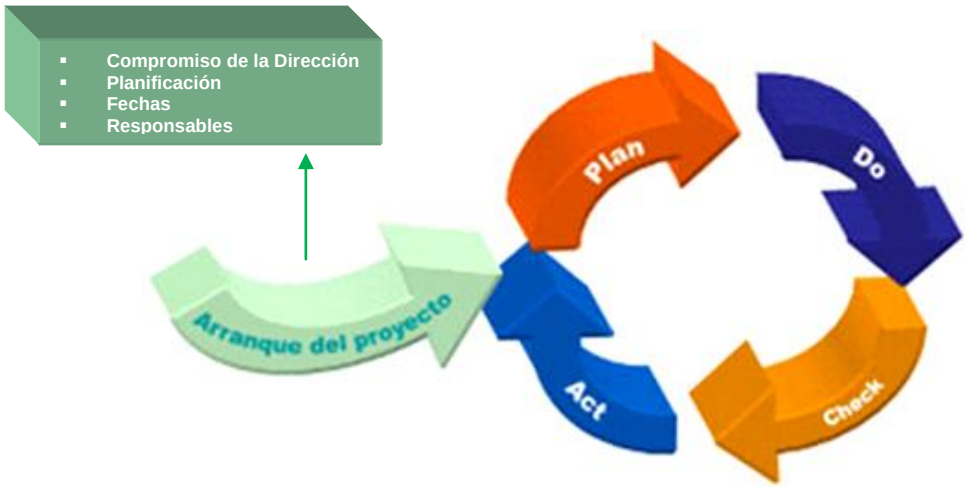


7.4.1 Arranque del Proyecto. Al decidir el inicio del proyecto de implementación de un SGSI en una organización, se debe establecer:

- El compromiso de apoyo de la Alta Dirección

- La planificación general del proyecto de implementación

Figura 10. Fase de inicio del SGSI.



Fuente: www.ISO27001.es

- El cronograma para la ejecución del proyecto

- Los responsables y sus funciones

7.4.2 Planificar: Establecer el SGSI. En esta fase se define:

- El alcance del SGSI, en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.

El alcance de un SGSI dependerá de la identificación de aquellos procesos considerados críticos y sobre los cuales se implementará el SGSI. Para Alexander (2007) al momento de definir el alcance del SGSI, el responsable del proyecto debe tener claros los siguientes aspectos:

- Las características del negocio. Tipos de productos y/o servicios ofrecidos, y clientes objetivo.

- Modelo de organización de la Institución. Por procesos, por productos o por funciones.

- Clasificación de todos los activos y tecnologías del proceso seleccionado.

- De acuerdo con el estándar ISO/IEC 27001:2005, para definir el alcance se deben incluir:

- Todas las interfaces que operan en la organización;

- Todas las áreas involucradas en los procesos, y

- Todos aquellos proveedores que incidan en el SGSI.

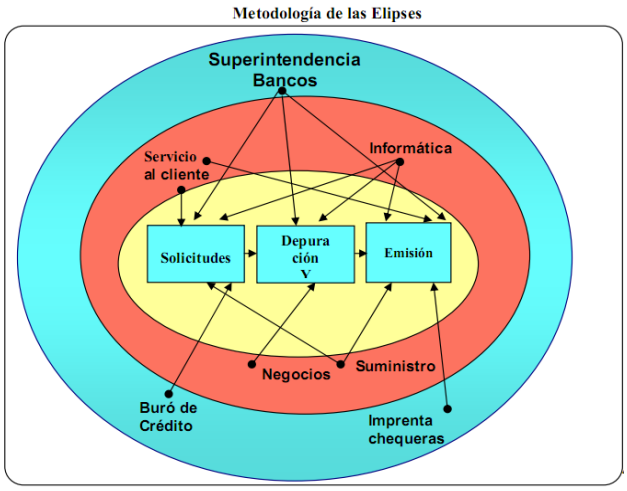
- Alexander (2007), señala que el método más preciso para determinar el alcance de un SGSI, es la metodología de las elipses. Este método establece que se han de tomar cada uno de los procesos de una organización y separarlos para su análisis de la siguiente manera:

- Identificar los procesos básicos y listar los subprocesos de cada uno de ellos. Estos se ubican en la elipse central o concéntrica;

- Ubicar en la elipse intermedia las interacciones que el proceso analizado tiene con otros procesos dentro de la organización, ligándolos a través de flechas

- En la última elipse o capa más externa, se identifican y se relacionan las organizaciones externas a la entidad y que tienen alguna relación con el proceso analizado.

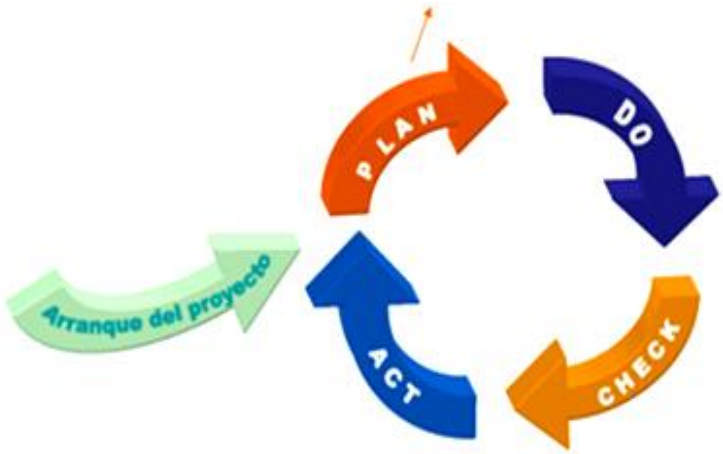
Figura 11. Ejemplo de utilización del Método de las Elipses.



Fuente: ALEXANDER, Alberto, Análisis y evaluación de riesgos: un ejemplo en la Banca.

Figura 12. Establecimiento del SGSI.

- Definir alcance del SGSI
- Definir política de seguridad
- Metodología de valoración de riesgos
- Inventario de activos
  - Identificar, riesgos, amenazas y vulnerabilidades
- Identificar impactos
- Análisis y evaluación de riesgos
- Selección de controles y SOA



Fuente: www.ISO27000.es

❖ Se debe definir una política de seguridad que:

- Incluya el marco general y los objetivos de la seguridad de la información de la organización;

- Considere requerimientos legales o contractuales relativos a la seguridad de la información;

- Esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI;

- Establezca los criterios con los que se va a valorar el riesgo;

- Esté aprobada por la dirección.

Definir una metodología de valoración del riesgo apropiada para el SGSI y los requerimientos Institucionales, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable. Lo fundamental de esta metodología es que los resultados obtenidos sean comparables y repetibles.

Existen numerosas metodologías estandarizadas para la valoración de riesgos, aunque es perfectamente aceptable por la norma definir una propia. Como parte de las recomendaciones de este estudio se sugiere la utilización de la **Metodología MAGERIT**[15], la cual se define en un capitulo posterior en este documento. Esta metodología comprende:

- Identificar los riesgos y los activos de información:

- Identificar los activos que están dentro del alcance del SGSI y sus responsables directos, denominados propietarios;

[15] *MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas, Ministerio de Administraciones Públicas, Madrid, 2006, disponible en http://publicaciones.administracion.es*

- Identificar las amenazas en relación a los activos;

- Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas;

- Identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.

❖ Analizar y evaluar los riesgos:

- Evaluar el impacto en el negocio de una falla de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información;

- Evaluar de manera real la probabilidad de ocurrencia de una falla de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados;

- Estimar los niveles de riesgo;

Determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.

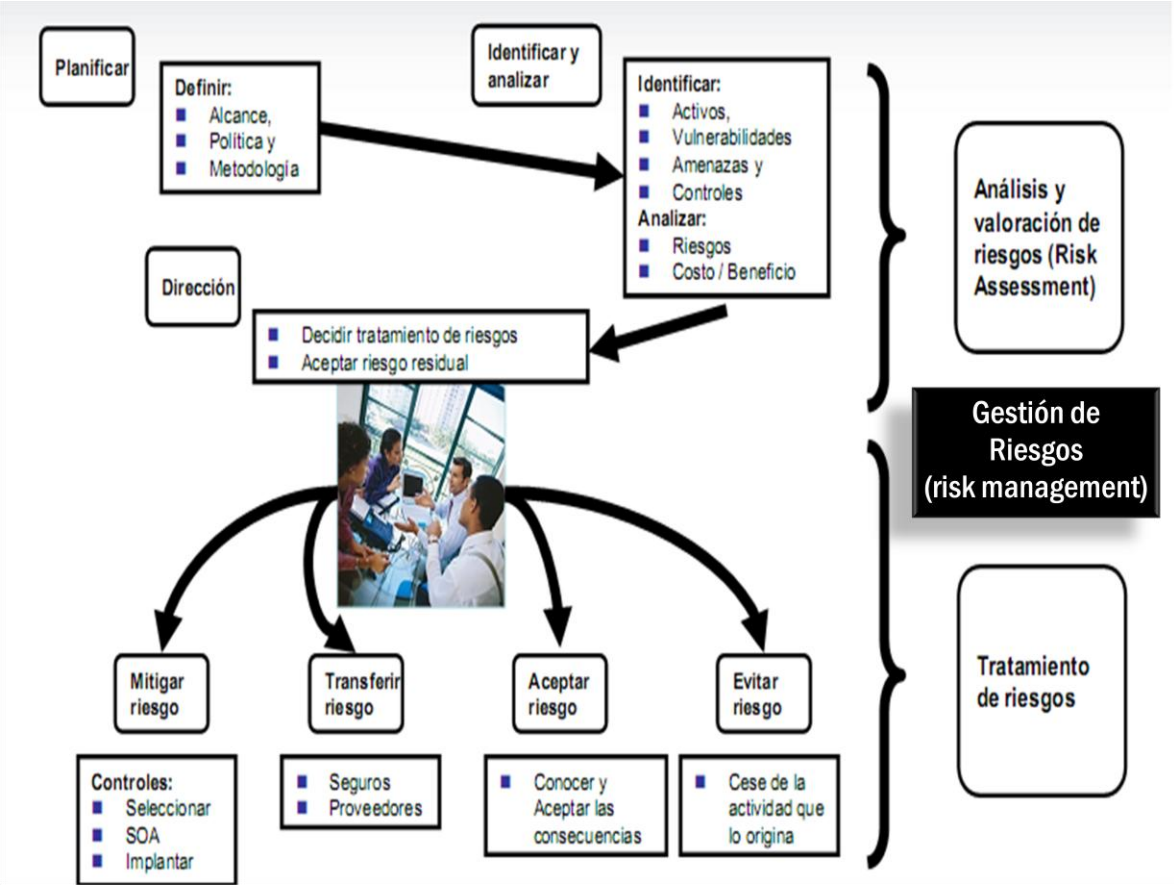
❖ Identificar y evaluar las distintas opciones de tratamiento del riesgo para:

- Aplicar controles adecuados;

- Aceptar el riesgo, siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos;
- Evitar el riesgo;

- Transferir el riesgo a terceros, por ejemplo, compañías de seguros o proveedores de *outsourcing*.

Figura 13. Ciclo de gestión de riesgos de ISO 27001.



- Seleccionar los objetivos de control y los controles del Anexo A de la norma NTC-ISO/IEC 27001:2005 para el tratamiento del riesgo que cumplan con los requerimientos identificados en el proceso de valoración del riesgo.

- Obtener de la Alta Dirección, la aprobación tanto para los riesgos residuales como para la implementación y uso del SGSI.

- Definir una Declaración de Aplicabilidad que incluya:

  - Los objetivos de control y controles seleccionados y los motivos para su elección;

  - Los objetivos de control y controles que actualmente ya están implementados;

  - Los objetivos de control y controles, del Anexo A de ISO 27001, excluidos y los motivos para su exclusión; este es un mecanismo que permite, además, detectar posibles omisiones involuntarias.

Con relación a los controles de seguridad, el estándar NTC-ISO/IEC 27002:2005 (anterior ISO 17799:2005) proporciona una completa guía de implementación que contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Esta norma es referenciada en ISO/IEC 27001:2005, en su segunda cláusula, en términos de *"documento indispensable para la aplicación de este norma"*, y deja abierta la posibilidad de incluir controles adicionales en el caso de que la guía no contemple todas las necesidades particulares de la organización.

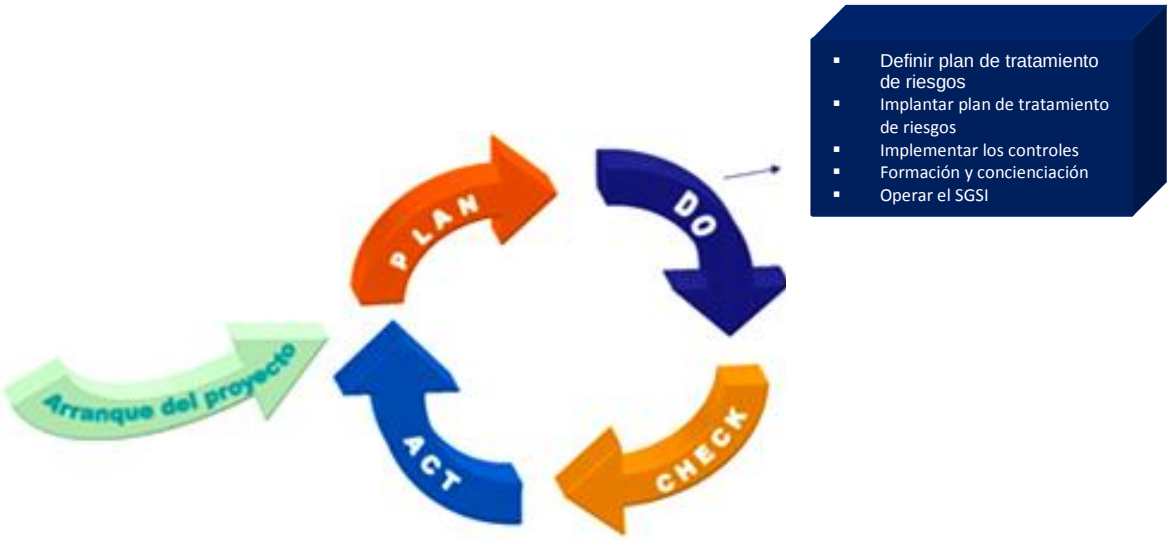
7.4.3 Hacer: Implementar y utilizar el SGSI. En esta fase se debe:

- Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.

- Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.

- Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.

Figura 14. Fase de puesta en ejecución del SGSI.



Fuente: www.ISO27000.es

- Definir un sistema de indicadores que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.

- Establecer y ejecutar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.

- Gestionar las operaciones del SGSI.

- Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.

- Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

7.4.4 Verificar: Monitorizar y revisar el SGSI. La organización deberá ejecutar procedimientos de monitorización y revisión para:

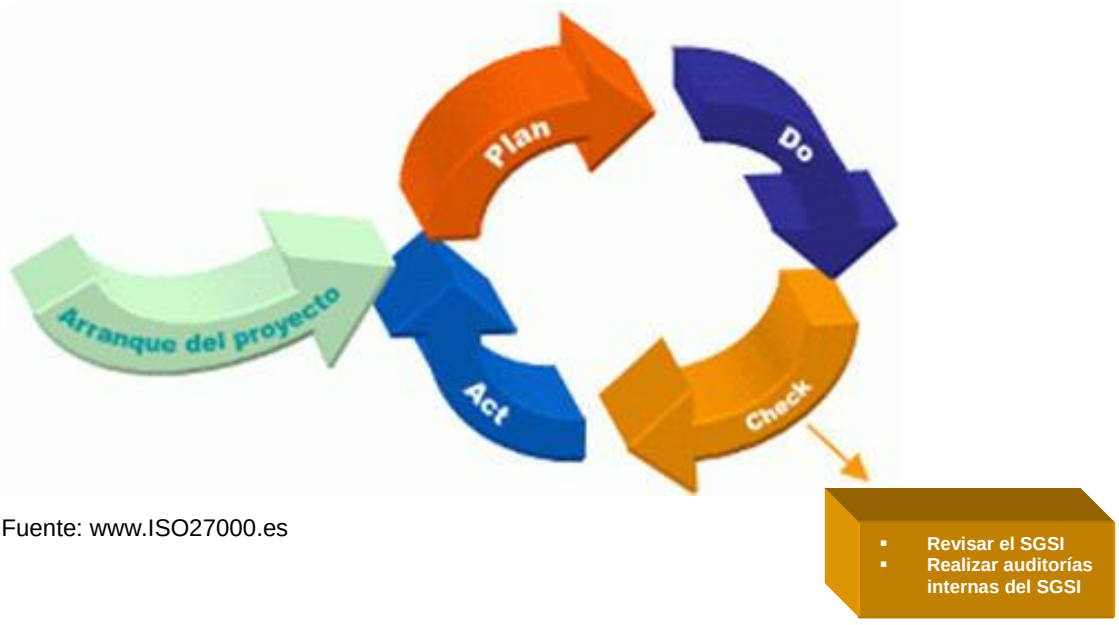
- ❖ Detectar a tiempo los errores en los resultados generados por el procesamiento de la información;

- ❖ Identificar brechas e incidentes de seguridad;

- ❖ Ayudar a la Dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos, para garantizar la seguridad de la información, se desarrollan en relación a lo previsto;

- ❖ Detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores;

Figura 15. Fase de Monitorización y revisión del SGSI.



Fuente: www.ISO27000.es

- Determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.

- Revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.

- Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.

- Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior (requerimientos legales, obligaciones contractuales, etc.).
- Realizar periódicamente auditorías internas del SGSI a intervalos planificados.

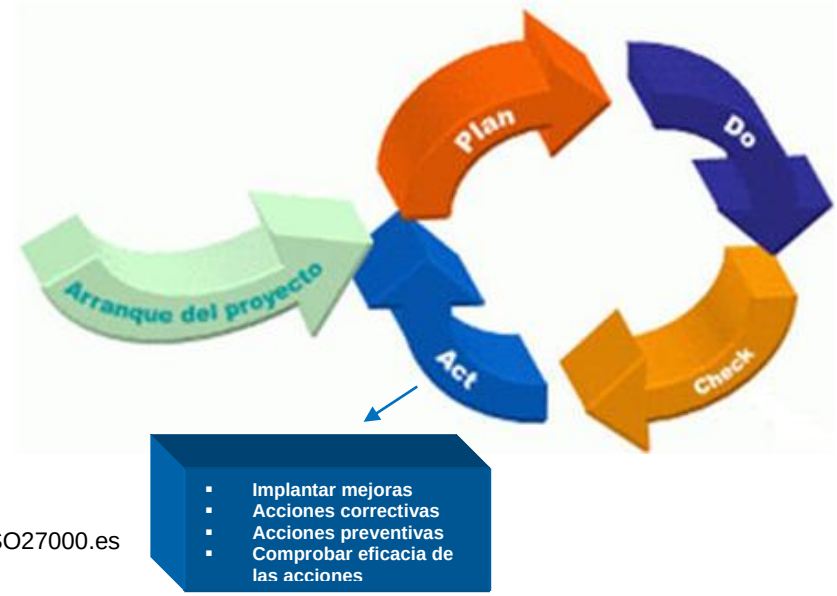
- Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.

- Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.

- Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

7.4.5 Actuar: Mantener y mejorar el SGSI. En esta fase la organización deberá regularmente:

Figura 16: Fase de mantenimiento y mejora del SGSI.



Fuente: www.ISO27000.es

- Implantar en el SGSI las mejoras identificadas.

- Realizar las acciones preventivas y correctivas adecuadas en relación a la cláusula 8 de ISO/IEC 27001 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.

- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.

- Asegurar que las mejoras implantadas alcanzan los objetivos previstos.

El modelo PHVA es un ciclo de vida continuo, lo cual quiere decir que la fase de Actuar lleva de nuevo a la fase de Planear para iniciar un nuevo ciclo de las cuatro fases. Es importante tener en cuenta que no tiene que haber una secuencia

estricta de las fases, sino que, por ejemplo, puede haber actividades de implantación que ya se lleven a cabo cuando otras de planificación aún no han finalizado; o que se monitoricen controles que aún no están implantados en su totalidad.

7.4.6 Compromisos de la Dirección en un SGSI. Uno de los componentes fundamentales en la implantación exitosa de un Sistema de Gestión de la Seguridad de la Información es la participación de la Dirección.

Desde un principio debe asumirse que un SGSI afecta fundamentalmente a la gestión del negocio y requiere, por tanto, de decisiones y acciones que sólo puede tomar la Dirección de la organización. No se debe caer en el error de considerar un SGSI como una simple cuestión técnica o tecnológica relegada a niveles inferiores del organigrama; se gestionan riesgos e impactos de negocio que son responsabilidad y decisión de la Dirección.

El término Dirección debe contemplarse siempre desde el punto de vista del alcance del SGSI. Es decir, se refiere al nivel más alto de gerencia de la parte de la organización afectada por el SGSI (la definida en el alcance).

Algunas de las tareas fundamentales del SGSI que ISO/IEC 27001 asigna a la Dirección se detallan en el análisis realizado a la norma {Véase el numeral 5.1}

7.4.7 Formación y concienciación. La formación y la concienciación en seguridad de la información son elementos básicos para el éxito de un SGSI. Por ello, la Dirección debe asegurar que todo el personal de la organización al que se le asignen responsabilidades definidas en el SGSI esté suficientemente capacitado {Véase análisis de la norma realizado anteriormente}

Además, la Dirección debe asegurar que todo el personal relevante esté consciente de la importancia de sus actividades de seguridad de la información y de cómo contribuye a la consecución de los objetivos del SGSI.

7.4.8 Revisión del SGSI. A la Dirección de la organización se le asigna también la tarea de, al menos una vez al año, revisar el SGSI, para asegurar que continúe siendo adecuado y eficaz.

Para ello, debe recibir una serie de informaciones, que le ayuden a tomar decisiones, entre las que se pueden enumerar:

- Resultados de auditorías y revisiones del SGSI.
- Observaciones de todas las partes interesadas.
- Técnicas, productos o procedimientos que pudieran ser útiles para mejorar el rendimiento y eficacia del SGSI.
- Información sobre el estado de acciones preventivas y correctivas.
- Vulnerabilidades o amenazas que no fueron tratadas adecuadamente en evaluaciones de riesgos anteriores.
- Resultados de las mediciones de eficacia.
- Estado de las acciones iniciadas a raíz de revisiones anteriores de la Dirección.
- Cualquier cambio que pueda afectar al SGSI.
- Recomendaciones de mejora.

Basándose en todas estas informaciones, la Dirección debe revisar el SGSI y tomar decisiones y acciones relativas a:

- Mejora de la eficacia del SGSI.

- Actualización de la evaluación de riesgos y del plan de tratamiento de riesgos.

- Modificación de los procedimientos y controles que afecten a la seguridad de la información, en respuesta a cambios internos o externos en los requisitos de negocio, requerimientos de seguridad, procesos de negocio, marco legal, obligaciones contractuales, niveles de riesgo y criterios de aceptación de riesgos.

- Necesidades de recursos.

- Mejora de la forma de medir la efectividad de los controles.

8. METODOLOGÍAS DE ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN

Conocer el riesgo al que están sometidos los activos de información es, simplemente, imprescindible para poder gestionarlos y para ello han aparecido multitud de metodologías y herramientas de soporte que buscan objetivar el análisis para saber qué tan seguros (o inseguros) son. El gran reto de todas estas aproximaciones es la complejidad del problema al que se enfrentan; complejidad en el sentido de que hay muchos elementos que considerar y que, si no se es riguroso, las conclusiones no serán fiables.

8.1 METODOLGÍA MAGERIT v2 2005

MAGERIT, siglas que significan: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas. Es una metodología de carácter público, perteneciente al Ministerio de Administraciones Públicas (MAP) de España. Su utilización no requiere autorización previa del MAP.

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que suministran beneficios evidentes para las organizaciones, pero que también dan lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

Magerit persigue los siguientes objetivos:

- **Directos**:

  - Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de controlarlos a tiempo;

- Ofrecer un método sistemático para analizar tales riesgos;

- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.

- **Indirectos**:

- Apoyar la preparación de la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

8.1.1 Guías de la metodología. MAGERIT versión 2 está estructurada en tres libros:

- **Método**. Describe los pasos y las tareas básicas para realizar un proyecto de análisis y gestión de riesgos (Ver página 79 en este documento), y proporciona una serie de aspectos prácticos.

- **Catálogo de Elementos**. Ofrece unas pautas y elementos estándar en cuanto a: tipos de activos, dimensiones de valoración de los activos, criterios de valoración de los activos, amenazas típicas sobre los sistemas de información y salvaguardas a considerar para proteger sistemas de información.

- **Guía de Técnicas**. Se trata de una guía de consulta que proporciona algunas técnicas que se emplean habitualmente para llevar a cabo proyectos de análisis y gestión de riesgos: técnicas específicas para el análisis de riesgos, análisis mediante tablas, análisis algorítmico, árboles de ataque, técnicas generales, análisis coste-beneficio, diagramas de flujo de datos, diagramas de procesos, técnicas gráficas, planificación de proyectos, sesiones de trabajo (entrevistas, reuniones y presentaciones) y valoración Delphi.

MAGERIT describe la metodología desde tres ángulos:

- Detalla los pasos para realizar un análisis del estado de riesgo y para gestionar su mitigación. Es una presentación netamente conceptual.

- Describe las tareas básicas para realizar un proyecto de análisis y gestión de riesgos, entendiendo que no basta con tener los conceptos claros, sino que es conveniente reglamentar roles, actividades, hitos y documentación para que la realización del proyecto de análisis y gestión de riesgos esté bajo control en todo momento.

- Aplica la metodología al caso del desarrollo de sistemas de información, con el fin de dar a conocer que los proyectos de desarrollo de sistemas deben tener en cuenta los riesgos desde el primer momento, tanto los riesgos a los que están expuestos, como los riesgos que las propias aplicaciones introducen en el sistema.

- Como complemento separa una serie de aspectos prácticos, derivados de la experiencia acumulada en el tiempo para la realización de un análisis y una gestión realmente efectivos.

La herramienta PILAR, de uso en la administración pública española, es un procedimiento informático-lógico para el análisis y la gestión de los riesgos de un sistema de información siguiendo la metodología MAGERIT. [DESCARGAR SOFTWARE EN: http://www.ar-tools.com/index.html?tools/pilar/index.html]

MAGERIT es la metodología recomendada en esta monografía para la realización del plan de gestión de riesgos de los sistemas de información de la UIS.

8.2 METODOLOGÍA OCTAVE

Evalúa amenazas y vulnerabilidades de los recursos tecnológicos y operacionales importantes de una organización.

El método OCTAVE (*Operationally Critical Thereat, Asset and Vulnerability Evaluation*) permite la comprensión del manejo de los recursos, identificación y evaluación de los riesgos que afectan la seguridad dentro de una organización. Exige llevar la evaluación de la organización y del personal de la tecnología de información (IT) por parte del equipo de análisis a través del apoyo de un patrocinador interesado en la seguridad.

Las funciones del equipo de análisis son:

- Identificar los recursos importantes mediante encuestas y entrevistas.
- Realizar actividades de análisis de riesgo.
- Relacionar amenazas y vulnerabilidades.
- Crear estrategias de protección, planes de mitigación y diseñar políticas de seguridad.

Octave es una marca registrada en la oficina de patentes y negocios de EEUU. Es una marca de servicio registrada por *Carnegie Mellon Univeristy*.

8.3 NIST 800-30ª

NIST 800-30ª es una metodología basada en los conceptos generales presentados en el Instituto Nacional de los Estándares y la Tecnología (NIST, *National Institute of Standards and Technology*).

El propósito de la guía es dar unos principios del desarrollo de un programa de gestión de riesgos y proporcionar información de controles de seguridad a un coste efectivo.

9. PROPUESTA DE DISEÑO DEL SGSI PARA EL PROCESO SERVICIOS INFORMÁTICOS Y DE TELECOMUNICACIONES DE LA UIS

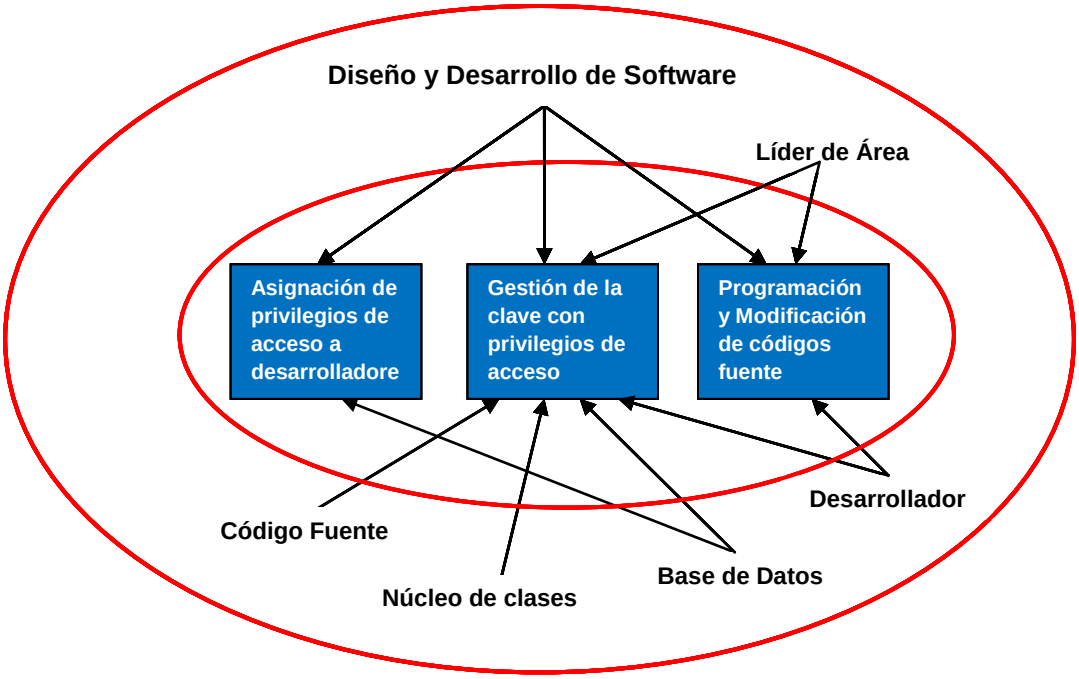
9.1 ALCANCE, LÍMITES, POLÍTICA Y ANÁLISIS DE GESTIÓN DE RIESGOS DEL SGSI DEFINIDO PARA LA UIS

Por razones estratégicas, la Universidad Industrial de Santander ha decidido implantar el SGSI, inicialmente, centrado en los activos y recursos informáticos de la red LAN/WAN que administra directamente la División de Servicios de Información - Proceso de Servicios Informáticos y de Telecomunicaciones de la UIS. El SGSI se limitará al campus central de la Universidad Industrial de Santander.

Para efectos de mostrar en esta monografía, la aplicación de los conceptos definidos para la determinación del alcance de un SGSI, se ha tomado de la firma *consultora Global SRL,* un ejemplo de análisis y evaluación de riesgos realizado en su proceso de "*Diseño y Desarrollo de Software*" con el fin de establecer un SGSI en dicha compañía.

Entonces, de acuerdo con la recomendación de Alexander (2007), utilizaron la Metodología de las Elipses para determinar el alcance, con el cual se trata de visualizar con precisión los distintos subprocesos que componen el mismo.

Figura 17. Método de las Elipses aplicado a un proceso de diseño y desarrollo de software para definir el alcance.



Fuente: GARCÏA, Pedro, Consultora Global SRL.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Por tratarse de una Institución de Educación Superior en constante crecimiento y actualización permanente en nuevas tecnologías de apoyo a la Misión y los objetivos institucionales, el SGSI podría formar parte como una de las bases para cumplir con el 100% de de todos los propósitos planeados para alcanzar la excelencia institucional. Por lo tanto, la política del SGSI debe estar en forma paralela con la Misión y la Visión de la Institución, la cual es brindar un servicio de educación de calidad, cumpliendo con las normas más altas de seguridad y protección de la información.

La política de seguridad de la información estará sustentada en los siguientes puntos:

- La seguridad y protección de la información tiene que ser uno de los pilares fundamentales en los servicios ofrecidos;

- Los activos más críticos dentro de la organización son: información de clientes, datos de contacto, bases de datos, servidor de pruebas, servidor web, servidor de correo, servidor de aplicaciones, equipo informático, red de comunicaciones y personal;

- Se tienen contratos de confidencialidad de datos de los clientes almacenados en las bases de datos de la organización;

- La alta dirección tiene que estar comprometida con la aplicación de Normas de calidad y seguridad de activos de información, y

- Brindar la máxima seguridad en confidencialidad, integridad y Disponibilidad de los datos e información almacenada en los servidores.

Como parte del SGSI propuesto para la UIS, en el **Anexo 6** se muestra una guía para la elaboración de la Política Institucional de la seguridad de la información.

A continuación se proporciona una lista de posibles políticas particulares que se pueden elaborar para el SGSI de la UIS:

- Política para el uso del correo electrónico
- Políticas para el acceso a Internet
- Política para el manejo de contraseñas
- Política para la seguridad de los servidores
- Política de uso aceptable de los recursos informáticos
- Política de auditoría de los sistemas de información
- Política de acceso remoto

- ❖ Política de uso de la red inalámbrica
- ❖ Política de cifrado de información aceptable
- ❖ Entre otras.

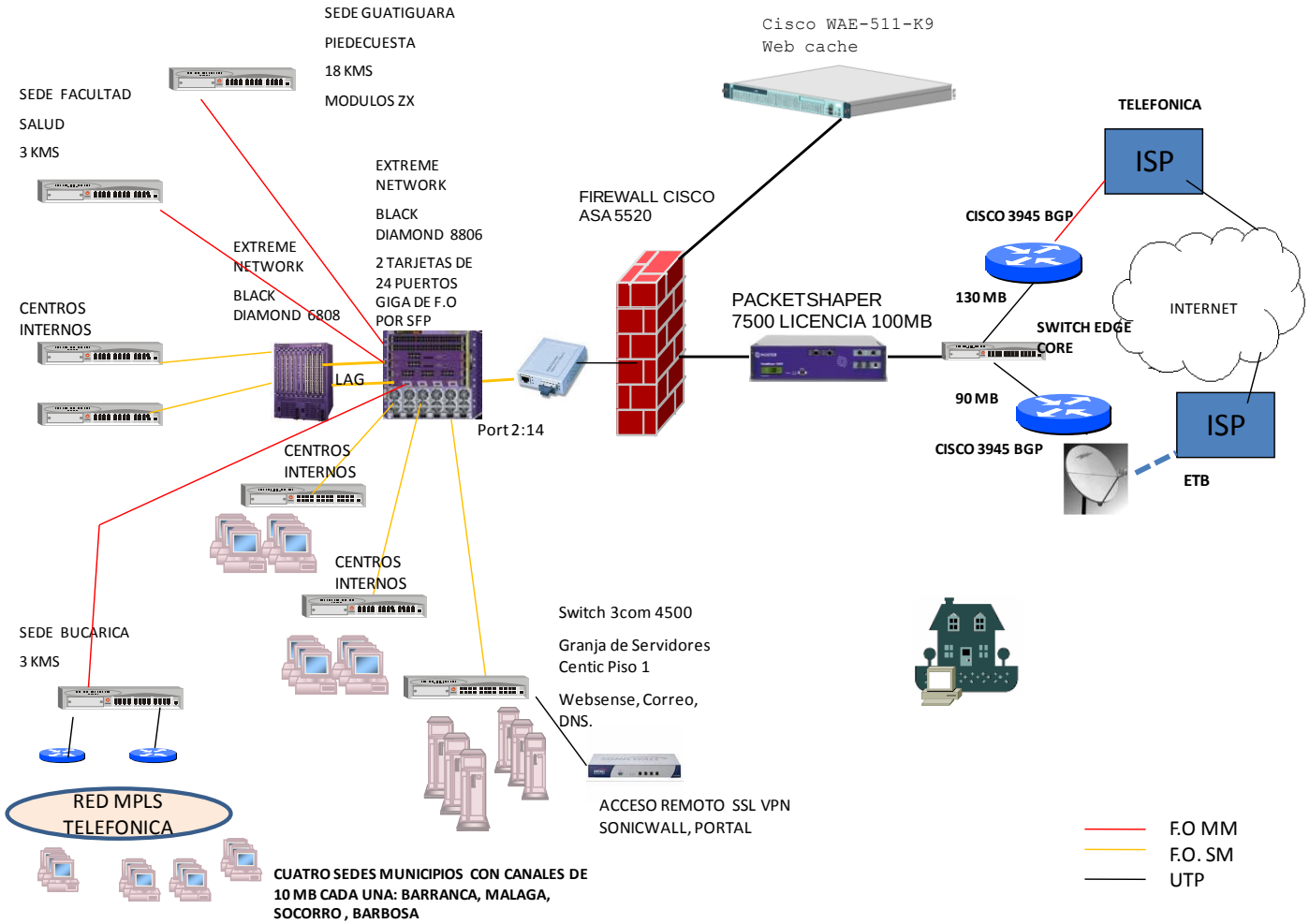
9.1.1 Topología de la RED WAN de la UIS

Con el fin de establecer el inventario preliminar de los activos de información de la DSI, se muestra a continuación la topología de la red WAN de la Universidad Industrial de Santander, en la cual existen equipos de infraestructura que se encuentran distribuidos en los campus de la institución, y que le corresponde monitorear a la División de Servicios de Información. En la Tabla 1 se relacionan los equipos más relevantes que conforman esta red y en las Figuras 17 y 18 se muestra la configuración actual y a futuro de la misma.

Tabla 2. Inventario preliminar de equipos de la red WAN de la UIS.

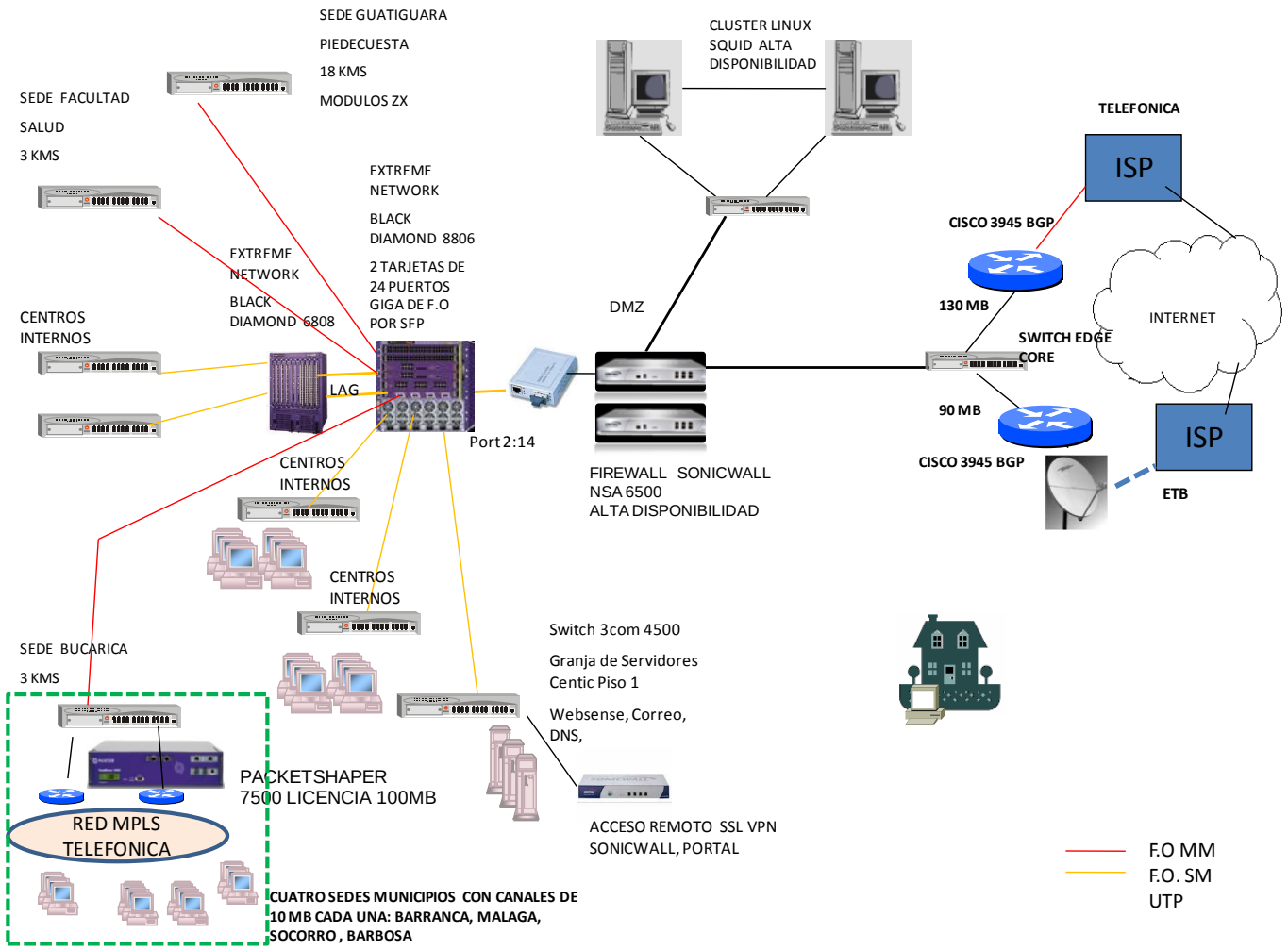
Ítem	Descripción Equipos	Cantidad
1	Servidor Extreme Network Black Diamond 8806	1
2	Servidor Extreme Network Black Diamond 6808	1
3	Firewall Cisco ASA 5520	1
4	Web Cache Cisco WAE-511-K9	1
5	Routers Cisco 3958 BGP	2
6	Switch 3Com 4500	
7	Centros de cableado internos	
8	Servidores en la granja del CENTIC	8
9	Packetshaper 7500	1
10	Switch Edge Core	1

Figura 18. Infraestructura actual de la red WAN de la UIS.



Fuente: DSI - División de Servicios de Información UIS.

Figura 19. Infraestructura de la red WAN de la UIS con FIREWALL SONICWALL (sugerida para nueva plataforma).



Fuente: División de Servicios de Información.

Continuando con el caso tomado como ejemplo, a continuación definen el enfoque de evaluación del riesgo:

Identificación, análisis y evaluación de riesgos. Utilizaron el método de las elipses, por ser más sencillo para aplicar al alcance del proceso. Se seleccionó entre los procesos resultantes, el de “Asignación de privilegios de acceso y control de versiones” en el área de Diseño y Desarrollo de Software, por ser esté uno de los procesos más vulnerables dentro del área de desarrollo, ya que con la incorporación de nuevos Desarrolladores, se hace necesario el control de accesos y asignación de privilegios que minimicen el robo de código fuente y el control de versiones.

Una vez identificados todos los activos de información comprendidos en el alcance, utilizando la metodología de las elipses, se procedió a establecer el SGSI, realizando un análisis y evaluación del riesgo de los activos identificados para determinar cuáles son aquellos que deben ser protegidos para mitigar su riesgo, así como definir también cual es el riesgo residual.

Los pasos que indica la metodología para el análisis y evaluación de los riesgos son:

- Identificación de Activos
- Tasación de Activos
- Identificación de amenazas
- Posibilidad de ocurrencia de amenazas
- Identificación de vulnerabilidades
- Posible explotación de vulnerabilidades
- Estimado del valor de los Activos en Riesgo
- Posibilidad de ocurrencia del riesgo
- Valor del riesgo de los Activos

En la tabla 3 se muestran los resultados obtenidos.

Como resultado del uso de la metodología de las elipses, se identificaron **seis** activos de información vitales.

Luego se procedió a la Tasación de Activos, para poder identificar la protección apropiada a los mismos; es necesario tasar su valor en términos de la importancia a la gestión de accesos de usuarios, o dadas ciertas oportunidades determinar su valor potencial.

En el caso de los activos de información del proceso de “Asignación de privilegios”, se tasó su impacto en relación a su confidencialidad e integridad. Se manejó una escala cualitativa que variando entre: ALTO, MEDIANO y BAJO.

Una vez realizada la tasación se efectuó la Identificación de Amenazas, una amenaza tiene el potencial de causar incidentes indeseables, los cuales podrían resultar causando daño al sistema, la organización y sus activos.

El paso siguiente fue establecer la Posibilidad de Ocurrencia de Amenazas, no todas las amenazas tienen la misma posibilidad de ocurrencia. Hay algunas que su presencia es remota y otras su probabilidad de que ocurran podrían ser altas.

Continuando con la metodología, se procedió a la Identificación de Vulnerabilidades; las vulnerabilidades son debilidades asociadas con cada activo de información. Son condiciones que pueden permitir que las amenazas las exploten y causen daño.

Seguidamente se identificó, la Posible Explotación de Vulnerabilidades. Se evaluó la posible explotación de vulnerabilidades por cada amenaza.

El paso siguiente de la metodología es el de evaluar el riesgo. El riesgo se evalúa contemplando dos elementos básicos: Estimado del Valor de los Activos en Riesgo; este elemento es fundamental para evaluar el riesgo. Lo que se pretende es determinar el daño o perdida del código fuente que el riesgo pudiera causar.

Posibilidad de Ocurrencia del Riesgo. Se visualizó por cada activo sus impactos, amenazas y posibilidad de ocurrencia así como las vulnerabilidades y su posibilidad de ser explotadas, se determinó la posibilidad de ocurrencia del riesgo por cada activo de información.

Tabla 3. Realización del análisis y evaluación del riesgo.

Activos	Tasación				Amenazas	Posibilidad ocurrencia	Vulnerabilidad	Posible explotación de vulnerabilidad	Valor activo	Posible ocurrencia	Total
	Confidencialidad	Integridad	Disponibilidad	Total							
1) Datos del programador	A	A	A	A	- Plagio - Falsificación - Alteración - Privacidad	A A A A	- Deficiencia organizativa - Deficiencia envió - Acceso no autorizado - Control documentos	A A A A	A	A	A
2) Medios de comunicaci-ón	A	A	A	A	- Fallas de funcionamien to - Falta de seguridad - Falta de personal	B A A	- Energía Eléctrica - Mala configuración - Poca disponibilidad	B A A	A	A	A
3) Software de control de cambio	A	A	A	A	- Error de funcionamien to - Códigos maliciosos - Fallos técnicos - Errores de usuario - Falta de seguridad - Falta de mantenimient o	A B A M A A	- Mala instalación - Controles de acceso - Energía eléctrica - Mal entrenamiento - Falta de políticas - Falta de políticas	A B B M A A	A	A	A
4) Base de datos de usuario	A	A	A	A	- Plagio - Alteración - Privacidad	M M A	- Deficiencia organizativa - Acceso no autorizado - Falta de criptografía	A B A	A	M	A

Tabla 3. (Continuación)

5) Código fuente de desarrollo	A	A	A	A	- Plagio - Alteración - Privacidad - Códigos maliciosos	A A A B	- Deficiencia organizativa - Acceso no autorizado o mala practica - control de acceso Controles de acceso	A A A A	A	A	A
6) Niveles de acceso	A	A	A	A	- Alteración - Privacidad	A A	- Acceso no autorizado - Control de documentos	A A	A	A	A

Leyenda:

Alto..... A
Mediano..... M
Bajo..... B

Fuente: GARCÍA ACHILLO, Pedro, Sistema de Gestión de Seguridad de la Información, Caso de Estudio, Consultores en Informática Global SRL.

Finalmente se estableció el Valor del Riesgo de los Activos. Se concluyó siguiendo de manera sistemática la metodología para los activos de información: a) Seguridad de los recursos humanos, b) Gestión del acceso del usuario y c) Seguridad en los procesos de desarrollo y soporte. Fueron los activos de información considerados de riesgo y, por lo tanto, serían aquellos a los cuales habría que identificar del Anexo A sus respectivos controles.

- Identificación y evaluación del tratamiento de los riesgos. En la cláusula 4.2.1 (g) se plantea que se deben seleccionar objetivos de control y controles apropiados del anexo A del estándar NTC-ISO/IEC 27001:2005 y la selección se debe justificar sobre la base de las conclusiones de la evaluación del riesgo y tratamiento del riesgo.

En el caso del proceso de “Asignación de privilegios de acceso y control de versiones”, una vez efectuado el análisis y evaluación del riesgo, se decidió mitigar los riesgos encontrados en los activos de información: a) Seguridad de los recursos humanos, b) Gestión del acceso del usuario y c) Seguridad en los procesos de desarrollo y soporte. El criterio establecido para aplicar los controles apropiados del Anexo A á estos activos fue el resultado de ALTO RIESGO en la evaluación del riesgo realizada.

No se tiene riesgos residuales, los cuales son aceptables en la organización, en el proceso analizado de “Asignación de privilegios de acceso y control de versiones”, siendo este un proceso de alta vulnerabilidad.

- **Declaración de la Aplicabilidad**. En la cláusula 4.2.1 (h) de la norma NTC-ISO/IEC 27001:2005 se exige que se documente un “enunciado de aplicabilidad”. En la cláusula 4.3.1 (g) se hace mención también al enunciado de aplicabilidad, considerándolo un documento importante del SGSI. Un enunciado de aplicabilidad es:

- Un documento en el cual deben incluirse los objetivos de control y los controles seleccionados, así como las razones para su selección. También debe registrarse la exclusión de cualquier objetivo de control y controles enumerados en el Anexo A de la norma.

En la Tabla 4 se muestra a nivel de ilustración un enunciado de aplicabilidad como producto del análisis y evaluación del riesgo efectuado al proceso de “Asignación de privilegios de acceso y control de versiones”.

Como recomendación del **SGSI** analizada en esta monografía, para la División de Servicios de Información de la UIS, se sugiere en el **Anexo 8** un formato de “Declaración de Aplicabilidad”.

Tabla 4. Enunciado de Aplicabilidad.

Activo de Información	Objetivo de Control	Control	Justificación
Seguridad de los recursos humanos	A.6.1	A.6.1.1	Proporcionar direccionalidad en la seguridad de información
	A.6.1	A.6.1.3	Minimizar errores humano en la seguridad de información
	A.8.1	A.8.1.1	Ejecutar de manera eficiente los roles y responsabilidades de seguridad de los empleados.
	A.8.1	A.8.1.2	Verificar los antecedentes sobre todos los candidatos para empleados (programadores)
	A.8.1	A.8.1.3	Para aplicar los términos y condiciones de la contratación al trabajo.
	A.8.2	A.8.2.2	Formación para la toma de conciencia y la actualizaciones regulares en la políticas y procedimientos de la organización
	A.8.2	A.8.2.3	Para ejecutar un proceso disciplinario formal para los empleados que cometan un incumplimiento de seguridad
	A.8.2	A.8.3.3	Minimizar el riesgo de acceso por empleados que ya fueron retirados de la organización.
Gestión del acceso del usuario	A.11.1	A.11.1.1	Para establecer, documentar y revisar una policía de control de accesos
	A.11.1	A.11.2.1	Ejecutar un procedimiento formal para la inscripción y des-inscripción para otorgar acceso.
	A.11.1	A.11.2.2	Restringir y controlar la asignación y uso de los privilegios.

Tabla 4. (Continuación)

	A.11.1	A.11.2.3	Permitirá controlar a través de un proceso de gestión formal la asignación de claves.
	A.11.1	A.11.2.4	Revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.
Seguridad en los procesos de desarrollo y soporte	A.12.5	A.12.5.1	Mejorar el control mediante el uso de procedimientos formales de control de cambios
	A.12.5	A.12.5.2	Minimizar el impacto adverso en las operaciones o seguridad organizacional.
	A.12.5	A.12.5.3	Para verificar que las modificaciones a los paquetes de software se limitarán a los cambios necesarios y todos los cambios deben ser controlados estrictamente.
	A.12.5	A.12.5.4	Evitar las oportunidades de filtraciones en la información.
	A.12.5	A.12.5.5	Mejorar la supervisión y monitoreo de software que ha sido outsourced.

Fuente: GARCÍA ACHILLO, Pedro, Sistema de Gestión de Seguridad de la Información, Caso de Estudio, Consultores en Informática Global SRL.

- **Activos de información de la red de datos de la UIS.** A manera de información general, en la Tabla 4 se relacionan a continuación los activos más significativos de la DSI, enmarcados dentro del concepto genérico de activos de información. El Proceso Servicios Informáticos y de Telecomunicaciones de la UIS deberá realizar el estudio para la identificación definitiva de los activos de información a considerar dentro del SGSI.

Tabla 5. Inventario preliminar de activos de información de la red de datos UIS.

Categoría: Infraestructura Física								
Activo No.	**Descripción**	**Marca o Modelo**	**Serie No.**	**Valoraciòn (1-5)**	**Propietario**	**Localización**	**Fecha de Registro**	**Sub-Categoría ó Dimensión**
1	SERVIDOR DE APLICACIONES		Altix 350 System	3	ÁREA DE SOPORTE DE RED	CENTIC	01/10/2010	Tangible
2	SERVIDOR WEB INSTITUCIONAL		Altix 350 System	3	ÁREA DE SOPORTE DE RED	CENTIC	01/10/2010	Tangible
3	SERVIDOR DE CORREO ELECTRÓNICO			3	ÁREA DE SOPORTE DE RED	CENTIC	01/10/2010	Tangible
4	FIREWALL	CISCO	ASA 5520	3	ÁREA DE SOPORTE DE RED	CENTIC	01/10/2010	Tangible
6	SERVIDOR DE DESARROLLO			3	ÁREA DE DISEÑO Y DESARROLLO	DSI	01/10/2010	Tangible

7	SWITCHs	3Com	4500	3	ÁREA DE SOPORTE DE RED	CENTROS DE CABLEADOS	01/10/2010	Tangible
8	ENRUTADORES			3	ÁREA DE SOPORTE DE RED	CENTROS DE CABLEADOS	01/10/2010	Tangible
9	PCs DE ESCRITORIO			1	USUARIOS	OFICINAS	01/10/2010	Tangible
10	PCs PORTÁTILES			1	USUARIOS	OFICINAS	01/10/2010	Tangible
11	SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA			3	ÁREA DE SOPORTE DE RED	CENTROS DE CABLEADOS EDIFICIOS DEL CAMPUS	01/10/2010	Tangible
12	CENTROS DE DATOS			5	ÁREA DE SOPORTE DE RED	CENTIC	01/10/2010	Tangible
13	SOFTWARE DE APLICACIÓN DE SERVIDOR			1	ÁREA DE SOPORTE DE RED	CENTIC	01/10/2010	Tangible
14	SOFTWARE DE APLICACIÓN DE USUARIO FINAL			1	ÁREA DE SOPORTE DE RED	OFICINAS DE USUARIOS	01/10/2010	Tangible
15	HERRAMIENTAS DE DESARROLLO			3	ÁREA DE DISEÑO Y DESARROLLO	DSI	01/10/2010	Tangible
16	MEDIOS EXTRAÍBLES (CD, DVD, CINTAS, USB, DISCO DURO PORTÁTIL, ETC.)			1	USUARIOS	OFICINAS DE USUARIOS	01/10/2010	Tangible
17	SISTEMA CONTRAINCENDIO			3	DSI	CENTIC	01/10/2010	Tangible
18	SISTEMA DE AIRE ACONDICIONADO			3	DSI y CENTIC	DSI y CENTIC	01/10/2010	Tangible
19	MANEJADOR DE BD INFORMIX	DINAMIC SERVER V.10		3	ÁREA DE DISEÑO Y DESARROLLO	DSI y CENTIC	01/10/2010	Tangible

Categoría: SOF - Software									
Activo No.	**Descripción**	**Marca**	**Serie No.**	**Clave de Activación**	**Valoración (1-5)**	**Propietario**	**Localización**	**Fecha de Registro**	**Sub-Categoría ó Dimensión**
1	WEB PREMIUN CS4				1	LÍDER DE ÁREA DSI	CENTIC	13/10/2010	Intangible
2	COREL DRAW GRAPHICS SUITE X4				1	DSI	CENTIC	13/10/2010	Intangible
3	SOFTWARE DE SERVIDOR WEB JBOSS V.5				3	LÍDER DE ÁREA DSI	CENTIC	13/10/2010	Intangible
4	CAMPUS AGREEMENT				1	ÁREA DE SOPORTE DE RED	CENTIC	13/10/2010	Intangible
5	EPI CENTER 5.0 CLIENT				1	DSI	DSI	13/10/2010	Intangible
6	WEBSENSE				3	ÁREA DE SOPORTE DE RED	CENTIC	13/10/2010	Intangible
7	NETWORK DIRECTOR				1	ÁREA DE SOPORTE DE RED	DSI	13/10/2010	Intangible
8	CISCO ASDM LAUNCHER				1	ÁREA DE SOPORTE DE RED	DSI	13/10/2010	Intangible

Categoría: SER – Servicios - Infraestructura Básica								
Activo No.	**Descripción**	**Valoración (1-5)**	**Propietario (Coordinador)**	**Área**	**Contrato o Cliente No.**	**Fecha de vigencia**	**Teléfono No.**	**Sub-Categoría ó Dimensión**
1	CORREO ELECTRÓNICO	3	LIDER DE ÁREA DSI	MENSAJERÍA		12/10/2010	(000) 000-0000	SERVICIO DE TI
2	MENSAJERÍA INSTÁNTANEA	1	LIDER DE ÁREA DSI	MENSAJERÍA		12/10/2010		SERVICIO DE TI
3	SISTEMA DE NOMBRES DE DOMINIO	3	ÁREA DE SOPORTE DE RED	RED LAN/WAN		12/10/2010		SERVICIO DE TI
4	PROTOCOLO DE CONFIGURACIÓN DINÁMICA DE HOST	3	ÁREA DE SOPORTE DE RED	RED LAN/WAN		12/10/2010		SERVICIO DE TI
5	HERRAMIENTAS DE ADMINISTRACIÓN	3	ÁREA DE SOPORTE DE RED	RED LAN/WAN		12/10/2010		SERVICIO DE TI
6	USO COMPARTIDO DE ARCHIVOS	3	ÁREA DE SOPORTE DE RED	RED LAN/WAN		12/10/2010		SERVICIO DE TI
7	ALMACENAMIENTO DE DATOS	3	ÁREA DE BACKUP	DSI		12/10/2010		SERVICIO DE TI
8	ACCESO A RED PRIVADA VIRTUAL	3	ÁREA DE SOPORTE DE RED	RED LAN/WAN		12/10/2010		SERVICIO DE TI

Categoría: INF – Información - Datos de Intranet - Internet - Extranet - Mensajería							
Activo No.	**Descripción**	**Valoraciòn (1-5)**	**Propietario**	**Localización**	**Medio o Formato**	**Fecha de Creación**	**Sub-Categoría ó Dimensión**
1	CÓDIGO FUENTE	5	ÁREA DE DISEÑO Y DESARROLLO DE SOFTWARE	DSI	DIGITAL	05/10/2010	Tangible
2	DATOS RECURSOS HUMANOS	5	LÍDER DE ÁREA DSI	DSI	DIGITAL	05/10/2010	Tangible
3	DATOS FINANCIEROS	5	LÍDER DE ÁREA DSI	DSI	DIGITAL	05/10/2010	Tangible
4	DATOS DE PUBLICIDAD	5	LÍDER DE ÁREA DSI	DSI	DIGITAL	05/10/2010	Tangible
5	CONTRASEÑAS DE EMPLEADOS	5	LÍDER DE ÁREA DSI	DSI	DIGITAL	05/10/2010	Tangible
6	CLAVES DE CIFRADO PRIVADAS DE EMPLEADOS	5	LÍDER DE ÁREA DSI	DSI	DIGITAL	05/10/2010	Tangible
7	CLAVES DE CIFRADO DE SISTEMAS INFORMÁTICOS	5	LÍDER DE ÁREA DSI	DSI	DIGITAL	05/10/2010	Tangible
8	PROPIEDAD INTELECTUAL	5	DSI	DSI	DIGITAL	05/10/2010	Tangible
9	DATOS DE COMPRAS	5	LÍDER DE ÁREA FINANCIERA DSI	DSI	DIGITAL	05/10/2010	Tangible
10	DATOS DE CONTACTO PERSONALES DE EMPLEADOS	3	ÁREA DE SOPORTE DE RED	DSI	DIGITAL	05/10/2010	Tangible

11	DATOS DE CONTACTO DE PROVEEDORES	3	LÍDER DE ÁREA FINANCIERA DSI	DSI	DIGITAL	05/10/2010	Tangible
12	CLAVES DE CIFRADO DE PROVEEDORES	5	LÍDER DE ÁREA DSI	DSI	DIGITAL	05/10/2010	Tangible
13	IMAGEN INSTITUCIONAL	5	COMUNICACIONES		DIGITAL	05/10/2010	Intangible
14	DATOS DE CONTACTO PERSONALES DE EMPLEADOS	3	LÍDER DE ÁREA RECURSOS HUMANOS DSI	DSI	DIGITAL	05/10/2010	Tangible
15	PRODUCTIVIDAD DE EMPLEADOS	3	JEFE DSI	DSI	DIGITAL	05/10/2010	Intangible
16	MORAL DE EMPLEADOS	3	JEFE DSI	DSI	DIGITAL	05/10/2010	Intangible

10. CONCLUSIONES

Un SGSI es, en primera instancia, un sistema de gestión, es decir, una herramienta de la que dispone la Alta Dirección para administrar y controlar un determinado ámbito, en este caso, la seguridad de la información.

La gestión de las actividades de las organizaciones se realiza, cada vez con más frecuencia, según sistemas de gestión basados en estándares internacionales: se gestiona la calidad según ISO 9001, sistema ya certificado en la UIS, el impacto medio-ambiental según ISO 14001 o la prevención de riesgos laborales según OHSAS 18001, ambas en etapa de diagnóstico en la Universidad. Ahora, se propone añadir ISO 27001 como estándar de gestión de la seguridad de la información.

La Universidad Industrial de Santander tiene la posibilidad de implantar un número variable de estos sistemas de gestión para mejorar la organización y beneficios sin imponer una carga a la organización.

El último objetivo sería poder llegar a un único sistema de gestión que contemple todos los aspectos necesarios para la Institución, basándose en el ciclo PHVA de mejora continua común a todos estos estándares. Las facilidades para la integración de las normas ISO son evidentes al consultar de sus anexos.

NTC-ISO/IEC 27001:2005, detalla en su Anexo C, punto por punto, la correspondencia entre esta norma y la ISO 9001 e ISO 14001. Ahí se observa la alta correlación existente y se puede intuir la posibilidad de integrar el SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN al sistema de gestión ya existente en la UIS. Algunos puntos que constituyen una novedad en ISO 27001 frente a otros estándares, son la evaluación de riesgos y el establecimiento de una declaración de aplicabilidad (SOA), aunque ya se plantea incorporarlos al

resto de normas en un futuro. Es claro que al implementar un SGSI son muchos los beneficios que se reciben, entre los cuales podemos mencionar algunos:

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.

- Reducción del riesgo de pérdida, robo o corrupción de información.

- Los clientes tienen acceso a la información a través de políticas de seguridad.

- Los riesgos y sus controles son continuamente revisados.

- Confianza de clientes y socios estratégicos, por la garantía de conservar la calidad y confidencialidad de la información.

- Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.

- Continuidad de las operaciones necesarias de negocio tras incidentes graves de seguridad.

- Conformidad con la legislación vigente sobre información personal, propiedad intelectual, entre otras.

- Imagen institucional, como elemento diferenciador con la competencia.

- Reducción de costos y mejora de los procesos y servicios.

- Aumento de la seguridad en base a la gestión de procesos en lugar de la compra sistemática de productos y tecnologías.

BIBLIOGRAFIA

ALEXANDER, Alberto G. Diseño de un sistema de gestión de seguridad de información, Óptica ISO 27001:2005. Bogotá:Alfaomega, 2007.

CENTRO CRIPTOLÓGICO NACIONAL: EAR PILAR **/** Entorno de análisis de riesgos. [Madrid: ES, 2010] EAR/PILAR, 2010. (Citado: Octubre 15 de 2010) Disponible en Internet: http://www.ar-tools.com/index.html?tools/pilar/index.html

COMISIÓN INTERAMERICANA DE LAS TELECOMUNICACIONES – CITEL. Impactos de fraude para la prestación de los servicios de telecomunicaciones para usuarios, operadores y estados. [Documento ppt]. Conferencia presentada el 21-Jun-07 2007.

DALTABUIT GODAS, Enrique. La seguridad de la información. México: Limusa, 2007.

G.A., ALBERTO. Sistema de Seguridad de Información". Lima: Pontificia Universidad Católica del Perú, Centro de Negocios Centrum, 2005. Implantación del ISO 27001:2005.

HERVALEJO SANCHEZ, Alberto.Manual de introducción a las metodologías de seguridad informática: Proyecto final de carrera presentado en la Universidad Politécnica de Valencia. [online]. Scribd, 2010. [Valencia: ES, 2009] (citado: Octubre 1 de 2010) Disponible en Internet: http://www.scribd.com/doc/17740680/Auditorias-de-Seguridad-Informatica-y-la-OSSTMM

INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. Sistema de gestión de la seguridad de la información (SGSI). Bogotá: ICONTEC, 2010. [NTC-ISO/IEC 27001, 27002, 5411-1, GTC 169, GTC 176].

INSTITUTO NACIONAL DE TECNOLOGIA DE LA COMUNICACIÓN (INTECO). Sistema de Gestión de Seguridad de la información en una Organización: SGSI [ONLINE] [León, España] Inteco, 2010. [Citado: Octubre 15 de 2010] Disponible en Internet: http://cert.inteco.es/extfrontinteco/img/File/intecocert/sgsi/index.html

MINISTERIO DE ADMINISTRACIONES PÚBLICAS: I METODO. MAGERIT – versión 2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información [online]. Catálogo general de publicaciones oficiales. [Madrid: ES, 2006] Ministerio de Administraciones Públicas: Junio, 2006. Disponible en Internet: http://www.csi.map.es/csi/pg5m20.htm

PARRA CORREA, Carlos Alberto. Propuesta de diseño de un modelo de seguridad informática para la red de datos institucional de la Universidad Industrial de Santander. Bucaramanga, 2006. 274p. Trabajo de Grado (Magister en Informática). Universidad Industrial de Santander, Facultad de Ingenierías Físico-Mecánicas, Escuela de Ingeniería de Sistemas.

PIATTINI VELTHUIS, Mario; DEL PESO NAVARRO, Emilio y DEL PESO RUIZ, Mar. Auditoría de tecnologías y sistemas de información. México: ALFAOMEGA/RAMA, 2008.

SHELDON, Tom. Manual de Seguridad de Windows. NT. 1ed. Madrid: McGraw-Hill, 1997.

SLATER, Derek. CSO SECURITY AND RISK. CSO MAGAZINE [ONLINE] Estado del Arte del CSO 2010: el progreso y el peligro. [Northbrook, IL, E.U] CSO SECURITY AND RISK, Julio, 2010. [citado: Octubre 15 de 2010] Disponible en Internet: http://cxo-community.com/articulos/estadisticas/79-management/3183-estado-del-arte-del-cso-2010-el-progreso-y-el-peligro.html

ANEXOS

DOCUMENTACIÓN PRELIMINAR PROPUESTA PARA LA IMPLEMENTACIÓN DEL SUBPROCESO SGSI

ANEXO 1

PROCEDIMIENTO ACCIONES PREVENTIVAS/CORRECTIVAS

(Actual del SGC modificado)

Universidad Industrial de Santander	**PROCESO SEGUIMIENTO INSTITUCIONAL**	**Código : PSE.02**
	PROCEDIMIENTO ACCIONES PREVENTIVAS/CORRECTIVAS	**Versión : 05** Página 1 de 5
Revisó: Director de Control Interno y Evaluación de Gestión Vicerrector Administrativo	Aprobó: Vicerrector Académico	Fecha de aprobación: Noviembre 19 de 2007 Resolución N° 1736

OBJETIVO	ALCANCE
Establecer el procedimiento para identificar, analizar y eliminar las causas de los problemas potenciales/reales con el fin de tomar las acciones preventivas/correctivas apropiadas para prevenir/evitar su ocurrencia.	Este procedimiento aplica para todas aquellas acciones preventivas/ correctivas que se generen en los Procesos del Sistema de Gestión de la Calidad de la Universidad Industrial de Santander.

NORMATIVIDAD

- **Norma Técnica GP 1000:2004.**
- **Norma Técnica Colombiana ISO 9001:2008**
- **Norma Técnica Colombiana ISO 17025:2005**
- **Norma Técnica Colombiana ISO/IEC 27001:2005}** → **CAMBIOS PROPUESTOS**
- **Norma Técnica Colombiana ISO/IEC 27002:2005}**

DEFINICIONES Y/O ABREVIATURAS

- **Acción Preventiva:** Acción emprendida para eliminar la causa de una no conformidad potencial u otra situación indeseable y evitar que suceda una no conformidad.
- **Acción Correctiva:** Acción tomada para eliminar la causa de una no conformidad detectada u otra situación indeseable.
- **No conformidad**: El no cumplimiento de un requisito especificado a la cual se debe dar tratamiento.
- **Incidente de Seguridad de la Información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados (INCLUIR)**

CONSIDERACIONES

Las Acciones de Mejora que se generen por iniciativa del personal interno o externo a los procesos y las observaciones de las auditorías internas de calidad que apunten a la optimización del proceso, se registran en el formato FSE.11 Acciones de Mejora.

Este procedimiento aplica al subproceso Gestión de Seguridad de la Información. (INCLUIR).

Este procedimiento aplica a los Laboratorios Acreditados, Certificados o en proceso de Acreditación, objeto de Auditoría por parte de Seguimiento Institucional. Para los efectos, el líder del proceso corresponde al Director de Laboratorio.

Inicio/Fin | Actividad | Decisión | Documento | Procesamiento en S.F. o intranet | Procedimiento predefinido | Conector | Conector de página

DIAGRAMA DE FLUJO	DESCRIPCIÓN	RESPONSABLE	DOCUMENTOS DE REFERENCIA
INICIO			
1. Identifica la no conformidad.	CAMBIO PROPUESTO 1. Identifica la no conformidad potencial/real con base en la información suministrada por el Sistema de Gestión de la Calidad **y el SGSI**: - Hallazgos de Auditorías Internas de Calidad. - Revisión por la Dirección. - Preguntas, Quejas, Reclamos de los beneficiarios. - Análisis de indicadores. - Evaluación de Satisfacción del beneficiario. - Incidentes de seguridad de la información - Productos No Conformes. - Otras fuentes de información.	Líder del Proceso y/o el personal involucrado. Equipo Auditor.	-FSE.04 Informe de Auditoría Interna de Calidad. - FSE.06 Recepción de Quejas y Reclamos. Link Quejas, Reclamos, Sugerencias -FSE.10 Informe de Desempeño de los Procesos
2. Describe la no conformidad encontrada.	2. Describe la no conformidad encontrada, en el *formato* FSE.07 Acciones Correctivas/ Preventivas/.	Líder del Proceso y/o Grupo Primario	FSE.07 Acciones Correctivas/ Preventivas.
1 → 3. Determina las causas para la no conformidad encontrada.	3. Determina las causas que originan la no conformidad potencial/real, para lo cual se realiza "El análisis de causas".	Líder del Proceso, Grupo Primario y/o el personal involucrado.	FSE.07 Acciones Correctivas/ Preventivas.
4. Establece el Plan de Acción.	4. Establece el Plan de Acción teniendo en cuenta: - Actividades necesarias para prevenir/evitar nuevamente la ocurrencia de la no conformidad potencial/real. - Responsable de la ejecución. - Fecha límite de cada actividad. **Nota 1**: Si la Acción Correctiva es producto de Auditoría, el plan de acción debe comunicarse a la Coordinación de **Nota 2**: Para el caso de los Laboratorios, no aplica esta	Líder del Proceso y/o Grupo Primario	FSE.07 Acciones Correctivas/ Preventivas.
1			

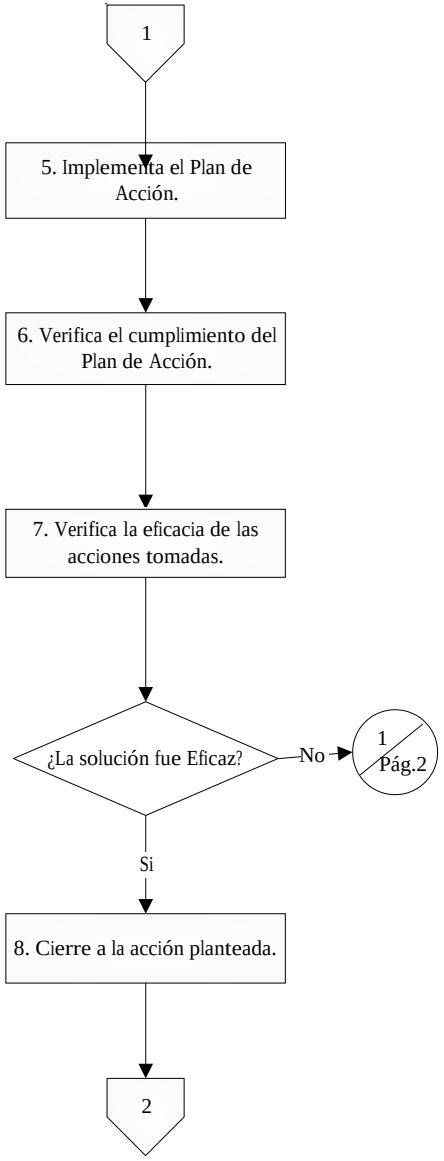
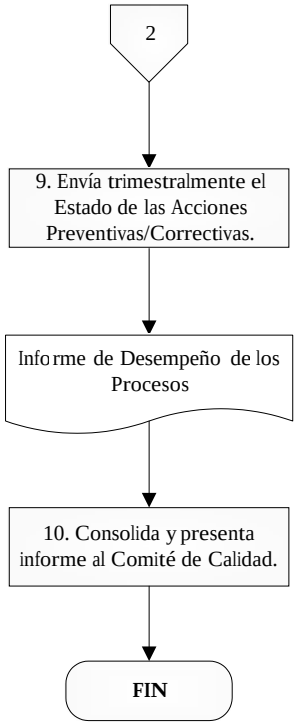
DIAGRAMA DE FLUJO	DESCRIPCIÓN	RESPONSABLE	DOCUMENTOS DE REFERENCIA
	5. Implementa el Plan de Acción.	Funcionario designado	FSE.07 Acciones Correctivas/ Preventivas.
	6. Verifica el cumplimiento del Plan de Acción.	Líder del Proceso	FSE.07 Acciones Correctivas/ Preventivas.
	7. Verifica si las acciones tomadas son eficaces. Si se detecta que las actividades realizadas no son eficaces, vuelve al numeral 3. **Nota:** Si las acciones correctivas fueron resultado de auditoría de calidad, el responsable de verificar la eficacia es el equipo auditor quienes adicionalmente diligenciarán el formato FSE.17, para el respectivo control.	Líder del Proceso Equipo Auditor	FSE.07 Acciones Correctivas/ Preventivas. FSE.17 Cronograma de Seguimiento de Acciones Correctivas de Auditoría
	8. Realiza cierre de la acción planteada. **Nota 1:** Si las acciones correctivas fueron resultado de auditoría interna de calidad, el responsable de cerrarla es el Líder del proceso Seguimiento Institucional. **Nota 2:** Para el caso de los Laboratorios, el responsable de cerrar las Acciones es el Auditor Líder que realizó la auditoría.	- Líder del Proceso - Líder del Proceso Seguimiento Institucional	FSE.07 Acciones Correctivas/ Preventivas.

DIAGRAMA DE FLUJO	DESCRIPCIÓN	RESPONSABLE	DOCUMENTOS DE REFERENCIA
	9. Envía trimestralmente el Estado de las Acciones Preventivas/Correctivas a la Dirección de Control Interno y Evaluación de Gestión. **Nota:** Ésta actividad no aplica a los Laboratorios. 10. Consolida y presenta resultados del Estado de las Acciones Preventivas/Correctivas al Comité de Calidad. **Nota 1:** Los Laboratorios presentan directamente estos resultados a la Alta Dirección. **Nota 2: Las Acciones de Mejora** que se generen por iniciativa del personal interno o externo y las observaciones de las auditorías de calidad que apunten a la optimización del proceso, se registran en el formato FSE.11 Acciones de Mejora.	Líder del Proceso Líder del Proceso Seguimiento Institucional	FSE.10 Informe de Desempeño de los Procesos. FSE.11 Acciones de Mejora.

CONTROL DE CAMBIOS

VERSIÓN	FECHA DE APROBACIÓN	DESCRIPCIÓN DE CAMBIOS REALIZADOS
01	Noviembre 19 de 2007	Creación del Documento
02	Octubre 03 de 2008	Cambio de la Norma NTC ISO 9001:2000 a la NTC GP1000:2004 y ampliación del alcance a todos los procesos del Sistema de Gestión de la Calidad de la Universidad Industrial de Santander
03	Marzo 11 de 2009	Inclusión del formato FSE.17 Cronograma de Seguimiento de Acciones Correctivas de Auditoría como documento de referencia.
04	Abril 15 de 2009	Eliminación del formato FSE.10 del diagrama de flujo e inclusión del documento Informe de desempeño como resultado de la actividad N° 9.
05	Abril 22 de 2010	Inclusión de la Norma Técnica Colombiana ISO 9001:2008. Inclusión de la Norma Técnica Colombiana ISO 17025:2005. **Inclusión de la Norma Técnica Colombiana ISO 27001:2005**. (INCLUIR) Inclusión en las consideraciones referente a Laboratorios Acreditados, Certificados o en proceso de Acreditación. Inclusión del formato FSE.10 como documento de referencia de la Actividad No. 1. En la Actividad No. 4 inclusión de la Nota 1 y la Nota 2 En la Actividad No. 8 inclusión de la Nota 2 referente a responsable de cierre de AC en los Laboratorios. En la Actividad No. 9 inclusión de la Nota referente a la no aplicación de la actividad para los Laboratorios. En la Actividad No. 10 inclusión de Nota 1 referente a Laboratorios.

ANEXO 2

PROCEDIMIENTO DE REPORTE DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN (Propuesto)

OBJETIVO	ALCANCE
Reglamentar el procedimiento de reportes de incidentes de seguridad de la información de la Universidad.	Aplica desde que se genere el incidente hasta que se toman las acciones correctivas correspondientes por parte de la DSI

NORMATIVIDAD

Norma NTC ISO/IEC 27001:2005
Norma NCT ISO/IEC 27002:2005

DEFINICIONES Y/O ABREVIATURAS

Incidente de seguridad. Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de la Universidad y amenazar la seguridad de la información.

Evento de seguridad: Presencia de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Seguridad de la información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (*Accountability*), no repudio y fiabilidad.

Riesgo: Combinación de la probabilidad de un evento y sus consecuencias.

Acción correctiva: Acción tomada para eliminar la causa de una no conformidad detectada u otra situación no deseable

Usuario: Es la persona que tiene alguna vinculación con la Universidad y utiliza los recursos o servicios informáticos ofrecidos por la misma.

CONSIDERACIONES

Para prestar el servicio de soporte técnico es necesario que el equipo este dentro del inventario de la Universidad.

Es deber de los técnicos estar en permanente capacitación con respecto a nuevas tecnologías informáticas que puedan mejorar su desempeño y así prestar un mejor servicio.

Cuando se preste el servicio de soporte técnico se debe velar por preservar la información de los usuarios y en caso que se requiera modificar debe ser con previa autorización por parte del usuario.

Para la prestación del servicio, el usuario debe estar presente.

Cuando se trata de soporte de hardware el equipo debe ser de marca Dell.

Inicio/Fin	Actividad	Decisión	Documento	Procesamiento en S.F. o intranet	Procedimiento predefinido	Conector	Conector de página

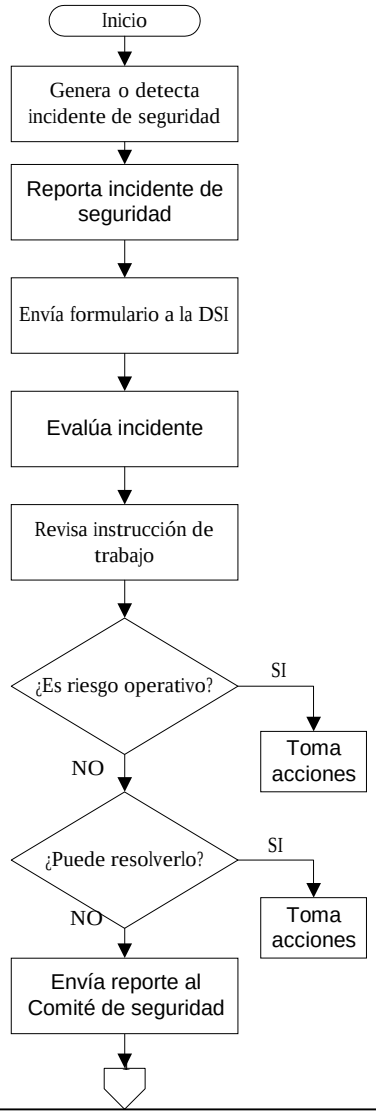
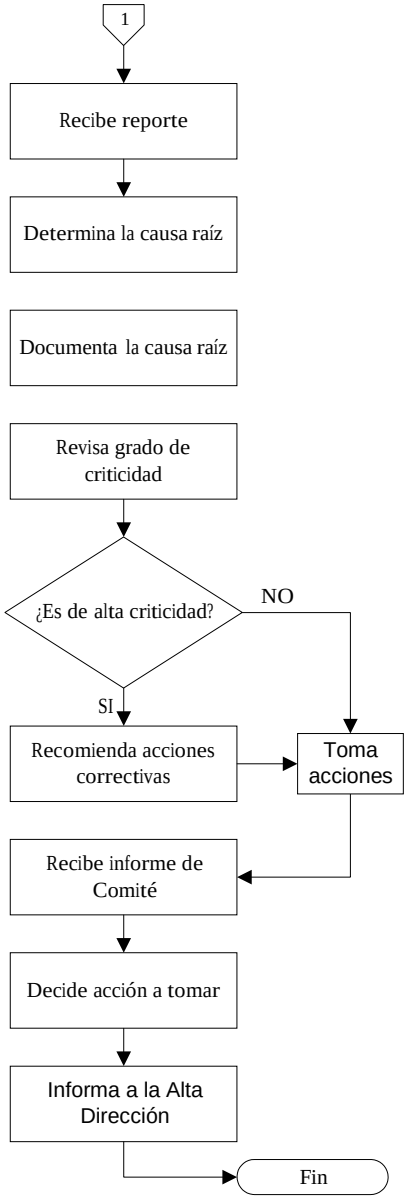
DIAGRAMA DE FLUJO	DESCRIPCIÓN	RESPONSABLE	DOCUMENTOS DE REFERENCIA
	1. Genera o detecta incidente de seguridad de la información	Usuario.	
	2. Reporta incidente de seguridad llenando el Formato FSI.XX.	Usuario.	Reporte de Incidentes de Seguridad de la Información, Formato FSI.XX
	3. Envía el Formato FSI.XX. a la División de Servicios de Información.	Usuario.	
	4. Evalúa incidente de seguridad reportado.	Coordinador de Seguridad de la Información.	
	5. Revisa instrucción de trabajo sobre naturaleza de riesgos.	Coordinador de Seguridad de la Información.	Instrucción de Trabajo sobre Naturaleza de Riesgos, Instrucción ISI.XX
	5.1 Si es riesgo operativo toma acciones pertinentes.	Coordinador de Seguridad de la Información.	
	5.2. Si no es riesgo operativo: 5.2.1. Si puede resolverlo toma acciones y completa el Formato FSI.XX. 5.2.2. Si no puede resolverlo, envía reporte al Comité de Seguridad.	Coordinador de Seguridad de la Información.	Reporte de Incidentes de Seguridad de la Información, Formato FSI.XX

DIAGRAMA DE FLUJO	DESCRIPCIÓN	RESPONSABLE	DOCUMENTOS DE REFERENCIA
	6. Recibe el reporte de incidentes de seguridad de la información. 7. Determina la causa raíz del incidente de seguridad de la información. 8. Documenta la causa raíz en el reporte de incidentes de seguridad de la información. 9. Revisa grado de criticidad en las instrucciones de trabajo ISI.XX 10. Averigua si es de alta criticidad. 10.1. Si No es de alta criticidad toma acciones pertinentes. 10.2. Si es de alta criticidad recomienda acciones correctivas e informa al Jefe de la DSI. 11. Recibe informe del Comité de Seguridad de la Información. 12. Decide la acción a tomar. 13. Informa a la Alta Dirección de la Universidad. 14. Fin.	Comité de Seguridad de la Información. Comité de Seguridad de la Información. Comité de Seguridad de la Información. Comité de Seguridad de la Información. Comité de Seguridad de la Información. Comité de Seguridad de la Información. Jefe DSI Jefe DSI Jefe dSI	Instrucción de Trabajo sobre Grado de Criticidad, Instrucción ISI.XX

CONTROL DE CAMBIOS

VERSIÓN	FECHA DE APROBACIÓN	DESCRIPCIÓN DE CAMBIOS REALIZADOS

ANEXO 3

GUÍA NIVELES DE CLASIFICACIÓN DE LA INFORMACIÓN

(Propuesta)

DEFINICIONES

Cuatro Niveles de Clasificación de la Información	
Secreta **(Altamente Restringida)**	Esta clasificación es asignada a la información más sensible, destinada estrictamente para uso interno. La divulgación no autorizada de información de este tipo podría seria y desfavorablemente impactar la organización, sus accionistas, socios o clientes.
Confidencial	Esta clasificación es asignada a la información menos sensible, sin embargo es destinada sólo para uso interno. La divulgación no autorizada de este tipo de información podría afectar desfavorablemente la organización, sus accionistas, socios o clientes.
Privada	Esta clasificación es reservada para la información utilizada dentro de la organización, y cuya divulgación no autorizada podría afectar seria y desfavorablemente la organización y sus empleados.
Sin Clasificar	Esta clasificación cubre la información que no se adapta claramente a cualquier otra clasificación. A pesar de que la divulgación no autorizada de este tipo de información va en contra de la política, tal vez no afecte seria o desfavorablemente la organización, sus accionistas, socios o clientes.
Tres Niveles de Clasificación de la Información	
Confidencial	Información menos sensible, sin embargo, es para uso interno esa clasificación. Su divulgación no autorizada podría tener repercusiones desfavorables para la organización, sus accionistas, socios o clientes.
Sólo para uso interno	La información en esta categoría solo se revelará a terceros que hayan firmado un acuerdo de confidencialidad. Su divulgación no debe causar un perjuicio grave a la organización. La información está disponible para todos los empleados a través de la Intranet de la organización. Esta clasificación se aplica a toda la información no clasificada de forma predeterminada, e incluye las guías telefónicas, documentos de formación, plantillas y horarios.
Pública	Información de Ventas o Departamentos de Relaciones Públicas, aceptada de forma explícita para su distribución pública, tales como las ventas de los folletos y comunicados de prensa.

NIVELES DE CLASIFICACIÓN

Procesamiento Requerido		Cuatro Niveles de Clasificación				Tres Niveles de Clasificación		
Procesamiento	**Medidas de Seguridad**	**Secreto**	**Confidencial**	**Privado**	**Sin Clasificar**	**Confidencial**	**Uso Interno**	**Pública**
Soportes de Almacenamiento	Cifrado o Controles de Acceso Tangibles	X	X	X		X	X	
	Cifrado (opcional)				X			
	No se recomienda Cifrado							X
Copia	Se recomienda obtener el consentimiento de los propietarios	X	X	X		X		
	Sin restricción				X		X	X
Fax	Dispositivos de recepción protegidos por contraseña o el destinatario presente en la recepción	X	X	X		X		
	Sin restricción				X		X	X
Transmisión a través de Redes Públicas	Cifrado	X	X	X		X		
	Cifrado (opcional)				X		X	
	No se recomienda Cifrado							X
Destrucción	Destrucción o eliminación en un lugar seguro para este propósito	X	X	X		X		
	Papelera				X		X	X
Divulgación a Terceros	Consentimiento del Propietario y Acuerdo de Confidencialidad	X	X	X		X		
	Acuerdo de Confidencialidad				X		X	

	Sin restricciones							X
Etiquetado de los Medios Electrónicos cuando sea necesario	Etiquetado Interno y Externo	X	X	X		X		
	Fecha de divulgación y clasificación							X
	No Requiere Etiquetado				X		X	
Documento Etiquetado cuando sea necesario	En cada página (si no está vinculada) y en la parte delantera y trasera y portadas de documentos encuadernados	X	X	X		X		
	Fecha de divulgación y clasificación							X
	No Requiere Etiquetado				X		X	
Envío de correo interno y externo	Dirigido a un destinatario específico y colocado dentro de dos sobres, con la etiqueta de clasificación en el sobre interno únicamente.	X	X	X		X		
	Un solo sobre sin ningún tipo específico de etiquetado				X		X	X
La concesión de derechos de acceso	Propietario único del activo	X	X	X		X		
	Gerente local				X		X	
	Sin restricciones							X
Pista de Auditoría	Destinatario, número de copias que se hagan, ubicación, dirección, destrucción, testigos.	X						
	Sólo es necesario si es privado		X	X		X		
	No se recomienda				X		X	X

CONTROL DE CAMBIOS		
VERSIÓN	FECHA DE APROBACIÓN	DESCRIPCIÓN DE CAMBIOS REALIZADOS

ANEXO 4

FORMATO DE INVENTARIO DE ACTIVOS DE INFORMACIÓN (Propuesto)

Universidad Industrial de Santander	**PROCESO SERVICIOS INFORMÁTICOS Y DE TELECOMUNICACIONES** **SUBPROCESO GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	**Código : PSI.XX**
		Versión : XX
	FORMATO DE INVENTARIO DE ACTIVOS DE INFORMACIÓN	Página I de X

Categoría: HAR – Computadores (Computer Hardware)

Activo No.	Descripción	Marca o Modelo	Serie No.	Valoraciòn	Propietario	Localización	Fecha de Registro	Sub-categoría ó Dimensión
							yyyy-mm-dd	

Confidencial		
Creado en: yyyy-mm-dd	Modificado en: yyyy-mm-dd	Revisado en: yyyy-mm-dd

Categoría: SOF - Software

Activo No.	Descripción	Marca	Serie No.	Clave de Activación	Valoración	Propietario	Localización	Fecha de Registro	Sub-categoría ó Dimensión
								yyyy-mm-dd	

Confidencial		
Creado en: yyyy-mm-dd	Modificado en: yyyy-mm-dd	Revisado en: yyyy-mm-dd

Categoría: SER – Servicios

Activo No.	Descripción	Valoración	Propietario (Coordinador)	Área	Contrato o Cliente No.	Fecha de vigencia	Teléfono No.	Sub-categoría ó Dimensión
						yyyy-mm-dd	(000) 000-0000	

Confidencial		
Creado en: yyyy-mm-dd	Modificado en: yyyy-mm-dd	Revisado en: yyyy-mm-dd

	PROCESO SERVICIOS INFORMÁTICOS Y DE TELECOMUNICACIONES SUBPROCESO GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Código : PSI.XX
Universidad Industrial de Santander	FORMATO DE INVENTARIO DE ACTIVOS DE INFORMACIÓN	Versión : XX
		Página 1 de 1

Categoría: PER – Personal

ID Personal No.	Nombre	Función	Sitio de Trabajo	Área	Teléfono No.	Sub-categoría ó Dimensión
					(000) 000-0000 / EXT 0000	

Confidencial		
Creado en: yyyy-mm-dd	Modificado en: yyyy-mm-dd	Revisado en: yyyy-mm-dd

Categoría: BUI – Edificios y Equipos

Activo No.	Descripción	Valoración	Propietario (Coordinador)	Localización	Sub-categoría ó Dimensión

Confidencial		
Creado en: yyyy-mm-dd	Modificado en: yyyy-mm-dd	Revisado en: yyyy-mm-dd

Universidad Industrial de Santander	**PROCESO SERVICIOS INFORMÁTICOS Y DE TELECOMUNICACIONES** **SUBPROCESO GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	**Código : PSI.XX**
		Versión : XX
	FORMATO DE INVENTARIO DE ACTIVOS DE INFORMACIÓN	Página 1 de X

Categoría: DOC - Documento (Electrónico o Papel)

Activo No.	Descripción	Valoración	Propietario (Coordinador)	Sub-categoría (Electrónico o Papel)

Confidencial		
Creado en: yyyy-mm-dd	Modificado en: yyyy-mm-dd	Revisado en: yyyy-mm-dd

ANEXO 5

FORMATO DE REPORTE DE

INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

(Propuesto)

Universidad Industrial de Santander	**PROCESO SERVICIOS INFORMÁTICOS Y DE TELECOMUNICACIONES** **SUBPROCESO GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	**Código: FSI.XX**
	FORMATO DE REPORTE DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	**Versión: XX**

Emisión:			Generado por:	Aprobado por:
Día	Mes	Año		

I. DETECCIÓN DE INCIDENTES

Nombre del Usuario que informa:			Área involucrada:
Día	Mes	Año	

Tipo de incidentes:

☐ Personas	☐ Actos internos
☐ Procesos	☐ Prácticas laborales
☐ Sistemas	☐ Clientes
☐ Eventos externos	☐ Daños a activos
☐ Aspectos legales	☐ Incumplimiento de normas

II. COODINADOR DE SEGURIDAD DE LA INFORMACIÓN

1. Nombre del Coordinador: _____

2. Fecha de recepción: _____

3. ¿Se trata de riesgo operativo? ☐ Sí ☐ No
4. Describir la acción tomada si fue riesgo operativo:
5. Si no es riesgo operativo, ¿puede tomar acciones correctivas? ☐ Sí ☐ No
III. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN
7. Revisa instrucción de trabajo y determina criticidad del riesgo. ¿Criticidad alta? ☐ Sí ☐ No 8. Definición de acciones correctivas para mitigar riesgo de criticidad no alta: 9. Recomendación de acciones para mitigar riesgo de criticidad alta:

IV. JEFE DIVISIÓN DE SERVICIOS DE INFORMACIÓN
10. Descripción de acciones a tomar:

CONTROL DE CAMBIOS		
VERSIÓN	FECHA DE APROBACIÓN	DESCRIPCIÓN DE CAMBIOS REALIZADOS

ANEXO 6

MODELO DE POLÍTICA INSTITUCIONAL PARA LA SEGURIDAD DE LA INFORMACIÓN

(Propuesta)

MODELO DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LA UIS

- El propósito de la política es proteger los activos de información de la organización de todas las amenazas tanto internas como externas, deliberadas o accidentales (4.2.1., 1)).
- La alta dirección deberá autorizar la política de seguridad de la información (4.2.1., 5)).
- La política deberá asegurar que:

- La información debe ser protegida contra cualquier acceso no autorizado
- La confidencialidad de la información deberá de ser asegurada
- La integridad de la información deberá de ser mantenida
- La disponibilidad de la información deberá de ser garantizada
- Los requerimientos regulatorios y legislativos deberán ser satisfechos (4.2.1, 2))
- BCP[16] y DRP[17] deberán ser establecidos, probados, mantenidos y actualizados
- La capacitación y entrenamiento sobre seguridad de la información deberá estar disponible a todos los miembros de la organización
- Todas las brechas de seguridad de la información, ya sean reales o sospechosas, deberán ser reportadas e investigadas por el CISO

- Estándares deberán ser implementados para soportar la política. Estos deben contener control de virus, contraseñas y encripción (4.2.1, 4))
- Requerimientos del negocio respecto a la disponibilidad de la información y sistemas de información deben ser satisfechos
- La función y responsabilidad para la gestión de la seguridad de la información referida al CISO deberá ser definida por:

- Comité de seguridad de la información
- Dirección de seguridad de la información (CIO)
- Dirección de TI

- El CISO es directamente responsable del mantenimiento y actualización de la política, de su difusión y guías sobre su implementación (4.2.1, 3))
- Todos los Directores son directamente responsables de la implementación de la política en sus áreas de negocio, y del apoyo por parte de su grupo de trabajo
- Es responsabilidad de cada empleado el apoyo a la política

Objetivo.

El objetivo de la seguridad de la información es asegurar la continuidad del negocio y minimizar los daños al mismo previniendo y minimizando el impacto de incidentes de seguridad.

Notas:

Esta política de seguridad de la información deberá ser elaborada y actualizada según los requerimientos del negocio y seguridad de la información e infraestructura.

Esta política de seguridad de la información debe ser revisada en intervalos planeados o si suceden cambios significativos para asegurar su continuidad, adecuación y efectividad.

Las actividades de seguridad de la información deben ser coordinadas por diferentes partes representativas de la organización con roles relevantes.

Todas las responsabilidades de seguridad de la información deberán ser claramente definidas.

Aprobó: _____

Cargo : _____

Fecha: _____

[16] BCP: Business Continuity Planning
[17] DRP: Disaster Recovery Planning

ANEXO 7

FORMATO DE ASIGNACIÓN DE FUNCIONES Y RESPONSABILIDADES SOBRE ACTIVOS

(Propuesto)

Universidad Industrial de Santander	**PROCESO SERVICIOS INFORMÁTICOS Y DE TELECOMUNICACIONES** **SUBPROCESO GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	**Código : GSI.XX**
	FORMATO DE ASIGNACIÓN DE FUNCIONES Y RESPONSABILIDADES SOBRE ACTIVOS	**Versión : XX**
		Página 1 de X

DESCRIPCIÓN DE RESPONSABILIDADES Y ACTIVOS

ADMINISTRADOR / PROPIETARIO	
Nombre	
Supervisor	
Área o Proceso	
Cargo	
Descripción de las responsabilidades	

Activo No.	Descripción	Clasificación

DESCRIPCIÓN DE RESPONSABILIDADES Y ACTIVOS					
USUARIO					
Nombre					
Supervisor					
Dependencia					
Cargo					
Descripción de Responsabilidades:					
Activo No.	**Descripción**	**Clasificación**	**Procesamiento Autorizado**	**Acceso Autorizado**	**Acceso Retirado**
				yyyy-mm-dd	yyyy-mm-dd

CONTROL DE CAMBIOS		
VERSIÓN	FECHA DE APROBACIÓN	DESCRIPCIÓN DE CAMBIOS REALIZADOS

ANEXO 8

MODELO DE DECLARACIÓN DE APLICABILIDAD

(Propuesto)

Statement of Applicability

Current as of:

Legend (for Selected Controls and Reasons for controls selection)

2007 September 20

LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO 27001:2005 Controls			Current Controls	Remarks (Justification for exclusion)	Selected Controls and Reasons for selection				Remarks (Overview of implementation)
					LR	CO	BR/BP	RRA	
Clause	**Sec**	**Control Objective/Control**							
Security Policy	5,1	Information Security Policy							
	5.1.1	Information Security Policy Document					□		
	5.1.2	Review of Information Security Policy					□		
Organization of Information security	6,1	Internal Organization							
	6.1.1	Management Commitment to information security	□						
	6.1.2	Information security Co-ordination	□						
	6.1.3	Allocation of information security Responsibilities					□		
	6.1.4	Authorization process for Information Processing facilities	□				□		
	6.1.5	Confidentiality agreements	□			□	□		
	6.1.6	Contact with authorities	□				□		

	6.1.7	Contact with special interest groups					□		
	6.1.8	Independent review of information security					□		
	6,2	External Parties							
	6.2.1	Identification of risk related to external parties	□				□		
	6.2.2	Addressing security when dealing with customers	□				□		
	6.2.3	Addressing security in third party agreements	□				□	□	
Asset Management	7,1	Responsibility for Assets							
	7.1.1	Inventory of assets	□				□		
	7.1.2	Ownership of Assets	□						
	7.1.3	Acceptable use of assets	□				□		
	7,2	Information classification							
	7.2.1	Classification Guidelines					□	□	
	7.2.2	Information Labeling and Handling					□	□	

Human Resource Security	8,1	Prior to Employment							
	8.1.1	Roles and Responsibilities	□						
	8.1.2	Screening	□						
	8.1.3	Terms and conditions of employment	□					□	
	8,2	During Employment							
	8.2.1	Management Responsibility	□						
	8.2.2	Information security awareness, education and training	□			□	□	□	
	8.2.3	Disciplinary process	□						
	8,3	Termination or change of employment							
	8.3.1	Termination responsibility	□				□		
	8.3.2	Return of assets	□						
	8.3.3	Removal of access rights	□			□	□		
Physical and Environmental Security	9,1	Secure Areas							
	9.1.1	Physical security Perimeter	■	Existing controls		■			
	9.1.2	Physical entry controls	■	Existing controls		■	■	■	Implement swipe card on all data centers and established visitor control logs
	9.1.3	Securing offices, rooms and facilities	■	Existing controls				■	

	9.1.4	Protecting against external and environmental threats	■	Existing controls					
	9.1.5	Working in secure areas	■	Existing controls			■		Policy created
	9.1.6	Public access, delivery and loading areas	■	Existing controls					
	9,2	Equipment security							
	9.2.1	Equipment sitting and protection	■	Existing controls		■		■	
	9.2.2	Support utilities	■	Existing controls		□		■	
	9.2.3	Cabling security	■	Existing controls		■			
	9.2.4	Equipment Maintenance	■	Existing controls		■	■	■	Formalized PM mechanism
	9.2.5	Security of equipment off-premises	■	Existing controls					
	9.2.6	Secure disposal or reuse of equipment					■		Implemented procedure
	9.2.7	Removal of Property	■	Existing controls. Use of gate pass.					
Communications and Operations Management	10,1	Operational Procedures and responsibilities							
	10.1.1	Documented operating Procedures					□	□	
	10.1.2	Change Management	□				□		
	10.1.3	Segregation of Duties	□						
	10.1.4	Separation of development and Operations facilities	□						

	10,2	Third Party Service Delivery Management							
	10.2.1	Service Delivery	□					□	
	10.2.2	Monitoring and review of third party services	□					□	
	10.2.3	Manage changes to the third party services	□					□	
	10,3	System Planning and Acceptance							
	10.3.1	Capacity management					□		
	10.3.2	System acceptance					□		
	10,4	Protection against Malicious and Mobile Code							
	10.4.1	Controls against malicious code	□					□	
	10.4.2	Controls against Mobile code	□						
	10,5	Back-Up							
	10.5.1	Information Backup	□				□	□	
	10,6	Network Security Management							
	10.6.1	Network controls	□				□		
	10.6.2	Security of Network services	□				□		
	10,7	Media Handling							
	10.7.1	Management of removable media					□		

	10.7.2	Disposal of Media					□		
	10.7.3	Information handling procedures					□		
	10.7.4	Security of system documentation					□		
	10,8	Exchange of Information							
	10.8.1	Information exchange policies and procedures	□						
	10.8.2	Exchange agreements	□						
	10.8.3	Physical media in transit	□				□		
	10.8.4	Electronic Messaging	□				□		
	10.8.5	Business Information systems	□				□		
	10,9	Electronic Commerce Services							
	10.9.1	Electronic Commerce							
	10.9.2	On-Line transactions							
	10.9.3	Publicly available information	□				□		
	10,10	Monitoring							
	10.10.1	Audit logging	□				□		
	10.10.2	Monitoring system use	□				□		
	10.10.3	Protection of log information	□				□		
	10.10.4	Administrator and operator logs	□				□		
	10.10.5	Fault logging	□				□		

	10.10.6	Clock synchronization					□		
Access control	11,1	Business Requirement for Access Control							
	11.1.1	Access control Policy	□				□	□	
	11,2	User Access Management							
	11.2.1	User Registration	□			□	□		
	11.2.2	Privilege Measurement					□		
	11.2.3	User password management	□				□		
	11.2.4	Review of user access rights					□		
	11,3	User Responsibilities							
	11.3.1	Password Use	□				□		
	11.3.2	Unattended user equipment					□		
	11.3.3	Clear Desk and Clear Screen Policy					□		
	11,4	Network Access control							
	11.4.1	Policy on use of network services	□				□		
	11.4.2	User authentication for external connections	□				□	□	
	11.4.3	Equipment identification in networks	□				□		
	11.4.4	Remote diagnostic and configuration port protection	□				□		

	11.4.5	Segregation in networks	□				□		
	11.4.6	Network connection control	□				□		
	11.4.7	Network Routing control	□				□		
	11,5	Operating System Access Control							
	11.5.1	Secure Log-on procedures	□				□		
	11.5.2	User identification and authentication	□				□	□	
	11.5.3	Password Management system	□				□		
	11.5.4	Use of system utilities	□				□		
	11.5.5	Session Time-out	□				□		
	11.5.6	Limitation of connection time	□				□		
	11,6	Application access control							
	11.6.1	Information access restriction	□						
	11.6.2	Sensitive system isolation							
	11,7	Mobile Computing and Teleworking							
	11.7.1	Mobile computing and communication					□		
	11.7.2	Teleworking					□		
	12,1	Security Requirements of Information Systems							

Information Systems Acquisition Development and Maintenance	12.1.1	Security requirement analysis and specifications	□				□		
	12,2	Correct Processing in Applications							
	12.2.1	Input data validation	□						
	12.2.2	Control of internal processing	□						
	12.2.3	Message integrity	□						
	12.2.4	Output data validation	□						
	12,3	Cryptographic controls							
	12.3.1	Policy on the use of cryptographic controls					□		
	12.3.2	Key Management					□		
	12,4	Security of System Files							
	12.4.1	Control of Operational software						□	
	12.4.2	Protection of system test data					□		
	12.4.3	Access control to program source library					□		
	12,5	Security in Development & Support Processes							
	12.5.1	Change Control Procedures	□				□		
	12.5.2	Technical review of applications after Operating system changes	□						

	12.5.3	Restrictions on changes to software packages					□		
	12.5.4	Information Leakage					□		
	12.5.5	Outsourced Software Development					□		
	12,6	Technical Vulnerability Management							
	12.6.1	Control of technical vulnerabilities					□		
Information Security Incident Management	13,1	Reporting Information Security Events and Weaknesses							
	13.1.1	Reporting Information security events	□				□		
	13.1.2	Reporting security weaknesses	□				□		
	13,2	Management of Information Security Incidents and Improvements					□		
	13.2.1	Responsibilities and Procedures					□		
	13.2.2	Learning for Information security incidents					□		
	13.2.3	Collection of evidence					□		
	14,1	Information Security Aspects of Business Continuity Management							

Business Continuity Management	14.1.1	Including Information Security in Business continuity management process					□	□	
	14.1.2	Business continuity and Risk Assessment					□	□	
	14.1.3	developing and implementing continuity plans including information security					□	□	
	14.1.4	Business continuity planning framework					□	□	
	14.1.5	Testing, maintaining and re-assessing business continuity plans					□	□	
Compliance	15,1	Compliance with Legal Requirements							
	15.1.1	Identification of applicable legislations	□						
	15.1.2	Intellectual Property Rights (IPR)	□		□		□		
	15.1.3	Protection of organizational records	□		□		□	□	
	15.1.4	Data Protection and privacy of personal information					□		
	15.1.5	Prevention of misuse of information processing facilities	□				□		
	15.1.6	Regulation of cryptographic controls							
	15,2	Compliance with Security Policies and Standards and Technical compliance							
	15.2.1	Compliance with security policy					□		

	15.2.2	Technical compliance checking					□		
	15,3	Information System Audit Considerations							
	15.3.1	Information System Audit controls					□		
	15.3.2	Protection of information system audit tools					□		

Fuente: *REGALADO, Richard O., Information Security Consultant.*