PRÁCTICA EMPRESARIAL, PROPUESTA DE IMPLEMENTACIÓN DE LA NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001:2013 EN EL ACUEDUCTO METROPOLITANO DE BUCARAMANGA amb S.A. E.S.P

MIGUEL ARMANDO SUÁREZ PEDRAZA

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD FÍSICO - MECÁNICA
ESCUELA DE INGENIERÍA DE SISTEMAS
BUCARAMANGA
2016

PRÁCTICA EMPRESARIAL, PROPUESTA DE IMPLEMENTACIÓN DE LA NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001:2013 EN EL ACUEDUCTO METROPOLITANO DE BUCARAMANGA amb S.A. E.S.P

MIGUEL ARMANDO SUÁREZ PEDRAZA

Trabajo de Grado presentado como requisito para obtener el título de Ingeniero de Sistemas

DIRECTOR

SERGIO FERNANDO CASTILLO CASTELBLANCO

Ingeniero de Sistemas Ph.D

CODIRECTOR

HUGO HELKCC LÓPEZ JIMÉNEZ

Especialista en Seguridad de la Información

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD FÍSICO - MECÁNICA
ESCUELA DE INGENIERÍA DE SISTEMAS
BUCARAMANGA
2016

Dedicatoria

A Dios por acompañarme todos los días de mi vida, a Él por darme la fortaleza y sabiduría necesaria para cada paso realizado y conseguir este importante logro, gracias a Dios hoy culminó esta etapa profesional demostrándome que no he estado solo.

A mis padres, quienes han depositado su confianza en mí, me han dado la motivación suficiente para culminar esta meta, a ellos gracias por todo el esfuerzo y apoyo, a ustedes quienes a pesar de las adversidades siempre han estado allí para brindarme su amor y comprensión, padres este triunfo es de ustedes.

A mis hermanas por su cariño, apoyo, motivación y respaldo incondicional durante este camino, ustedes han sido clave en mi formación personal y me han brindado apoyo constantemente.

A toda mi familia que ha sido mi inspiración más grande para seguir adelante en este camino.

A mis amigos por compartir grandes momentos conmigo y ser una parte de la inspiración para ser mejor cada día.

A las personas que han sido participes de este objetivo, de una u otra forma han contribuido en mi formación personal, académica y profesional.

Miguel Armando Suárez Pedraza

Agradecimientos

A Dios por todas las bendiciones que me ha regalado día a día, gracias por colmarme de fortaleza y sabiduría necesaria para llegar a lograr mis metas trazadas.

A mis padres que me han ofrecido todo su apoyo y amor incondicional.

Al CIDLIS, al IPRED y al amb SA ESP, por permitirme adquirir experiencia en un entorno laboral previo a egresar, ustedes me han permitido crecer profesionalmente.

Al Ing. Hugo López y al Ing. Miguel Ardila por su gran apoyo, por su paciencia y valiosa asesoría antes y durante el proyecto.

A la Universidad Industrial de Santander, por haber sido la promotora de mi formación académica como profesional.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

TÍTULO: PRÁCTICA EMPRESARIAL, PROPUESTA DE IMPLEMENTACIÓN DE LA NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001 EN EL ACUEDUCTO METROPOLITANO DE BUCARAMANGA amb SA ESP*

AUTOR: Miguel Armando Suarez Pedraza**

PALABRAS CLAVES: Seguridad de la Información, NTC ISO/IEC 27001:2013, Auditoria, GAP, Análisis de Riesgos, Controles, Incidentes, Sistema de Gestión de la Seguridad de la Información, SGSI.

DESCRIPCIÓN

El establecimiento de un Sistema de Gestión de la Seguridad de la Información SGSI en una empresa evidencia los procedimientos técnicos, políticas, controles organizacionales de forma estructurada, documentada, controlada y en mejora continua, este SGSI permite definir el nivel de riesgo de los activos de la información en una empresa y evitar los incidentes de la seguridad de la información.

En este trabajo se realiza un estudio preliminar para determinar un prototipo del plan de implementación de la Norma Técnica Colombiana NTC-ISO/IEC 27001 Requisitos para los Sistemas de Gestión de Seguridad de la Información en el Acueducto Metropolitano de Bucaramanga amb S.A. E.S.P, empresa prestadora del servicio de acueducto a más del 80 % de la zona metropolitana de Bucaramanga. Se realizó una auditoria interna diagnóstica para definir el estado de la seguridad de la información y generar un GAP, seguido a esto se llevó a cabo el análisis de riesgos y establecer una declaración de aplicabilidad inicial.

Un SGSI facilita el análisis de los respectivos engranajes del panorama de la Seguridad de la Información en una empresa, los mecanismos para salvaguardar los activos de información y los sistemas que los procesan, en conjunto con las políticas y planes estratégicos de la empresa, lo anterior forma los principales objetos de estudio del presente proyecto en base a los resultados de la Auditoria Interna Diagnóstica realizada.

Se propuso el planteamiento de controles a partir de los resultados arrojados de la auditoria, el análisis de riesgos y la declaración de aplicabilidad.

---

*Trabajo de Grado

** Facultad de Ingenierías Físico - Mecánicas. Escuela de Ingeniería de Sistemas e Informática. Director Profesor EISI Sergio Castillo, Tutor: Especialista en Seguridad de la Información Hugo Helkcc López.

ABSTRACT

TITLE: BUSINESS PRACTICE, PROPOSED IMPLEMENTATION OF COLOMBIAN TECHNICAL STANDARD NTC - ISO / IEC 27001 IN THE AQUEDUCT METROPOLITAN OF BUCARAMANGA amb SA ESP.

AUTOR: Miguel Armando Suarez Pedraza**

KEY WORDS: Information Security , NTC ISO / IEC 27001: 2013 , Auditing , GAP, Risk Analysis, Controls, Incident, information security management system, ISMS.

DESCRIPTION

The establishment of information security management system ISMS evidence enterprise technical, political, organizational controls in structured, documented, controlled and continuous improvement procedures, this ISMS can define the level of risk assets information in a company and avoid incidents of information security.

This paper presents a preliminary study is conducted to determine a prototype implementation plan of the Colombian Technical Standard NTC-ISO / IEC 27001 Requirements for Management Systems Information Security at the Metropolitan Aqueduct of Bucaramanga amb S.A. E.S.P, company that provides water service to more than 80% of the metropolitan area of Bucaramanga. a diagnostic internal audit was conducted to define the state of information security and generate a GAP followed this was conducted risk analysis and establish an initial statement of applicability.

A ISMS facilitates the analysis of the respective gears picture of information security in a company, the mechanisms for safeguarding the information assets and the systems that process , fourth of swindlers set the policies and strategic plans of the company, way above the main objects of study Project present at the base of a Realized the results Diagnóstica internal audit.

The approach proposed controls from the results obtained from the audit, risk analysis and applicability statement.

---

*Bachelor Tesis

** Faculty of Physical Engineering - Mechanical . Systems of Engineering and Information School . Director EISI Tecahcer Sergio Castillo, Tutor Specialist Information Security Helkcc Hugo Lopez.

INTRODUCCIÓN

Para definir la gestión realizada en el presente proyecto se plantea el escenario que define el contexto de la Seguridad de la Información en el Acueducto Metropolitano de Bucaramanga (amb) S.A E.S.P y su necesidad de establecer un conjunto de políticas, procedimientos y controles para destinar los recursos necesarios para implantar mecanismos para mejorar la Seguridad de su activo más valioso, la Información.

El marco de trabajo ofrecido por el estándar internacional NTC-ISO/IEC 27001:2013 expresa que un Sistema de Gestión de la Seguridad de la Información - SGSI facilita el análisis de los respectivos engranajes del panorama de la Seguridad de la Información en una empresa, los mecanismos para salvaguardar los activos de información y los sistemas que los procesan, en conjunto con las políticas y planes estratégicos de la empresa, lo anterior forma los principales objetos de estudio del presente proyecto en base a los resultados de la Auditoria Interna Diagnóstica realizada.

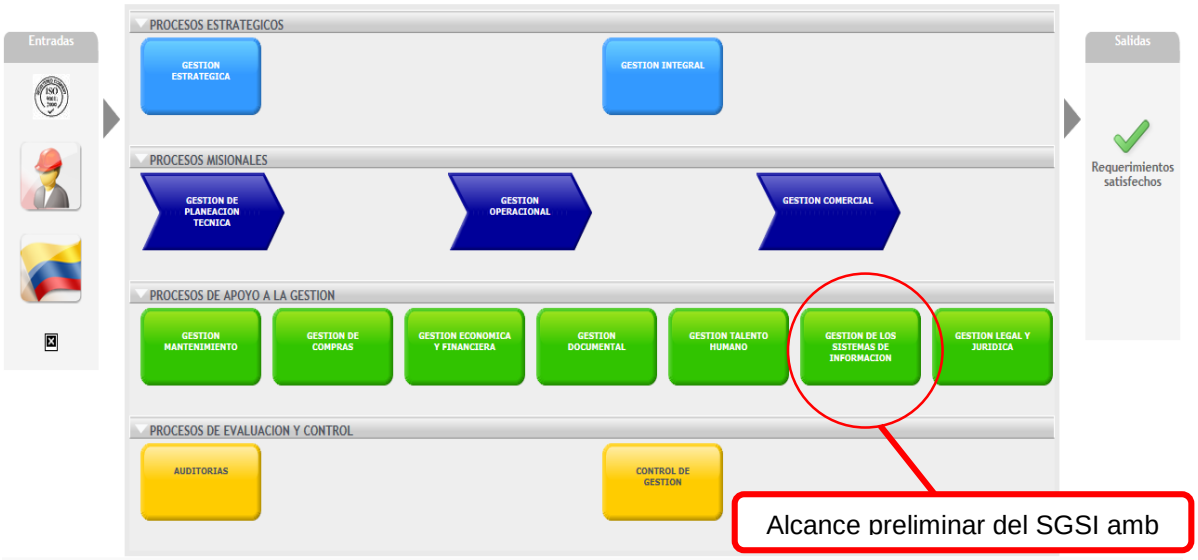
Por lo tanto se indica que la Gestión de la Seguridad de la Información debe abordarse como un proceso sistemático documentado y que debe ser establecido en la mayor parte de la empresa, definir un SGSI preliminar en la presente propuesta de proyecto permite reunir la información del Manual de Políticas de Seguridad de la Información del amb, por otro lado se estudió el análisis diferencial de los mecanismo de seguridad implementados en la empresa respecto a lo planteado en la NTC-ISO/IEC 27001:2013, revisando la gestión del riesgo de la infraestructura TI para la selección de respectivos controles de Seguridad de la Información, de esta

forma se realizan significativos aportes para reducir la aparición de incidentes, minimizando así su impacto negativo.

El Acueducto Metropolitano de Bucaramanga es una empresa que presta el servicio domiciliario del acueducto y saneamiento básico, el amb capta, procesa y distribuye el servicio de suministro de agua potable con valor agregado en forma complementaría, actualmente el amb participa como socia de otras Empresas de Servicios Públicos.

A nivel general de toda la empresa, en el amb se desarrollan políticas y estándares de calidad que aseguran la orientación y cumplimiento del objetivo del negocio, los procesos de la empresa organizan, fomentan y regulan la prestación del preciado líquido lo más eficiente y eficazmente posible, con una cobertura de aproximadamente del 80% del área metropolitana de Santander.

Figura 1. Estructura de organización por procesos del amb.



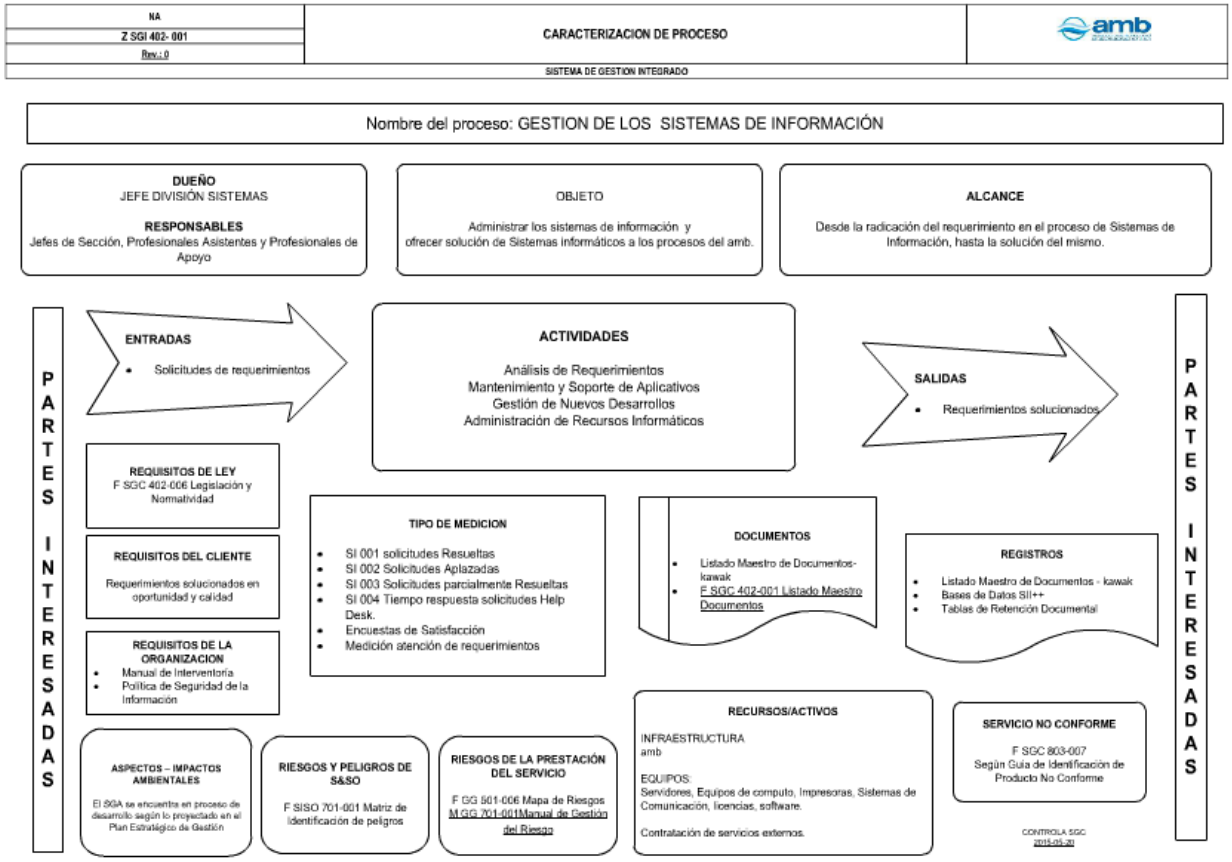
Fuente: Kawak, Sistema de Información Integrado para la Gestión de la calidad en el amb, 2013.

La estructura interna del amb es planteada mediante la organización de procesos Estratégicos, Misionales, de apoyo a la Gestión y de Evaluación y Control.

Fomentando una cultura preventiva y de control sobre los eventos de Seguridad Industrial y Salud Ocupacional, brindando un mejor entorno laboral, la estructura de la empresa está planteada por procesos, está representada en la **Figura.1**.

Kawak es el Sistema de Información que gestiona los procesos de Calidad basados en el estándar ISO 9001 en el amb, en este sistema de información se documentan todos los procesos anteriormente mencionados y expuestos en el mapa de procesos.

Figura 2. Caracterización Sistemas de Información Z SI 702-004



Fuente: Kawak, Sistema de Información Integrado para la Gestión de la calidad en el amb, 2013.

El amb gestiona programas de investigación para optimizar costos de captación, tratamiento y distribución de agua, la asistencia a los operadores del servicio, a los

técnicos en el lugar de las fases del tratamiento del agua permite regular y comercializar el producto en las mejores condiciones. Comprometido con la mejora continua y como empresa Socialmente Responsable, el amb asegura la gestión transparente y efectiva de sus procesos y la administración de los riesgos asociados con la prestación del servicio.

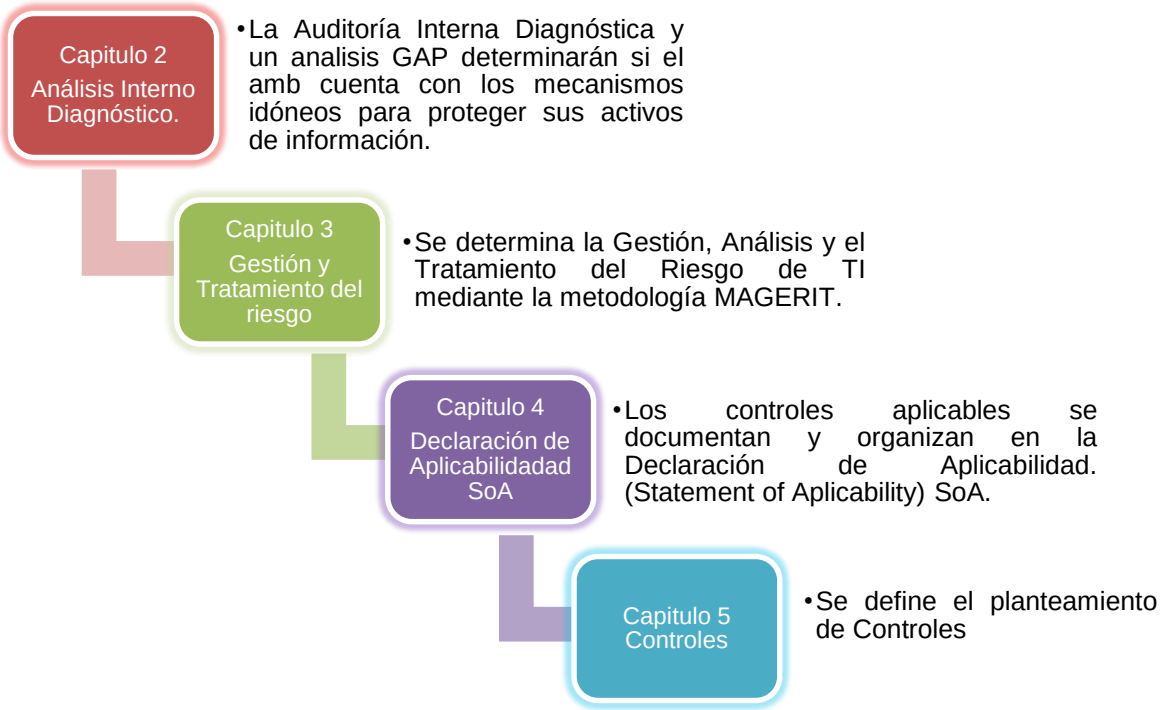
Como se especifica en la **Figura 1** el mapa de procesos de la empresa y se determina el alcance general del presente proyecto de implementación de la NTC ISO /IEC 27001:2013, formulación de un SGSI preliminar en el proceso de Apoyo a la Gestión denominado Gestión de los Sistemas de Información caracterizado en la **Figura 2.**

1. GESTIÓN DEL PROYECTO

1.1 OBJETIVO GENERAL

Proponer la implementación de la Norma Técnica Colombiana NTC-ISO/IEC 27001:2013 Requisitos para los Sistemas de Gestión de Seguridad de la Información SGSI en el Acueducto Metropolitano de Bucaramanga S.A. E.S.P, con miras a realizar aportes a la respectiva certificación del SGSI preliminar.

1.2 OBJETIVOS ESPECÍFICOS

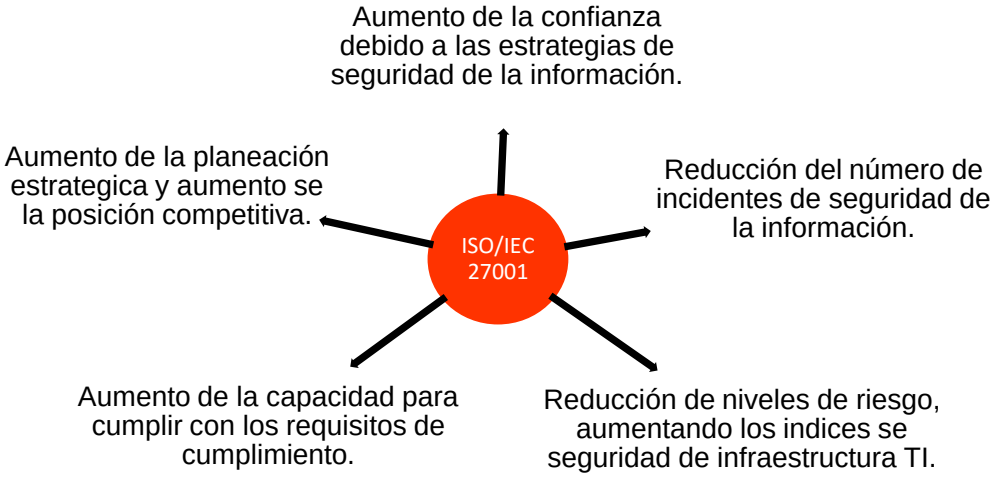


2. AUDITORIA INTERNA DIAGNÓSTICA Y ANÁLISIS GAP

2.1. NORMA TECNICO COLOMBIANA NTC ISO/IEC 27001:2013

La Organización Internacional de Estandarización ISO estableció la norma ISO/IEC 27001 en su versión más reciente 2013 como la principal norma para establecer un Sistema de Gestión de Seguridad de la Información, actualmente es utilizada en el contexto de empresas que se basan en procesos corporativos, la norma ISO 27001 está alineada con otros Sistemas de Gestión como el de Gestión de la Calidad de la norma 9001, también soporta la implementación y operación de procedimientos, controles y políticas lo cual la hace ideal para abordar el tema de la Seguridad de la Información a nivel empresarial.

Figura 3. Ventajas Implementación NTC ISO/IEC27001:2013



Esta norma técnica propone un escenario completo de la seguridad de la información en términos de: Confidencialidad, Integridad y Disponibilidad. La norma está estructurada de forma general en dos grandes partes, la primera hace

referencia a los requerimientos para establecer, implantar, documentar, y evaluar un SGSI y luego en el anexo A la norma plantea los objetivos de control o dominios.

2.2. ESTRUCTURA GENERAL DE LA NTC ISO/IEC 27001:2013

Figura 4. Requerimientos generales de la norma

Fuente: MAGAZCITUM, ISO-27001:2013, Trejo Dulce, 2013

La segunda parte de la norma hace referencia a los 14 objetivos de control que a su vez comprende 114 controles de forma estructurada (**Figura 4**).

2.3. VENTAJAS DE LA NTC ISO/IEC27001:2013 EN EL amb

La Dirección Administrativa de la empresa se encuentra centralizada en la ciudad de Bucaramanga donde se generan las reglas para los comités, divisiones, secciones de todo el amb. Esta empresa se encuentra ubicada en un edificio en el parque del agua, está estructura empresarial cuenta con una División de Sistemas de Información y un centro de cómputo principal Data Center (físico) utilizado para

administrar todos los recursos de infraestructura TI de las sedes que componen todo el amb.

Figura 5. Objetivos de Control NTC ISO/IEC27001:2013

A.5	•Politicas de seguridad
A.6	•Organizacion de la informaciòn
A.7	•Seguridad en recursos humanos
A.8	•Gestiòn de activos
A.9	•Control de acceso
A.10	•Criptografìa
A.11	•Seguridad fisica y ambiental
A.12	•Seguridad en las operaciones
A.13	•Transferencia de informaciòn
A.14	•Adquisisiòn de sistemas, desarrollo y mantenimiento
A.15	•Relaciòn con proovedores
A.16	•Gestiòn de os incidentes de seguridad
A.17	•Continuidad de negocio
A.18	•Cumplmiento con requerimientos legales y contractuales

Fuente: MAGAZCITUM, Anexo A NTC ISO/IEC 27001:2013, Trejo Dulce, 2013

Para el apoyo de los procesos del negocio realizados en el amb, la empresa implementa un Sistema de Información Transaccional o **ERP**, aplicaciones basadas en la web para uso de los usuarios, dispositivos de procesamiento para prestar los servicios, estos son establecidos y administrados a nivel de divisiones o departamentales que componen la estructura empresarial del amb a través de una red LAN corporativa con la que se interconectan todas las oficinas.

Uno de los principales objetivos de la formulación de un SGSI preliminar a partir de la implementación de la NTC ISO/IEC 27001:2013, es minimizar el riesgo de las amenazas que impactan negativamente sobre los activos de la infraestructura TI del amb, estas amenazas se presentan frecuente e inesperadamente, debido a la estructuración de los mecanismos de seguridad frente a esto riesgos y la naturaleza de los servicios ofrecidos por la División de Sistemas, se contemplan escenarios

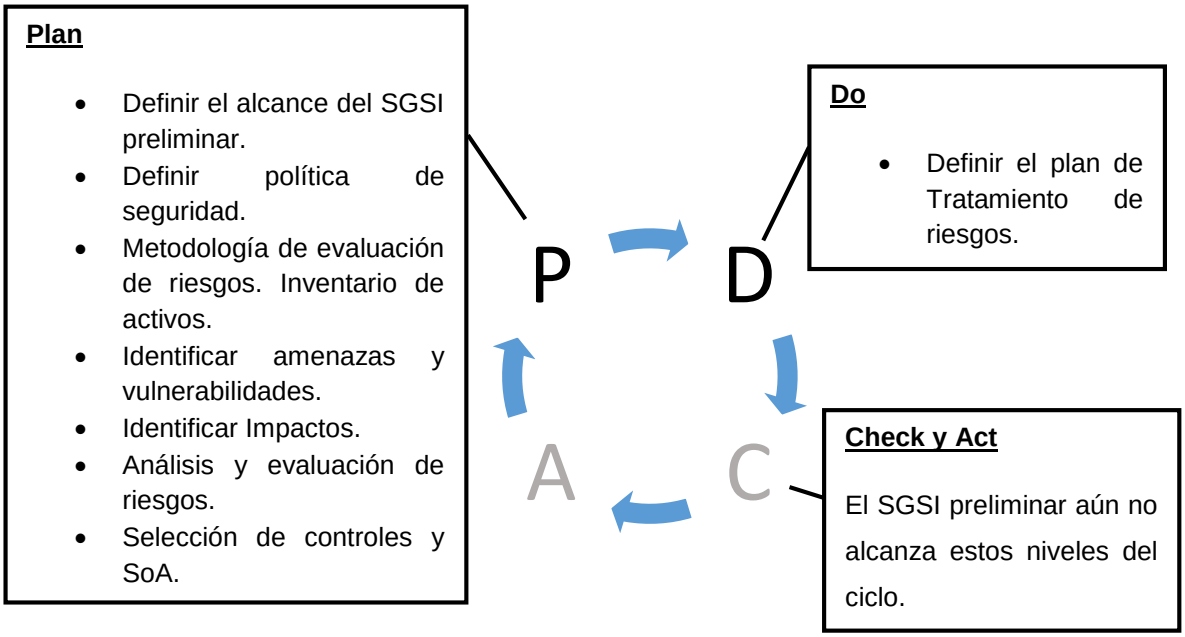
desde los accesos ilegales hasta el sabotaje físico o lógicos de los dispositivos que componen la infraestructura TI del amb..

La implementación de formal de un SGSI permitirá el aumento de los beneficios para poner las medidas de seguridad necesarias que permiten reforzar la reputación de la empresa y darle continuidad al negocio mediante el establecimiento de políticas, controles, procedimientos y protocolos, lo anterior permite el aumento significativo de la seguridad de la infraestructura TI de la empresa.

2.4. CICLO PDCA Y LA NORMA ISO

Se realizó un análisis y teniendo como punto de partida el plan del proyecto, se tiene en cuenta el compromiso de la dirección de la División de Sistemas para la definición de responsabilidades para el arranque del proyecto, se llevó a cabo la respectiva ubicación del estado de madurez del ciclo PDCA establecido para las normas ISO, se identificó que el alcance y respectiva ejecución del proyecto llegará hasta la primera parte del nivel Hacer ***(DO)***, **(Figura 6)**.

Figura 6. El Ciclo PDCA se cumple de forma parcial.



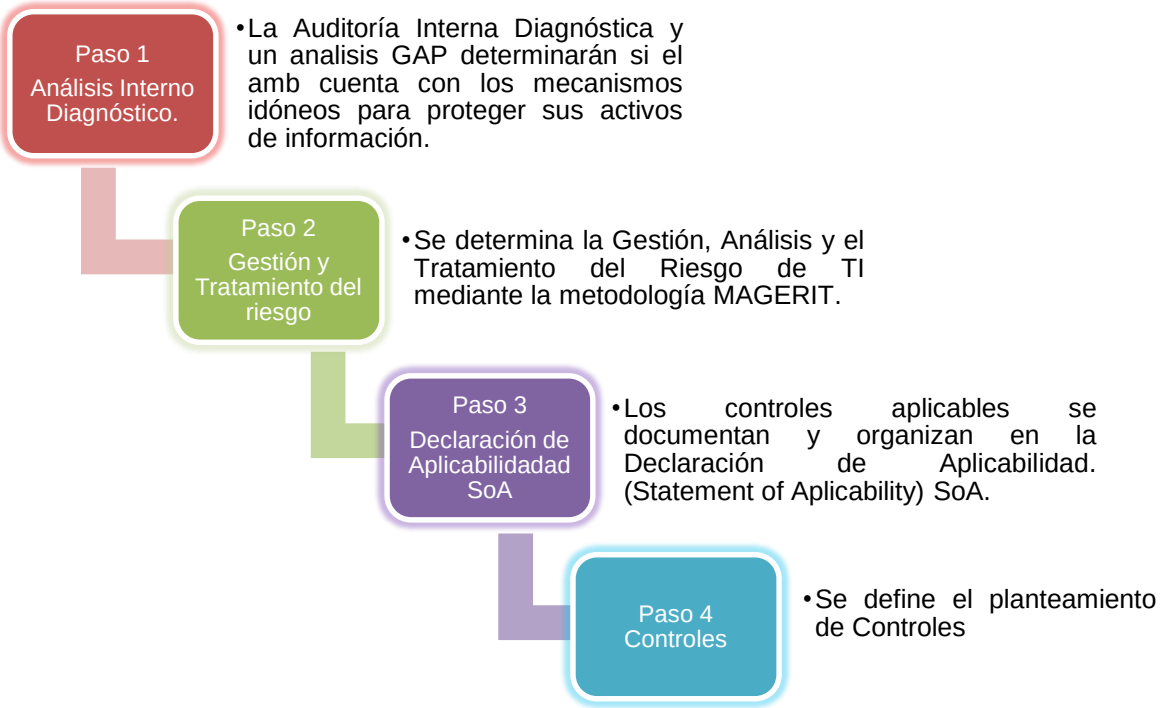
Para la ejecución del proyecto se tuvo en cuenta que actualmente se realiza la clasificación general de los activos más importantes en cuanto a la infraestructura TI del amb de la siguiente forma: Activos Hardware, Activos Software.

2.5. METODOLOGÍA, PLAN DE IMPLEMENTACIÓN DE LA NTC-ISO/IEC 27001:2013 PARA LOS REQUISITOS DE UN SGSI

Los pasos que fueron propuestos para el plan de implementación de la NTC ISO/IEC 27001:2013 en el amb corresponden a los objetivos específicos, estos son:

- Auditoria Interna Diagnóstica y análisis GAP.
- Gestión y Tratamiento del riesgo.
- Declaración de aplicabilidad o Statement of Aplicability, (SoA).
- Planteamiento de Controles a partir de la Implementación Norma Técnica Colombiana NTC-ISO/IEC 27001:2013 y la SoA.

Figura 7. Metodología implementación de la NTC-ISO/IEC 27001:2013 en el amb



2.6. INFORME AUDITORIA INTERNA DIAGNÓSTICA Y ANÁLISIS GAP

2.6.1. Definiciones. La Auditoría Interna Diagnóstica permitió realizar una evaluación independiente, critica y objetiva del contexto de la Seguridad de la Información en la División de Sistemas del amb , esta auditoria fue realizada por personal interno de la empresa y autor del proyecto, esta primera parte evaluó el cumplimiento de los requerimientos generales, objetivos de control, procesos y procedimientos de un SGSI preliminar en la División de Sistemas del amb, se evaluó el nivel de madurez de la Seguridad de la Información implementada en el amb respecto a los lineamientos planteados en la NTC-ISO/IEC 27001:2013.

Se identificaron los principales factores que han condicionado el desempeño de la Seguridad de la Información en la División de Sistemas del amb, dicho desempeño se evalúa para determinar el nivel de cumplimiento de un Sistema de Gestión de la Seguridad de la Información, se obtuvo como resultados la respectiva identificación de fortalezas, debilidades y oportunidades de mejora que presenta el contexto de la Seguridad de la Información en la División de Sistemas del amb.

Por lo tanto, se propuso iniciar con una Auditoria Interna Diagnóstica para determinar si el amb tiene mecanismos idóneos y estándares para proteger su información, esta Auditoría Interna Diagnóstica se llevó a cabo en el proceso o principal alcance definido en anteriormente: División de Sistemas de Información del amb.

Con los principales involucrados en el proyecto se estableció que los aspectos más importantes a considerar en la Auditoría Interna Diagnostico debían ser:

- La realización de una correcta planificación de la auditoria aprobada por la Dirección.

- Se estipulo la distribución de los objetivos de control a ser evaluados por el equipo auditor

- Toda la División de Sistemas de información del amb conoció el alcance y la agenda estipulada para la Auditoría Interna en una reunión de apertura realizada.

- Los informes y resultados fueron conocidos por todo el personal de la División de Sistemas de información involucrado dentro del alcance de la Auditoria.

- De acuerdo al informe y/o resultados presentados en la auditoría interna, el trabajo futuro es el compromiso de la empresa para gestionar los planes de mejora en cuanto a la eficacia de la Seguridad de la Información en la División de Sistemas del amb mediante la respectiva formalización de un SGSI.

2.6.2. Plan de Auditoria Interna

2.6.2.1. Objetivos de la auditoria interna diagnóstica

- Determinar la conformidad del Sistema de Gestión de la Seguridad de la Información SGSI con los requisitos de la Norma Técnica Colombiana NTC-ISO/IEC 27001:2013.

- Diagnosticar el estado de los procesos de la División de Sistemas de Información respecto a los Objetivos de Control establecidos en la NTC-ISO/IEC 27001:2013.

2.6.2.2. Alcance: Determinar el grado de implementación del Sistema de Gestión de Seguridad de la Información SGSI en la División de Sistemas del Acueducto Metropolitano de Bucaramanga S.A. ESP, amb respecto a la Norma Técnica Colombiana NTC-ISO/IEC 27001:2013 en cuanto a los Requerimientos Obligatorios

del SGSI y los Objetivos de Control planteados en el Anexo A de la norma.

La norma Técnica Colombiana ISO/IEC 27001:2013 indica los procedimientos y requerimientos generales para el establecimiento de un Sistema de Gestión de la Seguridad de la Información SGSI, esta norma permite el establecimiento, formalización y seguimiento de un SGSI en este caso particular el SGSI preliminar para el amb, con el fin de asegurar de un modo más eficaz todos los principales activos de la infraestructura TI de la empresa.

2.6.3. Ejecución. Para la ejecución de la Auditoria Interna diagnóstica se comunicó un plan de auditoria para definir las principales características de la auditoria tales como:

- La definición de los objetivos de la auditoria, el respectivo alcance, los criterios a tener en cuenta, el equipo auditor y las fechas programadas para llevar a cabo el proceso de auditoria tanto de los requerimientos generales de la ISO/IEC 27001 como de los objetivos de control del anexo A de la norma.
- Criterios: Se establecieron las normas y sistemas de gestión ante los cuales se lleva a cabo la comparación de hallazgos de la auditoria (**Tabla 1**).

Tabla 1. Criterios de la Auditoria Interna Diagnóstica

Norma Técnica Colombiana NTC-ISO/IEC 27001
Requisitos Legales asociados a la gestión de los activos de información.
Acto de Gerencia 012 – Política de seguridad establecida en el amb.

- Se estableció el Equipo auditor compuesto por el autor del proyecto: Miguel Armando Suarez Pedraza y un profesional de apoyo de la división se Sistemas de Información encargado del acompañamiento de la ejecución de la auditoria.

- Para realizar la auditoria interna diagnóstica se estructuró el plan de trabajo de acuerdo a la estructura de la norma, en un primer momento de la auditoria se plantea evaluar los requerimientos generales especificando la fecha, hora, el requerimiento general evaluado, auditado. Luego se evalúan los Dominios del Anexo A de la norma, se realizó una reunión de apertura para socializar esta primera fase de la auditoria y dar a conocer el plan correspondiente a todos los integrantes de la División de Sistemas de Información.

2.6.4. Resultados. A partir de la Auditoria referente a los requerimientos generales de la norma y a partir de la observación encontrada de No conformidad (**Tabla 2**), se establecen los requerimientos generales como se especifica a continuación (**Tabla 3**):

Tabla 2. Observaciones de Requerimientos Generales

Requerimientos Generales	Nc: No se plantea y formaliza un sistema de gestión de la seguridad de la información. Se propone documentar un Manual de políticas de la seguridad de la información. SGSI – Preliminar.

Tabla 3. Establecimiento de Requerimientos Generales

CONTROLAR	OBSERVACIONES
4. **Contexto de la organización** La empresa debe determinar los aspectos externos e internos que son necesarios para cumplir su propósito y que afectan su capacidad para lograr los resultados previstos en el SGSI. Se define el alcance del SGSI.	Se lleva a cabo la primera aproximación a la formalización de un Sistema de Gestión de la seguridad de la información SGSI en la División de Sistemas de información del amb, se identifican los principales involucrados. **Interesados**: Los usuarios de los sistemas de información e infraestructura tecnológica a nivel interno del amb junto a la Alta Gerencia.

CONTROLAR	OBSERVACIONES
	Se identifican los aspectos externos como terceros y vínculos con proveedores. Se documentan explícitamente los interesados previamente identificados. Se define claramente el **alcance** de un SGSI preliminar: Proceso de la Gestión de Sistemas de Información, los avances realizados y analizados han sido limitados a este proceso de la División de sistemas de información.
5. Liderazgo La Alta Dirección tiene la obligación de demostrar su liderazgo y compromiso con respecto al Sistema de Gestión de Seguridad de la Información. Asegurando que tanto la política de seguridad como los roles, responsabilidades y autoridades de la empresa para determinar los objetivos y dirección estratégica que garanticen la disponibilidad de los recursos necesarios para el SGSI.	Se identifica la necesidad de **plantear un proyecto específico** dentro del proceso de Gestión de los Sistemas de información para la solicitud de recursos destinados de acuerdo a las necesidades. Se identifica la ubicación de un proyecto en la estrategia general de Mejora continua, innovación y tecnología, la estrategia de Integración de sistemas y Tecnologías de la Información en la gestión por procesos, proyecto estratégico de estructuración del plan de gestión de tecnologías de la información. Se determina el compromiso de la Alta Gerencia mediante la Política de Seguridad actual: Acto de gerencia 012 y la respectiva transición a un **Manual de Políticas de Seguridad** de la Información planteado en el presente informe del proyecto, se asegura el establecimiento de la política y la asignación de respectivas responsabilidades. Se determinan recursos anuales de acuerdo al plan de necesidades gestionado por los directivos de la División de Sistemas del amb.
6. Planificación	Se define el panorama de riesgos, controles, historial, tabla de vulnerabilidades en el mapa

CONTROLAR	OBSERVACIONES
Planificar la empresa y establecer los objetivos de seguridad de la información y elegir los controles correctos de seguridad. Determinando el alcance del SGSI, presentación de una política de SGSI, planteando una metodología de evaluación de riesgos y determinar los criterios de aceptabilidad. Identificación de activos, vulnerabilidades y amenazas para evaluar la magnitud de los riesgos para el tratamiento de los riesgos.	de riesgos mediante la matriz de riesgo corporativa actual. A mayor riesgo se analizan los índices obtenidos en este mapa de riesgos para evidenciar que los controles existentes mitigan eficientemente los riesgos que se han identificado. Los controles son definidos con el riesgo asociado, la causa y los efectos del mismo, se lleva a cabo la aplicación de una metodología de semaforización a partir de la identificación de una serie de vulnerabilidades. Se plantea la transición a una nueva **metodología para el análisis y tratamiento del riesgo MAGERIT** para avanzar en el contexto de la seguridad de la información, analizando el riesgo de los activos de la infraestructura TI del amb.
7. Soporte Se debe determinar y proporcionar los recursos para establecer, implementar, mantener y mejorar el SGSI. Se establecen criterios o competencias de las personas que realizan trabajos que afecten el desempeño de la seguridad de la información. Las personas de la empresa toman conciencia de la política y la eficacia de la seguridad de la información. Se establecen protocolos de comunicación tanto para las comunicaciones internas y externas. Se realiza	El compromiso de la Alta Gerencia en el contexto de la seguridad de la información se ve reflejado al atender el **Plan de Necesidades** FGG 504-003, avalando actividades, programas, satisfacción de requerimientos, lo anterior mediante la asignación de recursos. Se realiza la propuesta un año directamente anterior para la adquisición de recursos para la mejora de la seguridad de la información y seguridad de los sistemas que soportan los procesos del amb. En el FGG 504-003 se formula el Plan de necesidades por parte de la División de sistemas de información, la Alta Dirección realiza la aprobación del presupuesto en cuanto a las necesidades. Los recursos dependen de la necesidad inmediata, con los proyectos que se definen actualmente y dependiendo de la disponibilidad

CONTROLAR	OBSERVACIONES
documentación de la gestión del riesgo.	presupuestal asignada. La Gestión del Recurso Humano establece perfiles, especificando las respectivas competencias para asegurar que las personas que ejecuten labores que impliquen acceso a la información sean competentes según educación, formación o experiencia. Los usuarios toman conciencia de la política y eficacia de la seguridad de la información mediante el acto de gerencia 012 disponible para los empleados del amb que tengan acceso a los activos de información.
8. Operación Se debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos y para implementar las acciones determinadas en 6.1. Se debe implementar planes para lograr los objetivos del SGSI. Se debe mantener información documentada, cuando sea necesaria para tener confianza en que los procesos se han llevado a cabo según lo planificado. Se debe controlar los cambios planificados y revisar las consecuencias de los cambios no previstos, mitigando los efectos adversos, cuando se requiera.	La División de Sistemas para cumplir la necesidad de gestionar los riesgos y abordar el tema de la seguridad de la información lleva a cabo la planificación e implementación de proyectos que mitigan la materialización de los riesgos. La planeación, ejecución y control de estos proyectos son documentados y almacenados en un directorio denominado **Gestión del Conocimiento** almacenado en servidor de archivos. El principal plan para lograr los objetivos de garantizar la seguridad de la información está registrado en el análisis de riesgos del mapa de riesgos corporativo que la empresa utiliza actualmente (MAGERIT próximamente), la dirección de la División asigna un representante en el comité de riesgos encargado del análisis de la gestión y tratamiento del riesgo. Los cambios son planificados, estos se controlan de acuerdo a las actividades ejecutadas por la División, teniendo en cuenta la revisión de las consecuencias de

CONTROLAR	OBSERVACIONES
	los cambios, los cambios es las tareas de procesos y operativos llevados a cabo por la División son controlados para mitigar los efectos adversos del cambio.
9. Evaluación y desempeño Se debe evaluar el desempeño del SGSI y la eficacia del SGSI. Planteando auditorías internas para evaluar el SGSI y revisiones periódicas por la Alta Gerencia respecto a la Gestión de la protección de los activos de información.	La empresa tiene comité de riesgos en cada sección, se tiene un representante en la División de Sistemas, el jefe de la División es quien gestiona los riesgos propios de la División de forma corporativa. La solución a los riesgos es gestionada por el jefe de la División gestionando la solicitud de recursos para la adquisición de herramientas que controlen la seguridad de la información. Se socializa la gestión del riesgo y se tiene planificado el proceso de revisión, los riesgos de forma corporativa se revisan cuando se realiza auditoria interna o auditoria de calidad. La gestión del riesgo también es revisada al momento de realizar cambios en la infraestructura tecnológica y cambios en los servicios ofrecidos. La evaluación del desempeño y eficacia del SGSI se plantea una vez formalizado el SGSI en el amb
10. Mejora Se debe reaccionar frente a las No Conformidades del contexto de la seguridad de la información para hacer cambios o implementar acciones.	Los incidentes registrados en casos específicos se formulan como No Conformidades observaciones debido a que el Sistema de Gestión de la Seguridad de la Información no se encuentra formalizado, la mejora continua se lleva a cabo atendiendo las observaciones y hallazgos. Los incidentes respecto a la administración de recursos informáticos o incidentes de acceso lógico o físico son registrados en una **Bitácora** que

CONTROLAR	OBSERVACIONES
	permite evidenciar la gestión del incidente. El jefe de la División determina que se debe realizar al momento de que se presente una inconformidad en el contexto de la seguridad de la información, formalmente se establece un historial de incidentes que determinan el estado acerca de la mejora continua de los controles en el contexto de la seguridad de la información (bitácora de incidentes).

Se realizó una reunión de apertura para socializar esta segunda fase de la auditoria y dar a conocer el plan correspondiente. La información de establecimiento del plan de la Auditoria Interna Diagnóstica de los objetivos de control del Anexo A de la NTC ISO/IEC 27001.

Se hizo referencia a algunas observaciones dentro del plan de la Auditoria Interna en términos de la disposición de la infraestructura para la ejecución de la Auditoria y la disposición de los auditados para la ejecución de las mismas; los procesos auditados son respaldados con soporte o evidencias que permitan formular los hallazgos una vez finalizada la auditoria.

En este segundo momento de la Auditoria se evaluaron los **Objetivos de Control del Anexo A** de la norma, especificando la fecha, hora, el requerimiento general evaluado y auditado, a continuación, se presenta el informe y resultados del proceso de evaluación, el cual se realizó con un checklist o lista de verificación.**,** la estructura general del Informe de Auditoria presentado a continuación es:

1. Se presentan los principales hallazgos en cada uno de los Objetivos de Control los cuales fueron auditados.
2. Se describen las observaciones expuestas en el informe de la auditoria interna diagnóstica y respectivas observaciones y no conformidades (tablas).

2.6.4.1. A.5. Política de la Seguridad de la Información. Se evidenció que en el amb se establece el Proceso Gestión de los Sistemas de Información, este proceso es soportado por el Sistema de Información Transaccional (ERP) Sii++ para las principales actividades de la empresa, se define un conjunto de políticas para la seguridad de la información en el acto de gerencia 012 del 2014 elaborada por la División de Sistemas y aprobada por la Gerencia General, la Política de Seguridad es publicada y comunicada a los empleados y partes interesadas. Se realizan observaciones para el planteamiento del ajuste de la Política de Seguridad de la información alineado con la NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001:2013.

Tabla 4. Observaciones Política de la Seguridad de la Información

Revisión de las Políticas para la Seguridad de la Información	Se considera pertinente mejorar la planificación respecto a los cambios y revisiones de la política de forma programada, se propone la transición al Manual de Políticas de la Seguridad de la Información

2.6.4.2. A.6. Organización de la Seguridad de la Información. Se evidenció que se realiza la asignación implícita de las responsabilidades de la Seguridad de la Información en los perfiles de la División, contemplados en el manual de perfiles y responsabilidades establecidas por la Gestión del Recurso Humano de la empresa. En el proceso de Gestión de los Sistemas de Información se determinan los principales involucrados: Jefe de División de Sistemas, Jefes de Sección, Profesionales Asistentes, Profesionales de Apoyo y Practicantes cada uno con sus actividades pertinentes.

Se evidenció que la Política de Seguridad establecida está regulada por las leyes pertinentes, leyes contempladas en la política colombiana respecto a la seguridad

de datos e información, el amb garantiza el cumplimiento de las leyes protección de datos y derechos de autor.

Se evidenció que se realiza la organización de un comité de riesgos corporativos para analizar las amenazas e impactos de las amenazas de los activos TI del amb, la División cuenta con un representante en este comité para abordar el tema de la seguridad de la información, se propuso la transición a una metodología de análisis y tratamiento del riesgo respecto a las amenazas de la infraestructura TI de la empresa.

Se evidenció el proceso de adopción y publicación de la política de las medidas de seguridad y de soporte, esta política aborda de forma general los principales riesgos introducidos por el uso de medios extraíbles en el acto de gerencia 012 literal de seguridad física.

Se establecieron las siguientes observaciones del objetivo de control de la organización de la seguridad de la información, para determinar la atención requerida a este dominio de la ISO/IEC 27001.

Tabla 5. Observaciones Organización de la Seguridad de la Información

Seguridad de la información roles y responsabilidades.	Se hace necesario definir de forma explícita los roles, responsabilidades y deberes de la seguridad de la información.
Contacto con grupos de interés especial.	Se considera pertinente establecer contacto con grupos de Investigación especializados en Seguridad de la Información.
Seguridad de la información en gestión de proyectos	Se hace necesario La inclusión de un proyecto específico dentro del Plan Estratégico del amb, **primera aproximación SGSI Preliminar**.

2.6.4.3. A.7. Seguridad de los Recursos Humanos. Se evidenció que se realiza el proceso de verificación de los antecedentes del personal que lleva a cabo el proceso de vinculación con el amb, el procedimiento Gestión del Recurso Humano realiza este proceso, se establecen perfiles para especificar las actividades que serán desempeñadas por cada uno de los vinculados al amb, incluidos los perfiles de la División de Sistemas, terceros y usuarios de la infraestructura TI.

Se evidenció el establecimiento de responsabilidades de los usuarios y los de la empresa en cuanto a la Seguridad de la Información mediante acuerdos contractuales con empleados y contratistas. Se evidenció la comunicación a todos los empleados del amb y a quienes sea pertinente las políticas y normas que promueven la toma de conciencia apropiada para generar una cultura se Seguridad de la Información, se realizan actualizaciones regulares sobre las políticas y procedimientos pertinentes para los cargos establecidos en la empresa y así promover la seguridad de la información, se evidenció que el amb cuenta con un proceso formal para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información, según el literal de sanciones en caso de violación de la política de seguridad de la información del actual acto de gerencia 012.

2.6.4.4. A.8. Gestión de Activos. Se evidenció que los activos de la infraestructura TI del amb son administrados por la Sección de Almacén General y también por el Administrador de Recursos Informáticos en términos de características y capacidad de los activos TI.

Se evidenció la gestión de la División respecto a la administración de los recursos informáticos, desde el momento de atender la necesidad de adquisición de los activos hasta la disposición o reubicación de los mismos, el inventario es registrado en hojas electrónicas de Excel para el respectivo seguimiento del inventario

hardware y software (licencias) utilizadas en la División, paralelo a esto el almacén administra los activos TI mediante los registros del Sii++.

Se evidenció el establecimiento de reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información, las reglas de uso aceptable se contemplan en el acto de gerencia 012 de 2014.

Se evidenció el control de la devolución de activos, los empleados y usuarios deben responder a los lineamientos planteados en el momento de la devolución de activos.

Se evidenció el desarrollo e implementación de procedimientos para el manejo de activos de información lógicos y físicos, el proceso de Gestión del Sistema de Información tiene documentados sus procedimientos en el Directorio de Gestión del conocimiento y en el Servidor de Producción.

Se evidenció la implementación de procedimientos para la gestión de medios de soporte removibles, se diligencia el acuerdo de confidencialidad para la gestión de medios de soportes removibles, se evidenció que la disposición de medios de soporte, se realiza de forma segura cuando ya no se requieran, estos medios son formateados a bajo nivel para la eliminación de información, controladores, licencias antes de dar de baja el dispositivo.

Se evidenció que la transferencia de medios de soportes físicos que contienen información se protegen contra acceso no autorizado para evitar el uso indebido o corrupción durante el transporte del soporte físico.

Se establecieron las siguientes observaciones del objetivo de control de gestión de activos, para determinar la atención requerida a este dominio de la ISO/IEC 27001.

Tabla 6. Observaciones Gestión de Activos

Uso aceptable de los activos.	Se hace necesario el planteamiento del **Manual de Políticas de la Seguridad de la Información** para detallar el uso aceptable de los activos y mejoras en la Seguridad de la infraestructura TI del amb.
Clasificación de la información. Etiquetado de la información	Nc: No se evidencia la clasificación de la información, falta establecer la clasificación y etiquetado de la Información de acuerdo a su nivel de confidencialidad, disponibilidad e integridad.
Manejo de activos.	Se hace necesario el planteamiento de un SGSI para el desarrollo e implementación de procedimientos para el manejo de activos.

2.6.4.5. A.9. Control de Acceso. Se evidenció la implementación de mecanismos para llevar a cabo el control de acceso lógico al sistema operado con la herramienta de Dominio: Directorio Activo de Windows, se establece una política de autenticación y contraseñas para la identificación y autenticación a los sistemas administrados por la red.

Se evidenció que la División específica y restringe el acceso a los servicios de red, de tal forma que el acceso solo es permitido a los usuarios previamente autorizados, se implementa la metodología de solicitudes de requerimientos para el registro, cancelación y suministro de los derechos de accesos a las principales herramientas implementadas Sii++ y directorio activo.

Se evidenció que la División restringe y controla la asignación del uso de derechos de acceso privilegiado a los servicios, se lleva a cabo la gestión de información de autenticación secreta de usuarios por medio de un procedimiento de gestión formal establecido en la política de seguridad del amb.

Se evidenció que se realiza la revisión de los derechos de acceso se usuarios esporádicamente, el uso de información secreta se exige a los usuarios internos del amb es decir el acceso lógico se controla por medio de un proceso de gestión formal, autenticación y contraseña, el cual se contempla en la política de seguridad.

Se evidenció la restricción del acceso a la información mediante la política por defecto de la herramienta de Dominio, las funciones de los sistemas o aplicaciones se asignan de acuerdo con la política de control de acceso descrita en el acto de gerencia 012, la División tiene sistemas de gestión de contraseñas de calidad debido al formato que maneja y el mecanismo de acceso lógico realizado en las herramientas de: directorio activo, correo, se implementa la política de grupo definida en la herramienta de directorio activo para restringir el uso de utilitarios y aplicaciones.

Se establecieron las siguientes observaciones del objetivo de control de acceso, para determinar la atención requerida a este dominio de la ISO/IEC 27001.

Tabla 7. Observaciones Control de Acceso

Política de control de acceso.	Se considera pertinente definir una Política de Control de Acceso que defina, documente y revise los mecanismos de control de acceso explícitamente.
Revisión de los derechos de acceso se usuarios.	Se hace necesario realizar la revisión de los derechos de acceso de usuarios siguiendo un cronograma establecido.
Sistema de gestión de contraseñas.	Se considera pertinente evaluar el sistema de gestión de contraseñas de las diferentes herramientas que no cumplen con calidad especificada.

Control de acceso a códigos fuente de programas	Nc: No se evidencia control de acceso a códigos fuentes de los programas, no se evidencia la respectiva restricción a los códigos fuentes formalmente.

2.6.4.6. A.10. Criptografía: Se evidenció que se realiza la implementación por parte de la División de mecanismos de criptografía embebidos en las herramientas de: Directorio Activo, PGP, Firewall y Tivoli, se desarrollan mecanismos sobre el uso y protección y tiempo de vida de claves criptográficas en las herramientas de directorio activo y Sii++.

Se evidenció el uso de la solución de seguridad *kaspersky* para el cifrado de forma parcial, se implementa el firewall para el cifrado de información para su transferencia en la red LAN del amb, se establecieron las siguientes observaciones del objetivo de control de criptografía, para determinar la atención requerida a este dominio de la ISO/IEC 27001.

Tabla 8. Observaciones Criptografía

Política sobre el uso de controles criptográficos.	Se hace necesario plantear una política sobre el uso de controles criptográficos en la cual se haga explicita la descripción de las especificaciones acerca de los tipos de algoritmos implementados por las diferentes herramientas gestionadas por la División, estas herramientas deben describir el mecanismo de criptografía a implementar para la protección de la información.
Gestión de claves.	Se considera necesario plantear documentación acerca del tiempo de vida de claves criptográficas.

2.6.4.7. A.11. Seguridad Física y Ambiental. Se evidenció que se realiza el establecimiento de un perímetro de seguridad de los principales dispositivos TI del amb o data center el cual almacena físicamente los equipos que almacenan información confidencial o critica, se implementan mecanismos tales como tarjetas de proximidad, tecnología biométrica para controlar el acceso físico al Data Center e instalaciones que contengan elementos de la infraestructura TI del amb.

Se evidenció que la División establece las medidas de protección de suministro de servicios públicos, se protegen de fallas de potencia y otras interrupciones causadas por fallas en los servicios públicos de soporte mediante la implementación de un mecanismo de potencia ininterrumpido UPS.

Se evidenció que se emplea el servidor de acceso Pegasys, con la implementación de la herramienta SICA, para el control de acceso físico a las instalaciones del amb por parte de terceros, se evidenció que se realiza el diseño y aplicación de procedimientos que garantizan el desarrollo de un trabajo en áreas seguras, la descripción se encuentra en la política se seguridad del amb, las áreas de despacho y carga son controladas, ubicadas a una distancia considerable del data center.

Se evidenció el control de acceso físico se lleva a cabo ubicando los equipos y protegiéndolos estratégicamente para reducir los riesgos de amenazas, peligros ambientales y las posibilidades de acceso no autorizado, se evidenció que el servicio público de soporte de potencia funciona en paralelo con un sistema de protección contra fallas eléctricas, el cableado de datos y telefónico está debidamente separado y distribuido por la empresa con su respectiva canaleta.

Se evidenció que la División lleva a cabo un plan de mantenimientos de equipos o estaciones de trabajo el cual es programado anualmente, el registro de los mantenimientos está planteado en la política de seguridad, el inventario de

hardware y software se registra en las hojas de vida de los equipos, el registro de los mantenimientos es controlado en el directorio de Gestión del Conocimiento.

Se evidenció que la División establece en la política de seguridad respecto a la instalación, traslado y configuración de computadores, elementos de red, servidores, periféricos integrados a la red solo será hecho por personal de la División, se aplican medidas de seguridad a los activos que se encuentran fuera del amb, en la política de seguridad, literal seguridad física. Los activos fuera de la empresa son respaldados por la Póliza de Daños Materiales Combinados.

Se evidenció la verificación que los equipos que almacenen información antes de su rehusó o disposición no tengan cualquier dato confidencial o software con licencia que haya sido instalado previamente, se evidenció el establecimiento de una norma que sugiere que los usuarios deben ocultar aquellos documentos o soporte de información al momento de ausentarse de su lugar de trabajo en la Política de Seguridad actual, se evidenció la Política de Seguridad donde se establece la política de escritorio limpio y pantalla limpia, el fondo y protector de pantalla deben corresponder al logo-símbolo de la imagen del amb, esta imagen será replicada por la sección se Administración de Recursos Informáticos. Se establecieron las siguientes observaciones del objetivo de control de seguridad física y ambiental, para determinar la atención requerida a este dominio de la ISO/IEC 27001.

Tabla 9. Observaciones Seguridad Física y Ambiental

Controles físicos de entrada.	Se hace necesario plantear una política sobre el uso de controles físicos de entrada.
Seguridad de oficinas, salones e instalaciones.	Se considera pertinente documentar especificaciones técnicas de las

	implementaciones respecto a la seguridad física.
Servicios públicos de soporte.	Se hace necesario la documentación de las especificaciones técnicas acerca de las medidas de protección ante interrupciones por fallas de potencia eléctrica.
Mantenimiento de equipos.	Se hace necesario el planteamiento de una política de mantenimiento de equipos formalmente.

2.6.4.8. A.12. Seguridad de las Operaciones. Se evidenció que la División de Sistemas documenta y pone a disposición de los usuarios interesados documentación de los procedimientos operativos realizados, estos procedimientos operativos son almacenados en el servidor de archivos exactamente en el Directorio de Gestión del Conocimiento.

Se evidenció que los ajustes de los procesos de negocio en las instalaciones y en los sistemas de procesamiento que afectan la seguridad de la información, son registrados en Gestión del Conocimiento, la gestión de cambios asegura la continuidad de los servicios TI.

Se evidenció que la División realiza el respectivo seguimiento al uso de los recursos y herramientas para hacer proyecciones de los requisitos de capacidad futura de herramientas y servicios, la separación de los ambientes de desarrollo, ensayo y operación se lleva a cabo parcialmente, la División separa explícitamente los ambientes de desarrollo y producción.

Se evidenció la implementación de la solución de seguridad *Kaspersky* instalado en una consola de administración, cada uno de los equipos tiene instalado un agente

de red de la solución de seguridad para la prevención detección de virus, malware y códigos maliciosos.

Se evidenció que la División realiza la copia de respaldo de la información con la herramienta *Tivoli Storage Manager*, TSM, se establece un esquema de back up compuesto por un servidor TSM, nodos clientes de producción, desarrollo y BD, también se establece una política de *backup* de respaldo a cinta: incremental diario, total quincenal, la información es almacenada en gestión del conocimiento.

Se evidenció el registro, ajuste y revisión de los eventos ejecutados en torno a la seguridad de la información, estos registros se almacenan en el servidor de gestión de archivos, los registros se eventos de la seguridad de la información se almacenan en la carpeta Bitácora.

Se evidenció que los eventos del desarrollo del Sii++ se registran mediante el control de versiones para conservar y revisar los registros de los eventos desarrollados en el sistema de información, se controlan los ajustes realizados, se evidenció la sincronización de los relojes de todos los sistemas de procesamiento de información del amb con una única fuente de referencia de tiempo, la identificación de vulnerabilidades técnicas es realizada en una matriz de riesgos corporativos, se plantea metodología para el análisis y tratamiento del riesgo MAGERIT.

Se evidenció que se realiza el registro de los procedimientos de Operación y procesos de Gestión del Sistema de Información para proteger la información de alteraciones y accesos no autorizados, estos registros se encuentran almacenados en el servidor de archivos, se implementa control de acceso físico y lógico a estos registros, se evidenció la restricción de la instalación de software, estableciendo reglamentos de instalación por parte de los usuarios, se evalúan los procesos de la División de sistemas, auditando las actividades que involucran la verificación de los servicios ti, se registran estas auditorías en *Kawak*.

Se establecieron las siguientes observaciones del objetivo de control de seguridad de las operaciones, para determinar la atención requerida a este dominio de la ISO/IEC 27001.

Tabla 10. Observaciones Seguridad de las Operaciones

Separación de los ambientes de desarrollo, ensayo y operación.	Se considera pertinente plantear la separación formal de los tres ambientes de desarrollo de forma independiente.
Copias de respaldo de la información.	Se hace necesario llevar a cabo una actualización de la política de respaldo acordada actualmente.
Gestión de las vulnerabilidades técnicas.	Se considera pertinente plantear una metodología para la gestión de vulnerabilidades de los componentes de la infraestructura ti (MAGERIT).

2.6.4.9. A.13. Seguridad de las Comunicaciones. Se evidenció la administración de la red de datos del amb mediante15 switches configurable ubicados en cuartos de comunicaciones organizados en racks, la División implementa el mecanismo de seguridad firewall SonicWall con contingencia de redundancia para la seguridad perimetral de la red de datos.

Se evidenció la segmentación de la red corporativa tanto física como lógicamente para el control del tráfico de paquetes dentro de las subredes o VLAN´s definidas aumentando el rendimiento de los servicios de red, se evidenció que la Sección de Recursos Informáticos ofrece el servicio de gestión de la red estableciendo niveles de servicios tales como la conexión a la red, la conexión e ingreso al dominio, servicio de correo, acceso al Sii++, se evidenció la determinación de los requisitos de los dispositivos de red de acuerdo a las necesidades y capacidad, se determina la disponibilidad de las herramientas y servicios ofrecidos.

Se evidenció la separación de las redes VLAN´s (redes de área local virtual) por parte de la División, esta separación desagrega grupos de trabajo por áreas o segmentos según la configuración en la topología de red establecida por la DSI del amb, estas configuraciones se documentan y almacenan en el directorio de Gestión del Conocimiento.

Se evidenció que la DSI administra un servidor de archivos y almacenamiento para compartir recursos tales como unidades de red y directorios, se asigna una cuota de usuario para cada empleado, el almacenamiento de información cual es respaldada mediante el TSM.

Se evidenció el control de las actividades de los usuarios externos del amb a fin de proteger la infraestructura TI. Esta conexión debe solicitarse mediante el formato de solicitud de requerimientos, y debe venir acompañada del acuerdo de confidencialidad conexión remota (revisión 01) debidamente firmado y autorizado.

Se evidenció que la División adquiere el servicio de correo electrónico corporativo con un tercero, el servicio externo implementa mecanismos de antiespam y antimalware para proteger apropiadamente la información transferida en los mensajes electrónicos.

Se evidenció que la División identifica, revisa regularmente y documenta el acuerdo de confidencialidad tanto con empleados internos y acuerdo de confidencialidad con terceros para la asignación, ajustes y cancelación de acceso para la protección de la información.

Se establecieron las siguientes observaciones del objetivo de control de seguridad de las comunicaciones, para determinar la atención requerida a este dominio de la ISO/IEC 27001.

Tabla 11. Observaciones Seguridad de las Comunicaciones

Controles de redes.	Se hace necesario la revisión de los contratos de mantenimiento de dispositivos de red. Llevar a cabo la actualización del esquema de la topología de red de datos del amb.
Políticas y procedimientos de transferencia de información.	Se considera pertinente el planteamiento de la política de control de comunicaciones.
Mensajes electrónicos.	Se hace necesario evaluar la solución de seguridad actual, para implementar una completa.
Acuerdos de confidencialidad o de no divulgación.	Se considera pertinente la inclusión de términos de referencia de seguridad de la información en las órdenes de prestación de servicios de acuerdo a la naturaleza del servicio.

2.6.4.10. A.14. Adquisición, Desarrollo y Mantenimiento de Sistemas. Se evidenció el establecimiento de dos procedimientos para la adquisición, desarrollo y mantenimiento de sistemas:

- Mantenimiento de soporte de aplicativos.
- Nuevos desarrollos de software.

Se evidenció la determinación de requisitos de seguridad (integridad, disponibilidad y confidencialidad) de la información para mejoras a los sistemas de información existentes o determinación de requisitos para los nuevos sistemas de información.

Se evidenció que se gestiona la información con el sistema de información se protege de la transferencia incompleta ya que es un sistema de información transaccional ERP, evitando el enrutamiento errado y la alteración no autorizada de mensajes.

Se evidenció que se lleva a cabo un procedimiento para el registro y control de cambios realizados en el Sistema de Información, se lleva a cabo un control de versiones registradas para controlar los ajustes realizados, la información que pasa sobre redes públicas en escenarios como PQR, contratación, generación de facturas por la página web del amb es protegida por mecanismos implementados por el proveedor de hosting Genesis Data.

Se evidenció el control del cambio de plataformas operativas pertinentes a los servicios y herramientas gestionadas por la División de Sistemas para que no haya impacto adverso en las operaciones o seguridad de la empresa.

Se evidenció la restricción de la DSI respecto a los cambios de paquetes de software, solo se realizan los cambios necesarios, y estos cambios son controlados, documentados y almacenados en el servidor de producción.

Se evidenció la segregación de dos entornos de programación del sistema de información, los dos ambientes se encuentran en servidores virtualizados:

- Producción
- Desarrollo

Se evidenció que el desarrollo del ERP gestionado externamente por la empresa de Software Empresarial y Sistemas Especializados SE & SE es supervisado y seguido por el interventor del contrato y los responsables del subproceso del desarrollo de aplicaciones.

Se evidenció que se realizan pruebas de seguridad de sistemas (disponibilidad, integridad y disponibilidad). Durante el desarrollo se llevan a cabo ensayos de funcionalidad de la seguridad, para los sistemas de información nuevos, actualizaciones y nuevas versiones se establecen programas de ensayo y criterios relacionados para determinar la aceptación del cambio.

Se establecieron las siguientes observaciones del objetivo de control de adquisición, desarrollo y mantenimiento de software, para determinar la atención requerida a este dominio de la ISO/IEC 27001.

Tabla 12. Observaciones Adquisición, Desarrollo y Mantenimiento de Sistemas

Seguridad de recursos der las aplicaciones en redes públicas.	Se hace necesario evaluar los mecanismos de seguridad de los servicios de las aplicaciones en las cuales pasan información sobre redes públicas.
Política de desarrollo seguro.	Nc: No se evidencia el establecimiento y aplicación de una política de desarrollo seguro para el desarrollo de software.
Procedimiento de control de cambios de sistemas.	Se considera pertinente definir el ciclo de vida del sistema de información.

2.6.4.11. A.15. Relaciones con los Proveedores. Se evidenció el establecimiento del procedimiento de manual de contratación para los vínculos con terceros y determinación de términos de referencias de las órdenes de prestación de servicios con los mismos.

Se evidenció que se determinan requisitos de la seguridad de la información en algunas órdenes de prestación de servicios según la naturaleza del servicio contratado, se incluyen requisitos de los riesgos de seguridad en la prestación de servicios asociados a la cadena de suministros de información de servicios TI.

Se evidenció la supervisión e intervención de los contratos y ordenes de prestación de servicios para el seguimiento de los servicios prestados, según en el manual de contratación del amb se asigna un interventor el cual supervisa la OPS

correspondiente, una vez finalizadas las órdenes de prestación de servicios se ajustan para el mantenimiento y la mejora de los términos de referencia, teniendo en cuenta procedimientos y controles de seguridad de la información existentes, se verifica la criticidad de la información, sistemas y procesos del negocio involucrados y la reevaluación de los riesgos.

Se establecieron las siguientes observaciones del objetivo de control de relaciones con proveedores, para determinar la atención requerida a este dominio de la ISO/IEC 27001.

Tabla 13. Observaciones Relaciones con los Proveedores

Política de seguridad de la información para las relaciones con proveedores.	Se hace necesario establecer una política de seguridad de la información para las relaciones con proveedores de infraestructura TI.
Gestión de cambios a los servicios de los proveedores.	Se considera pertinente contemplar posibles cambios a los servicios gestionados con los proveedores para incluir mantenimientos y mejoras de los términos de referencia.

2.6.4.12. A.16. Gestión de Incidentes de Seguridad de la Información. Se evidenció la asignación implícita de las responsabilidades y procedimientos para la gestión de asegurar una respuesta oportuna, eficaz y ordenada de los incidentes que se presentan.

Se evidenció que los eventos de seguridad de la infraestructura tecnológica son reportados una vez ocurren, de forma telefónica según procedimiento para help desk establecido por la DSI, los usuarios reportan las debilidades de seguridad a la

DSI mediante canales como: correo electrónico, teléfono, en algunas ocasiones por solicitudes formales establecidas por el Sistema de Gestión de Calidad del amb.

Se evidenció que los incidentes que se presentan son registrados en una Bitácora, para evidenciar el manejo de los eventos de seguridad que se han presentado y abordarlos de una mejor forma en una próxima incidencia.

Se evidenció que se documenta la solución para incidentes en el servidor de archivos en el Directorio de gestión del conocimiento, esto reduce el impacto de incidentes futuros en términos del tiempo de atención, paralelo a la gestión de los incidentes la DSI adelanta un proyecto de Mesa de Ayuda – ITIL para el manejo de los acuerdos de servicios y los respectivos escenarios de materialización y respuesta de los incidentes.

Tabla 14. Observaciones Gestión de Incidentes de Seguridad de la Información

Responsabilidades y procedimientos.	Se hace necesario establecer una política de gestión de los incidentes de la seguridad de la información para establecer formalmente responsabilidades y procedimientos.
Informe de eventos de seguridad de la información.	Se considera pertinente realizar una clasificación de eventos que afecten la seguridad de la información. Proyecto Mesa de Ayuda - ITIL.
Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	Nc: No se evidencia la clasificación ni de eventos ni de incidentes de seguridad.
Recolección de evidencia.	Se hace necesario plantear una cadena de custodia de forma oficial en términos de la seguridad informática.

2.6.4.13. A.17. Gestión de la Continuidad de Negocio. Se evidenció que se realiza la planificación de la continuidad de la seguridad de la información, se formaliza en el Plan de Contingencia con Redundancia para garantizar la disponibilidad, integridad y confiabilidad del servicio del sistema de información Sii++, este mecanismo se implementa a partir de un software de virtualización VMWARE de alta disponibilidad el cual proporciona una réplica del servidor de producción en caso de fallas del servidor principal, los datos se almacenan en una infraestructura de redundancia física para Storage.

Se evidenció la determinación de los mecanismos para controlar la continuidad del servicio de Gestión de Sistemas de Información en el amb, se verifica, revisa y evalúa la Continuidad debido a la planificación formal de la implementación de esta misma, se registran las pruebas realizadas del plan de contingencia.

Se evidenció que se cuenta con la disponibilidad de instalaciones de procesamiento de información, se implementan instalaciones de procesamiento con redundancia suficiente para cumplir los requisitos de disponibilidad.

2.6.4.14. A.18. Cumplimiento. Se evidenció la identificación, documentación y cumplimiento de la legislación referente a la protección de la información y datos, Ley 1581 octubre 17 de 2012, se evidencia el enfoque de la protección de datos manejados por el sistema de información e infraestructura tecnológica, política de seguridad acto de Gerencia n° 012 de octubre de 2014.

Se evidenció la implementación de los procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software licenciados según la ley 23 de 1982 sobre derechos de autor.

Se evidenció que los registros se protegen contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, ya que se almacenan en el servidor de archivos. Se implementan mecanismos de seguridad de acceso físico y lógico a los registros para garantizar su protección.

Se evidenció la identificación, documentación y cumplimiento parcial de la legislación referente a la protección de la información y datos, ley 1581 octubre 17 de 2012 según el congreso de la república, la política de seguridad de la información establece el compromiso parcial, organización y publicación para el cumplimiento de esta misma, de igual forma el amb mantiene protegidos sus activos de información, se plantean mecanismos de seguridad que se revisan independientemente, herramientas, servicios, acuerdos, políticas y procedimientos.

Se evidenció que las actividades de adquisición y compra de infraestructura TI son verificadas por la Contraloría General de la Republica.

Se establecieron las siguientes observaciones del objetivo de control de cumplimiento, para determinar la atención requerida a este dominio de la ISO/IEC 27001.

Tabla 15. Observaciones de Cumplimiento

Reglamentación de controles criptográficos.	Se hace necesario plantear la política de controles criptográficos, se hace la primera aproximación en el Manual de Políticas de la seguridad de la información.
Cumplimiento con las políticas y normas de seguridad.	Se considera pertinente establecer explícitamente los responsables del contexto de la seguridad de la información para continuar con el trabajo del Sistema de Gestión de la Seguridad de la Información SGSI.

2.6.5. Análisis diferencial. Se realizó la comparación del estado de la gestión de la Seguridad de la Información en el amb teniendo como punto de comparación y marco de trabajo la norma ISO/IEC 27001:2013.

Este mecanismo permite evaluar el estado actual del contexto de la seguridad de la información en el amb y realizar las recomendaciones se propuso un análisis de brecha o gap.

Esté análisis permitió analizar información pertinente a la gestión de la seguridad de la información en términos de los objetivos de control del anexo A, fue realizado para evaluar el esfuerzo, tiempo, dinero y recursos humanos requeridos para la implementación de la gestión de la seguridad de la información y mejoras en el amb.

Se llevó a cabo la evaluación de los Objetivos de Control planteados en el anexo A de la norma con un modelo establecido, se definen tres estados

- **Implementado,**
- **Parcialmente implementado,**
- **No implementado.**

Estos estados representan cualitativa y cuantitativamente una aproximación del trabajo adelantado por el amb en términos de la Seguridad de la Información, resumido de la siguiente forma se tiene en cuenta la valoración de los procesos presentados en la gráfica radial del análisis GAP.

Se concluye que el análisis de brecha realizado se basa en contrastar el “estado de la situación actual” y el “estado esperado o ideal”. Las diferencias entre ambas situaciones suponen los escenarios en los cuales se debe trabajar para que la brecha sea eliminada.

Figura 8. Análisis GAP

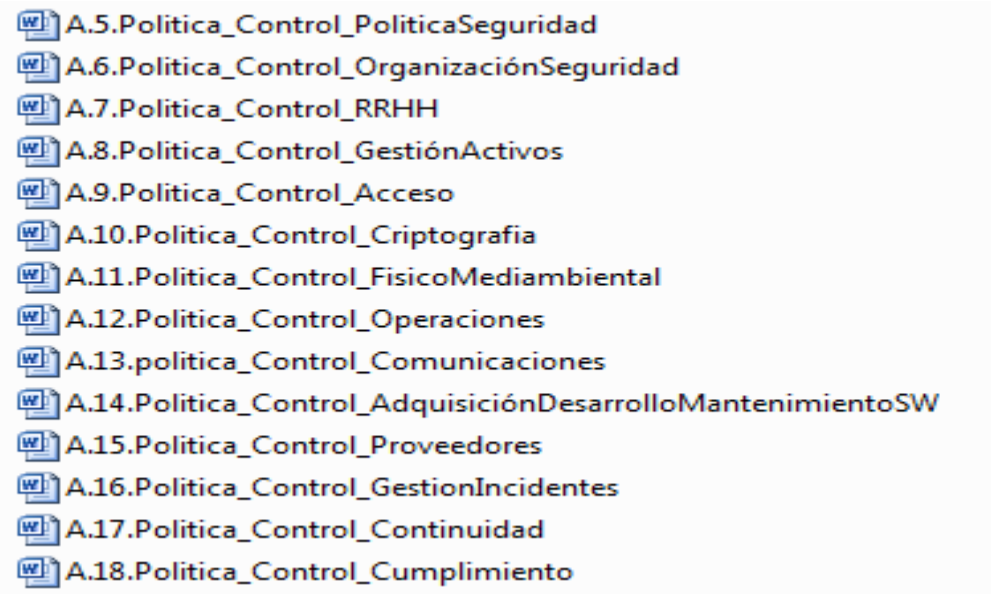
2.6.6. Manual de Políticas de la seguridad de la información. Paralelo a la ejecución de la Auditoria Interna Diagnóstica y el análisis GAP se elaboró un adelanto en uno de los componentes indispensables para la construcción y seguimiento de un Sistema de Gestión de la Seguridad de la Información en el amb, se describe la aproximación inicial de los documentos que describen las políticas y normas de seguridad de la información definidas para el amb, se toma como base leyes y regulaciones aplicables y respectivas recomendaciones del estándar ISO/IEC 27001:2013.

Las estructuras de las políticas del manual se plantearon de acuerdo a como se estructuran los objetivos de control en la Norma Técnica Colombiana ISO/IEC 27001:2013.

En cumplimiento a los diferentes Objetivos de Control del Anexo A de la NTC ISO/IEC 27001 respecto al establecimiento de una política que haga referencia a

cada dominio, se adelantó la aproximación del manual de políticas de seguridad de la información como valor agregado al proyecto realizado, se realizó en conjunto con el jefe de la División de Sistemas, el Administrador de Recursos Informáticos y el Profesional de apoyo del proyecto.

Figura 9. Estructura Manual de Políticas de la Seguridad de la Información



Este Manual de Políticas de Seguridad de la Información se propone como la siguiente versión de lo que actualmente el amb establece como acto de gerencia 012 el cual hace referencia a su política de seguridad.

3. GESTIÓN Y TRATAMIENTO DEL RIESGO

3.1. INTRODUCCIÓN DE LA METODOLOGÍA

La Gestión y tratamiento del riesgo es una de las principales actividades planteadas en la NTC-ISO/IEC 27001:2013, esta Gestión permitió identificar la acción de gestión apropiada frente a las amenazas a las cuales se ven enfrentados los activos de información administrados por la División de Sistemas de Información del amb.

La gestión y tratamiento del riesgo permitió clasificar de forma general los recursos, responsabilidades y prioridades para manejar los riesgos de seguridad de la información. De la misma forma se establecerán prioridades para lograr los objetivos de control identificados en el documento de Declaración de Aplicabilidad (*Statement of Aplicability*, SoA), considerando la asignación de funciones debido a los riesgos que representa la administración de los activos de información en la División de Sistemas del amb.

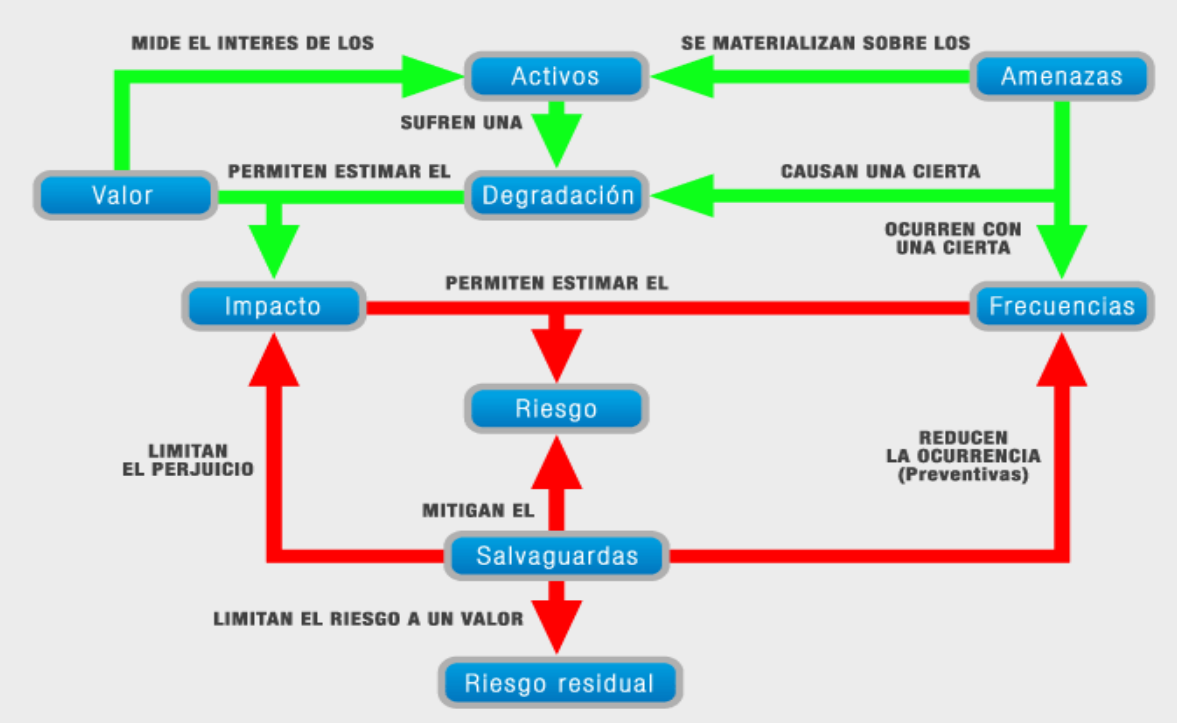
Se planteó la Implementación de MAGERIT: Metodología para el Análisis de Sistemas de Información y Gestión de Riesgos elaborada por el Consejo Superior de Administración Electrónica de España, esta metodología ofrece un enfoque sistemático para el análisis de los riesgos derivados del uso de las tecnologías de información y telecomunicaciones.

Se consideró la realización del ejercicio práctico ya que está dirigido a los medios electrónicos, informáticos y telemáticos, su uso en la actualidad es frecuente al momento de la Gestión, Análisis y tratamiento del riesgo de los activos de información.

Este proceso de análisis y gestión de riesgos de los principales activos que componen la infraestructura TI del amb, dentro del contexto de un SGSI - preliminar y teniendo como marco de trabajo la NTC-ISO/IEC 27001:2013, se pretende sensibilizar la Gestión de Riesgos y Seguridad de la Información a nivel de empresa.

Como principal eje de la propuesta del Análisis y Gestión de riesgos se utilizó el marco referencial MAGERIT (Metodología de Análisis y Gestión de Riesgos de Tecnologías de Información), denominada como una buena alternativa para el Análisis de Riesgos, el principal argumento de ser de MAGERIT está directamente relacionado con el análisis del riesgo y uso de los activos TI.

Figura 10. Metodología MAGERIT



Fuente: WIKISPACES, Seguridad Informática UFPS, Bogotá 2012.

Está Metodología da lugar al análisis de las amenazas frente a activos TI, inicialmente identificando las amenazas para el respectivo análisis de índices

respecto a la frecuencia de incidencia y el impacto que sufren los activos, la metodología plantea la identificación de salvaguardas o controles, se verificó el riesgo intrínseco y el riesgo residual para determinar en qué escenarios de la seguridad de la infraestructura TI de la empresa se deben implementar salvaguardas para evitar la materialización de las amenazas.

3.2. DESCRIPCIÓN DE LA METODOLOGÍA

1. Se realizó el establecimiento de parámetros y convenciones para realizar la respectiva valoración de los activos e índices de amenazas, riesgo e impacto.
2. Se identificaron los principales activos que conforman la infraestructura TI del amb y su respectiva clasificación general, estos activos son administrados por la División de Sistemas de Información.
3. Se verificó la valoración cuantitativa que merece cada uno de los activos de la infraestructura TI seleccionados.
4. Se identificaron las amenazas más representativas de acuerdo a la naturaleza de los activos de infraestructura TI seleccionados.
5. Se valoraron las amenazas en términos de frecuencia de ocurrencia.
6. La incidencia o materialización de las amenazas causan cierta degradación, se determinó el impacto sobre los activos previamente identificados.
7. Se realizó el cálculo del riesgo intrínseco, el cual hace referencia al riesgo sin implementación de controles al que se encuentran expuestos los activos de infraestructura TI analizados. Se identifican parcialmente elementos de la SoA de acuerdo a valor de riesgo intrínseco aceptable.
8. Se identificaron las salvaguardas existentes y controles posibles a implementar, se valora la eficacia de la implementación actual.
9. Se realizó el cálculo del riesgo residual, es aquel que se determina en un escenario de implementación de salvaguardas o controles para proteger los activos de la infraestructura TI analizados.

10. Se realizó el análisis del riesgo intrínseco o inherente: Sin implementación de salvaguardas y el riesgo residual o efectivo: Con implementación de Salvaguardas planteados.
11. Se determinaron las conclusiones a partir de la interpretación de los resultados arrojados por MAGERIT.

Luego que se determinó el riesgo intrínseco y el riesgo residual se verificó la eficacia de la implementación de las diferentes salvaguardas planteados durante la ejecución de la metodología, para determinar la asignación de recursos y propuesta de diferentes proyectos para la mejora del contexto de la seguridad de la información en el amb y después de llevarse a cabo la elección de una estrategia para mitigar el impacto y riesgo MAGERIT se planteó que para la implementación de la metodología se analizaron dos grandes momentos:

3.3. ANÁLISIS DE RIESGO

Permitió determinar que activos de información propios tiene la empresa y que podría pasar si se materializa alguna amenaza. Para ello se toma en consideración el siguiente esquema:

1. -Primero se identificaron los activos de infraestructura TI a tratar y se realizó una clasificación de forma macro para determinar la valoración que merecen.
2. -Se identificaron las amenazas significativas sobre los activos identificados y valorarlas en términos de frecuencia de ocurrencia (Vulnerabilidad) y degradación (Impacto) que causan sobre el valor del activo afectado.
3. –Se llevó a cabo la Identificación de las salvaguardas existentes y aquellas las cuales se pueden implementar, lo anterior para determinar y valorar la eficacia de su implementación.
4. –Se estimó el impacto y el riesgo al que están expuestos los activos del sistema.
5. -Interpretar el significado del riesgo intrínseco.

3.4. GESTIÓN DEL RIESGO

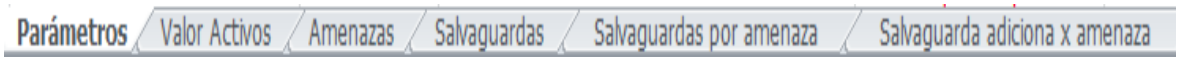
Se realizó la estructuración de las acciones de seguridad para satisfacer las necesidades detectadas por el análisis. Comprendió las actividades:

1. Se determinaron las salvaguardas oportunas para el objetivo anterior.
2. Se estableció la disminución de la frecuencia de ocurrencia y la disminución del impacto luego de la posible implementación de los controles o salvaguardas.
3. Se llevó a cabo el cálculo del riesgo residual, en este escenario de implementación de controles.
4. Se analizaron los resultados del riesgo intrínseco y el riesgo residual calculado para la asignación de esfuerzos y recursos para mejorar aspectos de la seguridad de la información.
5. Se determinó parcialmente la Declaración de Aplicabilidad SoA con base en la metodología y sus resultados arrojados.

3.5. EJECUCIÓN DE LA METODOLOGÍA MAGERIT

La ejecución de la metodología se llevó a cabo en un documento Excel el cual tiene una estructura planteada a continuación (**Figura 11**) explicada más adelante; la estructura del documento permite ingresar los datos respectivamente para la ejecución del análisis y tratamiento del riesgo mediante Magerit:

Figura 11. Estructura de la Metodología



3.5.1. Establecimiento de Parámetros. Se realizó el establecimiento de parámetros y convenciones para realizar la respectiva valoración cualitativa y cuantitativa para el respectivo desarrollo de la metodología, estos parámetros definen las escalas utilizadas para el análisis de los diferentes índices utilizados por la metodología de análisis y tratamiento del riesgo.

Los parámetros que deben identificarse serán:

3.5.1.1. Valor de los Activos. Se llevó a cabo la asignación de la valoración económica de los activos de infraestructura TI analizados, en esta valoración se tiene en cuenta el valor aproximado que representan los activos para la empresa al momento de su adquisición, es decir no hace referencia al valor comercial actual de los activos.

Se utilizó una escala de valores: muy alto, alto, medio, baja; a cada rango se le asignó un valor económico:

Tabla 16. Costos de los Activos

Tabla Costo de los Activos		
MA	Muy alto	2.100.000.000
A	Alto	300.000.000
M	Medio	72.000.000
B	Bajo	4.000.000

3.5.1.2. Frecuencia de Ocurrencia de las Amenazas. Se determinó la frecuencia con la que la empresa puede verse enfrentada a la materialización de una amenaza. Se llevó a cabo el planteamiento de una escala de valores los cuales son calculados de acuerdo a la probabilidad de ocurrencia en los 365 días de un año civil, la estimación de la frecuencia de ocurrencia es asignada según la información a continuación:

Tabla 17. Vulnerabilidad de las Amenazas

			Frecuencia de Ocurrencia de las amenazas
EF	Extremadamente frecuente	365/365=1	1 vez al día
MF	Muy Frecuente	26/365=0,071	1 vez cada 2 semanas
F	Frecuente	6/365=0,016	1 vez cada 2 meses
FN	Frecuencia Normal	2/365=0,005	1 vez cada 6 meses
PF	Poco Frecuente	1/365=0,003	1 vez al año

3.5.1.3. Impacto. De igual forma se estableció la relación del impacto o porcentaje del valor del activo que se pierde (degradación) en el escenario donde se materialice una amenaza está determinado según la siguiente escala:

Tabla 18. Degradación de los Activos

Tabla Degradación de los activos (Impacto)		
A	Alta	90
M	Media	50
B	Baja	10

3.5.1.4. Costos de Salvaguardas. Se llevó a cabo la asignación de la valoración económica de los salvaguardas implementadas o propuestas, en esta valoración se tiene en cuenta el valor aproximado que representan los salvaguardas para la empresa.

Se utilizó una escala de valores: muy alto, alto, medio, baja; a cada rango se le asigna un valor económico.

Tabla 19. Costos de Salvaguardas

Tabla Costo de Salvaguardas		
MA	Muy alto	100.000.000
A	Alto	30.000.000
M	Medio	10.000.000
B	Bajo	3.000.000

3.5.1.5. Efectividad del Control de Seguridad. La mejora o implementación de

salvaguardas representaran una influencia ante los riesgos detectados, se calculó de qué forma se reduce el riesgo identificado, estableciendo unos niveles de efectividad.

Tabla 20. Disminución de la Vulnerabilidad e Impacto

Tabla Disminución Vulnerabilidad		
A	Alta	90
M	Media	60
B	Baja	30

Tabla Disminución del Impacto		
A	Alto	90
M	Medio	60
B	Bajo	30

Se aclara que los parámetros establecidos deben ser utilizados tal y como se definen anteriormente para el entendimiento de ejecución de la metodología ejecutado verificar la metodología según la bibliografía citada.

3.5.2. Análisis de Activos. Se identificaron los activos pertinentes y más relevantes de la infraestructura TI gestionada por la División de Sistemas de Información del amb.

Para el inventario de activos se realizó el planteamiento y adaptación en base a lo sugerido por la metodología de análisis de riesgos MAGERIT, se realizó la clasificación en dos conjuntos de forma Macro de los elementos identificados:

1. **Activos Hardware**
2. **Activos Software**

3.5.2.1. Costos de Activos. Los valores en COP hacen referencia al valor de los activos para la empresa al momento de su adquisición, se estiman estos valores de forma aproximada según la información suministrada por profesionales del amb abstraídas del inventario de los activos de infraestructura TI más relevantes.

Los activos de la infraestructura TI del amb seleccionados fueron clasificados de forma general de acuerdo al grado de importancia de los activos, se tienen en

cuenta solo los activos más relevantes al momento de administrar los recursos informáticos en la empresa.

Tabla 21. Costos Activos Hardware

Código	Nombre	Valor COP
1	Servidores	179.044.581
2	Elementos de Red: Switch, Routers, Firewall	317.578.540
3	Almacenamiento y *BackUp*s de Respaldo	37.545.700

Valor Activos Hardware:

$ 534.168.821

	Activos	Valor COP
Servidores	Servidor telefonía ip	2.080.000
	Servidor IBM 3650m2	20.255.481
	Servidor IBM 3250m2	7.987.798
	storage DS3400	25.388.562
	Servidor t110	3.504.859
	Servidor IBM x 3250 (licencias)	1.859.714
	Servidor x 3650M4, storage ds3524, garantía extendida.	77.900.000
	Disco Duro IBM 450GB	1.543.021,56
	Disco Duro IBM 450GB	1.543.021,56
	Disco Duro IBM 450GB	1.543.021,56
	Disco Duro IBM para servidor	468.087
	Disco Duro IBM para servidor x series 345	546.802
	Memoria cache 1GB para ds 3000	2.084.114
	Memoria cache 1GB para ds 3000	2.084.114
	Memoria de 2GB	675.990
	Memoria de 2GB	675.990
	Memoria de 4GB	983.805
	Memoria de 4GB	983.805
	Servidor t110	3.504.859
	Unidad tape ts2900 LT05	13.545.700
	2 baterías de memoria para ds3000	4.901.500
	2 memorias para servidor 3650M4	1.220.320
	5 memorias para servidor 3650 M2	3.050.800
	Batería para memoria cache de storage	713.21

	Activos	Valor COP
Elementos de Red: Switch, Routers, Firewall	sonic wall de alta disponibilidad	8.615.600
	sonicwall sonicpoint	1.348.448
	sonicwall sonicpoint	1.646.500
	soporte firewall (3años), sonic wall con servicio de soporte	18.092.200
	equipo sonic wall alta disponibilidad incluye licencia	26.707.800
	switch 24 puertos	5.400.000
	switch 3COM E4800 24 puertos	5.397.400
	switch compatible con el servidor de voz ip	2.100.000
	switch de 48 puertos	13.610.280
	switch de 48 puertos	13.610.280
	switch de 48 puertos	13.610.280
	switchs para actualizacion de red	77.461.152,00
	switchs,fibra,transceiver	114.602.600
	switchs,fibra,transceiver, patchcord	14.086.000
	transceiver switch	1.290.000

	Activos	Valor COP
Sistema de Almacenamiento y *BackUps* de Respaldo	Unidad tape ts2900 LT05 - Lectora de cintas.	13.545.700
	Cintas LTO 5 30 unidades, en custodia 259 unidades.	6.400.000
	Contrato de Custodia de Medios de respaldo - MTI (2 años).	17.600.000

Tabla 22. Costos Activos Software

Código	Nombre	Valor COP
4	SII - ERP	400.000.000
5	Aplicaciones	218.135.880
6	Licencias	119.680.691
7	Servicios	270.500.000

Valor Activos Sotfware:

$ 1.008.316.571

	Activos	Valor COP
Aplicaciones: Servidor 172.16.1.29	Kawak	25.000.000
	Sistema Plantas de Tratamiento	12.000.000
	Taquilla	34.887.136
	Gestión documental	146.248.743

	Activos	Valor COP
SII - ERP	Programas Fuentes SII, Tablas SII	400.000.000

	Activos	Valor COP
Servicios	Departamentalización impresión	249.000.000
	Correo Electrónico	7.800.000
	Internet	4.000.000
	Custodia de Medios de respaldo - MTI	8.800.000
	Hosting - Servidor web	4.900.000

	Activos	Valor COP
Licencias	licencias discovery(270)	3.700.000
	licencias tiboli storage manager	29.076.977
	licencias windows server call 2012(310)	15.623.000
	licencias windows server DATA CENTER 2012(2)	18.863.000
	licencias windows server estándar 2012 (1)	1.347.000
	lincencias vmware 5.1 (1)	17.160.000

	Servidor IBM x 3250 (licencias)	1.859.714
	1 licencia ads version 11, licenciamiento para 250 usuarios, 1 licencia ads para desarrolladores (10 usuarios)	22. 044.000
	1 licencia alaska software professional suscription version 1.9 para cuatro desarrolladores	18.000.000
	antivirus *kaspersky*	14.051.000

3.5.3. Amenazas y Frecuencia de Ocurrencia. El proceso de identificación del riesgo es permanente e interactivo y se encuentra soportado en los objetivos del plan estratégico del amb.

En la etapa de identificación de amenazas, corresponde aplicar un criterio crítico, amplio y sistemático para la identificación de los riesgos potenciales. En la identificación de las amenazas se deben incluir la mayoría de los riesgos, estén o no bajo control de la organización. Los enfoques utilizados para identificar riesgos incluyen “checklist”, juicios basados en la experiencia y en los registros de incidencias de los procesos analizados. El enfoque utilizado dependerá de la naturaleza de las actividades bajo revisión y los tipos de riesgos.

De acuerdo a la caracterización del proceso de Sistemas de Información del amb y el inventario de activos se detalló un listado de las principales amenazas a considerar en el ámbito del análisis de riesgos propios de la infraestructura TI del amb.

Se trata de un consolidado del catálogo de amenazas propuesto por MAGERIT y adaptadas a las amenazas propias de la empresa, se identificó y planteó una clasificación de las amenazas para los activos software y los activos hardware propuestos anteriormente, se estableció la identificación de las amenazas, realizando convenciones de la siguiente forma:

HA: Amenaza Hardware; **SA**: Amenaza Software.

Tabla 23. Amenazas Activos Hardware

Amenaza	
HA1	Descargue completo de UPS debido a perdida de suministro de Energía Eléctrica.
HA2	Fuego, Daños por agua, desastres naturales.
HA3	Alteración en el esquema de virtualización debido a una falla humana.
HA4	Elemento de red no funciona (Switches, access point, cableado…)
HA5	Sistema de respaldo no funciona.
HA6	Unidad de aire acondicionado dañado Data Center.
HA7	Sabotaje Físico de Servidores desde afuera.
HA8	Límite de Vida Útil activos hardware.
HA9	No se realiza el tratamiento específico de los riesgos de infraestructura TI.

Tabla 24. Amenazas Activos Software

Amenaza	
SA1	No disponibilidad de algún archivo que compone el ERP. (tablas)
SA2	Perdida de integridad información del ERP, liberación de programas del ERP con errores.
SA3	Abuso de confianza respecto a la manipulación de la información para beneficio propio.
SA4	Cantidad de licencias de usuario (cal Windows server 2012, *Kaspersky*...) para instalar limitadas.
SA5	Desactualización de programas a su última versión, obsolescencia software.
SA6	Borrado o modificación de los programas fuentes de las aplicaciones. Sabotaje lógico.
SA7	Acceso no autorizado a la Información del servidor de archivos.
SA8	Difusión de software dañino, instalación de software no licenciado.
SA9	Fuga de información- Terceros

Seguido a esto se determinó la incidencia o materialización de las amenazas para determinar la degradación sobre los activos. Se llevó a cabo el análisis de amenazas y cálculo del Riesgo Intrínseco, este hace referencia al riesgo al cual se ven enfrentados los activos sin la implementación de ninguna salvaguarda o control.

Ecuación 1 Riesgo Intrínseco

$$(Riesgo\ Intrínseco = Valor\ Activos * Vulnerabilidad * (Impacto/100))$$

Fuente: GR2DEST, Metodología de Análisis de Riesgos: MAGERIT, 2014

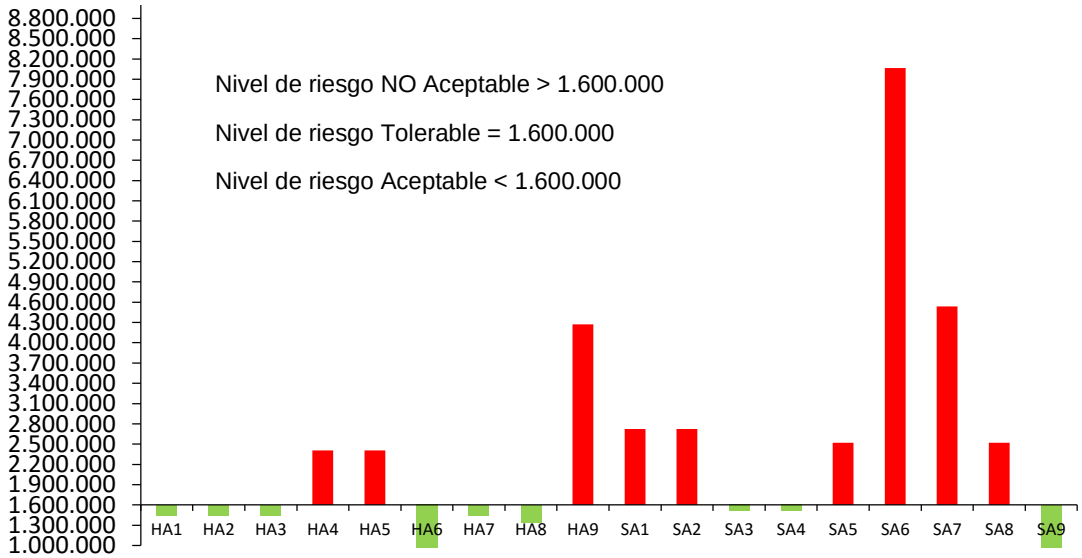
Así mismo los resultados obtenidos son revisados por la Dirección del proyecto para establecer un nivel de riesgo intrínseco aceptable por debajo de **$1.600.000**, por lo tanto, aquellas amenazas cuya materialización represente un monto igual o superior a este valor han sido seleccionadas para formar parte parcial de la Declaración de Aplicabilidad (Statement of Applicability – SoA).

Lo anterior sirvió para realizar una primera aproximación al diseño e implementación de salvaguardas o controles.

Esto permitió categorizar e identificar las principales amenazas que deben ser revisadas debido a su alto riesgo intrínseco, la vista de los resultados determinó un nivel de riesgo intrínseco aceptable establecido por la dirección del proyecto dispuestos a tolerar, de tal forma que por debajo de este nivel el riesgo es aceptable y por encima de este valor aceptable se deberá tomar decisiones en el planteamiento e implementación de controles.

Del ejercicio práctico de la metodología y el cálculo del riesgo intrínseco se obtuvo como resultado una lista de los riesgos correspondientes a los posibles impactos en caso de que se materialicen las amenazas a las que están expuestos los activos en mayor proporción.

Figura 12 Análisis del Riesgo Intrínseco



El análisis de riesgo en una siguiente fase debe determinar si el riesgo no aceptable debe considerarse en términos de ser:

- **Transferirlo:** Seguros, garantías, pólizas.
- **Eliminarlo:** No tiene mucha viabilidad debido a que equivale la eliminación del activo.
- **Mitigarlo:** Reducción del riesgo, aplicando controles de seguridad, es una de las opciones más gestionadas en el análisis de riesgos.
- **Asumirlo:** Se acepta el riesgo y se determina que no se puede hacer nada para la amenaza.

Tabla 25. Vulnerabilidad e Impacto sobre los Activos Hardware

Código	Amenaza	Vulnerabilidad		Impacto		Riesgo Intrínseco
HA1	Descargue completo de UPS debido a perdida de suministro de Energia Electrica.	PF	0,003	A	90	1.442.256

HA2	Fuego, Daños por agua, desastres naturales.	PF	0,003	A	90	1.442.256
HA3	Alteración en el esquema de virtualización debido a una falla humana.	PF	0,003	A	90	1.442.256
HA4	Elemento de red no funciona (Switches, access point, cableado…)	FN	0,005	A	90	2.403.760
HA5	Sistema de respaldo no funciona.	FN	0,005	A	90	2.403.760
HA6	Unidad de aire acondicionado dañado Data Center.	PF	0,003	M	50	801.253
HA7	Sabotaje Fisico de Servidores desde afuera.	PF	0,003	A	90	1.442.256
HA8	Límite de Vida Útil activos hardware.	FN	0,005	M	50	1.335.422
HA9	No se realiza el tratamiento específico de los riesgos de infraestructura TI.	F	0,016	M	50	4.273.351
				TOTAL		16.986.569

Tabla 26. Vulnerabilidad e Impacto sobre los Activos - Software

Código	Amenaza	Vulnerabilidad		Impacto		Riesgo Intrínseco
SA1	No disponibilidad de algún archivo que compone el ERP. (tablas)	PF	0,003	A	90	2.722.455
SA2	Perdida de integridad información del ERP, liberación de programas del ERP con errores.	PF	0,003	A	90	2.722.455
SA3	Abuso de confianza respecto a la manipulación de la información para beneficio propio.	PF	0,003	M	50	1.512.475
SA4	Cantidad de licencias de usuario (cal Windows server 2012, *Kaspersky*...) para instalar de forma limitada.	PF	0,003	M	50	1.512.475
SA5	Desactualización de programas, obsolescencia software.	FN	0,005	M	50	2.520.791

SA6	Borrado o modificación de los programas fuentes de las aplicaciones. Sabotaje lógico.	F	0,016	M	50	8.066.533
SA7	Acceso no autorizado a la Información del servidor de archivos.	FN	0,005	A	90	4.537.425
SA8	Difusión de software dañino, instalación de software no licenciado.	FN	0,005	M	50	2.520.791
SA9	Fuga de información-Terceros	PF	0,003	B	10	302.495
				TOTAL		26.417.894

3.5.4. Planteamiento de Salvaguarda. Se identificaron y seleccionaron las posibles mejores o soluciones, es decir se documentan las salvaguardas ya implementadas y las propuestas para reducir las amenazas identificadas, se realizó la estimación del costo promedio de forma aproximada de cada uno de las salvaguardas y se asigna la magnitud según corresponda. Se realizó una correspondencia de tal forma que para cada una de las amenazas identificadas exista una salvaguarda para mitigar el impacto.

Tabla 27. Medidas de Seguridad y Controles - Hardware

Medidas de Seguridad / Controles
Mejoras de la Implementación de la UPS, Protocolo para el Apagado y Encendido de Servidores.
Servicio de réplica a un Data Center Alterno (Permitiendo la continuidad del negocio en caso de desastres naturales.), PRD (Plan de Recuperación de Desastres).
Tecnología y Herramienta para realizar el back up que genera las imágenes o copias de seguridad de los servidores virtualizados. vSphere Data Protection del vMware.
Contrato de Mantenimiento Correctivo y Preventivo elementos de red (Garantía para cambio de partes), Actualización planos de la infraestructura de red del amb, condiciones ambientales adecuadas para los dispositivos de red.

Mantenimiento Preventivo y Correctivo de los elementos que componen el esquema de Back Up, Mejoras y actualizaciones del esquema de back up implementado actualmente TSM.
Contrato de Mantenimiento Correctivo y Preventivo de la unidad de aire acondicionado del Data Center.
Redundancia de Servidor (Servidor de Contingencia), Plan de contingencia.
Renovación Tecnológica de hardware
Mejora del Análisis del riesgo transición al tratamiento especializado del riesgo de infraestructura TI MAGERIT.

Tabla 28. Medidas de Seguridad y Controles - Software

Medidas de Seguridad / Controles
Mejora de los controles Físicos y de Accesos lógicos a los archivos del Sistema Información Integrado, mecanismo de respaldo implementado.
Definición formal del ambiente de pruebas de programación del sistema de información y hacer un plan de pruebas antes de liberar un cambio del SII++, registro bitácora de errores de programación.
Constante revisión a las restricciones de los usuarios del sistema mediante la creación y mejoras de los perfiles (plantillas), política de seguridad de la información.
Administración de licenciamiento para proyectar la capacidad de licencias necesarias para soporte de los procesos.
Actualización de las herramientas instaladas, Windows Server Update Services. WSUS
Mejoras de los controles de acceso lógico para limitar el acceso de los servidores que contienen los programas fuentes de las aplicaciones.
Compartir carpetas con acceso restringido.
Implementación de herramienta de seguridad completa - Opciones del Directorio activo.
Controles criptográficos para aumento de confidencialidad de la información manipulada y transferida por terceros.

Se llevó a cabo la asignación del costo aproximado de las salvaguardas planteadas, se estructura en la siguiente tabla donde se define para cada amenaza identificada una salvaguarda ya establecida o propuesta.Se estableció la identificación de las salvaguardas, realizando convenciones de la siguiente forma: **HS**: Salvaguarda Hardware; **SS**: Salvaguarda Software.

Tabla 29. Asignación Costos de Salvaguardas - Hardware

	COD HS	*Medidas de Seguridad / Controles*	Costo	Costo Unitario
HA1	HS1	Mejoras de la Implementación de la UPS, Protocolo para el Apagado y Encendido de Servidores.	A	35.000.000
HA2	HS2	Servicio de réplica a un Data Center Alterno (Permitiendo la continuidad del negocio en caso de desastres naturales.), PRD (Plan de Recuperación de Desastres).	MA	100.000.000
HA3	HS3	Tecnología y Herramienta para realizar el back up que genera las imágenes o copias de seguridad de los servidores virtualizados. vSphere Data Protection del vMware.	A	30.000.000
HA4	HS4	Contrato de Mantenimiento Correctivo y Preventivo elementos de red (Garantía para cambio de partes), Actualización planos de la infraestructura de red del amb, condiciones ambientales adecuadas para los dispositivos de red.	B	5.000.000
HA5	HS5	Mantenimiento Preventivo y Correctivo de los elementos que componen el esquema de Back Up, Mejoras y actualizaciones del esquema de back up implementado actualmente TSM.	B	5.000.000
HA6	HS6	Contrato de Mantenimiento Correctivo y Preventivo de la unidad de aire acondicionado del Data Center.	B	5.000.000
HA7	HS7	Redundancia de Servidor (Servidor de Contingencia), Plan de contingencia.	A	50.200.000
HA8	HS8	Renovación Tecnológica de hardware	A	50.000.000
HA9	HS9	Mejora del Análisis del riesgo transición al tratamiento especializado del riesgo de infraestructura TI MAGERIT.	M	10.000.000
		Total de Salvaguardas Hardware:		290.200.000

Tabla 30. Asignación Costos de Salvaguardas - Software

	COD SS	*Medidas de Seguridad / Controles*	Costo	Costo Unitario
SA1	SS1	Mejora de los controles Físicos y de Accesos lógicos a los archivos del Sistema Información Integrado, mecanismo de respaldo implementado.	M	10.000.000
SA2	SS2	Definición formal del ambiente de pruebas de programación del sistema de información y hacer un plan de pruebas antes de liberar un cambio del SII++, registro bitácora de errores de programación.	M	40.000.000

	COD SS	Medidas de Seguridad / Controles	Costo	Costo Unitario
SA3	SS3	Constante revisión a las restricciones de los usuarios del sistema mediante la creación y mejoras de los perfiles (plantillas), política de seguridad de la información.	M	10.000.000
SA4	SS4	Administración de licenciamiento para proyectar la capacidad de licencias necesarias para soporte de los procesos.	B	5.000.000
SA5	SS5	Actualización de las herramientas instaladas, Windows Server Update Services. WSUS	B	5.000.000
SA6	SS6	Mejoras de los controles de acceso lógico para limitar el acceso de los servidores que contienen los programas fuentes de las aplicaciones.	M	10.000.000
SA7	SS7	Compartir carpetas con acceso restringido.	M	10.000.000
SA8	SS8	Implementación de herramienta de seguridad completa - Opciones del Directorio activo.	M	15.000.000
SA9	SS9	Controles criptográficos para aumento de confidencialidad de la información manipulada y transferida por terceros.	M	20.000.000
		Total de Salvaguardas Software:		125.000.000

Se relacionó cada amenaza con su respectivo control o salvaguarda y se realizó la correspondencia de la amenaza identificada con el respectivo control planteado de acuerdo a los conceptos de los interesados en el proyecto, se asigna un valor cuantitativo y cualitativo de disminución de la vulnerabilidad o frecuencia de ocurrencia y magnitud de disminución del impacto o deterioro por cada salvaguarda asignado, esto se realizó de acuerdo a la clasificación establecida.

Estos valores son asignados de acuerdo a los registros de los eventos de incidentes en el amb, lo anterior se realiza teniendo en cuenta el tratamiento del riesgo corporativo realizado actualmente.

Tabla 31. Disminución de Vulnerabilidad e Impacto - Hardware

Amenaza	Control	Dism. Vulnerabilidad		Dism. Impacto	
HA1	HS1	A	90	M	60
HA2	HS2	B	30	M	60

Amenaza	Control	Dism. Vulnerabilidad		Dism. Impacto	
HA3	HS3	B	30	A	90
HA4	HS4	M	60	M	60
HA5	HS5	M	60	M	60
HA6	HS6	M	60	M	60
HA7	HS7	A	90	A	90
HA8	HS8	B	30	M	60
HA9	HS9	M	60	A	90

Tabla 32. Disminución de Vulnerabilidad e Impacto – Software

Amenaza	Control	Dism. Vulnerabilidad		Dism. Impacto	
SA1	SS1	A	90	M	60
SA2	SS2	B	30	A	90
SA3	SS3	A	90	M	60
SA4	SS4	A	90	M	60
SA5	SS5	A	90	M	60
SA6	SS6	M	60	B	30
SA7	SS7	A	90	M	60
SA8	SS8	A	90	M	60
SA9	SS9	M	60	M	60

Se determinó la disminución real de la vulnerabilidad según los controles planteados para determinar la proporción de la disminución de la vulnerabilidad.

Ecuación 2. Disminución Vulnerabilidad

$$\left(Disminución\ Real\ Vulnerabilidad = 1 - \frac{DismVulnerabilidad}{100}\right)$$

$$(Disminución\ Vulnerabilidad = 100 * (1 - Dism.RealVulnerabilidad)$$

Fuente: GR2DEST, Metodología de Análisis de Riesgos: MAGERIT, 2014

Se determinó la disminución real del impacto para determinar la proporción de la disminución del impacto según los controles planteados.

Ecuación 3. Disminución Impacto

$$\left(Disminución\ Real\ Impacto = 1 - \frac{DismImpacto}{100}\right)$$

$$(Disminución\ Impacto = 100 * (1 - Dism.RealImpacto)$$

Fuente: GR2DEST, Metodología de Análisis de Riesgos: MAGERIT, 2014

Tabla 33. Disminución de Vulnerabilidad - Hardware

Nombre de la Amenaza	Disminución Real de Vulnerabilidad	Disminución de Vulnerabilidad	Disminución Real de Impacto	Disminución de Impacto
Descargue completo de UPS debido a perdida de suministro de Energía Eléctrica.	0,1	90	0,4	60
Fuego, Daños por agua, desastres naturales.	0,7	30	0,4	60
Alteración en el esquema de virtualización debido a una falla humana.	0,7	30	0,1	90
Elemento de red no funciona (Switches, access point, cableado…)	0,4	60	0,4	60
Sistema de respaldo no funciona.	0,4	60	0,4	60
Unidad de aire acondicionado dañado Data Center.	0,4	60	0,4	60
Sabotaje Físico de Servidores desde afuera.	0,1	90	0,1	90
Límite de Vida Útil activos hardware.	0,7	30	0,4	60
No se realiza el tratamiento específico de los riesgos de infraestructura TI.	0,4	60	0,1	90

Tabla 34. Disminución de Vulnerabilidad - Software

Nombre de la Amenaza	Disminución Real de Vulnerabilidad	Disminución de Vulnerabilidad	Disminución Real de Impacto	Disminución de Impacto
No disponibilidad de algún archivo que compone el ERP. (tablas)	0,1	90	0,4	60
Perdida de integridad información del ERP, liberación de programas del ERP con errores.	0,7	30	0,1	90
Abuso de confianza respecto a la manipulación de la información para beneficio propio.	0,1	90	0,4	60
Restricción de cantidad de licencias de usuario (cal Windows server 2012, *Kaspersky*...) para instalar.	0,1	90	0,4	60
Actualización de programas a su última versión, obsolescencia software.	0,1	90	0,4	60
Borrado o modificación de los programas fuentes de las aplicaciones. Sabotaje lógico.	0,4	60	0,7	30
Acceso no autorizado a la Información del servidor de archivos.	0,1	90	0,4	60
Difusión de software dañino, instalación de software no licenciado.	0,1	90	0,4	60
Fuga de información-Terceros	0,4	60	0,4	60

3.5.5. Riesgo Intrínseco. Se calculó el riesgo intrínseco que cada amenaza representa para cada uno de los activos en su clasificación general, para obtener el riesgo intrínseco por amenaza y por activo. Se calculó el riesgo sin la implementación de salvaguardas o controles de seguridad, calculando el riesgo intrínseco que cada amenaza representa para cada uno de los activos hardware identificados se tiene que:

Ecuación 4. Riesgo Intrínseco

$$(Riesgo\ Intrínseco = Valor\ Activos * Vulnerabilidad * (Impacto/100))$$

Fuente: GR2DEST, Metodología de Análisis de Riesgos: MAGERIT, 2014

Tabla 35. Riesgo Intrínseco – Amenazas Activos - Hardware

Código activos	Riesgo Intrínseco – Amenazas Activos Hardware								
	Descargue completo de UPS debido a perdida de suministro de Energía Eléctrica.	Fuego, Daños por agua, desastres naturales.	Alteración en el esquema de virtualización debido a una falla humana.	Elemento de red no funciona (Switches, access point, cableado)	Sistema de respaldo no funciona.	Unidad de aire acondicionado dañado Data Center.	Sabotaje Físico de Servidores desde afuera.	Límite de Vida Útil activos hardware.	No se realiza el tratamiento específico de los riesgos de infraestructura TI.
1	483.420	483.420	483.420	805.701	805.701	268.567	483.420	447.611	1.432.357
2	857.462	857.462	857.462	1.429.103	1.429.103	476.368	857.462	793.946	2.540.628
3	101.373	101.373	101.373	168.956	168.956	56.319	101.373	93.864	300.366

∑ Riesgo Intrínseco activos hardware: **$ 16.986.568**

El riesgo intrínseco se calculó sin la implementación de salvaguardas o controles de seguridad, calculando el riesgo intrínseco que cada amenaza representa para cada uno de los activos software identificados se tiene que:

Valor del activo * Vulnerabilidad ante la amenaza* (Impacto ante la amenaza/100)

∑ Riesgo Intrínseco activos software: **$ 26.417.894**

Total del riesgo Intrínseco de la infraestructura TI del amb:

∑ Riesgo Intrínseco activos hardware: **$ 16.986.568** + ∑ Riesgo Intrínseco activos software **$ 26.417.894 = $ 44.404.462**

Tabla 36. Riesgo Intrínseco – Amenazas Activos - Software

Código activos	Riesgo Intrínseco – Amenazas Activos Software								
	No disponibilidad de algún archivo que compone el ERP. (tablas)	Perdida de integridad información del ERP, liberación de programas del ERP con errores.	Abuso de confianza respecto a la manipulación de la información para beneficio propio.	Restricción de cantidad de licencias de usuario (cal Windows server 2012, *Kaspersky…*) para	Actualización de programas a su última versión, obsolescencia software.	Borrado o modificación de los programas fuentes de las aplicaciones. Sabotaje lógico.	Acceso no autorizado a la Información del servidor de archivos.	Difusión de software dañino, instalación de software no licenciado.	Fuga de información- Terceros
4	1.080.000	600.000	600.000	600.000	1.000.000	3.200.000	1.800.000	1.000.000	120.000
5	588.967	327.204	327.204	327.204	545.340	1.745.087	981.611	545.340	65.441
6	323.138	179.521	179.521	179.521	299.202	957.446	538.563	299.202	35.904
7	730.350	405.750	405.750	405.750	676.250	2.164.000	1.217.250	676.250	81.150

Realizando un análisis acerca de los resultados obtenidos de la magnitud del riesgo intrínseco de:

- Los activos hardware
- Los activos software identificados se observa: La materialización de las amenazas representan mayor pérdida económica son los incidentes de los activos software.

3.5.6 Riesgo Efectivo o Riesgo Residual

Ecuación 5. Riesgo Efectivo o Residual

$$Riesgo\ Residual\ \left(1 - \frac{DismVulnerabilidad}{100}\right) * \left(1 - \frac{DismImpacto}{100}\right)$$

Fuente: GR2DEST, Metodología de Análisis de Riesgos: MAGERIT, 2014

Tabla 37. Riesgo Efectivo – Activos Hardware

Código activos hardware	Riesgo Efectivo – Amenazas Activos Hardware								
	Descargue completo de UPS debido a perdida de suministro de Energía Eléctrica.	Fuego, Daños por agua, desastres naturales.	Alteración en el esquema de virtualización debido a una falla humana.	Elemento de red no funciona (Switches, access point, cableado)	Sistema de respaldo no funciona.	Unidad de aire acondicionado dañado Data Center.	Sabotaje Físico de Servidores desde afuera.	Límite de Vida Útil activos hardware.	No se realiza el tratamiento específico de los riesgos de infraestructura TI.
1	19.337	135.358	33.839	128.912	128.912	42.971	4.834	125.331	57.294
2	34.298	240.089	60.022	228.657	228.657	76.219	8.575	222.305	101.625
3	4.055	28.385	7.096	27.033	27.033	9.011	1.014	26.282	12.015

El riesgo efectivo o residual se calcula con la implementación de salvaguardas o controles de seguridad, calculando el riesgo residual según los salvaguardas implementados para cada amenaza de cada uno de los activos hardware identificado, se tiene que:

∑ Riesgo Residual de los activos hardware: **$ 2.019.158**

Tabla 38. Riesgo Efectivo – Activos Software

Código activos software	Riesgo Efectivo – Amenazas Activos Software								
	No disponibilidad de algún archivo que compone el ERP. (tablas)	Perdida de integridad información del ERP, liberación de programas del ERP con errores.	Abuso de confianza respecto a la manipulación de la información para beneficio propio.	Restricción de cantidad de licencias de usuario (cal Windows server 2012, *Kaspersky*…) para instalar.	Actualización de programas a su última versión, obsolescencia software.	Borrado o modificación de los programas fuentes de las aplicaciones. Sabotaje lógico.	Acceso no autorizado a la Información del servidor de archivos.	Difusión de software dañino, instalación de software no licenciado.	Fuga de información- Terceros
4	43.200	75.600	24.000	24.000	40.000	896.000	72.000	40.000	19.200
5	23.559	41.228	13.088	13.088	21.814	488.624	39.264	21.814	10.471
6	12.926	22.620	7.181	7.181	11.968	268.085	21.543	11.968	5.745
7	29.214	51.125	16.230	16.230	27.050	605.920	48.690	27.050	12.984

∑ Riesgo Intrínseco de los activos software: **$3.110.657**

Total del riesgo Residual de la infraestructura TI del amb:

∑ Riesgo Residual de los activos hardware: $ **2.019.158**+ ∑ Riesgo Residual activos software: **$ 3.110.657 = $ 5.129.815**

3.5.7 Análisis del Riesgo. Se realizó el análisis del riesgo intrínseco o inherente: Sin implementación de salvaguardas y el riesgo residual o efectivo: Con implementación de Salvaguardas planteados para dar paso a la declaración de aplicabilidad (Statement of Aplicability, SoA) de forma parcial.

De acuerdo al nivel de riesgo intrínseco aceptable y conociendo los riesgos residuales de los activos TI del amb, se procedió a realizar criterios de selección de los escenarios específicos en los cuales se debe plantear proyectos que ayuden a alcanzar un mejor nivel se seguridad mejor.

Debido a la clasificación de los activos TI más relevantes realizada se facilita el planteamiento o sugerencia de proyectos, durante esta etapa del análisis de riesgos la implementación de la metodología se pretende minimizar los riesgos identificados a un nivel aceptable de tal forma que haya una contribución en el desarrollo corporativo mediante la adopción de mejores prácticas de la seguridad de los activos TI.

Llevar a cabo la cuantificación del riesgo realizado permitió identificar las debilidades de control o vulnerabilidades identificadas, permitiendo identificar cuáles son los activos que están expuestos a las vulnerabilidades identificadas en mayor proporción.

Retomando el marco de trabajo y la revisión de los objetivos de control de la norma 27001 se establece la Declaración de Aplicabilidad que permite definir de forma explícita a cuales objetivos de control se les debe dedicar una mayor atención y se

permitirá definir el direccionamiento de recursos para aumentar los niveles de seguridad de infraestructura TI mediante proyectos de implementación o mejora de salvaguardas o controles.

3.6. CONCLUSIONES DE LA METODOLOGÍA

Tabla 39. Conclusiones Finales - Hardware

	Valor de Activos	Riesgo Intrínseco	Riesgo Efectivo
TOTAL	534.168.821	16.986.568	2.019.158

El riesgo intrínseco para este estudio es de 3,1799% del valor de los activos y el riesgo efectivo es de 0,37799%

Tabla 40. Conclusiones Finales - Software

Conclusiones Finales			
	Valor de Activos	**Riesgo Intrínseco**	**Riesgo Efectivo**
TOTAL	1.008.316.571	26.417.894	3.110.657

El riesgo intrínseco para este estudio es de 2,4999% del valor de los activos y el riesgo efectivo es de 0,30009%

4. DECLARACIÓN DE APLICABILIDAD O STATEMENT OF APPLICABILITY, (SoA).

4.1. CARACTERÍSTICAS DE UNA DECLARACIÓN DE APLICABILIDAD

Definición: La Declaración de aplicabilidad lista de forma general el alcance del SGSI preliminar, por lo tanto, es necesario un documento que especifique los controles de seguridad de acuerdo a la normativa que aplica a la empresa en la que se implantará el SGSI.

Para la declaración de aplicabilidad se puede representar a través de una tabla que especifique cada uno de los objetivos de control y controles aplicables. Esta SoA inicialmente se plantea a partir del Gap análisis y de la gestión y tratamiento del riesgo para acordar los controles según las partes interesadas.

La declaración de aplicabilidad para el SGSI preliminar de la División de sistemas de información contiene los controles de seguridad establecidos en el anexo A de la NTC-ISO/IEC 27001:2013, el cual es utilizado como una referencia para la implementación de medidas de protección de la información.

La Declaración de Aplicabilidad se desarrolla luego del tratamiento de riesgos, que a su vez es la actividad a una evaluación de riesgos. El tratamiento tiene como objetivo la definición de las acciones a realizar para disminuir los riesgos identificados y analizados.

Se plantea incluir los objetivos de control y controles seleccionados del estándar, las razones por las cuales han sido seleccionados y medidas de seguridad adicionales si es el caso.

La presente declaración de aplicabilidad Statement of Aplicability SoA, tiene como finalidad, determinar cuáles de los objetivos de control de la 27001 que se deben revisar con más detalle para la asignación de recursos y respectiva generación o mejora de proyectos que permitan reforzar la seguridad de la información, se examinarán los objetivos de control y de acuerdo a lo siguiente se determina su aplicabilidad.

Controles sobre los cuales, se debe intervenir para la asignación de recursos, se deben para plantear proyectos aún no contemplados o ya en ejecución para mejorar la seguridad de la información. **SI**

Controles que no aplican o que ya se encuentran implementados eficientemente actualmente y en los cuales se cuenta con un nivel de riesgo aceptable por las partes interesadas del proyecto. **NO**

Se tienen los resultados del Análisis de Riesgos como punto de partida de la Declaración de Aplicabilidad SoA, se obtiene parcialmente información para establecer la Declaración de Aplicabilidad, para completar este formato se tiene en cuenta la revisión de los objetivos de control, Check list, **(Anexo a)** respectivamente apreciaciones del Tutor y Profesional de Apoyo del amb encargados del proyecto.

Se llevó a cabo la identificación de los respectivos objetivos de control del anexo A de la NTC ISO/IEC 27001:2013, en los cuales se debe intervenir, determinando el posicionamiento de las amenazas que pasan el riesgo intrínseco aceptable por los principales interesados del proyecto, en la norma luego de la presentación del informe de la metodología MAGERIT.

La SoA fue complementada con la información acerca de los hallazgos expuestos en los resultados del informe de la auditoria interna diagnóstica.

Tabla 41. Amenazas con Riesgo no Aceptable – Hardware, Objetivo de Control

Código	Amenaza	Vulnerabilidad		Impacto		Riesgo Intrínseco	27001
HA4	Elemento de red no funciona (Switches, access point, cableado…).	FN	0,005	A	90	2.403.760	A.13.1
HA5	Sistema de respaldo no funciona.	FN	0,016	A	90	2.403.760	A.12.3.1
HA9	No se realiza el tratamiento específico de los riesgos de infraestructura TI.	F	0,016	M	50	4.273.351	A.12.6.1

Tabla 42. Amenazas con Riesgo no Aceptable – Software, Objetivo de Control

Código	Amenaza	Vulnerabilidad		Impacto		Riesgo Intrínseco	27001
SA1	No disponibilidad de algún archivo que compone el ERP. (Tablas).	PF	0,003	A	90	2.722.455	A.14
SA5	Desactualización de programas a su última versión, obsolescencia software.	FN	0,005	M	50	2.520.791	A.12.5
SA6	Borrado o modificación de los programas fuentes de las aplicaciones. Sabotaje lógico.	F	0,016	M	50	8.066.533	A.9.5.1
SA7	Acceso no autorizado a la Información del servidor de archivos.	FN	0,005	A	90	4.537.425	A.9.4
SA8	Difusión de software dañino, instalación de software no licenciado.	FN	0,005	M	50	2.520.791	A.12.2.1

Se decidió establecer un formato para la SoA compuesta de 4 columnas, el contenido de la declaración de aplicabilidad permite determinar el panorama general de la seguridad de la información en el amb.

Tabla 43. Declaración de Aplicabilidad SoA

OBJETIVOS DE CONTROL	CONTROLES	APPLY		Justificación / Medida Seguridad
A.5 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN				
A 5.1 ORIENTACIÓN DE LA DIRECCIÓN PARA LA GESTIÓN DE LA	A 5.1.1 POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	1	SI	La DSI del amb identifica y gestiona los riesgos de la información, la División establece una política de seguridad de la información para focalizar el contexto de la seguridad de la
		2	SI	

OBJETIVOS DE CONTROL	CONTROLES	APPLY		Justificación / Medida Seguridad
SEGURIDAD DE LA INFORMACIÓN	A 5.1.2 REVISIÓN DE LAS POLITICAS PARA LA SEGURIDAD DE LA INFORMACIÓN			información, el principal objetivo es informar y concientizar sobre los riesgos y controles implementados actualmente para evitar la materialización de estos riesgos. Se definen los encargados o responsables del planteamiento, desarrollo, control e implementación de esta política. La revisión de la política y su transición a un Manual de Políticas de Seguridad de la Información se revisará periódicamente para garantizar el respectivo cumplimiento y efectividad.
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN				
A 6.1 ORGANIZACIÓN INTERNA	A 6.1.1 ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN	3	SI	La DSI del amb mediante la política de seguridad establecida y su transición a un Manual de Políticas de Seguridad de la Información establece la organización, compromiso y asignación de responsabilidades para el respectivo cumplimiento. La División asegura el contacto con las autoridades y grupos de interés especial, el establecimiento de esta organización interna es fundamental ya que se estructura el trabajo y organización del SGSI preliminar.
	A 6.1.2 SEPARACIÓN DE DEBERES	4	SI	
	A 6.1.3 CONTACTO CON LAS AUTORIDADES	5	SI	
	A 6.1.4 CONTACTO CON GRUPOS DE INTERÉS ESPECIAL	6	SI	
	A 6.1.5 SEGURIDAD DE LA INFORMACIÓN EN	7	SI	

OBJETIVOS DE CONTROL	CONTROLES	APPLY		Justificación / Medida Seguridad
	LA GESTIÓN DE PROYECTOS.			
A 6.2 DISPOSITIVOS MÓVILES Y TELETRABAJO	A 6.2.1 POLÍTICA PARA DISPOSITIVOS MÓVILES	8	SI	La DSI restringe la conexión a las redes inalámbricas de internet y potencia eléctrica por parte de dispositivos móviles de empleados y terceros.
	A 6.2.2 TELETRABAJO	9	NO	De acuerdo con lo establecido en la Ley 1221 de 2008 el amb no cuenta con Teletrabajo, ya que no se desempeñan actividades remuneradas de transferencia de información o de prestación de servicios por empleados o terceros utilizando como soporte las TIC´s.
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS				
A 7.1 ANTES DE ASUMIR EL EMPLEO	A 7.1.1 SELECCIÓN	10	SI	Para la respectiva ejecución de los procesos del amb, la contratación del recurso humano el cual tiene acceso a la información se realiza luego de la verificación de antecedentes para asignar roles y responsabilidades mediante los términos de referencia de los contratos celebrados, las leyes pertinentes son las encargadas de regular este control antes de asumir el empleo.
	A 7.1.2 TÉRMINOS Y CONDICIONES DEL EMPLEO	11	SI	
A 7.2 DURANTE LA EJECUCIÓN DEL EMPLEO	A 7.2.1 RESPONSABILIDADES DE LA DIRECCIÓN	12	SI	Se establecen controles para asegurar que el recurso humano es consciente de los riesgos, responsabilidades y deberes en el contexto de la seguridad de la información, de esta forma se pone en práctica la de concienciación pertinente a las funciones laborales, es decir la
	A 7.2.2 TOMA DE CONCIENCIA, EDUCACIÓN, Y FORMACIÓN EN S.I.	13	SI	
	A.7.2.3 PROCESO DISCIPLINARIO	14	SI	

OBJETIVOS DE CONTROL	CONTROLES	APPLY		Justificación / Medida Seguridad
				seguridad de información se refuerza cada vez más. Se estable de un proceso disciplinario que permite determinar cómo actuar en caso de que algún componente del recurso humano cometa alguna violación a la seguridad de la información, para evitar este escenario se exige el cumplimiento de la política de Seguridad o en efecto el conjunto de políticas del Manual de Políticas de la Seguridad de la Información.
A.7.3. TERMINACIÓN Y CAMBIO DE EMPLEO.	A.7.3.1. TERMINACIÓN O CAMBIO DE RESPONSABILIDADES DE EMPLEO.	15	SI	El cambio de las responsabilidades y los deberes asignados después de la terminación o cambio de empleo se definen, comunican y hacen cumplir al empleado o contratista para hacer cumplir los términos acerca de la caducidad de la vinculación con la empresa.
A.8 GESTIÓN DE ACTIVOS.				
A.8.1. RESPONSABLE DE LOS ACTIVOS.	A.8.1.1. INVENTARIO DE ACTIVOS.	16	SI	Se realiza la separación de activos de infraestructura TI, parte inicial del análisis y tratamiento de riesgos (Magerit). Se realiza un inventario de los activos TI de forma actualizada de acuerdo a la capacidad, este inventario es controlado en archivos de Excel.
	A.8.1.2. PROPIEDAD DE LOS ACTIVOS.	17	SI	Los activos de infraestructura TI se organizan según propiedad hardware (servidores, dispositivos de red, terminales de servicio) o software (ERP, licencias, herramientas).

OBJETIVOS DE CONTROL	CONTROLES	APPLY		Justificación / Medida Seguridad
	A.8.1.3. USO ACEPTABLE DE LOS ACTIVOS.	18	SI	Se establece un valor aceptable de los riegos por parte de los interesados del proyecto, se establecen reglas documentadas e implementadas.
	A.8.1.4. DEVOLUCIÓN DE ACTIVOS.	19	SI	Actualmente se determina la devolución de los activos por parte de los usuarios de la infraestructura TI del amb al finalizar vínculos laborales. Se contemplan escenarios de renuncias, terminaciones o cambios de la contratación de personal.
A.8.2. CLASIFICAR LA INFORMACIÓN.	A.8.2.1. CLASIFICACIÓN DE LA INFORMACIÓN.	20	SI	La División controla la transferencia de información de diferentes tipos, se establecen diferentes niveles de importancia y protección, se formaliza la gestión de la respectiva clasificación de la información, tomando en cuenta el valor que representa a la empresa, los requisitos legales, sensibilidad e importancia. (públicos, semiprivados, privados y sensibles) – Fersaco.
	A.8.2.2. ETIQUETADO DE LA INFORMACIÓN.	21	SI	
	A.8.2.3. MANEJO DE ACTIVOS.	22	SI	
A.8.3. MANEJO DE MEDIOS DE SOPORTE.	A.8.3.1. GESTIÓN DE MEDIOS DE SOPORTE REMOVIBLES.	23	SI	Los diferentes procesos del amb implican la transferencia de información utilizando medios para el intercambio de información tales como correo electrónico, USB, CD, actualmente se establecen controles para asegurar que se restringe el manejo de medios al momento de transferir la información. Política de seguridad – Manual de políticas de seguridad de la información.
	A.8.3.2. DISPOSICIÓN DE LOS MEDIOS DE SOPORTE.	24	SI	
	A.8.3.3. TRANSFERENCIA DE MEDIOS DE SOPORTE FÍSICOS.	25	SI	

OBJETIVOS DE CONTROL	CONTROLES	APPLY		Justificación / Medida Seguridad
A.9. CONTROL DE ACCESO.				
A.9.1. REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO.	A.9.1.1. POLÍTICA DE CONTROL DE ACCESO.	26	SI	Se establecen controles de seguridad que permitan asegurar que los propietarios de los activos TI controlan el acceso a la información formalmente en una política de Control de Acceso. Primera aproximación Política Control de Acceso.
	A.9.1.2. ACCESO A REDES Y A SERVICIOS EN RED.	27	SI	El amb tiene implementada y operando una red LAN única que soporta todas y cada una de las actividades de los procesos de la empresa, se establecen controles de los servicios de red para asegurar que los usuarios solo tienen acceso a los servicios autorizados.
A.9.2. GESTIÓN DE ACCESO DE USUARIOS.	A.9.2.1. REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS.	28	SI	La gestión de registro, suministro y cancelación del acceso de usuarios se encuentra revisada, implementada y operando ya que el amb maneja diferentes tipos de información, se establecen controles de seguridad para controlar y restringir el acceso de usuarios no autorizados, se controla la información fuera del área o escenarios habilitados. Se implementa una metodología y un respectivo sistema para la atención de solicitudes para la gestión de acceso de usuarios. La gestión de derechos de acceso privilegiado de los usuarios se realiza con la herramienta de Directorio Activo para el ingreso al sistema operativo y para accesos privilegiados al Sistema de
	A.9.2.2. SUMINISTRO DE ACCESO DE USUARIOS.	29	SI	
	A.9.2.3. GESTIÓN DE DERECHOS DE ACCESO PRIVILEGIADO.	30	SI	
	A.9.2.4. GESTIÓN DE INFORMACIÓN DE AUTENTICACIÓN SECRETA DE USUARIOS.	31	SI	
	A.9.2.5. REVISIÓN DE LOS DERECHOS DE ACCESO DE USUARIOS.	32	SI	
	A.9.2.6. CANCELACIÓN O AJUSTE DE LOS DERECHOS DE ACCESO.	33	SI	

OBJETIVOS DE CONTROL	CONTROLES	APPLY		Justificación / Medida Seguridad
				información integrado Sii++, se establecen plantillas que restringen el acceso a las opciones del ERP.
A.9.3. RESPONSABLE DE LOS USUARIOS.	A.9.3.1.USO DE INFORMACIÓN SECRETA.	34	SI	Los usuarios de los servicios de la División del amb actualmente manejan un usuario único e intransferible para el acceso a los servicios de red gestionados por la División.
A.9.4. CONTROL DE ACCESO A SISTEMAS Y APLICACIÓN.	A.9.4.1. RESTRICCIÓN DE ACCESO A INFORMACIÓN.	35	SI	Se implementa la herramienta de Directorio Activo de tal forma que para acceder a los servicios de red se restringe el acceso a la información, cada usuario tiene un login y password de forma única e intransferible para el control de accesos a sistemas y aplicaciones. Las diferentes herramientas software implementan un sistema de gestión de contraseñas, se plantea que se debe reforzar el control de accesos a los códigos fuente de dichas fuentes de programas.
	A.9.4.2. PROCEDIMIENTO DE CONEXIÓN SEGURA.	36	SI	
	A.9.4.3. SISTEMA DE GESTIÓN DE CONTRASEÑAS.	37	SI	
	A.9.4.4. USO DE PROGRAMAS UTILITARIOS PRIVILEGIADOS.	38	SI	
	A.9.4.5. CONTROL DE ACCESO A CÓDIGOS FUENTE DE PROGRAMAS.	39	SI	
A.10. CRIPTOGRAFÍA				
A.10.1. CONTROLES CRIPTOGRÁF.	A.10.1.1. POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS.	40	SI	Se plantea la política de controles criptográficos para formalizar los mecanismos de criptografía de los sistemas de información que se manejan en los diferentes proyectos del amb.
	A.10.1.2. GESTIÓN DE CLAVES.	41	SI	Con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de la información se debe plantear la gestión de

OBJETIVOS DE CONTROL	CONTROLES	APPLY		Justificación / Medida Seguridad
				llaves de los controles criptográficos.
A.11. SEGURIDAD FÍSICA Y AMBIENTAL.				
A.11.1. ÁREAS SEGURAS.	A.11.1.1. PERÍMETRO DE SEGURIDAD FÍSICA.	42	SI	El amb para el desarrollo de todos sus procesos actualmente ya cuenta con una infraestructura física, ubicada en el nororiente de ciudad de Bucaramanga, en la cual se ubica el 98 % de los activos TI de la empresa, de esta forma se gestionan controles de seguridad para evitar el acceso físico no autorizado, el deterioro de la infraestructura TI y perdida de activos de información de la empresa. Se establece el perímetro del Data Center, se plantea la política de controles de seguridad física y ambiental.
	A.11.1.2. CONTROLES FÍSICOS DE ENTRADA.	43	SI	
	A.11.1.3. SEGURIDAD DE OFICINAS, SALONES E INSTALACIONES.	44	SI	
	A.11.1.4. PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES.	45	SI	
	A.11.1.5. TRABAJO EN ÁREAS SEGURAS.	46	SI	
	A.11.1.6. ÁREAS DE DESPACHO Y CARGA.	47	SI	Las áreas de despacho y carga actualmente están ubicadas a una distancia considerable del Data Center. Se controla el ingreso mediante los Controles Físicos de entrada.
A.11.2. EQUIPOS.	A.11.2.1. UBICACIÓN Y PROTECCIÓN DE LOS EQUIPOS.	48	SI	Se establecen, implementan y operan controles que permiten evitar la ocurrencia de eventos como perdida, daño, robo o interrupción de los equipos dentro de las instalaciones físicas de infraestructura TI del amb. Se implementa un sistema de protección contra fallas eléctricas y otras interrupciones causadas por fallas en los servicios de suministro de potencia eléctrica.
	A.11.2.2. SERVICIOS PÚBLICOS DE SOPORTE.	49	SI	
	A.11.2.3. SEGURIDAD DEL CABLEADO.	50	SI	
	A.11.2.4. MANTENIMIENTO DE EQUIPOS.	51	SI	

OBJETIVOS DE CONTROL	CONTROLES	APPLY		Justificación / Medida Seguridad
	A.11.2.5. RETIRO DE ACTIVOS.	52	SI	La Política de Seguridad actual determina en el literal puesto de trabajo la gestión realizada en la gestión de retiro de activos, se establece la Póliza de Daños de Materiales Combinados para activos TI fuera del amb y se realiza la disposición segura de equipos e información contenida en estos mismos.
	A.11.2.6. SEGURIDAD DE EQUIPOS Y ACTIVOS FUERA DEL PREDIO.	53	SI	
	A.11.2.7. DISPOSICIÓN SEGURA O REUTILIZACIÓN DE EQUIPOS.	54	SI	
	A.11.2.8. EQUIPOS SIN SUPERVISIÓN DE LOS USUARIOS.	55	SI	En la política de seguridad se establecen los literales: “Puestos de trabajo para especificar el aseguramiento de los equipos sin supervisión de los usuarios y se plantea la política de escritorio limpio.
	A.11.2.9. POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA.	56	SI	
A.12. SEGURIDAD DE LAS OPERACIONES.				
A.12.1. PROCEDIM. OPERACIONAL Y RESPONSAB.	A.12.1.1. PROCEDIMIENTOS DE OPERACIÓN DOCUMENTADAS.	57	SI	Actualmente se formaliza el directorio de Gestión del Conocimiento donde se registra los procedimientos de operación: (incidencias, cambios y descripciones de los procedimientos operativos: Manuales de instalación de las herramientas, registros de actividades, y recursos disponibles para la consulta de los responsables del proceso.), se evalúa la gestión de capacidad llevando a cabo el seguimiento del uso de recursos para realizar proyecciones de los requisitos de capacidad. La Información es almacenada en el servidor de archivos.
	A.12.1.2. GESTIÓN DE CAMBIOS.	58	SI	
	A.12.1.3. GESTIÓN DE CAPACIDAD.	59	SI	
	A.12.1.4. SEPARACIÓN DE LOS AMBIENTES DE DESARROLLO, ENSAYO Y OPERACIÓN.	60	SI	Se plantea establecer, implementar y operar la separación formal de los tres

OBJETIVOS DE CONTROL	CONTROLES	APPLY		Justificación / Medida Seguridad
				ambientes de programación del ERP.
A.12.2. PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS.	A.12.2.1. CONTROLES CONTRA CÓDIGOS MALICIOSOS.	61	SI	Actualmente se implementa la solución de Seguridad *Kaspersky*, la consola de administración de la solución de seguridad y el agente de *Kaspersky* se encargan de la ejecución de las directivas de seguridad en la infraestructura TI del amb. Se plantea la implementación de una solución de seguridad completa.
A.12.3. COPIAS DE RESPALDO.	A.12.3.1. COPIAS DE RESPALDO DE LA INFORMACIÓN.	62	SI	Se encuentra establecido el procedimiento de Back up para el respaldo de información mediante la herramienta *Tivoli Storage Manager*. La frecuencia de respaldo es incremental diario y total quincenal, se realizan regularmente restauraciones, periódicamente se realizan pruebas de la información respaldada, manteniendo el registro respectivo.
A.12.4. REGISTRO Y SEGUIMIENTO.	A.12.4.1. REGISTRO DE EVENTOS.	63	SI	Actualmente las actividades de los usuarios que estén relacionadas con excepciones, fallas y eventos de seguridad son registradas en un directorio denominado Bitácora, esta información es protegida al mismo tiempo que se registran actividades del administrador en el directorio ADMON. Los sistemas de procesamiento de información se sincronizan con una única fuente de referencia de tiempo.
	A.12.4.2. PROTECCIÓN DE LA INFORMACIÓN DE REGISTRO.	64	SI	
	A.12.4.3. REGISTROS DEL ADMINISTRADOR Y DEL OPERADOR.	65	SI	
	A.12.4.4. SINCRONIZACIÓN DE RELOJES.	66	SI	

OBJETIVOS DE CONTROL	CONTROLES	APPLY		Justificación / Medida Seguridad
A.12.5. CONTROL DE SOFTWARE OPERACIONAL.	A.12.5.1. INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS.	67	SI	La División de sistemas de información del amb utiliza diferentes sistemas operativos en su infraestructura TI por lo tanto es establece controles para garantizar la protección, el control y correcta operación de los SO, la política de grupo de la herramienta Directorio Activo restringe la instalación de software en el sistemas operativo de los equipos.
A.12.6. GESTIÓN DE VULNERAB. TÉCNICA.	A.12.6.1. GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS.	68	SI	Se plantea determinar implementar y operar una metodología que gestione las vulnerabilidades técnicas de los activos TI del amb. Magerit.
	A.12.6.2. RESTRICCIONES SOBRE LA INSTALACIÓN DE SOFTWARE.	69	SI	Se realiza la restricción sobre la instalación de software en los equipos de cómputo del amb mediante privilegios y restricciones de la herramienta de Directorio Activo y su opción de la administración de las directivas de restricción de software.
A.12.7. CONSIDERAC. SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN.	A.12.7.1. CONTROLES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN.	70	SI	Se evidencian las auditorías para evaluar el proceso de Gestión de los Sistemas de Información del amb, se realiza una planeación periódica de las visitas de auditoria. Los registros son documentados en Kawak.
A.13. SEGURIDAD DE LAS COMUNICACIONES.				
A.13.1. GESTIÓN DE SEGURIDAD DE REDES.	A.13.1.1. CONTROLES DE REDES.	71	SI	Se gestionan y controlan todos los procesos que se realizan sobre la red LAN sobre la cual se desarrollan todas las aplicaciones ejecutados por los
	A.13.1.2. SEGURIDAD DE LOS SERVICIOS DE RED.	72	SI	

OBJETIVOS DE CONTROL	CONTROLES	APPLY		Justificación / Medida Seguridad
				usuarios TI del amb, los servicios de red actualmente se controlan mediante mecanismos para proteger la red y garantizar una buena infraestructura TI de soporte de los procesos. La División distribuye estratégicamente switches administrables para realizar el acceso de los puntos de red, estos dispositivos son asignados en una topología de red estrella, ubicados en 10 cuartos de comunicaciones organizados en racks en el edificio administrativo del parque del agua.
	A.13.1.3. SEPARACIÓN EN LAS REDES.	73	SI	En la DSI se realiza la respectiva documentación de la topología de red de datos que soporta la infraestructura TI del amb para su actualización. Se separan las redes VLAN´S (redes de área local virtual) en grupos de trabajo por áreas funcionales, la información de la topología de la red se documenta en el servidor de archivos en la ubicación lógica de Gestión del Conocimiento.
A.13.2. TRANSFEREN. DE INFORMACIÓN.	A.13.2.1. POLÍTICAS Y PROCEDIMIENTOS DE TRANSFERENCIA DE INFORMACIÓN.	74	SI	Para la ejecución de los procesos del amb se realiza el control de las operaciones de las comunicaciones, actualmente se cuenta con políticas y procedimientos de transferencia de información. Para la protección apropiada de la información incluida en los mensajes electrónicos se debe plantear la implementación de
	A.13.2.2. ACUERDOS SOBRE TRANSFERENCIA DE INFORMACIÓN.	75	SI	
	A.13.2.3. MENSAJES ELECTRÓNICOS.	76	SI	

OBJETIVOS DE CONTROL	CONTROLES	APPLY		Justificación / Medida Seguridad
				una herramienta se seguridad completa.
	A.13.2.4. ACUERDOS DE CONFIDENCIALIDAD O DE NO DIVULGACIÓN.	77	SI	Se establece el acuerdo de confidencialidad tanto para empleados internos y acuerdo de confidencialidad con terceros para la asignación, ajuste y cancelación de ajustes. Se debe realizar la revisión de las OPS.
A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.				
A.14.1. REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN.	A.14.1.1. ANÁLISIS Y ESPECIFICACIÓN DE REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN.	78	SI	Los procesos realizados sobre el ERP del amb se someten a análisis y especificación de requerimientos de seguridad de la información antes de implementar cambios en el sistema de información de la empresa.
	A.14.1.2. SEGURIDAD DE SERVICIOS DE LAS APLICACIONES EN REDES PÚBLICAS.	79	SI	
	A.14.1.3. PROTECCIÓN DE TRANSACCIONES DE SERVICIOS DE APLICACIONES.	80	SI	Debido a la transferencia de información a través de diferentes aplicaciones se aplican controles de seguridad para el desarrollo seguro de los procesos, la trasferencia de información se realiza de forma completa por ser un sistema de información transaccional. El proveedor debe especificar qué mecanismos de seguridad son implementados
A.14.2. SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE.	A.14.2.1. POLÍTICA DE DESARROLLO SEGURO.	81	SI	Se establece controles de seguridad para el desarrollo del ERP y respectivamente se debe establecer una política de desarrollo seguro que soporte los controles implementados respecto al desarrollo de software.

OBJETIVOS DE CONTROL	CONTROLES	APPLY		Justificación / Medida Seguridad
	A.14.2.2. PROCEDIMIENTO DE CONTROL DE CAMBIOS EN SISTEMAS.	82	SI	Los procedimientos de control de cambios se registran mediante el mantenimiento de soporte de aplicativos, se realiza la revisión técnica de aplicaciones después de cambios en el ERP del amb, se ponen a prueba los cambios antes de realizar el cambio total de los ajustes realizados si es necesario. Se establecen restricciones de cambios. Se debe establecer formalmente el ciclo de vida del Sistema de Información del amb.
	A.14.2.3. REVISIÓN TÉCNICA DE APLICACIONES DESPUÉS DE CAMBIOS EN LA PLATAFORMA DE OPERACIONES.	83	SI	
	A.14.2.4. RESTRICCIONES SOBRE LOS CAMBIOS DE PAQUETES DE SOFTWARE.	84	SI	
	A.14.2.5. PRINCIPIOS DE CONSTRUCCIÓN DE SISTEMAS DE SEGUROS.	85	SI	Se propone establecer la política de desarrollo seguro para exigir lo lineamientos y buenas prácticas para el desarrollo y construcción de sistemas de información seguros.
	A.14.2.6. AMBIENTE DE DESARROLLO SEGURO.	86	SI	Se considera necesario este control para la protección de la información al momento del desarrollo de las funciones del ERP, se debe establecer formalmente el ambiente de pruebas.
	A.14.2.7. DESARROLLO CONTRATADO EXTERNAMENTE.	87	SI	Se requiere el desarrollo de software contratado externamente, por lo tanto se deben establecer controles de seguridad para proteger el acceso al código fuente del ERP para evitar su alteración o uso malintencionado.
	A.14.2.8. PRUEBAS DE SEGURIDAD DE SISTEMAS	88	SI	

OBJETIVOS DE CONTROL	CONTROLES	APPLY		Justificación / Medida Seguridad
	A.14.2.9. PRUEBAS DE ACEPTACIÓN DE SISTEMAS.	89	SI	Las pruebas realizadas se llevan a cabo para comprobar la satisfacción del usuario, se debe establecer un programa de pruebas y criterios de aceptación formalmente. Se validan los nuevos desarrollos en un servidor de prueba-desarrollo antes de ser puestos en producción.
A.14.3. DATOS DE ENSAYO.	A.14.3.1. PROTECCIÓN DE DATOS DE ENSAYO.	90	SI	Se debe desagregar y establecer el ambiente de prueba y sus correspondientes datos de prueba que deben corresponder a los datos de producción.
A.15. RELACIONES CON LOS PROVEEDORES.				
A.15.1. SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON EL PROVEEDOR.	A.15.1.1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON PROVEEDORES.	91	SI	Debido al desarrollo de los procesos que se realizan externos a la DSI se hace necesario establecer controles de seguridad para garantizar que se tienen en cuenta los requisitos del negocio antes de la compra de bienes o servicios a terceros. Política de Seguridad de la información para la relación con proveedores.
	A.15.1.2. TRATAMIENTO DE LA SEGURIDAD DENTRO DE LOS ACUERDOS CON PROVEEDORES.	92	SI	
	A.15.1.3. CADENA DE SUMINISTRO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN.	93	SI	Se realizan órdenes de prestación de servicios asociadas con la cadena de suministros de tecnologías de información. Sin embargo, se deben identificar explícitamente los riesgos asociados a la cadena de suministro.
A.15.2. GESTIÓN DE LA PRESTACIÓN DE SERVICIOS	A.15.2.1. SEGUIMIENTO Y REVISIÓN DE LOS SERVICIOS DE LOS PROVEEDORES.	94	SI	Es necesario establecer controles de seguridad para garantizar que se tienen en

OBJETIVOS DE CONTROL	CONTROLES	APPLY		Justificación / Medida Seguridad
DE PROVEEDOR.	A.15.2.2. GESTIÓN DE CAMBIOS A LOS SERVICIOS DE LOS PROVEEDORES.	95	SI	cuenta los requisitos del negocio para la gestión con los proveedores, se incluyen términos de referencia acerca de la seguridad.
A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.				
A.16.1. GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN.	A.16.1.1. RESPONSABILIDADES Y PROCEDIMIENTOS.	96	SI	La asignación directa de responsabilidades y la descripción de los procedimientos para atender los incidentes de la seguridad de la información son tareas establecidas.
	A.16.1.2. INFORME DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN.	97	SI	Según la clasificación de los activos propuesta en el respectivo análisis de riesgos se hace importante establecer el reporte de eventos de seguridad y debilidades de seguridad de la información para llevar un control y evaluación de estos eventos para la mejora de la seguridad de la información. ITIL.
	A.16.1.3. INFORME DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN.	98	SI	
	A.16.1.4. EVALUACIÓN DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN Y DECISIONES SOBRE ELLOS.	99	SI	
	A.16.1.5. RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.	100	SI	Las respuestas a los incidentes de seguridad se encuentran actualmente registradas en una bitácora, se almacenan las evidencias de estos episodios para obtener aprendizaje respecto a los incidentes de seguridad de la información.
	A.16.1.6. APRENDIZAJE OBTENIDO DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.	101	SI	
	A.16.1.7. RECOLECCIÓN DE EVIDENCIA	102	SI	
A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO.				
A.17.1. CONTINUIDAD DE SEGURIDAD	A.17.1.1. PLANIFICACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN.	103	SI	La Alta Dirección del amb y la DSI planifican, implementan y verifican un plan de contingencia

OBJETIVOS DE CONTROL	CONTROLES	APPLY		Justificación / Medida Seguridad
DE LA INFORMACIÓN	A.17.1.2. IMPLEMENTACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN.	104	SI	para garantizar la continuidad del servicio del Sistema de Información Integrado Sii++, este proyecto controla y asegura una adecuada gestión de continuidad del negocio. La base de datos del sistema de información tiene un motor que se ejecuta dentro de un servidor virtual llamado producción, y guarda los datos en la unidad H de almacenamiento de disco STORAGE DS3400. Cuando se presenta una falla o un problema en el servidor de producción, automáticamente se establece mediante tecnología VMWARE de alta disponibilidad, que sube la réplica del servidor de producción apuntando a la misma unidad h de almacenamiento de disco.
	A.17.1.3. VERIFICACIÓN, REVISIÓN Y EVALUACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN.	105	SI	
A.17.2. REDUNDANC.	A.17.2.1. DISPONIBILIDAD DE INSTALACIONES DE PROCESAMIENTO DE INFORMACIÓN.	106	SI	Se establece la infraestructura de redundancia física para Storage (almacenamiento), servidores de producción y de réplica, también redundancia virtual para el servidor dominio para garantizar la continuidad del servicio, se realizan pruebas de cumplimiento de la contingencia implementada.
A.18. CUMPLIMIENTO.				
A.18.1. CUMPLIMIENT. REQUISITOS LEGAL CONTRCTUAL.	A 18.1.1 IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE Y DE LOS REQUISITOS CONTRACTUALES.	107	SI	Se realiza la identificación, documentación y cumplimiento de la legislación referente a la protección de la información y datos, Ley 1581 octubre 17 de 2012 según el congreso de la República, se evidencia el enfoque de la protección de
	A 18.1.2 DERECHOS DE PROPIEDAD INTELECTUAL	108	SI	
	A 18.1.3 PROTECCIÓN DE REGISTROS	109	SI	

OBJETIVOS DE CONTROL	CONTROLES	APPLY		Justificación / Medida Seguridad
	A 18.1.4 PRIVACIDAD Y PROTECCIÓN DE INFORMACIÓN DE DATOS PERSONALES	110	SI	datos manejados por el sistema de información. Todas las actividades se desarrollan en el marco del cumplimiento de la legislación Colombiana, las actividades de adquisición y compra de infraestructura TI son verificadas por la Contraloría General de la Republica.
	A 18.1.5 REGLAMENTACIÓN DE CONTROLES CRIPTOGRÁFICOS	111	SI	Se establece una primera aproximación a la política de controles criptográficos en el manual de políticas de seguridad de la información.
A 18.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN	A 18.2.1 REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN	112	SI	El amb formaliza la política de seguridad de la información y se propone la transición a un Manual de Políticas de la Seguridad de la Información demostrando el interés en mantener protegidos sus activos de información, se establecen acuerdos, mecanismos de control, planteando un Sistema de Gestión de la Seguridad de la Información. Se revisa la seguridad de la información de forma independiente.
	A 18.2.2 CUMPLIMIENTO CON LAS POLÍTICAS Y NORMAS DE SEGURIDAD	113	SI	La revisión del cumplimiento técnico de los sistemas de información es registrada y almacenada en el servidor de archivos, de igual forma se establecen los controles de seguridad para garantizar que todos los empleados conozcan y apliquen las políticas de seguridad de la información y respectivos controles.
	A 18.2.3 REVISIÓN DEL CUMPLIMIENTO TÉCNICO	114	SI	

5. PLANTEAMIENTO DE CONTROLES

De acuerdo a los resultados de los capítulos anteriores del presente informe, se analizan los resultados de la auditoria interna de la ISO 27001:2013, el GAP, el análisis de riesgos y la declaración de aplicabilidad para describir el plan de implementación, llevando a cabo el planteamiento de los Controles de acuerdo a la SoA con el fin de planificar la transición entre el Escenario Origen y el Escenario destino en la empresa al implementar un SGSI, se tiene en cuenta diversos criterios que se adapten a las características de la implementación de la NTC-ISO/IEC 27001:2013.

El Plan de Implementación e implementación de Controles permite definir y estructurar las acciones que deben ser aplicadas durante las fases de planeación, implementación del SGSI preliminar del amb.

Este plan de Implementación de la Norma Técnica Colombiana NTC-ISO/IEC 27001:2013 Requisitos para los Sistemas de Gestión de Seguridad de la Información SGSI preliminar es el avance que permitirá realizar la primera aproximación de un SGSI formal en el amb, permitiendo mejorar el contexto de la seguridad de la información en la División de sistemas del amb, el planteamiento de controles se realiza a partir de:

1. Los diferentes hallazgos de la auditoria interna diagnóstica, la información contenida en la Declaración de Aplicabilidad y en común acuerdo de los interesados del proyecto se plantean los controles pertinentes a las observaciones e información contenida. **(Anexo f: Informe, SoA).**
2. Los resultados del análisis de riesgos y la metodología implementada.

Tabla 44. Amenazas con Riesgo no Aceptable – Hardware

Código	Amenaza	Vulnerabilidad		Impacto		Riesgo Intrínseco
HA4	Elemento de red no funciona (Switches, access point, cableado…).	FN	0,005	A	90	2.403.760
HA5	Sistema de respaldo no funciona.	FN	0,016	A	90	2.403.760
HA9	No se realiza el tratamiento específico de los riesgos de infraestructura TI.	F	0,016	M	50	4.273.351

Tabla 45. Amenazas con Riesgo no Aceptable – Software

Código	Amenaza	Vulnerabilidad		Impacto		Riesgo Intrínseco
SA1	No disponibilidad de algún archivo que compone el ERP. (Tablas).	PF	0,003	A	90	2.722.455
SA2	Perdida de integridad información del ERP, liberación de programas del ERP con errores.	PF	0,003	A	90	2.722.455
SA5	Actualización de programas a su última versión, obsolescencia software.	FN	0,005	M	50	2.520.791
SA6	Borrado o modificación de los programas fuentes de las aplicaciones. Sabotaje lógico.	F	0,016	M	50	8.066.533
SA7	Acceso no autorizado a la Información del servidor de archivos.	FN	0,005	A	90	4.537.425
SA8	Difusión de software dañino, Instalación de software no licenciado.	FN	0,005	M	50	2.520.791

5.1. CONTROLES IDENTIFICADOS

Teniendo en cuenta el ciclo PHVA, se contemplan controles hasta el nivel hacer del ciclo **PH**VA, estos controles hacen referencia al establecimiento de un Manual de Políticas de la Seguridad de la Información, los planteamientos de estas políticas del manual se encuentran distribuidas en los objetivos de control del anexo A de la NTC ISO/IEC 27001:2013, en los objetivos de control:

- **A.12. Seguridad de las operaciones.**
- **A.13. Seguridad de las comunicaciones.**

- **A.14. Adquisición, desarrollo y mantenimiento de sistemas.**

Se realizaron varias observaciones para el planteamiento de controles contenidos en estos objetivos de control, en esta parte del proyecto en común acuerdo con los interesados en este mismo se establecen cuáles son los objetivos de control en los cuales se debe poner mayor número de recursos para la ejecución, verificación e implementación de respectivos controles para mitigar los incidentes de las amenazas que afectan la infraestructura TI del amb.

Además de esto se presentan los controles planteados a partir del análisis de riesgos realizado anteriormente, las principales amenazas que ponen en riesgo la ejecución del ERP del amb son:

- Fuego, Daños por agua, desastres naturales.
- Borrado o modificación de los programas fuentes de las aplicaciones. Sabotaje lógico.
- No disponibilidad de algún archivo que compone el ERP. (Tablas).

5.1.1. Replica en un Data Center Alterno

Nombre del proyecto: Data Center Virtual alterno del amb, Cloud Computing.

Responsable: Director del comité de seguridad de la información y su respectivo grupo de trabajo, alta dirección, jefe División de sistemas de información, administrador de recursos informáticos, proveedor servicio cloud computing.

Recursos requeridos: Definición explicita del proyecto para la asignación de recursos que permitan la implementación de una solución TI con tecnología de modelo en la nube, alta disponibilidad de ancho de banda para el acceso a máquinas virtuales, discos, BD y dispositivos del Data Center alterno.

(Permitiendo la continuidad del negocio en caso de desastres naturales o en caso de sabotaje lógico de los servidores del Data Center principal del amb), PRD (Plan de Recuperación de Desastres), Cloud Computing.

Tiempo: Se realiza una estimación de aproximadamente de 1 mes para la generación del requerimiento al proveedor, teniendo en cuenta que haya compromiso de la alta dirección para mejorar los mecanismos de seguridad de la información y continuidad del negocio, tiempo de implementación sujeto al proveedor, capacitación de la herramienta, transición al paradigma cloud.

Inversión: Personal capacitado, horas de trabajo por el personal capacitado para el trabajo relacionado con un Data Center Alterno.

Costo: Pago del recurso humano encargado de la supervisión de la implementación de la tecnología cloud como apoyo a los procesos realizados en el amb.

Nivel de prioridad del proyecto: Alto.

Figura 13. Control *Cloud Computing*

Fuente: DELL, Cloud Computing, Canadá, 2015.

5.1.2. Aproximación al manual del SGSI preliminar del amb

Nombre del proyecto: Sistema de Gestión de la Seguridad de la Información del amb S.A E.S.P.

Responsable: Director del comité de seguridad de la información y su respectivo grupo de trabajo.

Recursos requeridos: Definición explicita de la organización de la seguridad de la información para el planteamiento, implantación, verificación y control de las políticas, procedimientos y controles establecidos en el Sistema de Gestión de la Seguridad de la Información.

Tiempo: Se realiza una estimación de aproximadamente de 7 u 8 meses teniendo en cuenta el compromiso con la alta dirección y la interdisciplinariedad requerida para la formalización del SGSI en el amb.

Inversión: Personal capacitado, horas de trabajo por el personal capacitado para el trabajo relacionado con el Sistema de Gestión de la Seguridad de la Información.

Costo: Pago del recurso humano encargado del Sistema de Gestión de la Seguridad de la Información.

Tipos de acción sobre la amenaza, transferencia, prevención, detección, recuperación, reacción o notificación: Planteamiento e implantación de un Sistema de Gestión de Seguridad de la Información SGSI en el amb.

Controles, objetivos de control o procesos de normas, es decir se especifica cuáles cláusulas de la norma apoya el proyecto 27001: El manual de políticas

de Seguridad de la Información es planteado con las políticas enunciadas en cada uno de los objetivos de control de la 27001:2013.

Nivel de prioridad del proyecto: Medio.

5.1.3. Implementación de una solución completa de seguridad

Nombre del proyecto: Solución de Seguridad – Cifrado para la transferencia de información

Responsable: Alta Gerencia, Jefe División de Sistemas de Información, Administrador de recursos informáticos.

Recursos requeridos Servidor de administración de la solución de seguridad, personal capacitado para la administración de la herramienta, terminales de servicio para la aplicación de la herramienta.

Tiempo: Se realiza una estimación de aproximadamente de 1 mes para la generación del requerimiento al proveedor, teniendo en cuenta que haya compromiso de la alta dirección para mejorar los mecanismos de cifrado para la transferencia de información, tiempo de implementación sujeto al proveedor y capacitación de la herramienta.

Inversión: Personal capacitado, horas de trabajo por el personal capacitado para el trabajo relacionado con la administración de la herramienta.

Riesgo que mitiga: Perdida de integridad, disponibilidad o confidencialidad al momento de la transferencia de información en los diferentes procesos controlados por la División de Sistemas de Información del amb.

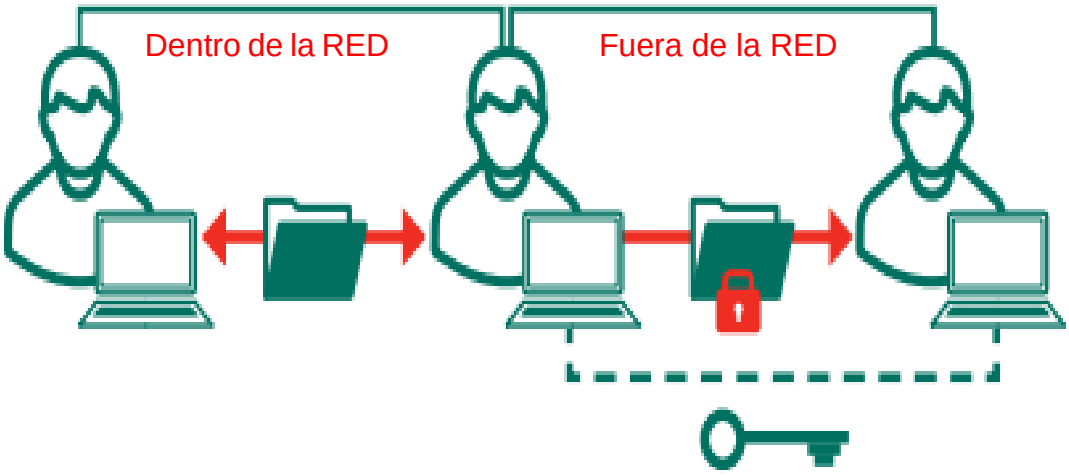
Impactos actuales de los riesgos actuales que mitiga: No se implementan mecanismos de cifrado y encriptación es decir la información es legible fácilmente al momento de su transferencia por la red de la empresa, el mecanismo de seguridad también debe abordar el tema de cifrado de la información transferida por correo electrónico.

Costo: Pago del recurso humano encargado de la administración de la solución de seguridad completa, pago del servicio de mantenimiento del servidor y herramienta de seguridad completa.

Controles, objetivos de control o procesos de normas, es decir se especifica cuáles cláusulas de la norma apoya el proyecto 27001: A.10 Controles Criptográficos

Nivel de prioridad del proyecto: Media.

Figura 14. Control Solución de Seguridad



Fuente: *KASPERSKY*, Endpoint Security for Business, Estados Unidos, 2015.

5.1.4. Establecimiento del ciclo de vida del Sistema de Información del amb

Nombre del proyecto: Ciclo de vida del Sii++

Responsable: Alta Gerencia, Jefe División de Sistemas de Información, Jefes: Análisis de requerimientos, Mantenimiento y Soporte de aplicativos, Gestión de Nuevos de Desarrollos, Externos encargados de proveer el servicio al amb.

Recursos requeridos: Personal capacitado y disposición del mismo para la documentación respectiva que permita formalizar el ciclo de vida del sistema de información transaccional implementado en el amb.

Tiempo: Se realiza una estimación de aproximadamente de 1 mes para la generación y planteamiento del proyecto en la División - proveedor y respectiva socialización del proyecto teniendo en cuenta que haya compromiso de la alta dirección, el tiempo de ejecución del proyecto debe ser estimado por el jefe de la División de Sistemas de Información del amb.

Inversión: Personal capacitado, horas de trabajo por el personal capacitado para el trabajo relacionado con el Análisis de requerimientos, Mantenimiento y Soporte de aplicativos, Gestión de Nuevos de Desarrollos para aportes significativos de la formalización del ciclo de vida del ERP.

Riesgo que mitiga: Perdida de la seguridad en los procesos de desarrollo y soporte ya que no se puede realizar una revisión técnica de aplicaciones después de cambios en la plataforma de operaciones Sii++, no se identifica el control de cambios de sistemas en partes especificas del ciclo de vida ni se establecen restricciones explicitas para realizar cambios de paquetes software.

Costo: Pago del recurso humano encargado de las tareas que implican la formalización del ciclo de vida del sistema de información.

Tipos de acción sobre la amenaza, transferencia, prevención, detección, recuperación, reacción o notificación: Documentación del ciclo de vida del sistema de información implementado en el amb.

Controles, objetivos de control o procesos de normas, es decir se especifica cuáles cláusulas de la norma apoya el proyecto 27001: A.14.2 Seguridad en los procesos de desarrollo y de soporte.

Nivel de prioridad del proyecto: Media.

5.1.5. Separación de los tres entornos de programación del ERP de la amb

Nombre del proyecto: Entornos de programación del Sii++

Responsable: Alta Gerencia, Jefe División de Sistemas de Información, Jefe División de Sistemas de Información, Jefes: Análisis de requerimientos, Mantenimiento y Soporte de aplicativos, Gestión de Nuevos de Desarrollos, Administrador de recursos Informáticos.

Recursos requeridos: Servidor de administración para gestionar la solución software que permite la virtualización del servidor donde se encontrará ubicado el ambiente de pruebas VMware, personal capacitado para la administración de la herramienta.

Tiempo: Se realiza una estimación de aproximadamente de 1 mes para la generación de la formulación y justificación del proyecto teniendo en cuenta que haya compromiso de la alta dirección para definir el ambiente de ensayos.

Inversión: Personal capacitado, horas de trabajo por el personal capacitado para el trabajo relacionado con la administración de la herramienta que permitirá virtualizar y administrar el servidor asignado al ambiente de pruebas.

Riesgo que mitiga: Perdida de integridad, disponibilidad o confidencialidad al momento del establecimiento de procedimientos de cambios realizados en los programas del sistema de información del amb.

Costo: Pago del recurso humano encargado de la administración de la herramienta para la segregación de los 3 escenarios de programación del Sii++, pago del servicio de mantenimiento del servidor y herramienta utilizada.

Tipos de acción sobre la amenaza, transferencia, prevención, detección, recuperación, reacción o notificación: Implementación de una solución software para la virtualización de un servidor de pruebas.

Controles, objetivos de control o procesos de normas, es decir se especifica cuáles cláusulas de la norma apoya el proyecto 27001: A.12.1.4 Separación de loa ambientes de desarrollo, ensayo y operación.

Nivel de prioridad del proyecto: Media.

5.1.6. Controles a partir del análisis de riesgos

Teniendo en cuenta los resultados del análisis de riesgos se hace correspondencia a las salvaguardas o controles planteados en la ejecución de MAGERIT. El planteamiento de controles incluye un documento que identifica los planes para enfrentar diferentes escenarios identificados como riesgosos. Las pruebas, los análisis del resultado de las pruebas y las acciones de mejoras del plan de

implementación de controles que mitiguen los incidentes de las amenazas de la infraestructura TI.

Tabla 46. Controles Hardware a partir del Análisis de Riesgos

Medidas de Seguridad / Controles
Contrato de Mantenimiento Correctivo y Preventivo elementos de red (Garantía para cambio de partes), Actualización planos de la infraestructura de red del amb, condiciones ambientales adecuadas para los dispositivos de red.
Mantenimiento Preventivo y Correctivo de los elementos que componen el mecanismo de Back Up, Mejoras y actualizaciones del mecanismo de back up implementado actualmente con su respectiva infraestructura.
Mejora del Análisis del riesgo transición al tratamiento especializado del riesgo de infraestructura TI MAGERIT.

Tabla 47. Controles Software a partir del Análisis de Riesgos

Medidas de Seguridad / Controles
Controles Físicos y de Accesos lógicos a los archivos del Sistema Información Integrado, mecanismo de respaldo implementado.
Definición ciclo de vida ERP, declaración ambiente de prueba y cronograma de ensayos antes de liberar un cambio.
Actualización de las herramientas instaladas, Windows Server Update Services. WSUS
Mejoras de los controles de acceso lógico para limitar el acceso de los servidores que contienen los programas fuentes de las aplicaciones.
Compartir carpetas con acceso restringido.
Implementación de herramienta de seguridad completa - Opciones del Directorio activo.

6. CONCLUSIONES

El proyecto de creación de un Sistema de Gestión de seguridad de la información preliminar en el amb comenzó en el área de manejo de infraestructura TI, incluyendo un alcance inicial del proceso de Gestión del Sistema de Información de la empresa.

La puesta en marcha y ejecución del proyecto permitió evidenciar el interés y compromiso por parte de los auditados respecto al contexto de la seguridad de la información, se evidencia mantenimiento de mecanismos para para la protección y mejora continua de la seguridad de la información, este proceso se realizó en la División de Sistemas de información DSI del amb, durante el transcurso de la misma se realizó la realimentación a todo el equipo de trabajo sobre las observaciones y sugerencias a realizar.

Se evidenció la necesidad de establecer un SGSI preliminar con el alcance inicial del proceso de Gestión de los Sistemas de Información, se evidenció el cumplimiento parcial de los requisitos de la norma ISO/IEC 27001, en cuanto la realización de acciones de mejora de la seguridad de la información, se notó que los procesos son planificados y desarrollados por el personal de la DSI; con alto sentido de responsabilidad en el cumplimiento de las actividades asignadas y por ende, se cumplió con el objetivo de evaluar éstos procesos respecto a la infraestructura TI de la empresa.

Como resultado de la auditoría se demostró parcialmente el direccionamiento estratégico y sistémico del amb para estructurar la seguridad de la información, se evaluó que el control ejercido desde la dirección del proyecto de un SGSI en el amb en la planificación y dirección de un proyecto de un SGSI aún no es el indicado.

El proceso y subprocesos de Gestión de los Sistemas de Información es parcialmente analizado desde el punto de vista de un Sistema de Gestión de la Seguridad de la Información, se evidencia el avance y la apropiación parcial del sistema mediante el correcto registro de formatos y evidencias, se evidenció la organización del proceso de Gestión de los Sistemas de Información mediante procedimientos establecidos y debidamente documentados, se evidenció la conveniencia, adecuación, eficacia, eficiencia y efectividad del SGSI en el proceso gestión de los sistemas de información.

Se cumplió la auditoria de acuerdo con el plan previsto y a las normas aplicables al proceso, una vez desarrollada la auditoría interna con todos los integrantes del proceso de gestión de los sistemas de información, se concluye que la auditoria cumplió con el objetivo propuesto para el cual fue planteada y se evidenció el análisis diagnóstico de los objetivos de control.

Se realizó la interpretación del análisis de brecha el cual permitió identificar los objetivos de control sobre los cuales se ha realizado mayores avances: Política de la seguridad de la información, Seguridad de los recursos humanos, control de acceso, seguridad física y ambiental, relaciones con los proveedores, cumplimiento. También se identificaron los objetivos de control con un avance significativo pero que de igual forma se deben implementar más controles respecto a: Criptografía, control de operaciones, control de comunicaciones y control de adquisición y mantenimiento de sistemas.

Se identificó el Análisis de Riesgos como parte fundamental para el planteamiento de un Sistema de Gestión de seguridad de la información de una empresa, en este caso un SGSI preliminar en el amb, de tal forma se evidenció que la idea de desarrollar una metodología para el análisis de los riesgos que impactan sobre los activos de la infraestructura TI se convierte en una necesidad empresarial.

Se eligió MAGERIT debido a su enfoque del análisis del riesgo intrínseco (sin implementación de controles) y del riesgo residual (con implementación de salvaguardas identificados y propuestos). Se analizaron las características de la metodología que ha sido utilizada para medir el riesgo de los activos TI para determinar los beneficios y problemáticas de aplicación.

En términos de la frecuencia de ocurrencia o vulnerabilidad y su impacto o deterioro de los activos ambos parámetros establecen de forma crítica el riesgo intrínseco, la disminución de la vulnerabilidad y la disminución del impacto influyen significativamente en el cálculo del riesgo residual, las escalas establecidas para la ejecución de MAGERIT fueron aceptadas a partir de la experticia y registros de los incidentes en la DSI respecto al contexto de la seguridad de la información.

En cuanto al riesgo intrínseco se determinó que las amenazas de los activos software representan mayores pérdidas para el amb con un valor cuantitativo de 26.417.894 COP en comparación con el riesgo intrínseco de los activos hardware de 16.986.568 COP.

En términos del riesgo residual se observó que la implementación o mejora de las salvaguardas disminuyen en gran proporción el riesgo representado por las amenazas identificadas, la reducción del riesgo de los activos hardware equivale a un riesgo efectivo calculado de 2.019.158 COP y en los activos software un riesgo residual de 3.110.657 COP, por lo tanto el riesgo efectivo de los activos hardware frente al valor de los activos es de 0,37799%, y del 0,30009% para el riesgo residual de los activos software.

Se identificó que MAGERIT presenta un sustento teórico, cualitativo y cuantitativo para determinar la viabilidad del planteamiento de la implementación de salvaguardas para la disminución del riesgo y determina la viabilidad de plantear

proyectos de identificación y mitigación de amenazas para disminuir el riesgo de la infraestructura TI.

Se documentaron las amenazas identificadas y analizadas durante la evaluación de riesgos, se determinó la respectiva declaración de aplicabilidad para la identificación del grado de aplicación de los objetivos de control del Anexo A de la NTC ISO/IEC 27001:2013, se realizó la comparación de los controles implementaos en el amb y los controles establecidos en el estándar internacional ISO/IEC 27001.

Se obtuvo un panorama amplio de la situación actual del amb en cuanto a la protección de su activo más importante, la información, el desarrollo de la declaración de aplicabilidad contribuyo a la identificación, organización y registro de las medidas de seguridad que hasta el momento se encuentran aplicadas y que se planean poner en marcha mediante la generación de proyectos que permitan mitigar los riesgos identificados en la División de Sistemas del amb.

Se estableció el principal documento de consulta durante una auditoria formal de las medidas de seguridad del amb, se permite identificar el resumen de la situación actual de los objetivos de control o dominios de la NTC ISO/IEC 27001:2013 y los respectivos controles implementados, en planeación o mejora.

Se determinó la justificación de la aplicabilidad de los controles definidos en los dominios en términos de: Requerimiento legal, Obligación contractual, Requerimientos del negocio y análisis de riesgos.

Se documentaron todos y cada uno de los objetivos de control justificando la inclusión o exclusión de estos mismos, lo anterior fue realizado como resultado de los procesos de evaluación y tratamiento de riesgo.

Se propuso una lista de controles a implementar luego del análisis de un informe de auditoría, el análisis GAP, la respectiva implementación de la metodología para el análisis y tratamiento del riesgo MAGERIT lo cual permitió determinar cuáles controles deben tenerse en cuenta según su prioridad. El planteamiento de controles se llevó a cabo teniendo en cuenta criterios de la declaración de aplicabilidad y el panorama general de la seguridad de la información.

Los controles planteados se ubican dentro de los Objetivos de Control identificados como más importantes de abordar, es decir la prioridad según con la cual se clasifican los objetivos de control de Comunicaciones, Operaciones y Seguridad en los Procesos de Desarrollo y Soporte de Software, logrando el objetivo específico de plantear controles pertinentes a los dominios más significantes de la NTC ISO/IEC 27001:2013 en el amb.

7. RECOMENDACIONES

Se recomienda incluir dentro del plan estratégico del amb el proyecto específico para la planeación y formalización del respectivo SGSI de la empresa ya que aumenta la capacidad para enfrentar la materialización de amenazas que debilitan la Seguridad de la Información de la empresa.

Considerar, complementar y evaluar las diferentes observaciones arrojadas del proceso de Auditoria Interna Diagnostica con más detalle, es decir realizar realimentación del procedimiento realizado en el presente proyecto.

Direccionar recursos por parte de la alta gerencia para disminuir la brecha analizada en el estudio del GAP realizado.

Realizar la transición completa a la Metodología de Análisis de Riesgos de infraestructura TI, lo cual permitirá la evaluación del riesgo visto desde el punto de vista del riesgo intrínseco y residual a partir de la ejecución de MAGERIT.

Refinar la Declaración de Aplicabilidad por parte de la División de Sistemas ya que se trata del documento que se revisaría en una Auditoria por un mecanismo externo a la empresa.

Analizar detalladamente los objetivos de control o Dominio en los cuales se deben fortalecer los controles o medidas que garantizan la seguridad de la información en el amb.

BIBLIOGRAFÍA

ACUEDUCTO METROPOLITANO DE BUCARAMANGA amb S.A. E.S.P, Acto de Gerencia 012, Reglas y mecanismos de seguridad para los sistemas de información e infraestructura tecnológica del amb, Bucaramanga, 2014.

ACUEDUCTO METROPOLITANO DE BUCARAMANGA amb S.A. E.S.P, Plan Estratégica de Gestión 2012-2018; amb: Agua Sostenible y Confiable, Bucaramanga, 2012.

AMUTIO G, Miguel, CANDAU, Javier, MAGERIT – versión 3.0. Libro I – Método, Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración, España, 2012.

Cuevas, Adriana, Ardila, Miguel, Análisis Riesgos, Acueducto Metropolitano de Bucaramanga amb S.A. E.S.P, Bucaramanga 2013.

DELL, Cloud Computing, Canada, 2015.

DIAZ, Andres, COLLASOZ, Gloria, LOZANO, Hermes, ORTIZ, Leidy, PÉREZ, Gustavo, Implementación de un Sistema de Gestión de Seguridad de la Información SGSI en la comunidad Nuestra Señora de Gracia, alineado tecnológicamente con la norma ISO 27001, Bogotá, 2011.

FERSACO S.A.S, Informe General de Intervención Fase I, Proyecto Prodato Fase I “Acueducto Metropolitano de Bucaramanga S.A. ESP.”, Bucaramanga, 2015.

GAONA, Karina, Aplicación de la metodología MAGERIT para el análisis y gestión de la seguridad de la información aplicado a la empresa pesquera e industrial bravito S.A. en la ciudad de Machala, España, 2013.

GARCÍA L, Paloma, Principales Novedades de la ISO 27001/ISO 27002, España, 2013.

GR2DEST, Metodología de análisis de riesgos: MAGERIT, 2014.

GUZMAN S, Carlos, diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso, Bogotá, 2015.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN (ICONTEC), Compendio: Sistema de Gestión de la Seguridad de La Información (SGSI), Bogotá 2006.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN (ICONTEC), Norma Técnica Colombiana NTC-ISO/IEC 27001:2013, Bogotá, 2013.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN (ICONTEC), Norma Técnica Colombiana NTC-ISO/IEC 27002:2005, Bogotá, 2005.

KASPERSKY, Endpoint Security for Business, Estados Unidos, 2015.

MINISTERIO DE COMUNICACIONES, República de Colombia, modelo de seguridad de la información – sistema sansi - SGSI -modelo de seguridad de la información para la estrategia de gobierno en línea, Bogotá, 2008.

PEREIRA, José, SEGOVIA, Antonio, Plan de Implementación de la norma ISO/IEC 27001:2005., Master Interuniversitario en Seguridad de las tecnologías de la información y las comunicaciones, España, 2013.

PRADA H, Nathalia, Diseño de un Sistema de Gestión de Seguridad de la Información, Alineado con la Norma ISO/IEC 27002, Para una Empresa del Sector Financiero, Bogotá, 2010.

RAMIREZ G, Leida, GARCIA L, Gerardo, Declaración de Aplicabilidad Sistema de Gestión de la Seguridad de la Información SGSI-DA, Bogotá, 2015.

SOTELO B, Marcos, TORRES U, José, RIVERA O, Juan, Un Proceso Práctico de Análisis de Riesgos de Activos de Información, Lima, Perú, 2012.

WIKISPACES, Seguridad Informática UFPS, Bogotá 2012.