DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN (SGSI) PARA LA EMPRESA BELISARIO LTDA. DE LA CIUDAD DE BOGOTÁ D.C.

DAVID HUMBERTO BOTERO VEGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
BOGOTÁ D.C.
2016

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN (SGSI) PARA LA EMPRESA BELISARIO LTDA. DE LA CIUDAD DE BOGOTÁ D.C.

DAVID HUMBERTO BOTERO VEGA

Proyecto de grado para optar al título de especialista en seguridad informática

Director de proyecto:
Ing. Erika Liliana Villamizar Torres

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
BOGOTÁ D.C.
2016

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bogotá, D.C. 02 de mayo de 2017

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE ANEXOS

pág.

INTRODUCCIÓN

La seguridad de la información se ha popularizado en los últimos años, ha dejado de verse como un gasto innecesario y se ha convertido en una inversión para las organizaciones que priorizan en el aseguramiento y protección de su activo más preciado, la información.

Aunque es un denominador común en los directivos de las compañías considerar que se deben tomar medidas y acciones en este campo, este proceso no suele tener el impacto y la aceleración deseada a sabiendas de que en la era donde se ubican ha cambiado la forma en que se interactúa con el entorno dejando expuestas a la organizaciones a potenciales amenazas y ataques.

Los profesionales en tecnologías de información se enfrentan cada día a múltiples escenarios en los que la información de la organización se ve expuesta y la complejidad en su análisis y el crecimiento exponencial de esta misma crea una desventaja notoria en la gestión y tratamiento de su riesgo.

La importancia de la adopción de un Sistema de Gestión de Seguridad de la Información reside en la aceptación de un modelo que permite el establecimiento, implementación, revisión y mantenimiento de la protección de los activos de la información enfocados en la confidencialidad, integridad y disponibilidad de los mismos. Un SGSI se adapta a cualquier tipo de organización, sin importar su actividad económica, estructura o tamaño y aunque se tenga la percepción de que su implementación está destinada a grandes corporaciones que estén en capacidad de hacer una inversión considerable para su diseño y sostenimiento, en muchas ocasiones se pueden aplicar principios en lugar del Sistema de Gestión de Seguridad de la Información como conjunto, obteniendo mejoras significativas y una reducción considerable en el nivel de riesgo aceptado por la organización.

1. TITULO

Diseño del Sistema de Gestión de Seguridad informática y de la Información (SGSI) para la empresa Belisario Ltda. de la ciudad de Bogotá D.C.

2. DESCRIPCIÓN DEL PROBLEMA

En la actualidad las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas, que aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a los activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo.

Los virus informáticos, el hacking o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria e involuntariamente, originados dentro de la propia organización o aquellos que son provocados por catástrofes naturales y fallos técnicos.

En este punto se hace necesario resaltar que siendo Belisario Ltda. una empresa de consultoría en derecho laboral, seguridad y salud en el trabajo, que maneja información muy importante en la que se encuentran títulos de valores, documentación confidencial de clientes, datos de procesos, entre otros, cobra una real importancia para la alta dirección de esta organización garantizar la custodia y reserva de dicha información, siendo esta el pilar del desarrollo de la actividad económica de la compañía.

Es de recalcar que en segundo periodo del año 2014 y el año 2015, la organización Belisario Ltda. se ha visto envuelta en perdida de información relevante, esto a causa de errores atribuibles a su personal en la manipulación de la información, fraude a sus cuentas bancarias y daños ocasionados por ejecución de software malicioso.

2.1 FORMULACIÓN DEL PROBLEMA

¿Cómo el diseño del sistema de gestión de seguridad informática y de la información (SGSI) ayudará a disminuir la pérdida de información y mejoramiento de la seguridad informática en la empresa Belisario Ltda. de la ciudad de Bogotá?

3. JUSTIFICACIÓN

El Sistema de Gestión de la Seguridad de la Información permite a las organizaciones en el actual mundo globalizado garantizar que los riesgos a la seguridad de la información a la cual se ven expuestos, puedan ser controlados y minimizados de una forma sistemática y eficiente bajo modelos tales como la norma ISO 27001, que brindan una guía para el establecimiento e implementación adecuada de la seguridad informática. En algunos sectores diferentes al financiero aún no se cuenta con la cultura de implementación y gestión de la seguridad de la información.

En razón a lo anterior se evidencia la necesidad de implementar un sistema de seguridad de la información en la empresa Belisario Ltda. acorde a la actividad económica de la empresa que le permita minimizar y especialmente controlar las condiciones variables del entorno y la protección adecuada de los objetivos de su negocio, y así asegurar el máximo beneficio y aprovechamiento de nuevas oportunidades de negocio.

El desarrollo del presente proyecto beneficia a la organización y permite una mejora continua en la gestión de su seguridad, que alineado al sistema de gestión de calidad permite un incremento en los niveles de confianza de sus clientes y aliados estratégicos, establece una garantía de continuidad y disponibilidad del negocio, aumentando el valor comercial y mejora de la imagen de la organización. La compañía se ve favorecida en la reducción de los costos vinculados con los incidentes y la no disponibilidad de su sistema e infraestructura tecnológica.

El cliente se ve favorecido, ya que su información se encuentra resguardada frente a posibles intrusiones que pongan en riesgo la confidencialidad de la misma, lo que se convierte en un factor decisivo para diferenciar a la organización de la competencia.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Ayudar a disminuir la pérdida de información y mejorar la seguridad informática mediante el diseño de un sistema de gestión de seguridad informática y de la información SGSI en la empresa Belisario Ltda.

4.2 OBJETIVOS ESPECÍFICOS

- Identificar y clasificar los activos de información de la organización con el fin de establecer que elementos son susceptibles a ser atacados deliberada o accidentalmente con consecuencias para la compañía.

- Realizar un análisis de riesgos basado en amenazas y vulnerabilidades que permita determinar el estado actual de la seguridad informática en la organización.

- Verificar la existencia de controles o salvaguardas para evaluar el nivel de mitigación ante amenazas, vulnerabilidades y riesgos.

- Diseñar el SGSI de la empresa Belisario Ltda. garantizando la continuidad y disponibilidad del negocio acorde a su objeto social.

5. ALCANCE Y DELIMITACIÓN DEL PROYECTO

El sistema de gestión de seguridad informática y de la información se aplicará específicamente a la infraestructura tecnológica de la organización y al personal que hace parte del proceso de gestión tecnológica.

El desarrollo del proyecto se llevará a cabo en la ciudad de Bogotá, en la empresa Belisario Ltda., durante el periodo de tiempo comprendido entre el año 2015 y 2016.

6. MARCO DE REFERENCIA

6.1 ANTECEDENTES

Para enfocar la investigación sobre la implementación del sistema de gestión de seguridad informática y de la información, se realizó una revisión bibliográfica basada en los siguientes proyectos que aportan elementos claves para el desarrollo del objeto de estudio:

Proyecto denominado “Diseño de un sistema de gestión de seguridad de la información (SGSI)” presentado por Laura Martin Iglesias en la Universidad Rey Juan Carlos en la ciudad de Madrid, España. Este proyecto permite establecer el desarrollo del modelo PDCA (Plan-Do-Check-Act).

“Sistema de gestión de seguridad de la información (SGSI) en el comando provincial de policía Imbabura Nro. 12” presentado por Paola Alexandra Díaz Parco en la Universidad Técnica del Norte en Ibarra, Ecuador. Para la elaboración del proyecto, permite definir y establecer el análisis de los riesgos, control de activos y control de amenazas.

Proyecto denominado “Elaboración y aplicación de un Sistema de Gestión de la Seguridad de la Información (SGSI) para la realidad tecnológica de la USAT” presentado por César Wenceslao De La Cruz Guerrero y Juan Carlos Vásquez Montenegro en la Universidad Católica Santo Toribio de Mogrovejo, en la ciudad de Chiclayo, Perú. El cual permite desarrollar el Sistema de Gestión de Seguridad de la Información en cuanto a las políticas y alcance del SGSI refiere.

“Análisis e implementación de la norma ISO 27002 para el departamento de sistemas de la Universidad Politécnica Salesiana sede Guayaquil” presentado por Daniel Romo Villafuerte y Joffre Valarezco Constante en la Universidad Politécnica Salesiana en Guayaquil, Ecuador. Este nos permite fundamentar y

desarrollar las políticas de la seguridad de la información dado el contexto actual.

6.2 MARCO TEÓRICO

6.2.1 Seguridad de la información. La Organización Internacional para la Estandarización (ISO) define Seguridad de la Información como la preservación de la confidencialidad, integridad y disponibilidad de la información; así como de los sistemas implicados en su tratamiento, dentro de una organización[1].

Los pilares de la seguridad de la información o triada CIA se definen de la siguiente manera:

- Confidencialidad*:* La información no se divulga a terceros ni procesos autorizados.
- Integridad*:* Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad*:* Acceso y uso de la información cuando se requiera.

En un contexto más general se puede definir la seguridad de la información como un conjunto de procedimientos, estrategias y medidas preventivas y reactivas de carácter tecnológico, organizacional y de recursos humanos que permiten proteger y garantizar la información de la organización y que en consecuencia sean un eje de apoyo en el cumplimiento de los objetivos de negocio, su misión y visión.

6.2.2 Seguridad informática. Es la disciplina que se encarga de proteger la infraestructura tecnológica y de comunicaciones de la organización incluyendo

[1] LÓPEZ, Agustín. El portal de ISO 27001 en español [en línea]. <http://www.iso27000.es/download/doc_sgsi_all.pdf > [citado en mayo del 2016]

todos los recursos informáticos tales como el hardware o el software, a través de la adopción de medidas adecuadas que ayuden a mitigar los riesgos y amenazas a los cuales se pueda estar expuesto a presente o a futuro.

6.2.3 Diferencia entre seguridad informática y seguridad de la información. Aunque la seguridad de la información se encuentre soportada en la tecnología, su propósito es proteger dicha información garantizando su confidencialidad, integridad y disponibilidad sin importar el medio de almacenamiento u obtención, ya sea de manera digital o física. Su campo de acción es mucho más amplio dentro de la organización y no solamente se encarga de los procesos técnicos sino de cualquier riesgo de seguridad existente en la empresa dando alcance a directivas y a la alta gerencia[2].

La seguridad informática en cambio, está enfocada en el análisis y prevención de vulnerabilidades y amenazas a nivel de los recursos informáticos dispuestos por la organización.

6.2.4 Normas ISO sobre gestión de seguridad de la información. El ISO (International Organization for Standardization u Organización Internacional para la Estandarización) es un organismo internacional que se dedica a desarrollar reglas de normalización en diferentes ámbitos, entre ellos la informática.

El IEC (International Electrotechnical Commision) es otro organismo que publica normas de estandarización en el campo de la electrónica.

La norma ISO/IEC 27000 se denomina requisitos para la especificación de sistemas de gestión de la seguridad de la información (SGSI). Esta norma proporciona un marco estandarización para la seguridad de la información para que sea aplicado por una organización o empresa y comprende un conjunto de

[2] ORMELLA, Carlos. ¿Seguridad informática vs. Seguridad de la información? [en línea]. < http://www.iso27000.es/download/seguridad%20informaticavsinformacion.pdf > [citado en mayo del 2016]

normas sobre sistemas de gestión de la seguridad de la información, valoración de riesgos y controles.

Este conjunto de normas establecen los requisitos para definir, implementar y mantener un SGSI (Sistemas de Gestión de Seguridad de la Información).

Seguridad de la información según la norma ISO 27001 se define como preservación de su confidencialidad, integridad y disponibilidad, así como la de los sistemas implicados en su tratamiento.

6.2.4.1 ISO 27000. Contiene una visión general de las normas de la serie al igual que un conjunto de términos y definiciones sobre la norma.

6.2.4.2 ISO 27001. Publicada el 15 de Octubre de 2005, es la norma principal de la familia de la ISO 27000, contiene los requisitos básicos que debe tener todo sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma sobre la cual se certifican, por auditores externos, los SGSI de las organizaciones. A pesar de no ser obligatoria la implementación de todos los controles, se debe argumentar la no aplicabilidad de los controles no implementados. Recomienda el uso del ciclo PHVA para el diseño de un SGSI[3].

La norma ISO 27001:2000 contiene las recomendaciones para el aseguramiento de la información que se basan en las mejores prácticas de seguridad, esta norma es una evolución del estándar británico BS 7799. Cubre aspectos como el manejo de equipos, la administración de políticas, los recursos humanos y los aspectos legales entre otros. La versión actual del estándar se remite al año 2013 en la cual se definen los siguientes dominios:

[3] CASTRO, Juan. Compilación bibliográfica ISO serie 27000, ISO 17799 [en línea]. https://auditoriauc20102mivi.wikispaces.com/file/view/ISO201091700623026.pdf [citado en mayo del 2016]

- Políticas de seguridad de la información.
- Organización de la seguridad de la información.
- Seguridad en los recursos humanos.
- Gestión de activos.
- Control de accesos.
- Criptografía.
- Seguridad física y ambiental.
- Seguridad en las operaciones.
- Seguridad en las comunicaciones.
- Adquisición, desarrollo y mantenimiento de sistemas.
- Relaciones con proveedores.
- Gestión de incidentes de seguridad de la información.
- Aspectos de seguridad de la información dentro de la continuidad del negocio.
- Conformidad.

6.2.4.3 ISO 27002. Es una guía de buenas prácticas para la gestión de la seguridad. Contiene una serie de recomendaciones sobre qué medidas tomar para asegurar los sistemas de información de una organización. Describe los objetivos de control (aspectos a analizar para garantizar la seguridad de la información) y especifica los controles recomendables a implantar (medidas a tomar). A diferencia de la ISO 27001 no es certificable[4].

6.2.4.4 ISO 27005. Es el estándar internacional que tiene como propósito la gestión de los riesgos que atentan contra la seguridad de la información. Dicha norma establece un conjunto de directrices aplicables a cualquier organización que permiten llevar a cabo el proceso de gestión del riesgo, estas se encuentran alineadas a los requisitos de la norma ISO 27001.

[4] ORMELLA, Carlos. Las nuevas versiones de las normas ISO 27001 e ISO 27002 [en línea]. < http://www.criptored.upm.es/descarga/NuevasVersionesISO27001eISO27002.pdf > [citado en mayo del 2016]

6.2.5 Metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT). Es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno.

Como se establece en MAGERIT, Libro I: Método, la metodología persigue los siguientes objetivos[5]:

Directos:

1. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
2. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

Indirectos:

4. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

6.2.5.1 Activos. Según la norma UNE 71504:2008 se define activo como un componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos

[5] MINISTERIO DE HACIENDA Y HACIENDAS PÚBLICAS. MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información [en línea] < https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html> [citado en mayo del 2016]

(hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos[6].

Como enmarca el Libro I de MAGERIT, en un sistema de información hay 2 cosas esenciales, la información que maneja y los servicios que presta. Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema. Basados en la anterior descripción la metodología propone identificar los activos de la siguiente manera[7]:

- Datos que materializan la información.
- Servicios auxiliares que se necesitan para poder organizar el sistema.
- Las aplicaciones informáticas (software) que permiten manejar los datos.
- Los equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y servicios.
- Los soportes de información que son dispositivos de almacenamiento de datos.
- El equipamiento auxiliar que complementa el material informático.
- Las redes de comunicaciones que permiten intercambiar datos.
- Las instalaciones que acogen equipos informáticos y de comunicaciones.
- Las personas que explotan u operan todos los elementos anteriormente citados.

6.2.5.2 Amenazas. La norma UNE 71504:2008 define amenaza como una causa potencial de un incidente que puede causar daños a un sistema de información o a una organización[8].

[6] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I – Método. Madrid, España octubre de 2012 p. 22
[7] Ibid., p.23
[8] Ibid., p.27

El libro II, catálogo de elementos de la metodología MAGERIT, categoriza las amenazas de la siguiente manera[9]:

- De origen natural: Hay accidentes naturales (terremotos, inundaciones, etc.). Ante esos avatares el sistema de información es víctima pasiva, pero de todas formas tendremos en cuenta lo que puede suceder.

- Del entorno (de origen industrial): Hay desastres industriales (contaminación, fallos eléctricos, etc.) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos.

- Defectos de las aplicaciones: Hay problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se denominan vulnerabilidades técnicas o, simplemente, vulnerabilidades.

- Causadas por las personas de forma accidental: Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.
- Causadas por las personas de forma deliberada: Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.

6.2.5.3 Riesgo. Magerit en su versión 3, en el libro I define el riesgo a la medida del daño probable sobre un sistema. Al saber el impacto de la amenaza

[9] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II – Catálogo de elementos. Madrid, España octubre de 2012 p. 25

sobre los activos, se determina dicho riesgo sobre la probabilidad de ocurrencia. La metodología define dos tipos de riesgo dado el impacto sobre los activos[10]:

- Riesgo acumulado: Se calcula en un activo teniendo en cuenta el impacto acumulado debido a una amenaza y la probabilidad de la amenaza.

- Riesgo repercutido: Se calcula en un activo teniendo en cuenta el impacto repercutido debido a una amenaza y la probabilidad de la amenaza.

6.2.6 Sistema de Gestión de Seguridad de la Información. Es un modelo que permite a las organizaciones analizar los posibles riesgos y establecer medidas de seguridad con el fin de mejorar la protección de la información. El termino de información no solo aplica a la dispuesta en recursos informáticos sino a cualquier conjunto de datos, sin importar su medio de obtención, almacenamiento o transmisión.

Un Sistema de Gestión de Seguridad de la Información permite adoptar un proceso sistemático en la gestión efectiva de los riesgos que se encuentran asociados a la seguridad de los activos de información, con el fin de alcanzar un nivel de riesgo mucho menor al establecido dentro de la organización, preservando la confidencialidad, integridad y disponibilidad de la información.
A nivel gerencial un SGSI brinda una visión general sobre los niveles de protección desplegados sobre los diferentes sistemas informáticos sin tener que conocer los detalles técnicos que conllevan dichas tareas, a su vez permite estar al tanto de las medidas de seguridad establecidas y el grado de eficacia

[10] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I – Método, Op. cit. p.30

obtenido, con el fin de tomar decisiones estratégicas más acertadas y acordes a la situación actual de la organización[11].

La implementación de un Sistema de Gestión de Seguridad de la Información provee un proceso de mejora continua a nivel organizacional preservando una adecuada gestión de los riesgos de seguridad y haciendo participe a todos los miembros de la organización en la selección e implementación de controles, procesos, políticas, procedimientos y cualquier medida que conlleve a la protección de la información. El SGSI se puede alinear con cualquier otro sistema de gestión que se encuentre implementado, tales como:

- Calidad ISO 9001
- Ambiental ISO 14001
- Seguridad y salud en el trabajo 18001

6.3 MARCO LEGAL

6.3.1 Ley 1273 de 2009[12]. Es de resaltar que con la expedición de la Ley 1273 de 2009, se incorporó al código penal colombiano, la protección de la información y de los datos, preservando así los sistemas que se utilizan en las tecnologías de la información. Es de resaltar que los sujetos que ejecutan estás conductas pueden ser sancionados con la privación de la libertad entre (36 a 120 meses) y en algunos casos con la imposición de multas que van hasta los 1.000 salarios, esto si un juez de la republica lo encuentre responsable de una o varias de las conductas que integran esta ley.

[11] MIFSUD, Elvira. monográfico: Introducción a la seguridad informática [en línea] < http://recursostic.educacion.es/observatorio/web/en/software/software-general/1040-introduccion-a-la-seguridad-informatica?showall=1> [citado en mayo del 2016]

[12] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (5, enero, 2009). Por la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado – denominado “de la protección de la información y de los datos. Diario Oficial. Bogotá D.C., 2009. no. 47223. 8 p.

Adicionalmente esta norma surge en razón a que la delincuencia se ha aprovechado del avance tecnológico para así mismo desarrollar o manipular herramientas tecnológicas para la realización de fraudes.

La norma categoriza nueve conductas como delitos, los cuales se explican a continuación.

- Acceso abusivo a un sistema informático: Esta conducta protege el acceso a un sistema informático, de igual forma relaciona varios sujetos que pueden cometer el delito, es de resaltar que el delito se comete sobre un sistema informático que se caracteriza por estar protegido o no con una medida de seguridad, los sujetos que pueden cometer el delito son de tres tipos; En primer lugar tenemos a los que sin autorización acceden a un sistema informático, en segundo lugar tenemos a los a los sujetos que aun estando autorizado para acceder al sistema informático se extralimitan en el permiso otorgado. En tercer lugar se encuentra aquel sujeto que se mantiene dentro del sistema informática encontrar de la voluntad de su creador o de quien tiene el derecho de utilizarlo.

- Obstaculización ilegítima de sistema informático o red de telecomunicación: esta disposición pretende proteger el funcionamiento y el acceso a un sistema informático, los datos y la red de telecomunicaciones, el delito puede ser cometido por cualquier persona que sin estar autorizado impida o manipule el contenido.

- Interceptación de datos informáticos: Este ítem pretende eleva a delito toda conducta que realice una persona con el ánimo de interceptar datos informáticos en un sistema informático bien sea en el origen interior o destino o loas emisiones electromagnéticas sin orden judicial es decir que esta solicitud este autorizada bien sea por la fiscalía, la policía o en efecto por un juez de la república.

- Daño informático: En este se pretende proteger los datos informáticos, los tratamientos de información o en efecto o sus componentes lógicos de alteraciones tales como que los mismos sean borrados, deteriorados, alterados o dañados, es de resaltar que la conducta puede ser desarrollada por una persona que no esté autorizada para realizar las maniobras anteriormente descritas.

- Uso de software malicioso. Esta categoría pretende castigar aquellas personas que produzcan trafiquen, adquieran distribuyan, vendan o envíen software malicioso u otras herramientas informáticas que tengan el objetivo de causar daño.

- Violación de datos personales: Esta categoría de delito pretende salvaguardar los datos personales de los ciudadanos colombianos, es por ello que castiga conductas tales como compilar, sustraer, vender intercambiar, enviar entre otros datos personales sin autorización para provecho propio o en efecto para beneficiar un tercero

- Suplantación de sitio web para capturar datos personales: En esta categoría se elevó a delito todo acto ilícito que pretenda captar datos personales y para ello se diseñe, desarrolle, trafique o venda programas envíe páginas electrónicas, así como el que modifique nombres de dominio.

- Hurto por medios informáticos y semejantes: En esta categoría se pretende sancionar las conductas maliciosas que se desarrollen en la modalidad de hurto, en sistemas informáticos, las redes de un sistema electrónico, u otro medio semejante.
- Transferencia no consentida de activos: En este ítem se pretenden sancionar las conductas que se realicen con el ánimo de sacar provecho valiéndose de alguna herramienta informática y así realizar

transferencias no autorizadas de activos pertenecientes a un tercero, que se verá perjudicado por la conducta desplegada.

Finalmente es de resaltar que las conductas descritas en la ley pueden ser agravadas es decir que la sanción es más alta cuando se utilicen medios informáticos, o electrónicos en la comisión o realización del delito o fraude, también serán agravadas cuando el delito se cometa en redes o sistemas informáticos, si el que comete el delito se aprovecha de la confianza depositada, cuando con el delito se contiene beneficio para sí mismo o para un tercero, cuando el delito se comete con fines terroristas, cuando quien ejecuta el delito es responsable de la administración y manejo de la información.

6.3.2 Ley estatutaria 1581 de 2012[13]. La Ley de protección de datos, es una norma que pretende proteger derechos fundamentales tales como el derecho a la intimidad y el buen nombre, el cual se sintetiza en lo conocido como dato personal, el cual fue definido por el legislador como cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Así mismo es importante señalar que la ley de protección de datos se encuentra basada en los principios de legalidad en materia de tratamiento de datos, finalidad, libertad, veracidad, transparencia, acceso, circulación restringida, seguridad y confidencialidad.

La materialización de estos derechos se formaliza dentro de la norma, básicamente con la autorización que los ciudadanos deben emitir para que la información que es almacenada en las bases de datos pueda ser consultada o entregados a terceros por las entidades de naturaleza pública o privada.

La norma ha otorgado a los ciudadanos o titulares de la información el derecho a actualizar y ratificar sus datos personales, así como el derecho a solicitar

[13] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581. (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá D.C., 2012. no. 48587 20 p.

evidencia que permita establecer que en la entidad o responsable del tratamiento de la información, contaba con la autorización del titular para trasmitirla a terceros, el derecho a ser informado previa solicitud de cuál ha sido el uso que le han dado a la información custodiada en la base de datos, presentar reclamación ante la superintendencia de industria y comercio, quejas o demandas por desatender lo establecido en la ley 1581, entre otros.

De igual forma esta norma establece que es y cómo se debe manejar los datos denominados como sensibles, aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos, indicando inicialmente una prohibición tacita del tratamiento de este tipo de información, no obstante se estableció una excepción, la cual es aplicable cuando el titular de la información da el aval para su trasmisión, si la misma es con el ánimo de salvaguardar la seguridad del titular, cuando el tratamiento de datos sea realizado por una ONG, cuando la información sea solicitada para la actuación de un proceso judicial o cuando la finalidad del tratamiento de la información tenga un propósito estadístico. Se señala la prohibición de realizar cualquier tipo de trasmisión respecto de los niños y adolescentes a no ser que el dato sea de naturaleza pública.

Así mismo la Ley 1581 establece los criterios que deben tener en cuenta los responsables del tratamiento para el suministro de información a terceros, tales como el deber de informar al titular el alcance de los datos personales y su finalidad., personas a quienes se le pueden suministrar la información, procedimiento de consultas y reclamos. Los responsables del tratamiento deben garantizar al titular de la información el derecho de hábeas data, conservar la información bajo las condiciones de seguridad necesaria actualizar

la información, rectificar la información cuando sea incorrecta, tramitar las consultas y reclamos formulados, informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad entre otros.

Esta norma esta creo el registro nacional de base de datos el cual tiene como finalidad consolidar las bases de datos que contengan datos personales cuyo tratamiento automatizado o manual se realice por personas naturales o jurídicas, de naturaleza pública o privada, en el territorio colombiano, es importante señalar que el desarrollo del registro nacional de base de datos se reglamentó en el Decreto 886 de 2014 y en el cual se establece la información mínima a registrar, términos y condiciones de inscripción.

La ley estatutaria estableció como ente de control a la Superintendencia de Industria y Comercio quien se encuentra facultado para realizar investigaciones a los responsables del tratamiento o el encargado del tratamiento, por el incumplimiento a lo señalado en la presente norma.

Es pertinente señalar que la ley 1581 fue reglamentada parcialmente por el decreto 1377 de 2013 y en el cual se definen los criterios de autorización para la recolección de datos personales, el tratamiento de datos personales sensibles, los modos de obtener autorización, limitaciones temporales al tratamiento de datos personales, requisitos que se deben cumplir para el tratamiento de datos de niños y adolescentes, políticas de tratamiento, avisos de privacidad, medidas de seguridad ejercicio de derecho de los titulares, transferencias y transmisiones internacionales de datos personales, entre otros.

6.4 MARCO CONCEPTUAL

Las siguientes definiciones se encuentran establecidas en las normas ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27005[14]:

6.4.1 Aceptación del riesgo**.** Admisión de la pérdida o ganancia proveniente de un riesgo particular.

6.4.2 Activo**.** Bienes o recursos de información que tienen valor para la compañía.

6.4.3 Amenaza**.** Origen, fuente potencial de afectación que causa un incidente no deseado y puede resultar en un daño a un sistema u organización y/o a sus activos.

6.4.4 Análisis de riesgo. Uso sistemático de una metodología para la identificación fuentes o amenazas a las cuales están expuestos los activos, bienes o recursos de la compañía y estimar el riesgo.

6.4.5 Comunicación del riesgo. Compartir la información acerca del riesgo entre las personas o área responsable que toma la decisión y otras partes interesadas.

6.4.6 Confidencialidad. Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

6.4.7 Control. Es una forma de mitigar el impacto generado por la materialización de los riesgos existentes. Un control incluye entre otras: la definición de políticas, la puesta en marcha de procedimientos, la definición de guías, la definición de cambios en una estructura

[14] BAUTISTA, Luis. Plan de seguridad de la información compañía XYZ soluciones [en línea] http://openaccess.uoc.edu/webapps/o2/bitstream/10609/19443/2/TFM_ENT05_AlejandroBautista.pdf [citado en mayo del 2016]

organizacional, o la ejecución de buenas prácticas que pueden ser de carácter administrativo, técnico o legal.

6.4.8 Declaración de aplicabilidad. Documento que describe los objetivos de control y los controles pertinentes y aplicables para el sistema de gestión de seguridad de la información de la compañía.

6.4.9 Disponibilidad. Propiedad que determina que la información sea accesible y utilizable bajo solicitud por individuos, entidades o procesos autorizados.

6.4.10 Estimación del riesgo. Proceso de asignación de valores a la probabilidad y consecuencias de un riesgo.

6.4.11 Evaluación del riesgo. Proceso para determinar la importancia del riesgo con base en la comparación del mismo contra unos criterios dados.

6.4.12 Evento de seguridad de la información. Presencia identificada de una condición de un bien o recurso (sistema, servicio, red, etc.), asociada a una posible violación de la política.

6.14.13 Gestión de riesgo. Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

6.14.14 Riesgo residual. Nivel restante de riesgo después del tratamiento del riesgo.

6.14.15 Tratamiento del riesgo. Proceso de selección e implementación de medidas para modificar el riesgo.

7 DISEÑO METODOLÓGICO

7.1 LÍNEA Y TIPO DE INVESTIGACIÓN

La línea de investigación correspondiente al proyecto es la de gestión de sistemas, la cual representa un amplio dominio condicionado al cambio constante en las tecnologías de la información. El resultado de la investigación se verá reflejado en la implementación de un sistema de gestión de seguridad informática y de la información.

Se define como una investigación descriptiva ya que se necesita de las actividades, procedimientos y demás factores que afecten la seguridad de la organización y su infraestructura con el fin de comprobar los riesgos existentes para posteriormente analizarlos y evaluarlos bajo la metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT).

Se realiza una investigación exploratoria, ya que a través de la información recolectada por medio de la revisión bibliográfica de temas que comparten una similitud con el objeto de estudio del proyecto, se estructura y fundamenta el marco teórico que permite determinar los factores relevantes para el desarrollo del trabajo.

Se utiliza la investigación explicativa ya que este proceso nos permite establecer de forma metódica los controles referentes a la seguridad de la información con el fin de mitigar los riesgos, amenazas y vulnerabilidades identificadas.

7.2 METODOLOGÍA DE DESARROLLO

El marco metodológico del proyecto se enmarca bajo las siguientes etapas que comprenden una serie de actividades encaminadas al desarrollo de cada una de las fases.

Etapa 1: Identificar y clasificar los activos de información de la organización con el fin de establecer que elementos son susceptibles a ser atacados deliberada o accidentalmente con consecuencias para la compañía.

Actividades:

- Efectuar visitas a las instalaciones de la organización con el fin de identificar los activos con los que se dispone.
- Solicitar y revisar el inventario de equipos y hojas de vida de los mismos.
- Realizar entrevistas con los miembros del área de tecnología con el fin de conocer el estado actual de los equipos soportados y administrados en la infraestructura tecnológica.

Etapa 2: Realizar un análisis de riesgos basado en amenazas y vulnerabilidades que permita determinar el estado actual de la seguridad informática en la organización.

Actividades:

- Valoración de los activos bajo las dimensiones de disponibilidad, integridad de los datos, confidencialidad de la información, autenticidad y trazabilidad.
- Determinar bajo que amenazas y vulnerabilidades están expuestas estos activos.
- Estimar el impacto y riesgo del activo bajo la materialización de una amenaza.

Etapa 3: Verificar la existencia de controles para evaluar el nivel de mitigación ante amenazas, vulnerabilidades y riesgos.

Actividades:

- Revisión del sistema de gestión de calidad en donde se encuentran caracterizados los diferentes procedimientos correspondientes al área de tecnología.
- Inspección y auditoria a la infraestructura tecnológica de la empresa.
- Entrevistas con el personal del área de tecnología que permita establecer controles que no estén documentados.

Etapa 4: Diseñar el SGSI de la empresa Belisario Ltda garantizando la continuidad y disponibilidad del negocio acorde a su objeto social.

Actividades:

- Definir el objetivo del SGSI.
- Definir el alcance del SGSI.
- Definir las políticas, procedimientos y controles.

8 ANÁLISIS Y GESTIÓN DE RIESGOS

8.1 IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

El libro II, catálogo de elementos de la Metodología de Análisis y Gestión de Riesgos MAGERIT en su versión 3 define los activos dentro de una jerarquía para una clasificación más acertada y que con lleve a una caracterización más precisa sobre las potenciales amenazas y las salvaguardas que se deben desplegar en función de cada activo.

Tabla 1. Clasificación de activos según MAGERIT

IDENTIFICACIÓN	TIPO DE ACTIVO	DESCRIPCIÓN
[D]	Datos/Información	Los datos son el principal insumo para cualquier tipo de organización, es por esto que se considera un activo abstracto, ya que su medio de almacenamiento, transmisión u obtención puede variar
[K]	Claves criptográficas	La criptografía se aplica a la protección de la información o como medio de autenticación en una comunicación síncrona o asíncrona. Las claves criptográficas garantizan el funcionamiento de dichos mecanismos
[S]	Servicios	Satisface las necesidades de los usuarios a nivel de servicio, aplica para los servicios prestados por el sistema
[SW]	Software - Aplicaciones informáticas	Cualquier proceso que ha sido automatizado para ejecutarse en un equipo de cómputo. Las aplicaciones generar nueva información a través de datos que permiten la prestación de servicios
[HW]	Equipamiento informático (hardware)	Los medios que soportan los servicios de la organización al igual que el almacenamiento de datos y

IDENTIFICACIÓN	TIPO DE ACTIVO	DESCRIPCIÓN
		transmisión de los mismos
[COM]	Redes de comunicaciones	Servicio de comunicaciones propios o de terceros destinados a la transmisión de información
[Media]	Soportes de información	Dispositivos físicos dispuestos a almacenar información de manera permanente o por un lapso de tiempo determinado
[AUX]	Equipamiento auxiliar	Elementos que soportan los diferentes sistemas de información
[L]	Instalaciones	Lugar donde residen los sistemas de información y equipos de comunicaciones
[P]	Personal	Las personas relacionadas con los sistemas de información

Fuente: Autor.

Como resultado del proceso de revisión exhaustiva de la infraestructura tecnológica de la organización y los elementos que la componen, se obtiene inicialmente la clasificación de los activos como se muestra en la tabla número 2.

Tabla 2. Clasificación general de activos en la organización

CLASIFICACIÓN	ACTIVO
ACTIVO DE INFORMACIÓN	Copias de seguridad
	Ficheros de datos en Cobol
SOFTWARE	Microsoft Office
	OpenOffice
	ERP Siesa 85
	Ponto Secullum

CLASIFICACIÓN	ACTIVO
	Siesa intelligence
	Sistemas operativos Windows 7, Windows 8, Centos 5.11
	Servidor de presentación
	Servidor de archivos
	Servidor de base de datos
	Putty
	SIIS
	Bitdefender Control Center
HARDWARE	Equipos de cómputo
	Teléfonos IP
	Servidor
	NAS
	DVR
RED	Switch
	Firewall
EQUIPAMIENTO AUXILIAR	UPS
INSTALACIÓN	Cableado estructurado
	Instalaciones eléctricas
SERVICIOS	Conectividad a internet
	Troncal SIP
	Servicios de mantenimiento UPS
	Soporte y mantenimiento del ERP
	Servicio de soporte y mantenimiento PBX IP
PERSONAS	Coordinador de sistemas
	Proveedores (Siesa, Qtech, Claro, OpenBox)
	Asistente de sistemas

Fuente: Autor.

Teniendo como referencia la tipificación definida en la metodología MAGERIT detallada anteriormente en la tabla número 1, se procede a clasificar los activos de la información de la organización, teniendo en cuenta las categorías establecidas en cada uno de los niveles jerárquicos.

Tabla 3. Clasificación de activos de la organización según MAGERIT

CLASIFICACIÓN	TIPO	ACTIVO
[D] DATOS/INFORMACIÓN	[backup]	Copias de seguridad
	[files]	Ficheros de datos en Cobol
[SW] SOFTWARE	[office]	Microsoft Office
	[office]	OpenOffice
	[std]	ERP Siesa 85
	[std]	Ponto Secullum
	[std]	Siesa intelligence
	[os]	Sistemas operativos Windows 7, Windows 8, Centos 5.11
	[file]	Servidor de archivos
	[www]	Servidor de presentacion
	[dbms]	Servidor de base de datos
	[std]	Putty
	[sub]	SIIS
	[av]	Bitdefender Control Center
[HW] HARDWARE	[pc]	Equipos de cómputo
	[ipphone]	Telefonos IP
	[host]	Servidor
	[switch]	Switch
	[firewall]	Firewall
[MEDIA] SOPORTE DE INFORMACIÓN	[san]	NAS
	[san]	DVR
[AUX] EQUIPAMIENTO AUXILIAR	[ups]	UPS
	[wire]	Instalaciones electricas
[COM] REDES DE COMUNICACIONES	[LAN]	Cableado estructurado
	[Internet]	Conectividad a internet
	[ISDN]	Troncal SIP
[P] PERSONAL	[adm]	Coordinador de sistemas
	[prov]	Provedores (Siesa, Qtech, Claro, OpenBox)
	[op]	Asistente de sistemas

Fuente: Autor.

8.2 VALORACIÓN DE ACTIVOS

La valoración de los activos de información se establece a través de sus dimensiones, características o atributos que dan un valor determinado a dicho activo.

Analizar y evaluar los activos bajo este criterio permite valorar las consecuencias al materializarse una amenaza. En consecuencia, la valoración que recibe un activo en cierta dimensión representa para la organización una medida de perjuicio si el activo se ve afectado en dicha dimensión.

Tabla 4. Dimensiones de valoración según MAGERIT

DIMENSIÓN	IDENTIFICACIÓN	DESCRIPCIÓN
Disponibilidad	[D]	Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieran
Integridad	[I]	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada
Confidencialidad	[C]	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados
Autenticidad	[A]	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos
Trazabilidad	[T]	Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad

Fuente: MAGERIT, libro II - Catálogo de elementos.

Teniendo presente las dimensiones a evaluar, se establece la siguiente escala de valoración.

Tabla 5. Escala de valoración

VALOR		DESCRIPCIÓN
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Fuente: MAGERIT, libro II - Catálogo de elementos.

En la tabla 6 se aprecia la valoración de los activos anteriormente identificados en cada una de sus dimensiones.

Tabla 6. Valoración de activos

CLASIFICACIÓN	TIPO	ACTIVO	DIMENSIONES				
			[D]	[I]	[C]	[A]	[T]
[D] DATOS/INFORMACIÓN	[backup]	Copias de seguridad	9	9	9	9	9
	[files]	Ficheros de datos en Cobol	9	9	9	9	9
[SW] SOFTWARE	[office]	Microsoft Office	2				7
	[office]	OpenOffice	2				7
	[std]	ERP Siesa 85	7	8	8	8	8
	[std]	Ponto Secullum	2	7	7		8
	[std]	Siesa intelligence	2				
	[os]	Sistemas operativos Windows 7, Windows 8, Centos 5.11	8			8	8
	[file]	Servidor de archivos	8	8	8	8	8
	[www]	Servidor de presentacion	6				7
	[dbms]	Servidor de base de datos	8	8	8	8	8
	[std]	Putty	5				6

CLASIFICACIÓN	TIPO	ACTIVO	DIMENSIONES				
			[D]	[I]	[C]	[A]	[T]
	[sub]	SIIS	7	8	8	8	8
	[av]	Bitdefender Control Center	8			8	8
[HW] HARDWARE	[pc]	Equipos de cómputo	8				8
	[ipphone]	Telefonos IP	8				8
	[host]	Servidor	9				9
	[switch]	Switch	7				
	[firewall]	Firewall	8			8	8
[MEDIA] SOPORTE DE INFORMACIÓN	[san]	NAS	6				
	[san]	DVR	7			7	7
[AUX] EQUIPAMIENTO AUXILIAR	[ups]	UPS	9				
	[wire]	Instalaciones electricas	9				
[COM] REDES DE COMUNICACIONES	[LAN]	Cableado estructurado	9				
	[Internet]	Conectividad a internet	6				
	[ISDN]	Troncal SIP	6				
[P] PERSONAL	[adm]	Coordinador de sistemas	7		8		
	[prov]	Provedores (Siesa, Qtech, Claro, OpenBox)	6		8		
	[op]	Asistente de sistemas	6		6		

Fuente: Autor

8.3 IDENTIFICACIÓN DE AMENAZAS

El libro II, catálogo de elementos de la metodología Magerit presenta un conjunto de amenazas que se pueden materializar sobre los activos de un sistema de información. Estas amenazas se clasifican en:

- Desastres naturales [N]
- Origen industrial [I]

- Errores y fallos no intencionados [E]
- Ataques intencionados [A]

Cada categoría comprende un número de amenazas específicas para los diferentes tipos de activos, además de indicar las dimensiones que se ven afectadas según el tipo de amenaza.

Teniendo presente la clasificación de los activos de información realizada en fases anteriores, se procede a identificar a que amenazas se encuentran expuestos dichos activos dadas las condiciones del entorno de la organización. El resultado de este proceso se evidencia en la tabla número 7.

Tabla 7. Identificación de amenazas

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS
[D] DATOS/INFORMACIÓN	[backup]	Copias de seguridad	[E.2] Errores del administrador
			[E.18] Destrucción de información
	[files]	Ficheros de datos en Cobol	[E.2] Errores del administrador
			[E.18] Destrucción de información
[SW] SOFTWARE	[office]	Microsoft Office	[E.1] Errores de los usuarios
			[E.20] Vulnerabilidades de los programas (Software)
			[E.21] Errores de mantenimiento / actualización de programas (software)
	[office]	OpenOffice	[E.1] Errores de los usuarios
			[E.20] Vulnerabilidades de los programas (Software)
			[E.21] Errores de mantenimiento / actualización de programas (software)

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS
	[std]	ERP Siesa 85	[I.5] Avería de origen físico o lógico
			[E.1] Errores de los usuarios
			[E.2] Errores del administrador
			[E.15] Alteración accidental de la información
			[E.18] Destrucción de información
			[E.20] Vulnerabilidades de los programas (software)
			[E.21] Errores de mantenimiento / actualización de programas (software)
			[A.5] Suplantación de la identidad del usuario
			[A.6] Abuso de privilegios de acceso
	[std]	Ponto Secullum	[I.5] Avería de origen físico o lógico
			[E.20] Vulnerabilidades de los programas (software)
			[E.21] Errores de mantenimiento / actualización de programas (software)
	[std]	Siesa intelligence	[I.5] Avería de origen físico o lógico
			[E.20] Vulnerabilidades de los programas (software)
			[E.21] Errores de mantenimiento / actualización de programas (software)
	[os]	Sistemas operativos Windows 7, Windows 8, Centos 5.11	[I.5] Avería de origen físico o lógico
			[E.1] Errores de los usuarios
			[E.2] Errores del

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS
			administrador
			[E.8] Difusión de software dañino
			[E.20] Vulnerabilidades de los programas (software)
			[A.5] Suplantación de la identidad del usuario
			[A.6] Abuso de privilegios de acceso
			[A.7] Uso no previsto
			[A.8] Difusión de software dañino
			[A.11] Acceso no autorizado
	[file]	Servidor de archivos	[I.5] Avería de origen físico o lógico
			[E.1] Errores de los usuarios
			[E.2] Errores del administrador
			[E.20] Vulnerabilidades de los programas (software)
			[E.21] Errores de mantenimiento / actualización de programas (software)
			[A.5] Suplantación de la identidad del usuario
	[www]	Servidor de presentación	[I.5] Avería de origen físico o lógico
			[E.2] Errores del administrador
			[E.20] Vulnerabilidades de los programas (software)
	[dbms]	Servidor de base de datos	[I.5] Avería de origen físico o lógico
			[E.2] Errores del administrador
			[E.20] Vulnerabilidades de los programas (software)

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS
			[E.21] Errores de mantenimiento / actualización de programas (software)
			[A.5] Suplantación de la identidad del usuario
			[A.6] Abuso de privilegios de acceso
			[A.11] Acceso no autorizado
	[std]	Putty	[E.1] Errores de los usuarios
			[E.21] Errores de mantenimiento / actualización de programas (software)
	[sub]	SIIS	[I.5] Avería de origen físico o lógico
			[E.1] Errores de los usuarios
			[E.2] Errores del administrador
			[E.15] Alteración accidental de la información
			[E.18] Destrucción de información
			[E.20] Vulnerabilidades de los programas (software)
			[E.21] Errores de mantenimiento / actualización de programas (software)
			[A.5] Suplantación de la identidad del usuario
			[A.6] Abuso de privilegios de acceso
	[av]	Bitdefender Control Center	[I.5] Avería de origen físico o lógico
			[E.2] Errores del administrador
			[E.20] Vulnerabilidades de los programas (software)

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS
			[E.21] Errores de mantenimiento / actualización de programas (software)
[HW] HARDWARE	[pc]	Equipos de cómputo	[N.1] Fuego
			[N.2] Daños por agua
			[N.*] Desastres naturales
			[I.5] Avería de origen físico o lógico
			[I.6] Corte del suministro eléctrico
			[I.7] Condiciones inadecuadas de temperatura y/o humedad
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)
			[E.24] Caída del sistema por agotamiento de recursos
			[A.7] Uso no previsto
			[A.11] Acceso no autorizado
			[A.25] Robo
	[ipphone]	Teléfonos IP	[N.1] Fuego
			[N.2] Daños por agua
			[N.*] Desastres naturales
			[I.5] Avería de origen físico o lógico
			[I.6] Corte del suministro eléctrico
			[I.7] Condiciones inadecuadas de temperatura y/o humedad
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)
			[A.7] Uso no previsto

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS
			[A.25] Robo
	[host]	Servidor	[N.1] Fuego
			[N.2] Daños por agua
			[N.*] Desastres naturales
			[I.5] Avería de origen físico o lógico
			[I.6] Corte del suministro eléctrico
			[I.7] Condiciones inadecuadas de temperatura y/o humedad
			[E.2] Errores del administrador
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)
			[E.24] Caída del sistema por agotamiento de recursos
			[A.7] Uso no previsto
			[A.25] Robo
	[switch]	Switch	[N.1] Fuego
			[N.2] Daños por agua
			[N.*] Desastres naturales
			[I.5] Avería de origen físico o lógico
			[I.6] Corte del suministro eléctrico
			[I.7] Condiciones inadecuadas de temperatura y/o humedad
	[firewall]	Firewall	[N.1] Fuego
			[N.2] Daños por agua
			[N.*] Desastres naturales
			[I.5] Avería de origen físico o lógico
			[I.6] Corte del suministro eléctrico

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS
			[I.7] Condiciones inadecuadas de temperatura y/o humedad
			[A.5] Suplantación de la identidad del usuario
			[A.24] Denegación de servicio
[MEDIA] SOPORTE DE INFORMACIÓN	[san]	NAS	[N.1] Fuego
			[N.2] Daños por agua
			[N.*] Desastres naturales
			[I.5] Avería de origen físico o lógico
			[I.6] Corte del suministro eléctrico
	[san]	DVR	[N.1] Fuego
			[N.2] Daños por agua
			[N.*] Desastres naturales
			[I.5] Avería de origen físico o lógico
			[I.6] Corte del suministro eléctrico
			[I.7] Condiciones inadecuadas de temperatura y/o humedad
			[E.2] Errores del administrador
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)
			[A.11] Acceso no autorizado
			[A.18] Destrucción de información
[AUX] EQUIPAMIENTO AUXILIAR	[ups]	UPS	[N.1] Fuego
			[N.2] Daños por agua
			[N.*] Desastres naturales
			[I.*] Desastres

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS
			industriales
	[wire]	Instalaciones electricas	[N.1] Fuego
			[N.2] Daños por agua
			[N.*] Desastres naturales
			[I.*] Desastres industriales
[COM] REDES DE COMUNICACIONES	[LAN]	Cableado estructurado	[I.8] Fallo de servicios de comunicaciones
			[E.10] Errores de secuencia
			[A.5] Suplantación de la identidad del usuario
			[A.7] Uso no previsto
			[A.9] [Re-]encaminamiento de mensajes
			[A.12] Análisis de tráfico
			[A.14] Interceptación de información (escucha)
	[Internet]	Conectividad a internet	[I.8] Fallo de servicios de comunicaciones
			[A.7] Uso no previsto
			[A.12] Análisis de tráfico
			[A.14] Interceptación de información (escucha)
	[ISDN]	Troncal SIP	[I.8] Fallo de servicios de comunicaciones
			[A.7] Uso no previsto
			[A.12] Análisis de tráfico
			[A.14] Interceptación de información (escucha)
			[E.9] Errores de [re-]encaminamiento
			[E.24] Caída del sistema por agotamiento de recursos
[P] PERSONAL	[adm]	Coordinador de sistemas	[E.19] Fugas de información
			[E.28] Indisponibilidad del personal
			[A.28] Indisponibilidad del personal
			[A.30] Ingeniería social

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS
			(picaresca)
	[prov]	Provedores (Siesa, Qtech, Claro, OpenBox)	[E.19] Fugas de información
			[E.28] Indisponibilidad del personal
			[A.28] Indisponibilidad del personal
			[A.30] Ingeniería social (picaresca)
	[op]	Asistente de sistemas	[E.19] Fugas de información
			[E.28] Indisponibilidad del personal
			[A.28] Indisponibilidad del personal
			[A.30] Ingeniería social (picaresca)

Fuente: Autor

8.4 VALORACIÓN DE AMENAZAS

Con la identificación de las amenazas para cada activo de información, se procede a valorar la influencia de dicha amenaza en el valor del activo, para esto se tiene en cuenta la degradación, el grado de perjuicio en el activo y la probabilidad, la medida de ocurrencia de materialización de dicha amenaza. Cabe aclarar que cada amenaza afecta en una o varias dimensiones el activo y esta afectación repercute en cierta nivel su valor.

Para valorar la degradación se hace uso de la siguiente escala:

Tabla 8. Escala de la degradación del valor del activo

MA	muy alta	casi seguro	fácil
A	alta	muy alto	medio
M	media	posible	difícil
B	baja	poco probable	muy difícil
MB	muy baja	muy raro	extremadamente difícil

Fuente: MAGERIT, libro I - Método

Para valorar la escala de probabilidad de ocurrencia se utiliza la siguiente escala:

Tabla 9. Escala para la probabilidad de ocurrencia

MA	100	muy frecuente	a diario
A	10	frecuente	mensualmente
M	1	normal	una vez al año
B	1/10	poco frecuente	cada varios años
MB	1/100	muy poco frecuente	siglos

Fuente: MAGERIT, libro I - Método

En la tabla siguiente se determina para cada activo y sus amenazas identificadas la degradación y probabilidad de afectación en cada una de sus dimensiones.

Tabla 10. Valoración de amenazas

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	PROB.	DIMENSIONES				
					[D]	[I]	[C]	[A]	[T]
[D] DATOS/ INFORMACIÓN	[backup]	Copias de seguridad	[E.2] Errores del administrador	M	A	A	A		
			[E.18] Destrucción de información	B	MA				
	[files]	Ficheros de datos en Cobol	[E.2] Errores del administrador	M	A	A	A		
			[E.18] Destrucción de información	B	MA				
[SW] SOFTWARE	[office]	Microsoft Office	[E.1] Errores de los usuarios	A	B	B	B		

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	PROB.	DIMENSIONES				
					[D]	[I]	[C]	[A]	[T]
			[E.20] Vulnerabilidades de los programas (Software)	B	M	M	M		
			[E.21] Errores de mantenimiento / actualización de programas (software)	B	B	M			
	[office]	OpenOffice	[E.1] Errores de los usuarios	A	B	B	B		
			[E.20] Vulnerabilidades de los programas (Software)	B	M	M	M		
			[E.21] Errores de mantenimiento / actualización de programas (software)	B	B	M			
	[std]	ERP Siesa 85	[E.1] Errores de los usuarios	MA	B	M	M		
			[E.2] Errores del administrador	M	A	A	A		
			[E.15] Alteración accidental de la información	A		A			
			[E.18] Destrucción de información	M	A				
			[E.20] Vulnerabilidades de los programas (software)	B	M	M	M		
			[E.21] Errores de mantenimiento / actualización de programas (software)	M	A	A			
			[A.5] Suplantación de la identidad del usuario	B		MA	MA	MA	
			[A.6] Abuso de privilegios de acceso	B	M	A	A		
	[std]	Ponto Secullum	[E.20] Vulnerabilidades de los programas (software)	B	M	M	M		
			[E.21] Errores de mantenimiento / actualización de programas (software)	B	M	M			
	[std]	Siesa intelligence	[E.20] Vulnerabilidades de los programas (software)	B	B	B	B		
			[E.21] Errores de mantenimiento / actualización de programas (software)	B	M	M			
	[os]	Sistemas operativos Windows 7, Windows 8, Centos 5.11	[E.1] Errores de los usuarios	A	B	B	B		
			[E.2] Errores del administrador	M	A	B	A		
			[E.8] Difusión de software dañino	MB	A	A	A		
			[E.20] Vulnerabilidades de los programas (software)	MB	A	A	A		
			[A.5] Suplantación de la identidad del usuario	MB		MA	MA	MA	
			[A.6] Abuso de privilegios de acceso	B	A	A	A		
			[A.7] Uso no previsto	M	B	B	B		
			[A.8] Difusión de software dañino	MB	M	A	A		

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	PROB.	DIMENSIONES				
					[D]	[I]	[C]	[A]	[T]
			[A.11] Acceso no autorizado	MB		A	B		
	[file]	Servidor de archivos	[E.1] Errores de los usuarios	A	B	B	B		
			[E.2] Errores del administrador	M	A	A	A		
			[E.20] Vulnerabilidades de los programas (software)	MB	M	M	M		
			[E.21] Errores de mantenimiento / actualización de programas (software)	B	M	M			
			[A.5] Suplantación de la identidad del usuario	M		A	A	A	
	[www]	Servidor de presentación	[E.2] Errores del administrador	B	A	A	A		
			[E.20] Vulnerabilidades de los programas (software)	MB	M	M	M		
	[dbms]	Servidor de base de datos	[E.2] Errores del administrador	B	A	A	A		
			[E.20] Vulnerabilidades de los programas (software)	MB	M	A	A		
			[E.21] Errores de mantenimiento / actualización de programas (software)	B	M	M			
			[A.5] Suplantación de la identidad del usuario	MB		A	A	A	
			[A.6] Abuso de privilegios de acceso	MB	A	A	A		
			[A.11] Acceso no autorizado	MB		A	B		
	[std]	Putty	[E.1] Errores de los usuarios	A	M	MB	MB		
			[E.21] Errores de mantenimiento / actualización de programas (software)	MB	M	MB			
	[sub]	SIIS	[E.1] Errores de los usuarios	A	B	M	M		
			[E.2] Errores del administrador	M	A	A	A		
			[E.15] Alteración accidental de la información	A		A			
			[E.18] Destrucción de información	M	A				
			[E.20] Vulnerabilidades de los programas (software)	B	M	M	M		
			[E.21] Errores de mantenimiento / actualización de programas (software)	M	A	A			
			[A.5] Suplantación de la identidad del usuario	B		MA	MA	MA	
			[A.6] Abuso de privilegios de acceso	B	M	A	A		
	[av]	Bitdefender Control Center	[E.2] Errores del administrador	M	A	B	B		
			[E.20] Vulnerabilidades de los programas (software)	MB	B	M	M		

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	PROB.	DIMENSIONES				
					[D]	[I]	[C]	[A]	[T]
			[E.21] Errores de mantenimiento / actualización de programas (software)	MB	M	M			
[HW] HARDWARE	[pc]	Equipos de cómputo	[N.1] Fuego	MB	MA				
			[N.2] Daños por agua	MB	MA				
			[N.*] Desastres naturales	MB	M				
			[I.5] Avería de origen físico o lógico	M	B				
			[I.6] Corte del suministro eléctrico	B	B				
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	B	B				
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	A				
			[E.24] Caída del sistema por agotamiento de recursos	A	A				
			[A.7] Uso no previsto	B	B	B	B		
			[A.11] Acceso no autorizado	B		M	B		
			[A.25] Robo	B	MA		MA		
	[ipphone]	Telefonos IP	[N.1] Fuego	MB	MA				
			[N.2] Daños por agua	MB	MA				
			[N.*] Desastres naturales	MB	M				
			[I.5] Avería de origen físico o lógico	M	B				
			[I.6] Corte del suministro eléctrico	B	B				
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	B	B				
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	A				
			[A.7] Uso no previsto	A	B	B	B		
			[A.25] Robo	B	M		MB		
	[host]	Servidor	[N.1] Fuego	MB	MA				
			[N.2] Daños por agua	MB	MA				
			[N.*] Desastres naturales	MB	M				
			[I.5] Avería de origen físico o lógico	MB	B				
			[I.6] Corte del suministro eléctrico	M	B				
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	B	B				
			[E.2] Errores del administrador	M	A	A	A		

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	PROB.	DIMENSIONES				
					[D]	[I]	[C]	[A]	[T]
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	A				
			[E.24] Caída del sistema por agotamiento de recursos	M	A				
			[A.7] Uso no previsto	B	M	M	M		
			[A.25] Robo	B	MA		MA		
	[switch]	Switch	[N.1] Fuego	MB	MA				
			[N.2] Daños por agua	MB	MA				
			[N.*] Desastres naturales	MB	M				
			[I.5] Avería de origen físico o lógico	M	B				
			[I.6] Corte del suministro eléctrico	M	B				
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	B	M				
	[firewall]	Firewall	[N.1] Fuego	MB	MA				
			[N.2] Daños por agua	MB	MA				
			[N.*] Desastres naturales	MB	M				
			[I.5] Avería de origen físico o lógico	B	B				
			[I.6] Corte del suministro eléctrico	M	B				
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	B	M				
			[A.5] Suplantación de la identidad del usuario	B		A	A	A	
			[A.24] Denegación de servicio	B	A				
[MEDIA] SOPORTE DE INFORMACIÓN	[san]	NAS	[N.1] Fuego	MB	MA				
			[N.2] Daños por agua	MB	MA				
			[N.*] Desastres naturales	MB	M				
			[I.5] Avería de origen físico o lógico	M	B				
			[I.6] Corte del suministro eléctrico	M	B				
	[dvd]	Copias de seguridad	[N.1] Fuego	MB	MA				
			[N.2] Daños por agua	MB	B				
			[N.*] Desastres naturales	MB	M				
			[I.10] Degradación de los soportes de almacenamiento de la información	B	M				
	[san]	DVR	[N.1] Fuego	MB	MA				
			[N.2] Daños por agua	MB	MA				
			[N.*] Desastres naturales	MB	M				
			[I.5] Avería de origen físico o lógico	B	B				
			[I.6] Corte del suministro eléctrico	M	B				

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	PROB.	DIMENSIONES				
					[D]	[I]	[C]	[A]	[T]
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	M	M				
			[E.2] Errores del administrador	M	A	B	A		
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	A				
			[A.11] Acceso no autorizado	B		A	A		
			[A.18] Destrucción de información	B	A				
[AUX] EQUIPAMIENTO AUXILIAR	[ups]	UPS	[N.1] Fuego	MB	MA				
			[N.2] Daños por agua	MB	MA				
			[N.*] Desastres naturales	MB	M				
			[I.*] Desastres industriales	B	M				
	[wire]	Instalaciones eléctricas	[N.1] Fuego	MB	MA				
			[N.2] Daños por agua	MB	MA				
			[N.*] Desastres naturales	MB	M				
			[I.*] Desastres industriales	B	A				
[COM] REDES DE COMUNICACIONES	[LAN]	Cableado estructurado	[I.8] Fallo de servicios de comunicaciones	B	A				
			[E.10] Errores de secuencia	MB		A			
			[A.5] Suplantación de la identidad del usuario	MB		M	M	M	
			[A.7] Uso no previsto	B	A	B	B		
			[A.9] [Re-]encaminamiento de mensajes	MB			MA		
			[A.12] Análisis de tráfico	MB			B		
			[A.14] Interceptación de información (escucha)	MB			B		
	[Internet]	Conectividad a internet	[I.8] Fallo de servicios de comunicaciones	M	A				
			[A.7] Uso no previsto	M	A	B	B		
			[A.12] Análisis de tráfico	B			B		
			[A.14] Interceptación de información (escucha)	MB			B		
	[ISDN]	Troncal SIP	[I.8] Fallo de servicios de comunicaciones	M	A				
			[A.7] Uso no previsto	M	A	B	B		
			[A.12] Análisis de tráfico	B			B		
			[A.14] Interceptación de información (escucha)	MB			B		
			[E.9] Errores de [re-]encaminamiento	MB			A		
			[E.24] Caída del sistema por agotamiento de recursos	M	A				
[P] PERSONAL	[adm]	Coordinador de sistemas	[E.19] Fugas de información	B			A		
			[E.28] Indisponibilidad del personal	M	A				
			[A.28] Indisponibilidad del personal	MB	A				
			[A.30] Ingeniería social	MB	M	A	A		

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	PROB.	DIMENSIONES				
					[D]	[I]	[C]	[A]	[T]
			(picaresca)						
	[prov]	Proveedores (Siesa, Qtech, Claro, OpenBox)	[E.19] Fugas de información	B			B		
			[E.28] Indisponibilidad del personal	A	M				
			[A.28] Indisponibilidad del personal	MB	M				
			[A.30] Ingeniería social (picaresca)	MB	B	B	B		
	[op]	Asistente de sistemas	[E.19] Fugas de información	B			M		
			[E.28] Indisponibilidad del personal	M	A				
			[A.28] Indisponibilidad del personal	MB	B				
			[A.30] Ingeniería social (picaresca)	MB	B	M	M		

Fuente: Autor

8.5 IMPACTO POTENCIAL

La medida del daño sobre un activo de información al materializarse una amenaza se denomina impacto. Se considera potencial ya que en este análisis no se tiene presente las salvaguardas desplegadas, es decir, no existe implementado ningún tipo de control. Teniendo como información primordial el valor de los activos para cada una de sus dimensiones y la degradación que producen las amenazas, se procede a calcular dicho impacto teniendo como recurso de estimación la siguiente tabla:

Tabla 11. Escala de valoración del impacto potencial

impacto		***degradación***		
		1%	10%	100%
valor	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Fuente: MAGERIT, libro III - Guía de técnicas

Tabla 12. Valoración de impacto potencial

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	DIMENSIONES				
				[D]	[I]	[C]	[A]	[T]
[D] DATOS/INFORMACIÓN	[backup]	Copias de seguridad	[E.2] Errores del administrador	MA	MA	MA		
			[E.18] Destrucción de información	MA				
	[files]	Ficheros de datos en Cobol	[E.2] Errores del administrador	MA	MA	MA		
			[E.18] Destrucción de información	MA				
[SW] SOFTWARE	[office]	Microsoft Office	[E.1] Errores de los usuarios	MB				
			[E.20] Vulnerabilidades de los programas (Software)	MB				
			[E.21] Errores de mantenimiento / actualización de programas (software)	MB				
	[office]	OpenOffice	[E.1] Errores de los usuarios	MB				
			[E.20] Vulnerabilidades de los programas (Software)	MB				
			[E.21] Errores de mantenimiento / actualización de programas (software)	MB				
	[std]	ERP Siesa 85	[E.1] Errores de los usuarios	M	M	M		
			[E.2] Errores del administrador	A	A	A		
			[E.15] Alteración accidental de la información		A			
			[E.18] Destrucción de información	A				
			[E.20] Vulnerabilidades de los programas (software)	M	M	M		
			[E.21] Errores de mantenimiento / actualización de programas (software)	A	A			
			[A.5] Suplantación de la identidad del usuario		A	A	A	
			[A.6] Abuso de privilegios de acceso	M	A	A		
	[std]	Ponto Secullum	[E.20] Vulnerabilidades de los programas (software)	MB	M	M		
			[E.21] Errores de mantenimiento / actualización de programas (software)	MB	M			
	[std]	Siesa intelligence	[E.20] Vulnerabilidades de los programas (software)	MB				
			[E.21] Errores de mantenimiento / actualización de	MB				

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	DIMENSIONES				
				[D]	[I]	[C]	[A]	[T]
			programas (software)					
	[os]	Sistemas operativos Windows 7, Windows 8, Centos 5.11	[E.1] Errores de los usuarios	M				
			[E.2] Errores del administrador	A				
			[E.8] Difusión de software dañino	A				
			[E.20] Vulnerabilidades de los programas (software)	A				
			[A.5] Suplantación de la identidad del usuario				A	
			[A.6] Abuso de privilegios de acceso	A				
			[A.7] Uso no previsto	M				
			[A.8] Difusión de software dañino	M				
			[A.11] Acceso no autorizado					
	[file]	Servidor de archivos	[E.1] Errores de los usuarios	M	M	M		
			[E.2] Errores del administrador	A	A	A		
			[E.20] Vulnerabilidades de los programas (software)	M	M	M		
			[E.21] Errores de mantenimiento / actualización de programas (software)	M	M			
			[A.5] Suplantación de la identidad del usuario		A	A	A	
	[www]	Servidor de presentación	[E.2] Errores del administrador	A				
			[E.20] Vulnerabilidades de los programas (software)	M				
	[dbms]	Servidor de base de datos	[E.2] Errores del administrador	A	A	A		
			[E.20] Vulnerabilidades de los programas (software)	M	A	A		
			[E.21] Errores de mantenimiento / actualización de programas (software)	M	M			
			[A.5] Suplantación de la identidad del usuario		A	A	A	
			[A.6] Abuso de privilegios de acceso	A	A	A		
			[A.11] Acceso no autorizado		A	M		
	[std]	Putty	[E.1] Errores de los usuarios	B				
			[E.21] Errores de mantenimiento / actualización de programas (software)	B				
	[sub]	SIIS	[E.1] Errores de los usuarios	M	M	M		
			[E.2] Errores del administrador	A	A	A		

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	DIMENSIONES				
				[D]	[I]	[C]	[A]	[T]
			[E.15] Alteración accidental de la información		A			
			[E.18] Destrucción de información	A				
			[E.20] Vulnerabilidades de los programas (software)	M	M	M		
			[E.21] Errores de mantenimiento / actualización de programas (software)	A	A			
			[A.5] Suplantación de la identidad del usuario		A	A	A	
			[A.6] Abuso de privilegios de acceso	M	A	A		
	[av]	Bitdefender Control Center	[E.2] Errores del administrador	A				
			[E.20] Vulnerabilidades de los programas (software)	M				
			[E.21] Errores de mantenimiento / actualización de programas (software)	M				
[HW] HARDWARE	[pc]	Equipos de cómputo	[N.1] Fuego	A				
			[N.2] Daños por agua	A				
			[N.*] Desastres naturales	M				
			[I.5] Avería de origen físico o lógico	M				
			[I.6] Corte del suministro eléctrico	M				
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	M				
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A				
			[E.24] Caída del sistema por agotamiento de recursos	A				
			[A.7] Uso no previsto	M				
			[A.11] Acceso no autorizado					
			[A.25] Robo	A				
	[ipphone]	Teléfonos IP	[N.1] Fuego	A				
			[N.2] Daños por agua	A				
			[N.*] Desastres naturales	M				
			[I.5] Avería de origen físico o lógico	M				
			[I.6] Corte del suministro eléctrico	M				
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	M				

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	DIMENSIONES				
				[D]	[I]	[C]	[A]	[T]
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A				
			[A.7] Uso no previsto	M				
			[A.25] Robo	M				
	[host]	Servidor	[N.1] Fuego	MA				
			[N.2] Daños por agua	MA				
			[N.*] Desastres naturales	A				
			[I.5] Avería de origen físico o lógico	M				
			[I.6] Corte del suministro eléctrico	M				
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	M				
			[E.2] Errores del administrador	MA				
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	MA				
			[E.24] Caída del sistema por agotamiento de recursos	MA				
			[A.7] Uso no previsto	MA				
			[A.25] Robo	MA				
	[switch]	Switch	[N.1] Fuego	A				
			[N.2] Daños por agua	A				
			[N.*] Desastres naturales	M				
			[I.5] Avería de origen físico o lógico	M				
			[I.6] Corte del suministro eléctrico	M				
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	M				
	[firewall]	Firewall	[N.1] Fuego	A				
			[N.2] Daños por agua	A				
			[N.*] Desastres naturales	M				
			[I.5] Avería de origen físico o lógico	M				
			[I.6] Corte del suministro eléctrico	M				
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	M				
			[A.5] Suplantación de la identidad del usuario			A		
			[A.24] Denegación de servicio	A				
[MEDIA] SOPORTE DE	[san]	NAS	[N.1] Fuego	A				

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	DIMENSIONES				
				[D]	[I]	[C]	[A]	[T]
INFORMACIÓN			[N.2] Daños por agua	A				
			[N.*] Desastres naturales	M				
			[I.5] Avería de origen físico o lógico	M				
			[I.6] Corte del suministro eléctrico	M				
	[dvd]	Copias de seguridad	[N.1] Fuego	MA				
			[N.2] Daños por agua	A				
			[N.*] Desastres naturales	A				
			[I.10] Degradación de los soportes de almacenamiento de la información	A				
	[san]	DVR	[N.1] Fuego	A				
			[N.2] Daños por agua	A				
			[N.*] Desastres naturales	M				
			[I.5] Avería de origen físico o lógico	M				
			[I.6] Corte del suministro eléctrico	M				
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	M				
			[E.2] Errores del administrador	M	M	A		
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A				
			[A.11] Acceso no autorizado		A	A		
			[A.18] Destrucción de información	A				
[AUX] EQUIPAMIENTO AUXILIAR	[ups]	UPS	[N.1] Fuego	MA				
			[N.2] Daños por agua	MA				
			[N.*] Desastres naturales	A				
			[I.*] Desastres industriales	A				
	[wire]	Instalaciones eléctricas	[N.1] Fuego	MA				
			[N.2] Daños por agua	MA				
			[N.*] Desastres naturales	A				
			[I.*] Desastres industriales	MA				
[COM] REDES DE COMUNICACIONES	[LAN]	Cableado estructurado	[I.8] Fallo de servicios de comunicaciones	MA				
			[E.10] Errores de secuencia		MA			
			[A.5] Suplantación de la identidad del usuario		A	A	A	
			[A.7] Uso no previsto	MA	A	A		
			[A.9] [Re-]encaminamiento de			MA		

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	DIMENSIONES				
				[D]	[I]	[C]	[A]	[T]
			mensajes					
			[A.12] Análisis de tráfico			A		
			[A.14] Interceptación de información (escucha)			A		
	[Internet]	Conectividad a internet	[I.8] Fallo de servicios de comunicaciones	A				
			[A.7] Uso no previsto	A				
			[A.12] Análisis de tráfico					
			[A.14] Interceptación de información (escucha)					
	[ISDN]	Troncal SIP	[I.8] Fallo de servicios de comunicaciones	A				
			[A.7] Uso no previsto	A				
			[A.12] Análisis de tráfico					
			[A.14] Interceptación de información (escucha)					
			[E.9] Errores de [re-]encaminamiento					
			[E.24] Caída del sistema por agotamiento de recursos	A				
[P] PERSONAL	[adm]	Coordinador de sistemas	[E.19] Fugas de información			A		
			[E.28] Indisponibilidad del personal	A				
			[A.28] Indisponibilidad del personal	A				
			[A.30] Ingeniería social (picaresca)	M		A		
	[prov]	Provedores (Siesa, Qtech, Claro, OpenBox)	[E.19] Fugas de información			M		
			[E.28] Indisponibilidad del personal	M				
			[A.28] Indisponibilidad del personal	M				
			[A.30] Ingeniería social (picaresca)	M		M		
	[op]	Asistente de sistemas	[E.19] Fugas de información			M		
			[E.28] Indisponibilidad del personal	A				
			[A.28] Indisponibilidad del personal	M				
			[A.30] Ingeniería social (picaresca)	M		M		

Fuente: Autor

8.6 RIESGO POTENCIAL

El riesgo es definido como una medida referente al daño probable sobre un sistema. Habiendo determinado el impacto de las amenazas sobre los activos, se calcula el riesgo en función de la probabilidad de ocurrencia.

La valoración del riesgo se realiza bajo el siguiente esquema:

Tabla 13. Escala de valoración de riesgo potencial

riesgo		***probabilidad***				
		MB	B	M	A	MA
impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: MAGERIT, libro III - Guía de técnicas

En la siguiente tabla se expone el riesgo potencial para cada uno de los activos de información.

Tabla 14. Valoración de riesgo potencial

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	PROB.	DIMENSIONES				
					[D]	[I]	[C]	[A]	[T]
[D] DATOS/INFORMACIÓN	[files]	Ficheros de datos en Cobol	[E.2] Errores del administrador	M	MA	MA	MA		
			[E.18] Destrucción de información	B	MA				
	[backup]	Copias de seguridad	[E.2] Errores del administrador	M	MA	MA	MA		
			[E.18] Destrucción de información	B	MA				
[SW] SOFTWARE	[office]	Microsoft Office	[E.1] Errores de los usuarios	A	B				
			[E.20] Vulnerabilidades de los programas (Software)	B	MB				
			[E.21] Errores de mantenimiento / actualización de programas (software)	B	MB				
	[office]	OpenOffice	[E.1] Errores de los usuarios	A	B				
			[E.20] Vulnerabilidades de los programas (Software)	B	B				
			[E.21] Errores de mantenimiento / actualización de	B	MB				

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	PROB.	DIMENSIONES				
					[D]	[I]	[C]	[A]	[T]
			programas (software)						
	[std]	ERP Siesa 85	[E.1] Errores de los usuarios	MA	A	A	A		
			[E.2] Errores del administrador	M	A	A	A		
			[E.15] Alteración accidental de la información	A		MA			
			[E.18] Destrucción de información	M	A				
			[E.20] Vulnerabilidades de los programas (software)	B	M	M	M		
			[E.21] Errores de mantenimiento / actualización de programas (software)	M	A	A			
			[A.5] Suplantación de la identidad del usuario	B		A	A	A	
			[A.6] Abuso de privilegios de acceso	B	M	A	A		
	[std]	Ponto Secullum	[E.20] Vulnerabilidades de los programas (software)	B	MB	M	M		
			[E.21] Errores de mantenimiento / actualización de programas (software)	B	MB	M			
	[std]	Siesa intelligence	[E.20] Vulnerabilidades de los programas (software)	B	MB				
			[E.21] Errores de mantenimiento / actualización de programas (software)	B	MB				
	[os]	Sistemas operativos Windows 7, Windows 8, Centos 5.11	[E.1] Errores de los usuarios	A	A				
			[E.2] Errores del administrador	M	A				
			[E.8] Difusión de software dañino	MB	M				
			[E.20] Vulnerabilidades de los programas (software)	MB	M				
			[A.5] Suplantación de la identidad del usuario	MB				M	
			[A.6] Abuso de privilegios de acceso	B	A				
			[A.7] Uso no previsto	M	M				
			[A.8] Difusión de software dañino	MB	B				
	[file]	Servidor de archivos	[E.1] Errores de los usuarios	A	M	M	M		
			[E.2] Errores del administrador	M	A	A	A		
			[E.20] Vulnerabilidades de los programas (software)	MB	B	B	B		
			[E.21] Errores de mantenimiento / actualización de programas (software)	B	M	M			

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	PROB.	DIMENSIONES				
					[D]	[I]	[C]	[A]	[T]
			[A.5] Suplantación de la identidad del usuario	M		A	A	A	
	[www]	Servidor de presentacion	[E.2] Errores del administrador	B	A				
			[E.20] Vulnerabilidades de los programas (software)	MB	B				
	[dbms]	Servidor de base de datos	[E.2] Errores del administrador	B	A	A	A		
			[E.20] Vulnerabilidades de los programas (software)	MB	B	M	M		
			[E.21] Errores de mantenimiento / actualización de programas (software)	B	M	M			
			[A.5] Suplantación de la identidad del usuario	MB		M	M	M	
			[A.6] Abuso de privilegios de acceso	MB	M	M	M		
			[A.11] Acceso no autorizado	MB		M	M		
	[std]	Putty	[E.1] Errores de los usuarios	A	M				
			[E.21] Errores de mantenimiento / actualización de programas (software)	MB	MB				
	[sub]	SIIS	[E.1] Errores de los usuarios	A	M	M	M		
			[E.2] Errores del administrador	M	A	A	A		
			[E.15] Alteración accidental de la información	A		MA			
			[E.18] Destrucción de información	M	A				
			[E.20] Vulnerabilidades de los programas (software)	B	M	M	M		
			[E.21] Errores de mantenimiento / actualización de programas (software)	M	A	A			
			[A.5] Suplantación de la identidad del usuario	B		A	A	A	
			[A.6] Abuso de privilegios de acceso	B	M	A	A		
	[av]	Bitdefender Control Center	[E.2] Errores del administrador	M	A				
			[E.20] Vulnerabilidades de los programas (software)	MB	B				
			[E.21] Errores de mantenimiento / actualización de programas (software)	MB	B				
[HW] HARDWARE	[pc]	Equipos de cómputo	[N.1] Fuego	MB	M				
			[N.2] Daños por agua	MB	M				
			[N.*] Desastres naturales	MB	B				
			[I.5] Avería de origen físico o lógico	M	A				
			[I.6] Corte del	B	M				

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	PROB.	DIMENSIONES				
					[D]	[I]	[C]	[A]	[T]
			suministro eléctrico						
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	B	M				
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	A				
			[E.24] Caída del sistema por agotamiento de recursos	A	MA				
			[A.7] Uso no previsto	B	M				
			[A.25] Robo	B	A				
	[ipphone]	Teléfonos IP	[N.1] Fuego	MB	M				
			[N.2] Daños por agua	MB	M				
			[N.*] Desastres naturales	MB	B				
			[I.5] Avería de origen físico o lógico	M	A				
			[I.6] Corte del suministro eléctrico	B	M				
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	B	M				
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	A				
			[A.7] Uso no previsto	A	A				
			[A.25] Robo	B	M				
	[host]	Servidor	[N.1] Fuego	MB	A				
			[N.2] Daños por agua	MB	A				
			[N.*] Desastres naturales	MB	M				
			[I.5] Avería de origen físico o lógico	MB	B				
			[I.6] Corte del suministro eléctrico	M	M				
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	B	M				
			[E.2] Errores del administrador	M	MA				
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	MA				
			[E.24] Caída del sistema por agotamiento de recursos	M	MA				
			[A.7] Uso no previsto	B	MA				
			[A.25] Robo	B	MA				
	[switch]	Switch	[N.1] Fuego	MB	M				

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	PROB.	DIMENSIONES				
					[D]	[I]	[C]	[A]	[T]
			[N.2] Daños por agua	MB	M				
			[N.*] Desastres naturales	MB	B				
			[I.5] Avería de origen físico o lógico	M	M				
			[I.6] Corte del suministro eléctrico	M	M				
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	B	M				
	[firewall]	Firewall	[N.1] Fuego	MB	M				
			[N.2] Daños por agua	MB	M				
			[N.*] Desastres naturales	MB	B				
			[I.5] Avería de origen físico o lógico	B	M				
			[I.6] Corte del suministro eléctrico	M	M				
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	B	M				
			[A.5] Suplantación de la identidad del usuario	B			A		
			[A.24] Denegación de servicio	B	A				
[MEDIA] SOPORTE DE INFORMACIÓN	[san]	NAS	[N.1] Fuego	MB	M				
			[N.2] Daños por agua	MB	M				
			[N.*] Desastres naturales	MB	B				
			[I.5] Avería de origen físico o lógico	M	M				
			[I.6] Corte del suministro eléctrico	M	M				
	[san]	DVR	[N.1] Fuego	MB	M				
			[N.2] Daños por agua	MB	M				
			[N.*] Desastres naturales	MB	B				
			[I.5] Avería de origen físico o lógico	B	M				
			[I.6] Corte del suministro eléctrico	M	M				
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	M	M				
			[E.2] Errores del administrador	M	M	M	A		
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	A				
			[A.11] Acceso no autorizado	B		A	A		
			[A.18] Destrucción de información	B	A				
[AUX] EQUIPAMIENTO AUXILIAR	[ups]	UPS	[N.1] Fuego	MB	A				
			[N.2] Daños por agua	MB	A				
			[N.*] Desastres	MB	M				

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	PROB.	DIMENSIONES				
					[D]	[I]	[C]	[A]	[T]
			naturales						
			[I.*] Desastres industriales	B	A				
	[wire]	Instalaciones eléctricas	[N.1] Fuego	MB	A				
			[N.2] Daños por agua	MB	A				
			[N.*] Desastres naturales	MB	M				
			[I.*] Desastres industriales	B	MA				
[COM] REDES DE COMUNICACIONES	[LAN]	Cableado estructurado	[I.8] Fallo de servicios de comunicaciones	B	MA				
			[E.10] Errores de secuencia	MB		A			
			[A.5] Suplantación de la identidad del usuario	MB		M	M	M	
			[A.7] Uso no previsto	B	MA	A	A		
			[A.9] [Re-]encaminamiento de mensajes	MB			MA		
			[A.12] Análisis de tráfico	MB			M		
			[A.14] Interceptación de información (escucha)	MB			M		
	[Internet]	Conectividad a internet	[I.8] Fallo de servicios de comunicaciones	M	A				
			[A.7] Uso no previsto	M	A				
	[ISDN]	Troncal SIP	[I.8] Fallo de servicios de comunicaciones	M	A				
			[A.7] Uso no previsto	M	A				
			[E.24] Caída del sistema por agotamiento de recursos	M	A				
[P] PERSONAL	[adm]	Coordinador de sistemas	[E.19] Fugas de información	B			A		
			[E.28] Indisponibilidad del personal	M	A				
			[A.28] Indisponibilidad del personal	MB	A				
			[A.30] Ingeniería social (picaresca)	MB	B		M		
	[prov]	Provedores (Siesa, Qtech, Claro, OpenBox)	[E.19] Fugas de información	B			M		
			[E.28] Indisponibilidad del personal	A	A				
			[A.28] Indisponibilidad del personal	MB	B				
			[A.30] Ingeniería social (picaresca)	MB	B		B		
	[op]	Asistente de sistemas	[E.19] Fugas de información	B			M		
			[E.28] Indisponibilidad del personal	M	A				
			[A.28] Indisponibilidad del personal	MB	B				
			[A.30] Ingeniería social (picaresca)	MB	B		B		

Fuente: Autor

8.7 IDENTIFICACIÓN Y VALORACIÓN DE SALVAGUARDAS

En el análisis de impacto y riesgo potencial realizado anteriormente no se ha tenido en cuenta ninguna salvaguarda desplegada o implementada, por ende no habría ningún tipo de protección. Las salvaguardas se establecen como mecanismos, técnicas o procedimientos que garantizan una reducción del riesgo determinado.

La metodología MAGERIT define los diferentes tipos de salvaguardas de la siguiente manera:

Tabla 15. Tipos de salvaguardas

EFECTO	TIPO
preventivas: reducen la probabilidad	[PR] preventivas
	[DR] disuasorias
	[EL] eliminatorias
acotan la degradación	[IM] minimizadoras
	[CR] correctivas
	[RC] recuperativas
consolidan el efecto de las demás	[MN] de monitorización
	[DC] de detección
	[AW] de concienciación
	[AD] administrativas

Fuente: MAGERIT, libro I - Método

Teniendo en cuenta el catálogo de salvaguardas dispuesto por la metodología y su correspondiente clasificación, se realiza la identificación de los mecanismos utilizados en la organización con el fin de proteger los activos de información frente a las diferentes amenazas, donde se evidencia el nivel de eficacia frente a estas.

Tabla 16. Identificación de salvaguardas

SALVAGUARDAS	TIPO	EVALUACIÓN
Protecciones generales u horizontales	Identificación y autenticación	60%
	Control de acceso lógico	70%
	IDS/IPS: Herramienta de detección / prevención de intrusión	70%
	Herramienta de monitorización de tráfico	50%
	Herramienta para análisis de logs	60%
Protección de los datos / información	Copias de seguridad de los datos (backup)	40%
	Cifrado de la información	70%
Protección de los servicios	Se aplican perfiles de seguridad	70%
	Protección de servicios y aplicaciones web	70%
	Protección del directorio	70%
Protección de las aplicaciones (software)	Copias de seguridad (backup)	50%
	Cambios (actualizaciones y mantenimiento)	70%
Protección de los equipos (hardware)	Se aplican perfiles de seguridad	80%
	Protección de la centralita telefónica (PABX)	30%
Protección de las comunicaciones	Internet: uso de acceso	60%
	Seguridad Wireless (WiFi)	50%
Protección de los elementos auxiliares	Suministro eléctrico	30%
	Climatización	20%
Seguridad física – Protección de las instalaciones	Control de los accesos físicos	60%

Fuente: Autor

8.8 IMPACTO RESIDUAL

El nivel de eficacia de las salvaguardas identificadas permite conocer el impacto real en la degradación de las dimensiones de los diferentes activos de información al configurarse las amenazas descritas.

Tabla 17. Valoración del impacto residual

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	DIMENSIONES				
				[D]	[I]	[C]	[A]	[T]
[D] DATOS/INFORMACIÓN	[files]	Ficheros de datos en Cobol	[E.2] Errores del administrador	M	M	M		
			[E.18] Destrucción de información	M				
	[backup]	Copias de seguridad	[E.2] Errores del administrador	M	M	M		
			[E.18] Destrucción de información	M				
[SW] SOFTWARE	[office]	Microsoft Office	[E.1] Errores de los usuarios	MB				
			[E.20] Vulnerabilidades de los programas (Software)	MB				
			[E.21] Errores de mantenimiento / actualización de programas (software)	MB				
	[office]	OpenOffice	[E.1] Errores de los usuarios	MB				
			[E.20] Vulnerabilidades de los programas (Software)	MB				
			[E.21] Errores de mantenimiento / actualización de programas (software)	MB				
	[std]	ERP Siesa 85	[E.1] Errores de los usuarios	M	M	M		
			[E.2] Errores del administrador	M	M	M		
			[E.15] Alteración accidental de la información		B			
			[E.18] Destrucción de información	B				
			[E.20] Vulnerabilidades de los programas (software)	M	M	M		
			[E.21] Errores de mantenimiento / actualización de programas (software)	M	M			
			[A.5] Suplantación de la identidad del usuario		A	A	A	
			[A.6] Abuso de privilegios de acceso	M	M	M		
	[std]	Ponto Secullum	[E.20] Vulnerabilidades de los programas (software)	MB	M	M		
			[E.21] Errores de mantenimiento / actualización de programas (software)	MB	M			
	[std]	Siesa intelligence	[E.20] Vulnerabilidades de los programas (software)	MB				
			[E.21] Errores de mantenimiento / actualización de programas (software)	MB				
	[os]	Sistemas operativos Windows 7, Windows 8,	[E.1] Errores de los usuarios	M				

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	DIMENSIONES				
				[D]	[I]	[C]	[A]	[T]
		Centos 5.11	[E.2] Errores del administrador	B				
			[E.8] Difusión de software dañino	M				
			[E.20] Vulnerabilidades de los programas (software)	M				
			[A.5] Suplantación de la identidad del usuario				M	
			[A.6] Abuso de privilegios de acceso	B				
			[A.7] Uso no previsto	M				
			[A.8] Difusión de software dañino	M				
			[A.11] Acceso no autorizado					
	[file]	Servidor de archivos	[E.1] Errores de los usuarios	M	M	M		
			[E.2] Errores del administrador	M	M	M		
			[E.20] Vulnerabilidades de los programas (software)	M	M	M		
			[E.21] Errores de mantenimiento / actualización de programas (software)	M	M			
			[A.5] Suplantación de la identidad del usuario		B	B	B	
	[www]	Servidor de presentación	[E.2] Errores del administrador	M				
			[E.20] Vulnerabilidades de los programas (software)	M				
	[dbms]	Servidor de base de datos	[E.2] Errores del administrador	M	M	M		
			[E.20] Vulnerabilidades de los programas (software)	M	A	A		
			[E.21] Errores de mantenimiento / actualización de programas (software)	M	M			
			[A.5] Suplantación de la identidad del usuario		M	M	M	
			[A.6] Abuso de privilegios de acceso	M	M	M		
			[A.11] Acceso no autorizado		M	M		
	[std]	Putty	[E.1] Errores de los usuarios	B				
			[E.21] Errores de mantenimiento / actualización de programas (software)	B				
	[sub]	SIIS	[E.1] Errores de los usuarios	M	M	M		
			[E.2] Errores del administrador	M	M	M		
			[E.15] Alteración accidental de la información		M			
			[E.18] Destrucción de información	B				

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	DIMENSIONES				
				[D]	[I]	[C]	[A]	[T]
			[E.20] Vulnerabilidades de los programas (software)	M	M	M		
			[E.21] Errores de mantenimiento / actualización de programas (software)	A	A			
			[A.5] Suplantación de la identidad del usuario		M	M	M	
			[A.6] Abuso de privilegios de acceso	B	B	B		
	[av]	Bitdefender Control Center	[E.2] Errores del administrador	M				
			[E.20] Vulnerabilidades de los programas (software)	M				
			[E.21] Errores de mantenimiento / actualización de programas (software)	M				
[HW] HARDWARE	[pc]	Equipos de cómputo	[N.1] Fuego	M				
			[N.2] Daños por agua	M				
			[N.*] Desastres naturales	M				
			[I.5] Avería de origen físico o lógico	M				
			[I.6] Corte del suministro eléctrico	M				
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	M				
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
			[E.24] Caída del sistema por agotamiento de recursos	M				
			[A.7] Uso no previsto	M				
			[A.11] Acceso no autorizado					
			[A.25] Robo	M				
	[ipphone]	Teléfonos IP	[N.1] Fuego	M				
			[N.2] Daños por agua	M				
			[N.*] Desastres naturales	M				
			[I.5] Avería de origen físico o lógico	M				
			[I.6] Corte del suministro eléctrico	M				
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	M				
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
			[A.7] Uso no previsto	M				
			[A.25] Robo	M				
	[host]	Servidor	[N.1] Fuego	M				

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	DIMENSIONES				
				[D]	[I]	[C]	[A]	[T]
			[N.2] Daños por agua	M				
			[N.*] Desastres naturales	M				
			[I.5] Avería de origen físico o lógico	M				
			[I.6] Corte del suministro eléctrico	M				
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	M				
			[E.2] Errores del administrador	M				
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M				
			[E.24] Caída del sistema por agotamiento de recursos	M				
			[A.7] Uso no previsto	M				
			[A.25] Robo	M				
	[switch]	Switch	[N.1] Fuego	M				
			[N.2] Daños por agua	M				
			[N.*] Desastres naturales	M				
			[I.5] Avería de origen físico o lógico	M				
			[I.6] Corte del suministro eléctrico	M				
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	M				
	[firewall]	Firewall	[N.1] Fuego	M				
			[N.2] Daños por agua	M				
			[N.*] Desastres naturales	M				
			[I.5] Avería de origen físico o lógico	M				
			[I.6] Corte del suministro eléctrico	M				
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	M				
			[A.5] Suplantación de la identidad del usuario			M		
			[A.24] Denegación de servicio	M				
[MEDIA] SOPORTE DE INFORMACIÓN	[san]	NAS	[N.1] Fuego	M				
			[N.2] Daños por agua	M				
			[N.*] Desastres naturales	M				
			[I.5] Avería de origen físico o lógico	M				
			[I.6] Corte del suministro eléctrico	M				
	[san]	DVR	[N.1] Fuego	M				
			[N.2] Daños por agua	M				
			[N.*] Desastres naturales	M				

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	DIMENSIONES				
				[D]	[I]	[C]	[A]	[T]
			[I.5] Avería de origen físico o lógico	M				
			[I.6] Corte del suministro eléctrico	M				
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	M				
			[E.2] Errores del administrador	B	B	B		
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A				
			[A.11] Acceso no autorizado		B	B		
			[A.18] Destrucción de información	B				
[AUX] EQUIPAMIENTO AUXILIAR	[ups]	UPS	[N.1] Fuego	M				
			[N.2] Daños por agua	M				
			[N.*] Desastres naturales	M				
			[I.*] Desastres industriales	M				
	[wire]	Instalaciones eléctricas	[N.1] Fuego	M				
			[N.2] Daños por agua	M				
			[N.*] Desastres naturales	M				
			[I.*] Desastres industriales	M				
[COM] REDES DE COMUNICACIONES	[LAN]	Cableado estructurado	[I.8] Fallo de servicios de comunicaciones	B				
			[E.10] Errores de secuencia		B			
			[A.5] Suplantación de la identidad del usuario		B	B	B	
			[A.7] Uso no previsto	B	B	B		
			[A.9] [Re-]encaminamiento de mensajes			B		
			[A.12] Análisis de tráfico			B		
			[A.14] Interceptación de información (escucha)			B		
	[Internet]	Conectividad a internet	[I.8] Fallo de servicios de comunicaciones	M				
			[A.7] Uso no previsto	M				
			[A.12] Análisis de tráfico					
			[A.14] Interceptación de información (escucha)					
	[ISDN]	Troncal SIP	[I.8] Fallo de servicios de comunicaciones	M				
			[A.7] Uso no previsto	M				
			[A.12] Análisis de tráfico					
			[A.14] Interceptación de información (escucha)					
			[E.9] Errores de [re-]encaminamiento					
			[E.24] Caída del sistema por agotamiento de recursos	M				

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	DIMENSIONES				
				[D]	[I]	[C]	[A]	[T]
[P] PERSONAL	[adm]	Coordinador de sistemas	[E.19] Fugas de información			M		
			[E.28] Indisponibilidad del personal	M				
			[A.28] Indisponibilidad del personal	M				
			[A.30] Ingeniería social (picaresca)	M		M		
	[prov]	Provedores (Siesa, Qtech, Claro, OpenBox)	[E.19] Fugas de información			M		
			[E.28] Indisponibilidad del personal	M				
			[A.28] Indisponibilidad del personal	M				
			[A.30] Ingeniería social (picaresca)	M		M		
	[op]	Asistente de sistemas	[E.19] Fugas de información			M		
			[E.28] Indisponibilidad del personal	M				
			[A.28] Indisponibilidad del personal	M				
			[A.30] Ingeniería social (picaresca)	M		M		

Fuente: Autor

8.9 RIESGO RESIDUAL

Se evalúa el riesgo residual en función de la probabilidad de las amenazas y el impacto pero en esta ocasión, el impacto residual.

Tabla 18. Valoración del riesgo residual

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	PROB.	DIMENSIONES				
					[D]	[I]	[C]	[A]	[T]
[D] DATOS/INFORMACIÓN	[files]	Ficheros de datos en Cobol	[E.2] Errores del administrador	M	M	M	M		
			[E.18] Destrucción de información	B	M				
	[backup]	Copias de seguridad	[E.2] Errores del administrador	M	M	M	M		
			[E.18] Destrucción de información	B	M				
[SW] SOFTWARE	[office]	Microsoft Office	[E.1] Errores de los usuarios	A	B				
			[E.20] Vulnerabilidades de los programas (Software)	B	MB				

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	PROB.	DIMENSIONES				
					[D]	[I]	[C]	[A]	[T]
			[E.21] Errores de mantenimiento / actualización de programas (software)	B	MB				
	[office]	OpenOffice	[E.1] Errores de los usuarios	A	B				
			[E.20] Vulnerabilidades de los programas (Software)	B	MB				
			[E.21] Errores de mantenimiento / actualización de programas (software)	B	MB				
	[std]	ERP Siesa 85	[E.1] Errores de los usuarios	MA	A	A	A		
			[E.2] Errores del administrador	M	M	M	M		
			[E.15] Alteración accidental de la información	A		M			
			[E.18] Destrucción de información	M	B				
			[E.20] Vulnerabilidades de los programas (software)	B	M	M	M		
			[E.21] Errores de mantenimiento / actualización de programas (software)	M	M	M			
			[A.5] Suplantación de la identidad del usuario	B		A	A	A	
			[A.6] Abuso de privilegios de acceso	B	M	M	M		
	[std]	Ponto Secullum	[E.20] Vulnerabilidades de los programas (software)	B	MB	M	M		
			[E.21] Errores de mantenimiento / actualización de programas (software)	B	MB	M			
	[std]	Siesa intelligence	[E.20] Vulnerabilidades de los programas (software)	B	MB				
			[E.21] Errores de mantenimiento / actualización de programas (software)	B	MB				
	[os]	Sistemas operativos Windows 7, Windows 8, Centos 5.11	[E.1] Errores de los usuarios	A	A				
			[E.2] Errores del administrador	M	B				
			[E.8] Difusión de software dañino	MB	B				

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	PROB.	DIMENSIONES				
					[D]	[I]	[C]	[A]	[T]
			[E.20] Vulnerabilidades de los programas (software)	MB	B				
			[A.5] Suplantación de la identidad del usuario	MB				B	
			[A.6] Abuso de privilegios de acceso	B	B				
			[A.7] Uso no previsto	M	M				
			[A.8] Difusión de software dañino	MB	B				
	[file]	Servidor de archivos	[E.1] Errores de los usuarios	A	A	A	A		
			[E.2] Errores del administrador	M	M	M	M		
			[E.20] Vulnerabilidades de los programas (software)	MB	B	B	B		
			[E.21] Errores de mantenimiento / actualización de programas (software)	B	M	M			
			[A.5] Suplantación de la identidad del usuario	M		B	B	B	
	[www]	Servidor de presentación	[E.2] Errores del administrador	B	M				
			[E.20] Vulnerabilidades de los programas (software)	MB	B				
	[dbms]	Servidor de base de datos	[E.2] Errores del administrador	B	M	M	M		
			[E.20] Vulnerabilidades de los programas (software)	MB	B	M	M		
			[E.21] Errores de mantenimiento / actualización de programas (software)	B	M	M			
			[A.5] Suplantación de la identidad del usuario	MB		B	B	B	
			[A.6] Abuso de privilegios de acceso	MB	B	B	B		
			[A.11] Acceso no autorizado	MB		B	B		
	[std]	Putty	[E.1] Errores de los usuarios	A	M				
			[E.21] Errores de mantenimiento / actualización de programas (software)	MB	MB				
	[sub]	SIIS	[E.1] Errores de los usuarios	A	A	A	A		
			[E.2] Errores del administrador	M	M	M	M		

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	PROB.	DIMENSIONES				
					[D]	[I]	[C]	[A]	[T]
			[E.15] Alteración accidental de la información	A		M			
			[E.18] Destrucción de información	M	B				
			[E.20] Vulnerabilidades de los programas (software)	B	M	M	M		
			[E.21] Errores de mantenimiento / actualización de programas (software)	M	A	A			
			[A.5] Suplantación de la identidad del usuario	B		M	M	M	
			[A.6] Abuso de privilegios de acceso	B	B	B	B		
	[av]	Bitdefender Control Center	[E.2] Errores del administrador	M	M				
			[E.20] Vulnerabilidades de los programas (software)	MB	B				
			[E.21] Errores de mantenimiento / actualización de programas (software)	MB	B				
[HW] HARDWARE	[pc]	Equipos de cómputo	[N.1] Fuego	MB	B				
			[N.2] Daños por agua	MB	B				
			[N.*] Desastres naturales	MB	B				
			[I.5] Avería de origen físico o lógico	M	M				
			[I.6] Corte del suministro eléctrico	B	M				
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	B	M				
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	M				
			[E.24] Caída del sistema por agotamiento de recursos	A	A				
			[A.7] Uso no previsto	B	M				
			[A.25] Robo	B	M				
	[ipphone]	Teléfonos IP	[N.1] Fuego	MB	B				
			[N.2] Daños por agua	MB	B				
			[N.*] Desastres naturales	MB	B				
			[I.5] Avería de origen físico o lógico	M	M				

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	PROB.	DIMENSIONES				
					[D]	[I]	[C]	[A]	[T]
			[I.6] Corte del suministro eléctrico	B	M				
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	B	M				
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	M				
			[A.7] Uso no previsto	A	A				
			[A.25] Robo	B	M				
	[host]	Servidor	[N.1] Fuego	MB	B				
			[N.2] Daños por agua	MB	B				
			[N.*] Desastres naturales	MB	B				
			[I.5] Avería de origen físico o lógico	MB	B				
			[I.6] Corte del suministro eléctrico	M	M				
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	B	M				
			[E.2] Errores del administrador	M	M				
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	M				
			[E.24] Caída del sistema por agotamiento de recursos	M	M				
			[A.7] Uso no previsto	B	M				
			[A.25] Robo	B	M				
	[switch]	Switch	[N.1] Fuego	MB	B				
			[N.2] Daños por agua	MB	B				
			[N.*] Desastres naturales	MB	B				
			[I.5] Avería de origen físico o lógico	M	M				
			[I.6] Corte del suministro eléctrico	M	M				
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	B	M				
	[firewall]	Firewall	[N.1] Fuego	MB	B				
			[N.2] Daños por agua	MB	B				
			[N.*] Desastres naturales	MB	B				
			[I.5] Avería de origen físico o lógico	B	M				

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	PROB.	DIMENSIONES				
					[D]	[I]	[C]	[A]	[T]
			[I.6] Corte del suministro eléctrico	M	M				
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	B	M				
			[A.5] Suplantación de la identidad del usuario	B			M		
			[A.24] Denegación de servicio	B	M				
[MEDIA] SOPORTE DE INFORMACIÓN	[san]	NAS	[N.1] Fuego	MB	B				
			[N.2] Daños por agua	MB	B				
			[N.*] Desastres naturales	MB	B				
			[I.5] Avería de origen físico o lógico	M	M				
			[I.6] Corte del suministro eléctrico	M	M				
	[san]	DVR	[N.1] Fuego	MB	B				
			[N.2] Daños por agua	MB	B				
			[N.*] Desastres naturales	MB	B				
			[I.5] Avería de origen físico o lógico	B	M				
			[I.6] Corte del suministro eléctrico	M	M				
			[I.7] Condiciones inadecuadas de temperatura y/o humedad	M	M				
			[E.2] Errores del administrador	M	B	B	B		
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	A				
			[A.11] Acceso no autorizado	B		B	B		
			[A.18] Destrucción de información	B	B				
[AUX] EQUIPAMIENTO AUXILIAR	[ups]	UPS	[N.1] Fuego	MB	MB				
			[N.2] Daños por agua	MB	MB				
			[N.*] Desastres naturales	MB	MB				
			[I.*] Desastres industriales	B	M				
	[wire]	Instalaciones eléctricas	[N.1] Fuego	MB	B				
			[N.2] Daños por agua	MB	B				
			[N.*] Desastres naturales	MB	B				
			[I.*] Desastres industriales	B	M				
[COM] REDES DE COMUNICACIONES	[LAN]	Cableado estructurado	[I.8] Fallo de servicios de comunicaciones	B	B				
			[E.10] Errores de	MB		MB			

CLASIFICACIÓN	TIPO	ACTIVO	AMENAZAS	PROB.	DIMENSIONES				
					[D]	[I]	[C]	[A]	[T]
			secuencia						
			[A.5] Suplantación de la identidad del usuario	MB		MB	MB	MB	
			[A.7] Uso no previsto	B	B	B	B		
			[A.9] [Re-]encaminamiento de mensajes	MB			MB		
			[A.12] Análisis de tráfico	MB			MB		
			[A.14] Interceptación de información (escucha)	MB			MB		
	[Internet]	Conectividad a internet	[I.8] Fallo de servicios de comunicaciones	M	M				
			[A.7] Uso no previsto	M	M				
	[ISDN]	Troncal SIP	[I.8] Fallo de servicios de comunicaciones	M	M				
			[A.7] Uso no previsto	M	M				
			[E.24] Caída del sistema por agotamiento de recursos	M	M				
[P] PERSONAL	[adm]	Coordinador de sistemas	[E.19] Fugas de información	B			M		
			[E.28] Indisponibilidad del personal	M	M				
			[A.28] Indisponibilidad del personal	MB	B				
			[A.30] Ingeniería social (picaresca)	MB	B		B		
	[prov]	Proveedores (Siesa, Qtech, Claro, OpenBox)	[E.19] Fugas de información	B			M		
			[E.28] Indisponibilidad del personal	A	A				
			[A.28] Indisponibilidad del personal	MB	B				
			[A.30] Ingeniería social (picaresca)	MB	B		B		
	[op]	Asistente de sistemas	[E.19] Fugas de información	B			M		
			[E.28] Indisponibilidad del personal	M	M				
			[A.28] Indisponibilidad del personal	MB	B				
			[A.30] Ingeniería social (picaresca)	MB	B		B		

Fuente: Autor

8.10 DECLARACIÓN DE APLICABILIDAD

Teniendo como referencia el anexo A de la norma NTC/ISO 27001 en su versión 2013, se establecen los controles aplicables para la correcta operación del Sistema de Gestión de Seguridad de la Información, teniendo en cuenta los resultados obtenidos en la valoración de riesgos.

Tabla 19. Declaración de aplicabilidad

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	**Sección**	**Objetivo de control / control**	
5 Políticas de Seguridad	5,1	Dirección de la alta gerencia para la seguridad de la información	
	5.1.1	Políticas de seguridad de la información	Se debe establecer un documento con las políticas de seguridad de la organización, este debe ser aprobado por la gerencia y posteriormente debe ser socializado a todos los funcionarios de la empresa y terceros involucrados
	5.1.2	Revisión de las políticas de seguridad de la información	Periódicamente se debe hacer una revisión de la políticas y hacer los cambios necesarios cuando allá lugar a modificaciones del SGSI
6 Organización	6,1	Organización interna	

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	**Sección**	**Objetivo de control / control**	
de la Seguridad de la Información	6.1.1	Roles y responsabilidad de seguridad de la información	La gerencia dispondrá y definirá los principales responsables con el fin de garantizar la seguridad de la información dentro de la compañía
	6.1.2	Segregación de deberes	Definir las funciones para cada actor dentro SGSI, con el fin de evitar que una sola persona sea responsable del proceso. Dichas responsabilidades serán definidas en el manual de funciones de cada colaborador
	6.1.3	Contacto con autoridades	Establecer procedimientos para determinar ante qué situación y con qué autoridad competente se debe establecer comunicación con el fin de dar oportuna respuesta a un incidente o novedad de seguridad

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	Sección	Objetivo de control / control	
	6.1.4	Contacto con grupos de interés especial	Se debe mantener un canal de comunicación con grupos de intereses especializados con el fin de comprender el ambiente actual de la seguridad informática y conocer de primera mano ataques, amenazas, tecnologías que permitan una gestión más eficaz
	6.1.5	Seguridad de la información en la gestión de proyectos	Para cualquier proyecto que se desarrolle a nivel organizacional debe incluirse como pilar la seguridad de la información, para esto, los objetivos de seguridad deben ser incluidos entre los objetivos del proyecto
	6,2	Dispositivos móviles y teletrabajo	
	6.2.1	Política de dispositivos móviles	Definir políticas de uso sobre el acceso de los dispositivos móviles con el fin de asegurar la información de la organización. Entre algunos aspectos que debe

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	**Sección**	**Objetivo de control / control**	
			contemplar la política esta el uso de servicios, instalación de software y protección contra malware
	6.2.2	Teletrabajo	Definir una política y medidas de seguridad con el fin de determinar controles adecuados para el acceso a la información fuera de la organización
7 Seguridad en los Recursos Humanos	7,1	Previo al empleo	
	7.1.1	Verificación de antecedentes	La verificación de los antecedentes para los aspirantes deben realizarse con base en las leyes actuales nacionales y bajo un principio de ética. Se debe incluir la verificación de referencias laborales y personales junto con la validación de títulos profesionales y demás información académica que incluya el

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	Sección	Objetivo de control / control	
			candidato
	7.1.2	Términos y condiciones del empleo	Se debe establecer las obligaciones contractuales de los empleados o contratistas a través de acuerdos de confidencialidad donde se exprese el manejo de información confidencial de la organización y las posibles consecuencias ante divulgación de la misma
	7,2	Durante el empleo	
	7.2.1	Responsabilidades de la Alta Gerencia	La alta dirección tiene como compromiso asegurar que todos los funcionarios o personas involucradas con la organización tengan claros sus responsabilidades y roles frente al SGSI

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	Sección	Objetivo de control / control	
	7.2.2	Conciencia, educación y entrenamiento de seguridad de la información	Programa de capacitación, formación y actualización a todos los funcionarios de la organización involucrados en el aseguramiento de la información. Dicho programa incluye jornadas de sensibilización con el fin de dar a conocer los peligros y amenazas a las que se encuentran expuestos los usuarios
	7.2.3	Proceso disciplinario	Se tiene documentado un proceso donde se establece que medidas tomar en caso de que se compruebe que un funcionario a cometido una violación a la seguridad de la información
	7,3	Terminación y cambio de empleo	

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	**Sección**	**Objetivo de control / control**	
	7.3.1	Termino de responsabilidades o cambio de empleo	Dado el acuerdo de confidencialidad, se tiene establecido los términos y responsabilidades legales contractuales con la organización referentes a la información dada la confidencialidad y divulgación de la misma.
8 Gestión de Activos	8,1	Responsabilidad de los activos	
	8.1.1	Inventario de activos	Procedimiento para la gestión, administración y clasificación de los activos de información
	8.1.2	Propiedad de activos	Procedimiento para asignar los activos a los funcionarios, garantizando una gestión y administración eficiente y garantizando que el responsable gestione de una manera correcta el activo durante todo su ciclo de vida

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	Sección	Objetivo de control / control	
	8.1.3	Uso aceptable de los activos	Procedimiento para asignar los activos a los funcionarios, garantizando una gestión y administración eficiente y garantizando que el responsable gestione de una manera correcta el activo durante todo su ciclo de vida
	8.1.4	Devolución de activos	Procedimiento donde se estipula la devolución de los activos que previamente han sido asignados al funcionario
	8,2	Clasificación de la información	
	8.2.1	Clasificación de la información	Se debe clasificar la información según su importancia y de esta manera desplegar los controles para su correcta administración y gestión
	8.2.2	Etiquetado de la información	Establecer un procedimiento para el etiquetado de información conforme establece el numeral 8.2.1

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	Sección	Objetivo de control / control	
	8.2.3	Manejo de activos	Definir un procedimiento para el manejo de los activos teniendo como referencia el esquema de clasificación adoptado por la organización. En este se debe contemplar las restricciones de acceso, protección y almacenamiento
	8,3	Manejo de medios	
	8.3.1	Gestión de medios removibles	Establecer un procedimiento que permita gestionar de manera eficiente los medios extraíbles teniendo como base el esquema de clasificación de información adoptado por la organización
	8.3.2	Eliminación de medios	Definir un procedimiento que defina los métodos de eliminación segura con el fin de minimizar el riesgo de pérdida de información confidencial de la organización

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	**Sección**	**Objetivo de control / control**	
	8.3.3	Transporte de medios físicos	Definir mecanismo que permitan proteger el acceso no autorizado a los medios con el fin de garantizar la integridad y confidencialidad de la información
9 Control de Acceso	9,1	Requerimientos de negocio para el control de acceso	
	9.1.1	Política de control de acceso	La compañía cuenta con política de control en donde determina las normas adecuadas de acceso a nivel físico y lógico
	9.1.2	Acceso a redes y servicios de red	Se dispone de una política de acceso de red donde cada usuario hace uso exclusivo de lo servicios autorizados
	9,2	Gestión de accesos de usuario	
	9.2.1	Registro y baja del usuario	Procedimiento que establece de manera formal el registro y cancelación de usuarios conforme los requerimientos de seguridad establecidos por la organización

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	Sección	Objetivo de control / control	
	9.2.2	Provisión de acceso a usuarios	Se disponen de mecanismos que permite gestionar los derechos de acceso a cualquier usuario y a cualquier sistema de información
	9.2.3	Gestión de derechos de acceso privilegiados	Procedimiento que se basa en la política de control de acceso donde se establece que cualquier acceso privilegiado debe ser previamente autorizado y documentado
	9.2.4	Gestión de información de autenticación secreta de usuarios	Los funcionarios deben firmar una declaración para mantener la confidencialidad de la información de autenticación. Dicho documento puede ser establecido en la sección 7.1.2
	9.2.5	Revisión de derechos de acceso de usuarios	Se realizan auditorias recurrentes sobre los roles y accesos sobre los diferentes activos y sistemas de información

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	Sección	Objetivo de control / control	
	9.2.6	Eliminación o ajuste de derechos de acceso	Se cuenta con un procedimiento donde se establece que para cualquier funcionario o ente externo que tenga permisos sobre un determinado activo o sistema de información, se debe revocar cualquier acceso. De igual manera si se realiza un cambio de funciones se realizaran las modificaciones pertinentes determinadas por su perfil
	9,3	Responsabilidades del usuario	
	9.3.1	Uso de información de autenticación secreta	Se tienen definidas políticas de contraseñas seguras para todos los niveles de usuario junto con cambio periódicos dependiendo de la criticidad de la aplicación o servicio
	9,4	Control de acceso de sistemas y aplicaciones	

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	Sección	Objetivo de control / control	
	9.4.1	Restricción de acceso a la información	Las diferentes aplicaciones cuentan con perfiles y roles donde se determina que usuarios acceden o no a ciertos niveles de información
	9.4.2	Procedimientos de inicio de sesión seguro	En la política de control de acceso se define diferentes métodos de inicio de sesión seguro entre los que se encuentran tokens criptográficos, tarjetas inteligentes y dispositivos biométricos
	9.4.3	Sistema de gestión de contraseñas	Se tienen definidas políticas de contraseñas seguras para todos los niveles de usuario junto con cambio periódicos dependiendo de la criticidad de la aplicación o servicio. Cada usuario puede gestionar de manera autónoma las contraseñas generadas para los diferentes accesos

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	**Sección**	**Objetivo de control / control**	
	9.4.4	Uso de programas y utilidades privilegiadas	Revisión periódica de los programas usados por los usuarios y restricción sobre las instalaciones de software que no se contemplen como necesarias para la ejecución de sus labores
	9.4.5	Control de acceso al código fuente del programa	Controles estrictos sobre el código fuente, diseños y especificaciones con el fin de impedir cambios o modificaciones no autorizadas e involuntarias que pongan en riesgo la funcionalidad del producto
10 Criptografía	10,1	Controles criptográficos	
	10.1.1	Política en el uso de controles criptográficos	Desplegar una infraestructura de clave pública PKI
	10.1.2	Gestión de llaves	Gestionar las llaves través de dispositivos criptográficos tales como Smart card y Smart token.
11 Seguridad	11,1	Áreas seguras	

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	**Sección**	**Objetivo de control / control**	
Física y del Entorno	11.1.1	Perímetro de seguridad físico	Revisión periódica sobre el diseño y disposición del centro de datos con el fin de garantizar un espacio seguro para el procesamiento de la información
	11.1.2	Controles físicos de entrada	Implementar un sistema de tarjetas de proximidad que garantizan el acceso e identificación de los funcionarios
	11.1.3	Seguridad de oficinas, habitaciones y facilidades	Revisión periódica del diseño de las oficinas con el fin de garantizar que a nivel exterior no se pueda determinar el tipo de actividad de la organización
	11.1.4	Protección contra amenazas externas y del ambiente	Implementar equipos para el control de la temperatura y sistemas de detección de incendios
	11.1.5	Trabajo en áreas seguras	Procedimiento que indique las condiciones para realizar cualquier actividad en áreas que se consideren criticas y que puedan generar una

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	Sección	Objetivo de control / control	
			indisponibilidad sobre un servicio o aplicación
	11.1.6	Áreas de entrega y carga	La organización no dispone de áreas de entrega y carga dado que su actividad económica difiere de dicho requerimiento
	11,2	Equipo	
	11.2.1	Instalación y protección de equipo	Procedimiento que indica las pautas para la instalación y protección de los equipos teniendo como prioridad la protección de amenazas ambientales y accesos no autorizados
	11.2.2	Servicios de soporte	Disponer servicios de respaldo adaptables a la necesidad de la organización a nivel eléctrico y de telecomunicaciones
	11.2.3	Seguridad en el cableado	Certificación RETIE y RETILAP para las instalaciones eléctricas y el cableado estructurado

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	Sección	Objetivo de control / control	
	11.2.4	Mantenimiento de equipos	Cronograma de mantenimientos para los diferentes equipos y el procedimiento se encuentra documentado según las políticas de seguridad adoptadas por la organización
	11.2.5	Retiro de activos	Generar un procedimiento que indique el registro de cualquier cambio y el estado actual en la hoja de vida de los equipos
	11.2.6	Seguridad del equipo y activos fuera de las instalaciones	Se debe disponer de controles suficientes para los equipos que se encuentren fuera de las instalaciones con el fin de mantener la confidencialidad e integridad de la información de la compañía
	11.2.7	Eliminación segura o reuso del equipo	Establecer un procedimiento que garantice el tratamiento adecuado de la información y licencias de software para cualquier equipo o medio que deba ser reutilizado o

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	**Sección**	**Objetivo de control / control**	
			dado de baja
	11.2.8	Equipo de usuario desatendido	Concientizar a los usuarios a través de capacitaciones sobre la protección que se debe dar a las sesiones de servicios y aplicaciones que no se encuentren en uso al igual que el acceso a dispositivos
	11.2.9	Política de escritorio limpio y pantalla limpia	La compañía debe implementar el plan de las 5S con alcance a los dispositivos y activos de información
12 Seguridad en las Operaciones	12,1	Procedimientos Operacionales y Responsabilidades	
	12.1.1	Documentación de procedimientos operacionales	Documentar los procedimientos críticos operacionales y socializarlos a los directos responsables a nivel de administración y copias de seguridad

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	Sección	Objetivo de control / control	
	12.1.2	Gestión de cambios	Definir un procedimiento que garantice la correcta identificación, evaluación, tratamiento, y documentación de los cambios
	12.1.3	Gestión de la capacidad	Monitorear y ajustar el uso de los recursos junto a proyecciones necesarias de requisitos de capacidad en el futuro con el objetivo de garantizar el rendimiento adecuado en los sistemas
	12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	La organización ha dispuesto la separación de los ambientes de desarrollo, pruebas y operación con el fin de evitar problemas de funcionamiento
	12,2	Protección de Software Malicioso	
	12.2.1	Controles contra software malicioso	Disponer de políticas que restringen la instalación de software de fuentes desconocidas. De igual manera se cuenta con una

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	Sección	Objetivo de control / control	
			consola centraliza de antivirus, firewall y monitorización de recursos
	12,3	Respaldo	
	12.3.1	Respaldo de información	La compañía debe contar con procedimiento de copias de seguridad que implementa replica y cifrado de la información en una localización externa que se encuentra protegida y segura
	12,4	Bitácoras y monitoreo	
	12.4.1	Bitácoras de eventos	Generar una bitácora de eventos para los diferentes servicios y aplicaciones con los que cuenta la compañía
	12.4.2	Protección de información en bitácoras	Las bitácoras deben contar con protección para la manipulación y acceso no autorizado de su información
	12.4.3	Bitácoras de administrador y operador	El registro de eventos se debe encontrar definido para las actividades operativas

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	Sección	Objetivo de control / control	
	12.4.4	Sincronización de relojes	Configuración del protocolo NTP definiendo una fuente confiable de actualización
	12,5	Control de software operacional	
	12.5.1	Instalación de software en sistemas operacionales	Implementar un procedimiento que permite una gestión eficaz sobre instalaciones de software en los sistemas operativos
	12,6	Gestión de vulnerabilidades técnicas	
	12.6.1	Gestión de vulnerabilidades técnicas	Disponer de un inventario de activos que cuente con información referente al tipo de software, proveedor y versión, con el fin de realizar una gestión adecuada de las vulnerabilidades y parches
	12.6.2	Restricciones en la instalación de software	Definir reglas claras sobre qué tipo de usuarios puede realizar instalaciones basándose en el principio de privilegio mínimo
	12,7	Consideraciones de auditoria de sistemas de información	

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	**Sección**	**Objetivo de control / control**	
	12.7.1	Controles de auditoría de sistemas de información	Se deben establecer los requisitos de auditoria y actividades relacionadas con la verificación y cumplimiento
13 Seguridad en las Comunicaciones	13,1	Gestión de seguridad en red	
	13.1.1	Controles de red	Implementar controles tales como sistemas de detección y prevención de intrusos, firewall, que junto con políticas establecidas acorde a los requerimientos de seguridad de la organización permiten una gestión adecuada sobre los recursos de red
	13.1.2	Seguridad en los servicios en red	Definir acuerdos de servicio dado los mecanismos de seguridad, niveles de servicio y requisitos de administración sobre todos los servicios de red
	13.1.3	Segregación en redes	Segmentar los diferentes servicios de red al igual que los dominios y áreas de la

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	Sección	Objetivo de control / control	
			organización
	13,2	Transferencia de información	
	13.2.1	Políticas y procedimientos para la transferencia de información	Definir procedimientos, políticas y controles que permitan garantizar la transferencia de información bajo cualquier canal de comunicación
	13.2.2	Acuerdos en la transferencia de información	Definir acuerdos que permitan la transferencia segura de información entre la organización y partes externas
	13.2.3	Mensajería electrónica	Disponer de mecanismos de cifrado para garantizar la integridad y confidencialidad de la información que es utilizada en la mensajería electrónica
	13.2.4	Acuerdos de confidencialidad o no-revelación	Identificar, documentar y revisar con regularidad los requisitos para establecer los acuerdos de confidencialidad o no divulgación dados los

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	**Sección**	**Objetivo de control / control**	
			requerimientos de seguridad de la organización
14 Adquisición, Desarrollo y Mantenimiento de Sistemas	14,1	Requerimientos de seguridad en sistemas de información	
	14.1.1	Análisis y especificación de requerimientos de seguridad	La compañía desarrolla actividades de Consultoría e Interventoría para los cuales utiliza herramientas ofimáticas y tecnológicas, en tal sentido es necesario establecer controles de seguridad para garantizar que tienen en cuenta los requisitos del negocio antes de implementar cambios en la tecnología de la empresa

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	Sección	Objetivo de control / control	
	14.1.2	Aseguramiento de servicios de aplicación en redes públicas	La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas
	14.1.3	Protección de transacciones en servicios de aplicación	Dados los controles y mecanismos criptográficos se debe asegurar la protección de las transacciones en los diferentes servicios de aplicación
	14,2	Seguridad en el proceso de desarrollo y soporte	
	14.2.1	Política de desarrollo seguro	La organización para el desarrollo de actividades de los proyectos puede establecer sistemas de información, por lo cual es necesario establecer controles de seguridad para el desarrollo seguro de sistemas de información por terceros, que permitan garantizar

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	Sección	Objetivo de control / control	
			que cumplen con las características técnicas y de seguridad que se requiere
	14.2.2	Procedimientos de control de cambios del sistema	Procedimientos que aseguran la gestión de cambios realizados durante el ciclo de vida de desarrollo del software
	14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	Antes de realizar un cambio de plataforma se deben realizar las validaciones y verificaciones pertinentes en un entorno de prueba
	14.2.4	Restricción de cambios en paquetes de software	Políticas y mecanismos que previenen la modificación y cambios realizados a los paquetes de software
	14.2.5	Principios de seguridad en la ingeniería de sistemas	Definir y documentar principios para la construcción de sistemas seguros aplicados a cualquier actividad

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	Sección	Objetivo de control / control	
			de implementación
	14.2.6	Entorno de desarrollo seguro	La organización debe establecer y mantener los ambientes de desarrollo seguro que comprendan el ciclo de vida de desarrollo de software
	14.2.7	Desarrollo tercerizado	Disponer de controles y mecanismos que permitan validar y controlar el desarrollo realizado por terceras partes
	14.2.8	Pruebas de seguridad del sistema	La organización debe definir procedimientos en los que se establece la periodicidad de las pruebas de seguridad del sistema durante el ciclo de desarrollo
	14.2.9	Pruebas de aceptación del sistema	Realizar pruebas de aceptación sobre actualizaciones o modificaciones a sistemas ya existentes o desarrollos nuevos con el fin de

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	**Sección**	**Objetivo de control / control**	
			garantizar que se cumple con los criterios establecidos
	14,3	Datos de prueba	
	14.3.1	Protección de datos de prueba	Se debe realizar un tratamiento sobre los datos de prueba con el fin de garantizar su protección, confidencialidad y accesos no autorizados
15 Relaciones con Proveedores	15,1	Seguridad de la información en relaciones con el proveedor	
	15.1.1	Política de seguridad de la información en las relaciones con el proveedor	Definir los requisitos de seguridad de la información asociados con el acceso de los proveedores a los activos de los que dispone la organización
	15.1.2	Atención de tópicos de seguridad en los acuerdos con el proveedor	Definir el alcance que tienen los acuerdos con los proveedores los cuales tienen relación directa con la información de la organización

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	**Sección**	**Objetivo de control / control**	
	15.1.3	Cadena de suministros de tecnologías de la información y comunicaciones	Los acuerdos con proveedores deben incluir requisitos de seguridad que gestionen los riesgos derivados del suministro de productos y servicios
	15,2	Gestión de entrega de servicios de proveedor	
	15.2.1	Monitoreo y revisión de servicios del proveedor	La organización debe verificar y revisar los servicios prestados por terceros a través de auditorías periodos
	15.2.2	Gestión de cambios a los servicios del proveedor	Gestionar los cambios en el suministro de servicios por parte de los proveedores incluyendo mejora de las políticas, procedimientos y controles de seguridad
16 Gestión de Incidentes de Seguridad de la Información	16,1	Gestión de incidentes de seguridad de la información y mejoras	
	16.1.1	Responsabilidades y procedimientos	Definir las responsabilidades sobre la gestión de la seguridad de la información para dar una respuesta pronta y eficaz ante cualquier incidencia

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	Sección	Objetivo de control / control	
	16.1.2	Reporte de eventos de seguridad de la información	Establecer canales de comunicación apropiados para una correcta gestión de un evento propio de la seguridad de la información
	16.1.3	Reporte de debilidades de seguridad de la información	Procedimiento en el que se establecen los mecanismos para informar por parte de funcionarios y terceros sobre alguna debilidad que afecte significativamente la seguridad de la información
	16.1.4	Valoración y decisión de eventos de seguridad de la información	Valorar y gestionar los eventos de seguridad conforme los procedimientos establecidos por la organización que a su vez son definidos por los requisitos de seguridad de la información
	16.1.5	Respuesta a incidentes de seguridad de la información	Procedimientos que establezcan el tratamiento de los incidentes de seguridad de la información

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	**Sección**	**Objetivo de control / control**	
	16.1.6	Aprendizaje de incidentes de seguridad de la información	Se cuenta con una base de conocimiento referente a la gestión y solución de incidentes de seguridad de la información
	16.1.7	Colección de evidencia	Implementar mecanismos que permiten identificar y gestionar cualquier información que pueda considerarse evidencia
17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio	17,1	Continuidad de la seguridad de la información	
	17.1.1	Planeación de la continuidad de la seguridad de la información	Definir los requisitos para garantizar la seguridad de la información ante situaciones adversas
	17.1.2	Implementación de la continuidad de la seguridad de la información	Establecer procesos, procedimientos y controles que permitan asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	**Sección**	**Objetivo de control / control**	
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Establecer una revisión periódica de los mecanismos dispuestos para garantizar la continuidad del negocio y que estos sean efectivos ante una situación adversa
	17,2	Redundancias	
	17.2.1	Disponibilidad de facilidades de procesamiento de información	Las instalaciones de procesamiento de información se deben implementar con redundancia garantizando una alta disponibilidad
18 Cumplimiento	18,1	Cumplimiento con Requerimientos Legales y Contractuales	
	18.1.1	Identificación de legislación aplicable y requerimientos contractuales	El enfoque de la organización para la gestión de la seguridad junto con los diferentes controles, políticas y procesos deben ser revisados periódicamente garantizando el cumplimiento ante cualquier requerimiento
	18.1.2	Derechos de propiedad intelectual (IPR)	Procedimientos que garantizan el cumplimiento de los requisitos legales relacionados con la

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	Sección	Objetivo de control / control	
			propiedad intelectual y el uso de software patentado
	18.1.3	Protección de registros	Procedimientos y mecanismos que garantizan la protección de los registros conforme los requisitos legales, contractuales y de la organización
	18.1.4	Privacidad y protección de información personal identificable (PIR)	Se cuentan con mecanismos para la protección de la información personal como exige la legislación nacional y las obligaciones contractuales con los clientes de la organización
	18.1.5	Regulación de controles criptográficos	Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes
	18,2	Revisiones de seguridad de la información	
	18.2.1	Revisión independiente de seguridad de la información	Revisión periódica sobre la gestión de la seguridad de la información y su correcta

ISO 27001:2013 Controles de Seguridad			Controles
Cláusula	Sección	Objetivo de control / control	
			implementación
	18.2.2	Cumplimiento con políticas y estándares de seguridad	Los responsables de las diferentes áreas deben revisar periódicamente el cumplimiento de las políticas y normas de seguridad dentro de su dependencia
	18.2.3	Revisión del cumplimiento técnico	Los sistemas de información deben ser revisados de manera regular con el fin de determinar el cumplimiento con las políticas y normas de seguridad de la información

Fuente: Autor

9 DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

9.1 OBJETIVO DEL SGSI

Los objetivos propuestos para el Sistema de Gestión de Seguridad de la Información son los siguientes:

- Reducir el nivel de riesgo establecido dentro de la organización, preservando la confidencialidad, integridad y disponibilidad de la información.

- Garantizar el acceso a la información dentro de la compañía según los diferentes procesos establecidos y criterios de seguridad definidos por la alta gerencia.

- Preservar la integridad de la información basándose en los diferentes requisitos de seguridad y resultados obtenidos del proceso de gestión y análisis de riesgos.

- Asegurar que la información dentro de la organización esté disponible para los diferentes procesos o funcionarios cuando estos así lo requieran.

9.2 ALCANCE DEL SGSI

El alcance del Sistema de Gestión de Seguridad de la Información debe abarcar el proceso de gestión de las tecnologías de la información y comunicación, encargado de la gestión de la infraestructura y plataforma tecnológica de la organización, con el fin de garantizar la seguridad de los diferentes activos mediante la adopción e implementación de mecanismos, técnicas, controles y buenas prácticas.

9.3 POLÍTICA DEL SGSI

La política del Sistema de Gestión de Seguridad de la Información se define como la posición que representa la directiva de la organización en relación a la

seguridad de la información, teniendo en cuenta los requisitos comerciales y legales derivados del propósito de la compañía:

Belisario Ltda. con el fin de dar cumplimiento a su misión, visión y objetivo estratégico y teniendo como base sus valores corporativos, la necesidad de satisfacer a sus clientes internos y externos y manteniendo la mejora continua como un pilar organizacional, establece la función de seguridad de la información en la organización con el objetivo de:

- Velar por el cumplimiento de los principios de seguridad de la información.
- Cumplir con los requisitos legales y regulatorios aplicables al objeto social de la organización y al Sistema de Gestión de Seguridad de la Información.
- Implementar el Sistema de Gestión de Seguridad de la Información.
- Gestionar los riesgos a través de la adopción de estándares y controles orientados a preservar la información como el activo más importante de la organización.
- Establecer políticas, procedimientos y manuales relacionados con la correcta operación del Sistema de Gestión de Seguridad de la Información.
- Fortalecer la cultura de la seguridad de la información dentro de la organización.
- Garantizar la continuidad de la compañía frente a cualquier incidente.

9.3.1 Aplicabilidad de la política del SGSI

La política del Sistema de Gestión de Seguridad de la Información aplica a toda la organización, funcionarios, procesos, proveedores, terceros y demás partes que tengan relación directa o indirecta con la compañía.

9.4 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

9.4.1 Políticas de la organización de la seguridad de la información

La organización debe establecer una estructura que permita identificar roles y responsabilidades que garanticen la correcta gestión de la seguridad de la información.

Responsabilidades de la dirección:

- Definir y establecer los roles y responsabilidades referentes a la administración y operación de la seguridad de la información en todos los niveles jerárquicos de la organización.

- Estipular el procedimiento de contacto con las diferentes autoridades cuando sea necesario y de igual manera establecer los responsables para efectuar dicho proceso.

- Revisar y aprobar las políticas de seguridad de la información y solicitar los ajustes pertinentes cuando se requieran.

- Promover y fortalecer la cultura de la seguridad de la información dentro de la organización.

- Proveer los recursos necesarios para garantizar una gestión eficiente de la seguridad de la información.

Responsabilidades del área de gestión de tecnología:

- Asignar las funciones y responsabilidades para los diferentes funcionarios que estén a cargo de la administración de la infraestructura tecnológica de la organización. Dicho proceso debe ser documentado y de amplio conocimiento para todo el personal que tenga relación con este propósito.

- Requerir a la alta dirección los recursos necesarios con el fin de mantener una operación adecuada sobre la seguridad de la información.

Responsabilidades de los usuarios:

- Acatar y dar cumplimiento a las políticas y procedimientos referentes a la seguridad de la información.

9.4.2 Políticas de seguridad del personal

Se debe garantizar que en los procesos de selección, contratación, permanencia y desvinculación laboral del recurso humano se cumplan criterios que permitan salvaguardar la información de la organización.

Responsabilidades de talento humano:

- Realizar las verificaciones pertinentes a la información suministrada por las personas que aspiren a una determinada vacante.

- Garantizar que los funcionarios conozcan y acepten el acuerdo de confidencialidad y las políticas de seguridad de la información dispuestas por la organización.

Responsabilidades de la dirección:

- Establecer un proceso disciplinario que contemple las fallas e incumplimiento a las políticas de seguridad de la información.

Responsabilidades de coordinadores de área:

- Informar a las diferentes dependencias de cualquier novedad referente a la desvinculación o cambio de funciones del personal a su cargo.

Responsabilidades del área de gestión de tecnología:

- Revocar o modificar las credenciales de autenticación para los diferentes aplicativos, servicios o recursos de red que disponga el funcionario.

Responsabilidades de los usuarios:

- Todo el personal que haga uso de la información de la organización debe dar cumplimiento a las políticas y procedimientos establecidos dentro de la compañía.

9.4.3 Políticas sobre la gestión de los activos de información

Se debe velar por que la información y activos propiedad de la organización y que son proporcionados a los funcionarios con el fin ejecutar las diferentes actividades relacionadas con su cargo, se deban gestionar de manera eficiente y garantizando su protección ante cualquier amenaza.

Responsabilidades del área de gestión de tecnología:

- Garantizar la correcta operación y administración de los activos.

- Establecer para cada activo de información su correspondiente hoja de vida que permita identificar sus características y el funcionario al cual ha sido asignado.

- Registrar los movimientos que se realicen sobre los activos donde se pueda evidenciar la fecha, funcionario o dependencia asignada.

- Generar los mantenimientos preventivos según cronograma y periodicidad establecida.

- Definir un plan de inversión que contemple la actualización de activos según evaluación de requerimientos.

Responsabilidad de los usuarios:

- Dar uso adecuado a los activos asignados.

- Hacer uso de los activos únicamente para las funciones referentes al desempeño del cargo.

- Reportar sobre cualquier incidencia o novedad sobre el funcionamiento del activo.

9.4.4 Políticas de uso para medios de almacenamiento

El uso de medios de almacenamiento debe ser un proceso que ejerza un control eficiente sobre el uso de la información de la organización garantizando la integridad, confidencialidad y disponibilidad de la misma.

Responsabilidades del área de gestión de tecnología:

- Implementar controles que garanticen el uso de los diferentes medios de almacenamiento conforme los lineamientos de seguridad establecidos por la organización.

- Establecer procedimientos para dar de baja o ejecutar eliminación segura de medios de almacenamiento.

Responsabilidades de los usuarios:

- No usar los medios de almacenamiento con uso personal.

- No realizar uso de dichos medios con el fin de transferir información confidencial de la organización o que ponga en riesgo su operación u objeto social con el fin de obtener un beneficio propio o favoreciendo a un tercero.

- Custodiar los medios que sean asignados de una manera responsable.

9.4.5 Políticas de acceso a redes y servicios de red

El área de gestión tecnológica de la organización y en su facultad de administrar la red de datos de la organización, debe disponer de mecanismos de control de acceso a la red de datos de la organización con el fin de proteger accesos no autorizados y uso malintencionado.

Responsabilidades del área de gestión de tecnología:

- Gestionar el acceso y autorización de los recursos de red a los diferentes procesos y colaboradores que lo requieran dado el alcance a sus funciones dentro de la organización.

- Disponer de mecanismos de seguridad suficientes para garantizar la conexión a las redes inalámbricas de la organización.

Responsabilidades de los usuarios:

- Solicitar la aprobación del superior o jefe inmediato para la asignación o modificación de las credenciales de autenticación al área de gestión tecnológica para los recursos de red de los cuales disponga su área o dependencia.
- Acceder únicamente a los recursos de red establecidos.

- Hacer uso de los servicios dispuestos únicamente para las funciones asignadas al cargo.

9.4.6 Políticas de gestión de accesos de usuarios

Se debe administrar por parte del área de gestión tecnológica los usuarios dispuestos para los diferentes servicios, recursos y sistemas de información, garantizando la gestión en la creación, modificación, inhabilitación o eliminación de dichas cuentas.

Responsabilidades del área de gestión de tecnología:

- Se deben crear, modificar, eliminar o inhabilitar las cuentas de usuario para los diferentes servicios, recursos o sistemas de información, previo requerimiento aprobado por parte de los líderes de los procesos o en su defecto, la alta dirección.

- Establecer los perfiles y permisos de los usuarios para los diferentes recursos, servicios y sistemas de información basados en el principio de privilegio mínimo.

- Definir directivas de contraseñas seguras basadas en una complejidad robusta y cambio periódico.

- Realizar auditorías sobre los diferentes activos que posean proceso de autenticación basada en registros de eventos.

Responsabilidades de los usuarios:

- Los funcionarios se hacen responsables sobre cualquier acción realizada sobre los servicios, recursos y sistemas de información de igual manera sobre las credenciales de autenticación suministradas.
- Los usuarios y contraseñas son de uso personal e intransferible.

- Informar al área de gestión tecnológica cuando se encuentre comprometida alguna cuenta de usuario asignada.

- No almacenar cuentas de usuario en medios que puedan ser expuestos o accedidos por cualquier otro funcionario o tercero, ya sea en medio físico o digital.

9.4.7 Políticas de áreas seguras

La organización debe garantizar e implementar mecanismos de seguridad física y control de acceso que permitan proteger las instalaciones y áreas destinadas al procesamiento y almacenamiento de datos velando por la protección de amenazas internas y externas.

Responsabilidades del área de gestión de tecnología:

- Garantizar que cualquier actividad dentro del centro de cómputo sea supervisada por un funcionario del área de gestión tecnológica.

- Registrar el ingreso del personal al centro de cómputo junto con las actividades que se desarrollen, ya sean funcionarios de la organización, terceros o proveedores.

- Proteger los recursos de la infraestructura tecnológica en el centro de cómputo a través de sistemas de control ambiental, sistemas de detección y extinción de incendios, sistema de alarmas y video vigilancia. Cualquier incidente generado por alguno de los sistemas desplegados, debe ser registrado y documentado.

9.4.8 Políticas de seguridad para equipos institucionales

La organización debe proveer los recursos necesarios para garantizar la protección de los elementos que componen la infraestructura tecnológica de la compañía, con el fin de reducir el riesgo de la materialización de amenazas a los que se encuentren expuestos.

Responsabilidades del área de gestión de tecnología:

- Establecer controles y mecanismos que garanticen los principios de seguridad de la información en los elementos que componen la infraestructura tecnológica de la organización.
- Ejecutar los mantenimientos correctivos y registrar las actividades realizadas en la hoja de vida de los equipos.

- Definir un cronograma de mantenimiento preventivo sobre los diferentes recursos de la infraestructura tecnológica e informar a los responsables de los equipos sobre la fecha y tiempo requerido para la ejecución de dicha actividad.

- Establecer configuraciones de uso seguro para los equipos de cómputo asignados a los funcionarios de la organización.

- Garantizar que los equipos que se encuentren expuestos al público en general cumplan con condiciones restrictivas de uso y seguridad física.

Responsabilidades de los usuarios:

- Acatar las instrucciones de uso de los equipos asignados por el área de gestión tecnológica.

- No realizar ningún movimiento o asignación sobre los recursos de la infraestructura tecnológica de la organización.

- Informar al área de gestión tecnológica sobre cualquier incidencia que se presente sobre los equipos concedidos.

- Abstenerse de realizar la instalación, mantenimiento o retiro de cualquier recurso que compone la infraestructura tecnológica.

- Bloquear el equipo de cómputo cuando se retire del puesto de trabajo.

- Apagar la estación de trabajo asignada cuando se culmine la jornada laboral.

- Los equipos portátiles deben ser transportados en condiciones que garanticen su integridad física.

- Cuando se disponga de algún recurso que deba ser traslado fuera de las instalaciones de la compañía y este sea hurtado, se debe informar de manera inmediata al área de gestión tecnológica.

9.4.9 Políticas de seguridad en las operaciones

El área de gestión tecnológica es la encargada de administrar y operar la infraestructura tecnológica de la organización, por ende debe garantizar que los procesos soportados por los recursos de la plataforma sean gestionados de manera adecuada por los funcionarios que hacen de parte de dicho proceso.

Responsabilidades del área de gestión de tecnología:

- Documentar los procedimientos referentes a la gestión de la infraestructura tecnológica de la organización y actualizarlos cuando se requieran.

- Proporcionar a los diferentes colaboradores los manuales de instalación, configuración y administración de los diferentes elementos que componen la plataforma tecnológica de la compañía.

- Realizar análisis de escalabilidad de los recursos de la infraestructura tecnológica garantizando que el desempeño y capacidad estén acorde a las necesidades de los procesos de la organización.

9.4.10 Políticas de protección sobre el software malicioso

La organización debe disponer de mecanismos y controles que garanticen la protección de la confidencialidad, disponibilidad e integridad de la información que es almacenada y procesada en los diferentes elementos que conforman la plataforma tecnológica frente a las amenazas que puedan perpetrarse por cualquier software malicioso.

Responsabilidades del área de gestión de tecnología:

- Proveer herramientas y mecanismos que permitan minimizar el riesgo al que pueda ser expuesto cualquier recurso que conforma la plataforma tecnológica de la organización.

- Garantizar que las herramientas dispuestas para la protección de software malicioso se actualicen de forma periódica.

- Hacer auditoria recurrente sobre las incidencias generadas por las diferentes herramientas y mecanismos implementados.

- Restringir las opciones de configuración de las herramientas a los usuarios finales.

Responsabilidades de los usuarios:

- No realizar cambios, ni eliminar las herramientas dispuestas para proteger los recursos tecnológicos del software malicioso.

- Realizar análisis con las herramientas dispuestas sobre información a la cual se acceda por primera vez y que este contenida en medios de almacenamiento externos o provenga de fuentes no confiables.

- No descargar información de fuentes desconocidas y si no se tiene plena certeza de su procedencia, informar al área de tecnología con el fin de no comprometer la plataforma tecnológica ni los servicios soportados en esta.

- Reportar al área de gestión tecnológica cualquier evento del cual se sospeche o se tenga plena certeza de una ejecución de software malicioso sobre un determinado recurso tecnológico.

9.4.11 Políticas para el respaldo de información

La organización debe establecer procedimientos eficaces que garanticen el respaldo de la información que soporta y genera los diferentes procesos organizacionales, definiendo lineamientos entorno al almacenamiento y retención de dicha información.

Responsabilidades del área de gestión de tecnología:

- Generar procedimientos de respaldo, restauración, transferencia, retención y almacenamiento para las copias de respaldo de la información, garantizando que se cumpla con la confidencialidad, disponibilidad e integridad de las mismas.

- Disponer de mecanismos apropiados para la correcta identificación de los medios resultantes del proceso de copias de respaldo de información.

- Realizar periódicamente los procedimientos de restauración de la copias de respaldo de información y documentar los hallazgos o incidencias generadas.

- Definir las condiciones de almacenamiento y transporte de los medios que contienen las copias de respaldo de información cuando estas deban ser custodiadas fuera de las instalaciones de la organización.

- Garantizar que las copias de respaldo de información crítica se encuentran en una ubicación diferente a las instalaciones de la organización, debidamente custodiadas y protegidas de cualquier amenaza.

Responsabilidades de los usuarios:

- Seguir las instrucciones impartidas por el área de gestión tecnológica con el fin de garantizar que la información sea respaldada de manera correcta.

- Utilizar los recursos y herramientas suministradas por la organización para generar las copias de respaldo de la información únicamente sobre los datos referentes a las actividades laborales.

- La información de uso personal debe ser responsabilidad del usuario y será este el que acorde a sus necesidades genere copias de ella cuando lo requiera.

9.4.12 Políticas sobre el control del software operacional

El área de gestión tecnológica debe definir e implementar procedimientos referentes al control de la instalación de software operacional, garantizando que se cumplan los principios de seguridad de la información y avalando que dicho software cuente con el soporte necesario para la correcta operación de los procesos que allí se desarrollen.

Responsabilidades del área de gestión de tecnología:

- Establecer procedimientos que permita controlar la instalación de software operacional.

- Asegurar que el software operacional cuente con el soporte del proveedor.

- Garantizar que se cuente con una licencia de uso del software operacional.
- Implementar entornos de prueba en que el proveedor pueda realizar las configuraciones y cambios significativos sobre el software operacional sin afectar la operación de la organización ni los procesos allí desarrollados.

- Restringir las instalaciones de software operacional en las estaciones de trabajo de los funcionarios.

9.4.13 Políticas para la gestión y aseguramiento de la red de datos

El área de gestión tecnológica debe establecer mecanismos de control y seguridad que garanticen la disponibilidad de la red de datos y los servicios allí desplegados, velando por la integridad y confidencialidad de los datos transmitidos.

Responsabilidades del área de gestión de tecnología:

- Implementar medidas que aseguren la disponibilidad de los diferentes recursos que conforman la red de datos de la organización.

- Segmentar la red de datos por servicios, grupos de usuarios o ubicaciones.

- Implementar controles de seguridad que permitan garantizar la protección de los datos transmitidos a través de la red de datos.

- Establecer configuraciones adecuadas de los recursos que conforman la red de datos de la organización.

- Hacer auditorias periódicas sobre el trafico de la red de datos y los registros de eventos generados por los diferentes recursos de red, documentando los hallazgos encontrados.

9.4.14 Políticas de uso del correo electrónico

La organización comprende que el correo electrónico es una herramienta que facilita la comunicación entre los colaboradores y partes de interés, es por eso que debe garantizar el uso adecuado basado en los principios de seguridad de la información.

Responsabilidades del área de gestión de tecnología:

- Establecer un procedimiento para la creación y asignación de cuentas de correos corporativas.

- Definir y socializar a los funcionarios las normas de uso del correo electrónico.

- Implementar controles que permitan proteger la plataforma de correo electrónico de cualquier tipo de divulgación y transmisión de código malicioso.

Responsabilidades de los usuarios:

- La cuenta de correo electrónico asignada por la organización es de uso personal e intransferible.

- Toda la información contenida en el correo electrónico debe ser únicamente relacionada con el desempeño de las funciones designadas en la organización, por ende, no debe ser utilizada para uso personal.

- Abstenerse de utilizar el correo electrónico con el fin de enviar información que atente contra los valores corporativos y resulte ofensiva para los diferentes colaboradores de la organización.
- Los mensajes enviados deben conservar la imagen corporativa y esta no debe ser modificada bajo ninguna situación.

9.4.15 Políticas de uso de internet

La organización comprende la importancia de internet en el desarrollo de las funciones que desempeñan sus colaboradores, proporcionando lineamientos que garanticen una navegación segura y velando por la protección de la información derivada de los procesos institucionales, que pueda llegar a ser expuesta por un uso inadecuado de los recursos.

Responsabilidades del área de gestión de tecnología:

- Implementar mecanismos y controles que garanticen una prestación eficiente y segura del acceso a internet.
- Monitorear continuamente el canal de servicio de internet.

- Restringir la descarga de aplicaciones o software malicioso y a su vez, limitar la navegación de los usuarios a sitios categorizados como no relevantes para el desempeño de sus funciones.

- Establecer mecanismos que permitan hacer seguimiento a la navegación de los usuarios.

- Generar reportes de navegación y consumo de ancho de banda por usuario y por aplicación.

Responsabilidades de los usuarios:

- Hacer uso del servicio de internet únicamente para el desempeño de las funciones asignadas al cargo.

- Evitar la descarga de software e instalación en los equipos de cómputo asignados.

- No acceder a servicios de mensajería instantánea, redes sociales, juegos, música, páginas de ocio, o cualquiera que se considere afecte la productividad y el desempeño en las actividades laborales.

- No intercambiar información confidencial de la organización con terceros.
- Abstenerse de ingresar a páginas que atenten contra la moral y la ética promulgada en la organización y que estén categorizadas en las leyes vigentes.

9.4.16 Políticas de adquisición, desarrollo y mantenimiento de sistemas de información

La organización debe asegurar que cualquier sistema de información adquirido o desarrollado dentro de la compañía o por cualquier parte externa, cumpla con requisitos de calidad, siendo la seguridad parte integral del mismo.

Responsabilidades de la dirección:

- Gestionar las solicitudes de adquisición y actualización de software presentadas por el área de gestión tecnológica.
- Proveer los recursos necesarios para cumplir con las políticas de adquisición, desarrollo y mantenimiento de sistemas de información.

Responsabilidades del área de gestión de tecnología:

- Asegurar que el software dispone de controles de seguridad y este acorde a las políticas de seguridad de la compañía.

- Garantizar que en el caso de realizarse desarrollos dentro de la empresa, estos estén debidamente documentados y que exista un control del versionamiento del software.

- Registrar los desarrollos propios ante la Dirección General de Derechos de Autor.

- Asegurar que el software adquirido no sea copiado ni distribuido a terceros.

- Realizar la instalación del software en las estaciones de trabajo de la organización.

- Presentar a la alta dirección dadas las necesidades y requerimientos contractuales, solicitud de actualización y adquisición de software.

9.4.16 Políticas de relación con los proveedores

La organización debe implementar mecanismos de control en las relaciones establecidas con los proveedores, garantizando que la información a la que tienen acceso y los servicios que son prestados por estos mismos cumplan con los criterios y parámetros establecidos en las políticas de seguridad de la información.

Responsabilidades del área de gestión de tecnología:

- Definir acuerdos de niveles de servicio para los diferentes servicios prestados por los proveedores y terceros.

- Establecer requisitos de seguridad para la prestación de los servicios del proveedor garantizando la protección de la información de la organización.
- Implementar acuerdos de confidencialidad entre las partes relacionadas.

- Establecer condiciones de conexiones seguras para los proveedores y terceros que accedan a los recursos y plataforma tecnológica de la organización.

- Disponer de un entorno seguro y controlado para la operación de los proveedores o terceros dentro de las instalaciones de la organización.

9.4.17 Políticas de gestión de incidentes de seguridad de la información

La organización propende por la gestión eficiente y eficaz de la gestión de incidencias de seguridad de la información que se presente en cualquier elemento o recurso que conforma la infraestructura tecnológica de la compañía, a través de la implementación de procedimientos y asignación de responsabilidades para el tratamiento de dichas incidencias.

Responsabilidades del área de gestión de tecnología:

- Definir los procedimientos que permitan gestionar las incidencias respecto a la seguridad de la información.

- Generar las acciones preventivas que permitan eliminar las causas de un incidente que pueda afectar la seguridad de la información.
- Establecer acciones correctivas junto con el análisis de causas cuando se presente un incidente que afecte la seguridad de la información.

- Presentar a la alta dirección informes periódicos sobre la gestión y tratamiento de incidentes.

- En caso de que el incidente no pueda ser tratado, acudir a personal externo calificado o de ser necesario, a las autoridades competentes.

Responsabilidades de los usuarios:

- Reportar sobre cualquier incidente o evento relacionado que afecte la confidencialidad, disponibilidad e integridad de la información y los recursos tecnológicos que estén bajo su custodia.

- Informar cuando se tenga conocimiento de cualquier actividad que atente contra las políticas de seguridad de la información.

9.4.18 Políticas para la gestión de la continuidad del negocio

La organización debe proveer los recursos y establecer las acciones pertinentes con el fin de mantener la continuidad del negocio ante cualquier evento que afecte su operación y procesos, garantizando que la recuperación y restablecimiento de sus operaciones sea un proceso eficiente.

Responsabilidades de la dirección:

- Aprobar el plan de continuidad de negocio y el plan de recuperación ante desastres.

- Proveer los recursos necesarios para cumplir con las políticas para la gestión de la continuidad del negocio.

Responsabilidades del área de gestión de tecnología:

- Definir los requerimientos de seguridad para la gestión de continuidad del negocio.

- Elaborar el plan de continuidad de negocio y recuperación ante desastres, junto con los procedimientos necesarios que garanticen que la operación de la organización tenga una afectación mínima.

- Realizar periódicamente las pruebas de recuperación antes desastres, registrando y documentando los resultados del proceso.

- Evaluar periódicamente diferentes herramientas y mecanismos que permitan optimizar los procesos de continuidad del negocio.

9.4.19 Políticas de cumplimiento

La organización debe velar por el cumplimiento de la legislación referente a la seguridad de la información y todo lo que respecta a la protección de los derechos de autor, propiedad intelectual y la privacidad y protección de datos personales.

Responsabilidades de la dirección:

- Establecer en la organización las responsabilidades y funciones referentes al cumplimiento de la legislación.

- Proveer los recursos necesarios para identificar y dar cumplimiento a la normatividad y legislación relacionada con la operación de la organización y los requisitos de seguridad de la información.

Responsabilidades del área de gestión de tecnología:

- Garantizar que cualquier software instalado en los recursos tecnológicos de la organización cuente con una licencia de uso.

- Administrar y gestionar la instalación y el inventario del software.

- Implementar controles y mecanismos que garanticen la privacidad y protección de los datos personales que se almacén y procesen en la plataforma tecnológica de la organización.

9.5 PROCEDIMIENTOS DE APOYO EN LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

9.5.1 Acciones de mejora

9.5.1.1 Objetivo. Establecer los criterios para implementar las acciones generales, correctivas o preventivas que sean necesarias para tratar las no conformidades detectadas o potenciales e identificar, analizar y eliminar sus causas para prevenir su ocurrencia o evitar que se vuelvan a presentar, garantizando la seguridad de la información para los servicios y recursos que dispone la plataforma tecnológica de la organización.

9.5.1.2 Alcance. Este procedimiento aplica a todas las áreas de la organización y procesos que tengan una relación directa o indirecta con los recursos o elementos que conforman la infraestructura tecnológica de la organización y la información que se almacena o procesa en dichos elementos.

9.5.1.3 Documentos de referencia

- NTC ISO 27001:2013.
- Informes y registros de auditorías internas y externas.

9.5.1.4 Responsabilidad

De la alta dirección:

- Proveer los recursos necesarios para dar cumplimiento a este procedimiento.
- Estar continuamente informado del estado de las acciones de mejora generales, acciones correctivas y preventivas y del resultado de la aplicación de las mismas, si son adecuadas, convenientes y eficaces.

Del coordinador del área de gestión tecnológica:

- Definir el impacto previo de la no conformidad detectada.

- Investigar e identificar las causas o posibles causas, aplicando las herramientas y mecanismos apropiados

- Identificar la causa raíz del problema.

- Establecer el plan de acción propuesto.

- Obtener los recursos necesarios para implementar las acciones propuestas.

- Asegurar que la ejecución de la solución planteada este de acuerdo con los tiempos establecidos en el informe acción de mejora.

- Apoyar a los responsables de proceso en la identificación y búsqueda de posibles causas raíces.

- Hacer seguimiento al estado de los informes de acción de mejora.

- Realizar la aprobación del análisis del hallazgo, verificando que las acciones planeadas den respuesta al hallazgo y cierre a la causa raíz del problema.

- Hacer seguimiento a la implementación de las acciones tomadas de los informes de acciones de mejora.

- Evaluar si la implementación de acciones planeadas es adecuada, conveniente y fue eficaz para el cierre del hallazgo.

- Dar cierre a los hallazgos cuando se verifique la eficacia de las actividades planteadas.

De los colaboradores:

- Identificar y reportar situaciones de no-conformidad que detecten en el desarrollo de sus labores.

- Participar en la búsqueda y evaluación de las causas que originen una no conformidad.

- Participar en la identificación de los planes de acción de mejora.

9.5.1.5 Aspectos críticos

- Identificar y reportar posibles situaciones de no conformidad
- Analizar las causas del posible problema o desviación.
- Hacer seguimiento a las acciones de mejora
- Evaluar adecuación, conveniencia y eficacia de la solución tomada.

9.5.1.6 Registros

- Informe acción de mejora.
- Seguimiento acciones de mejora.

9.5.1.7 Definiciones

- No conformidad: Es el incumplimiento a un requisito establecido.
- No conformidad potencial: Es una situación que representa un riesgo para la seguridad de la información y se debe mitigar para evitar que se convierta en un incumplimiento de un requisito o una especificación.
- Corrección: Es una acción tomada para eliminar una no conformidad detectada. No requiere eliminar la causa de la no conformidad. Una corrección puede realizarse junto con una acción correctiva.
- Acción general: Se establece para mejorar los procesos y procedimientos, permiten aumentar la eficacia del Sistema de Gestión de Seguridad de la Información.
- Acción correctiva. Tipo de acción para eliminar las causas de las no conformidades y evitar que vuelvan a ocurrir. Se inicia con la evaluación del impacto que puede ocasionar la no conformidad detectada. En caso

de que el impacto sea alto, se establece la necesidad de iniciar con un informe acción de mejora, el cual debe contener las acciones apropiadas a los efectos de las no conformidades encontradas.

- Acción preventiva: Tipo de acción para mitigar los riesgos y eliminar las causas de no conformidades potenciales para prevenir su ocurrencia**.**

9.5.1.8 Clasificación de no conformidades

No conformidad crítica (NC):

- Afecta de manera directa la seguridad de la información generando afectación en la operación de los procesos de la organización.

- La fecha máxima de implementación de acciones es de máximo 30 días.

No conformidad mayor (NM):

- Incumple de la norma.

- Incumplimiento de un procedimiento que afecte el cumplimiento de la norma.

- La fecha máxima de implementación de acciones es de máximo 60 días.

No conformidad menor (Nm):

- No diligenciamiento de formatos.

- Diligenciamiento incompleto de formatos.

- La fecha máxima de implementación de acciones es de máximo 60 días.

9.5.1.9 Reporte de acciones de mejora

En el informe de acción de mejora se debe evidenciar la siguiente información:

- Tipo: Si es una acción correctiva se debe redactar el hallazgo tal cual se encuentra en el informe de auditoría. Si es una acción preventiva se redacta la causa de falla determinada.
- No conformidad: Según clasificación de no conformidades.

- Origen: Proceso que origina la acción de mejora.

- Código de la acción de mejora: Identificación única del hallazgo.

- Análisis de causa: Identificación de los hallazgos que conllevan a la acción correctiva o preventiva.

- Plan de acción propuesto: Técnicas, mecanismos o herramientas planteadas para la consecución de la acción propuesta.

- El reporte de acciones de mejora debe ser almacenado y controlado por el responsable del procedimiento, esto con el fin de dar seguimiento a la ejecución de las actividades propuestas.

9.5.2 Control de documentos

9.5.2.1 Objetivo. Proveer la evidencia de que los documentos del Sistema de Gestión de Seguridad de la Información se encuentran controlados, actualizados y están disponibles para ser utilizados por parte del personal autorizado.

9.5.2.2 Alcance. Se aplica a todos los documentos relacionados con el Sistema de Gestión de Seguridad de la Información, incluyen los documentos de origen externo que contribuyan o estén relacionados con la seguridad de la información en la organización.

9.5.2.3 Documentos de referencia

- NTC ISO 27001:2013

9.5.1.4 Responsabilidad

Del coordinador del área de gestión tecnológica:

- Elaborar los documentos requeridos para el buen ejercicio de sus labores.

- Realizar la inclusión de documentos nuevos, cambios y anulaciones, así como de divulgar e implementar.

- Controlar la eliminación de documentos en borrador de la elaboración de los documentos nuevos.

De los colaboradores:

- Realizar la solicitud de documentos nuevos, cambios y anulaciones.

9.5.1.5 Aspectos críticos

- Mantener los documentos y la lista maestra de documentos actualizados.
- Identificar la naturaleza del cambio en los documentos.
- Aprobar los documentos en cuanto a su adecuación antes de su registro.

9.5.1.6 Registros

- Solicitud de creación, actualización o anulación de documentos.

- Lista maestra de documentos.

- Repositorio documental del Sistema de Gestión de Seguridad de la Información.

9.5.1.7 Estructura documental. La documentación del Sistema de Gestión de Seguridad de la Información debe estructurarse por niveles, siendo cada estrato sucesivo más detallado, esta representación se realiza de manera jerárquica evidenciando la dependencia de los documentos.

9.5.1.8 Creación, anulación o actualización. La creación, anulación o actualización de los documentos se realiza a través del formato establecido. Todo documento debe ser revisado y actualizado cada dos años a partir de la

entrada en vigencia, en caso de no sufrir ningún cambio se genera una nueva versión con la justificación de revisión del documento.

9.5.1.9 Manejo documentos obsoletos. Se considera un documento obsoleto aquel que ya no sea adecuado a las necesidades previamente establecidas, por ello aquí se encuentran los documentos anulados y las versiones anteriores a la vigente. Sin tener en cuenta su origen, el documento obsoleto debe retirarse del Sistema de Gestión de Seguridad de la Información y restringirse su uso y divulgación.

9.5.1.10 Copia controlada. Todo documento que haga parte del Sistema de Gestión de Seguridad de la Información debe distribuirse con la leyenda de COPIA CONTROLADA. Los documentos que no cuenten con este requisito se consideran como no controlados y por ningún motivo deben utilizarse.

9.5.1.11 Aprobación. Todo documento al finalizar su contenido debe contener las firmas de la persona que lo elaboro o modifico, de quien reviso y quien aprobó, solo así se considera un documento vigente y listo para difundir.

9.5.1.12 Distribución. Previa aprobación, el responsable del procedimiento dispondrá de diferentes canales para distribuir el documento de una manera controlada.

9.5.3 Control de registros

9.5.3.1 Objetivo. Definir los criterios para el control de los registros del Sistema de Gestión de Seguridad de la Información, permitiendo así la consecución de evidencias del grado en que se ha cumplido la conformidad con los requisitos, asegurando la identificación, el almacenamiento, la protección, la recuperación, el tiempo de retención y la disposición final de los registros.

9.5.3.2 Alcance. Este procedimiento aplica a los registros que se generan en las diferentes actividades derivadas del proceso de aseguramiento de la información en la organización.

9.5.3.3 Documentos de referencia

- NTC ISO 27001:2013

9.5.3.4 Responsabilidad

Del coordinador del área de gestión tecnológica:

- Velar por la legibilidad, protección y recuperación de los registros.

Colaboradores:

- Mantener actualizados los registros según las necesidades del proceso o normatividad vigente.
- Asegurar que se utilice el registro vigente.
- Garantizar la identificación, el almacenamiento, la protección, la recuperación, el tiempo de retención y la disposición final de los registros.
- Cumplir con los parámetros establecidos para los registros.

9.5.3.5 Aspectos críticos

- Mantener la lista maestra de documentos actualizada.
- Disponibilidad de consulta de los registros en los medios habilitados para tal fin.
- La legibilidad en su presentación.
- Confidencialidad, disponibilidad e integridad de los registros.

9.5.3.6 Registros

- Lista maestra de documentos.

9.5.3.7 Identificación. Todos los registros deben tener un código asignado y estar vigente dentro del listado maestro de documentos.

9.5.3.8 Almacenamiento. El almacenamiento de los registros debe realizarse en los recursos dispuestos por el responsable del proceso y estar debidamente identificados.

9.5.3.9 Tiempo de retención. El Responsable del proceso determina el tiempo de retención de cada registro y el método de disposición, basándose en las disposiciones obligatorias de ley y en su experiencia en el manejo de los mismos.

9.5.4 Gestión de incidentes de seguridad de la información

9.5.4.1 Objetivo. Definir las actividades necesarias para la detección y gestión eficiente de cualquier incidencia o evento que afecte la seguridad de la información de la organización.

9.5.4.2 Alcance. Incidencias que afecten la confidencialidad, integridad y disponibilidad en los activos de información, aplicable a todos los colaboradores, terceros o proveedores que presten un servicio a la organización de forma eventual o permanente.

9.5.4.3 Documentos de referencia

- NTC ISO 27001:2013

9.5.4.4 Responsabilidad

Del coordinador del área de gestión tecnológica:

- Implementación y cumplimiento del procedimiento.
- Seguimiento al reporte y gestión de las incidencias.
- Establecer contacto con las autoridades competentes.

De los funcionarios:

- Informar sobre cualquier incidencia o evento que se considere como una posible causa de afectación a la seguridad de la información.

De los colaboradores:

- Evaluación del incidente.
- Identificar e implementar los controles pertinentes para mitigar y eliminar las causas de la incidencia.
- Generar las acciones pertinentes para dar respuesta al incidente.

9.5.4.5 Aspectos críticos

- Identificación de incidencia.
- Reporte de incidencia.
- Tratamiento de la incidencia.

9.5.4.6 Registros

- Reporte de incidencia o evento.
- Informe de gestión de incidencia.

9.5.4.7 Reporte de incidencia. Todo funcionario de la organización, tercero o proveedor que preste un servicio a la compañía al identificar una incidencia,

genera el reporte por medio de los canales de comunicación establecidos por el responsable del procedimiento.

9.5.4.8 Evaluación de incidencia. La incidencia se debe asignar a un funcionario del área de tecnología quien realiza la evaluación del incidente y la categoriza según su tipo y criticidad. En caso de que la novedad reportada no se considere una incidencia de seguridad de la información, se debe informar a la persona que la genera sobre el cierre de la actividad.

9.5.4.9 Identificación e implementación de mecanismos y controles. Se realiza el análisis del incidente y el impacto del mismo con el fin de identificar los mecanismos y controles idóneos para salvaguardar el activo de información expuesto. El personal que atiende la incidencia genera el informe de gestión de incidencia donde se evidencia los hallazgos y acciones referentes a la atención y cierre del caso.

9.5.4.10 Continuidad del negocio. Si el incidente repercute en la operación de la organización y la indisponibilidad de su plataforma tecnológica en cuanto a recursos y servicios se refiere, se despliegan los mecanismos y procedimientos establecidos para garantizar la continuidad del negocio.

9.5.4.10 Comunicación con autoridades competentes. El responsable del procedimiento entablara comunicación con las autoridades competentes cuando la incidencia sea crítica y no pueda ser atendida ni gestionada por la organización.

10. PRODUCTO RESULTADO A ENTREGAR

Al culminar el proyecto, la empresa Belisario Ltda. obtendrá una guía que brinde a la compañía un instrumento conceptual aplicable a la gestión eficiente de la seguridad de la información de la organización conformada por:

- Políticas y procedimientos del SGSI según el alcance establecido.
- Matriz de activos identificados, clasificados y valorados.
- Matriz de amenazas y riesgos.

11. RECURSOS NECESARIOS PARA EL DESARROLLO

Recurso humano:

- Asesor en seguridad informática con amplio recorrido y conocimiento en diseño e implementación de SGSI.
- Profesional en ingeniería de sistemas responsable de la ejecución del proyecto.
- Personal de la organización responsable y directamente implicado en los procesos definidos por la organización para el desarrollo del proyecto.

Recursos tecnológicos:

- Equipos de cómputo y herramientas de ofimática.

Normas, estándares y documentación:

- ISO 27001.
- ISO 27002.
- Metodología MAGERIT.
- Sistema de Gestión de Calidad de la organización.

12. CRONOGRAMA DE ACTIVIDADES

Para la ejecución del proyecto se desarrolla el siguiente cronograma de actividades con base en los objetivos propuestos:

Tabla 19. Cronograma del proyecto

Objetivo	Fecha Inicio	Fecha finalización
Identificación y clasificación de activos de información	7 de septiembre 2016	30 de septiembre 2016
Análisis y gestión de riesgos basado en amenazas	1 de octubre 2016	28 de octubre 2016
Verificar la existencia de controles y nivel de mitigación de los mismos	29 de octubre 2016	11 de noviembre 2016
Diseño del Sistema de Gestión de Seguridad de la Información	12 de noviembre 2016	28 de noviembre 2016

Fuente: Autor

13. CONCLUSIONES

Con la adopción de la metodología de análisis y gestión de riesgos MAGERIT, se permite identificar los activos a proteger y que hacen parte fundamental en la ejecución de los diferentes procesos organizacionales, determinando el impacto y riesgo derivado de la posible materialización de amenazas.

El instrumento de la declaración de aplicabilidad relaciona un conjunto de mecanismos y controles aplicables a la organización siendo adaptable a los cambios y necesidades que surjan dentro de la compañía, sin ser este un elemento restrictivo para la inclusión de medidas de protección que no estén contempladas dentro de su estructura.

La compañía no realiza análisis de causas a los sucesos que han generado indisponibilidad a la plataforma tecnológica de la organización afectando la operación de la misma, lo que conlleva a establecer medidas correctivas y no acciones preventivas.

Los riesgos asociados a los activos de información son establecidos en la matriz de tratamiento de riesgos la cual debe mantenerse acorde a la evolución de la organización y su entorno, con el fin de garantizar la confidencialidad, integridad y disponibilidad de estos mismos.

La implementación de los mecanismos y controles sugeridos permiten a la alta dirección alinear la seguridad de la información a los objetivos estratégicos de la organización, estableciendo lineamientos que apoyen su gestión y permitiendo reducir la aceptación del riesgo a un nivel mínimo.

Las políticas y procedimientos identificados y desarrollados en el proyecto se presentan como elementos para una administración y operación eficiente del Sistema de Gestión de Seguridad de la Información y deben ser adaptados según la madurez que adquiera el SGSI en procura de la mejora continua.

14. RECOMENDACIONES

Ampliar el alcance del Sistema de Gestión de Seguridad de la Información con el fin de contemplar las diferentes áreas o procesos que componen la organización.

Establecer un plan estratégico de inversión que contemple la adquisición y mantenimiento de los diferentes mecanismos y controles dispuestos para la protección de la seguridad de la información.

La empresa debe iniciar un proceso de capacitación al personal de la organización en aspectos relevantes de la seguridad de la información.

Es importante que la organización inicie un proceso de formación en la gestión y operación del Sistema de Gestión de Seguridad de la Información aplicable al área de gestión tecnológica.

Se sugiere que la organización realice auditorias de seguimiento al Sistema de Gestión de Seguridad de la Información, como minino una vez al año.

Establecer roles y responsabilidades según la estructura organizacional en la gestión del SGSI vinculado personal de diferentes procesos con el fin de concientizar a los usuarios sobre la importancia del proyecto para la organización.

La compañía debe establecer políticas y procedimientos con el fin de dar cumplimiento a las disposiciones impartidas por la ley 1581 del 2012 en el tratamiento adecuado a los datos personales que estén bajo la responsabilidad de la organización, de igual manera se deben registrar las bases de datos en el Registro Nacional de Base de Datos siguiendo los lineamientos establecidos por la Superintendencia de Industria y Comercio.

15. DIVULGACIÓN

El proyecto es entregado a la alta dirección de la organización, y es esta quien establece los medios de comunicación y divulgación de los hallazgos, resultados y recomendaciones a los colaboradores y miembros de la compañía. De igual manera se utiliza el repositorio de la Universidad Nacional Abierta y a Distancia UNAD con el fin de publicar el documento como un recurso de consulta y referencia para el público en general.

BIBLIOGRAFÍA

ALEGRE RAMOS, María del Pilar. Seguridad informática. Ed. 11. Madrid: Parainfo, 2011. 168p.

ALEXANDRA PARCO, Paola Alexandra. Sistema de gestión de seguridad de la información (SGSI) en el comando provincial de policía Imbabura Nro. 12. Trabajo de grado Ingeniero electrónico. Ibarra, Ecuador: Universidad Técnica del Norte. Facultad de ingeniería, 2013. 399 p

BOLIVAR LEON, Yeinny Andrea. Diseño de un sistema de gestión de seguridad de la información en la intranet del Policlínico del sur Olaya Bogotá, bajo la norma ISO 27001. Tesis de grado especialista en seguridad informática. Bogotá: Universidad Nacional Abierta y a Distancia. Escuela de ciencias básicas tecnología e ingeniería, 2015. 79 p.

DE LA CRUZ GUERRERO, César Wenceslao y VÁSQUEZ MONTENEGRO, Juan Carlos. Elaboración y aplicación de un Sistema de Gestión de la Seguridad de la Información (SGSI) para la realidad tecnológica de la USAT. Trabajo de grado Ingeniero de Sistemas. Chiclayo, Perú: Universidad Católica Santo Toribio de Mogrovejo. Facultad de ingeniería, 2008. 160 p.

DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA ESPAÑOLA, “MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”.

GARAVITO ROBLES, Hina Luz. Análisis y gestión del riesgo de la información en los sistemas de una entidad del estado, enfocado en un sistema de seguridad de la información. Tesis de grado especialista en seguridad informática. Bogotá: Universidad Nacional Abierta y a Distancia. Escuela de ciencias básicas tecnología e ingeniería, 2015. 108 p.

GUZMÁN GARCÍA, Alexánder y TABORDA BEDOYA, Carlos Alberto. Diseño de un sistema de gestión de la seguridad informática -SGSI-, para empresas del área textil en las ciudades de Itagui, Medellin y Bogotá D.C. a través de la auditoria. Trabajo de grado especialista en seguridad informática. Bogotá: Universidad Nacional Abierta y a Distancia. Escuela de ciencias básicas tecnología e ingeniería, 2015. 311 p.

GUZMÁN SILVA, Carlos Alberto. Diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso. Trabajo de grado especialista en seguridad de la información. Bogotá: Politécnico Grancolombiano. Facultad de ingeniería y ciencias básicas, 2015. 173 p.

MARTIN IGLESIAS, Laura. Diseño de un sistema de gestión de seguridad de la información (SGSI). Trabajo de grado Ingeniero técnico en informática de gestión. Madrid, España: Universidad Rey Juan Carlos. Facultad de ingeniería. 2010, 61 p.

ROMO VILLAFUERTE, Daniel y VALAREZCO CONSTANTE, Joffre. Análisis e implementación de la norma ISO 27002 para el departamento de sistemas de la Universidad Politécnica Salesiana sede Guayaquil. Trabajo de grado Ingeniero de sistemas. Guayaquil, Ecuador: Universidad Politécnica Salesiana. Faculta de ingeniería, 2012. 183 p.

SARRIA CUÉLLAR, Mercedes. Diseño de un modelo de un Sistema de Gestión de Seguridad de la Información para la empresa social del estado Fabio Jaramillo Londoño mediante la norma ISO/IEC 27001:2013. Tesis de grado especialista en seguridad informática. Florencia: Universidad Nacional Abierta y a Distancia. Escuela de ciencias básicas tecnología e ingeniería, 2015. 175 p.

ANEXO A LISTA DE VERIFICACIÓN CUMPLIMIENTO EN NORMA ISO 27001:2013

PROCESO	FECHA	HORA	LUGAR
AUDITADOS	**NOMBRE**	**CARGO**	**FIRMA**
Responsable del Proceso			
Acompañante(s)			
GRUPO AUDITOR	**NOMBRE**	**CARGO**	**FIRMA**
Auditor Líder			
Auditor(res) Acompañante(s)			
DOCUMENTO DE REFERENCIA			

Clausula 5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Numeral	PREGUNTA o GUÍA (Se debe formular con base en el requisito)	TIPO[1]	Cumple/ No Cumple	OBSERVACIONES o EVIDENCIA
A 5.1.1	¿La Empresa ha establecido un conjunto de políticas para la seguridad de la información?			
A 5.1.2	¿La organización ha establecido intervalos planificados para la revisión de políticas para la seguridad de la información?			

Clausula 6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Numeral	PREGUNTA o GUÍA (Se debe formular con base en el requisito)	TIPO[1]	Cumple/ No Cumple	OBSERVACIONES o EVIDENCIA
A 6.1.1	¿La compañía ha definido los roles y responsabilidades frente al sistema de gestión de seguridad de la información?			
A 6.1.2	¿Se tiene separados los deberes a nivel de la operación del proceso de gestión tecnológica y del SGSI?			
A 6.1.3	¿Se han identificado las autoridades pertinentes con relación al cumplimiento de la ley, los organismos de regulación y las autoridades de supervisión?			
A 6.1.4	¿Se tiene contacto con grupos de interés especial, foros o asociaciones de profesionales especializados en seguridad de la información?			

Numeral	PREGUNTA o GUÍA (Se debe formular con base en el requisito)	TIPO[1]	Cumple/ No Cumple	OBSERVACIONES o EVIDENCIA
A 6.1.5	¿En la gestión de proyectos se trata la seguridad de la información independiente del tipo de proyecto?			
A 6.2.1	¿Se adoptó una política para dispositivos móviles?, ¿Se tienen medidas de seguridad de soporte para gestionar los riesgos introducidos por el uso de los dispositivos móviles?			
A 6.2.2	¿Se ha implementado una política de teletrabajo en la organización?, ¿Se tienen medidas de seguridad de soporte para proteger la información a la que se tiene acceso, procesa o almacena en el lugar del teletrabajo?			

Clausula 7. SEGURIDAD DE LOS RECURSOS HUMANOS

Numeral	PREGUNTA o GUÍA (Se debe formular con base en el requisito)	TIPO[1]	Cumple/ No Cumple	OBSERVACIONES o EVIDENCIA
A 7.1.1	¿Se verifican los antecedentes de los candidatos a un empleo de acuerdo con las leyes, reglamentaciones y ética pertinentes?			
A 7.1.2	¿En el contrato se establecen las responsabilidades con relación a la seguridad de la información?			
A 7.2.1	¿La dirección exige a los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con la política y los procedimientos establecidos por la organización?			
A 7.2.2	¿Los funcionarios y contratistas de la organización tienen las competencias necesarias y la toma de conciencia apropiada sobre la política y procedimientos asociados a la seguridad de la información?			
A 7.2.3	¿La organización cuenta con un proceso formal para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información?			
A 7.3.1	¿Se retiran los privilegios sobre los sistemas de información, aplicativos y demás cuando sea pertinente en el caso que un colaborador o contratista cambie de cargo o se retire de la organización?			

Clausula 8. GESTIÓN DE ACTIVOS

Numeral	PREGUNTA o GUÍA (Se debe formular con base en el requisito)	TIPO[1]	Cumple/ No Cumple	OBSERVACIONES o EVIDENCIA
A 8.1.1	¿Se identifica y mantiene un inventario de activos asociados con información e instalaciones de procesamiento de información?			
A 8.1.2	¿Los activos mantenidos en el inventario tienen un propietario?			

Numeral	PREGUNTA o GUÍA (Se debe formular con base en el requisito)	TIPO[1]	Cumple/ No Cumple	OBSERVACIONES o EVIDENCIA
A 8.1.3	¿Se tienen reglas para el uso aceptable de los activos?			
A 8.1.4	¿Se tiene un procedimiento o instructivo guía para la devolución de activos?			
A 8.2.1	¿Se tiene clasificada la información en función de los requisitos legales y el valor que tiene para el negocio?			
A 8.2.2	¿Se ha desarrollado e implementado un procedimiento, instructivo o guía para el etiquetado de la información que esté de acuerdo con el esquema de clasificación de la información adoptado por la organización?			
A 8.2.3	¿Hay implementadas políticas, procedimientos o guías para el manejo de los activos que esté de acuerdo con el esquema de clasificación de la información adoptado por la organización?			
A 8.3.1	¿La organización cuenta con una política o procedimiento para la gestión de medios removibles que esté de acuerdo con el esquema de clasificación de la información adoptado por la organización?			
A 8.3.2	¿Se dispone en forma segura de los medios cuando ya no se requieren, utilizando procedimientos formales?			
A 8.3.3	¿Se protege contra acceso no autorizado, uso indebido o corrupción, los medios durante el transporte?			

Clausula 9. CONTROL DE ACCESO

Numeral	PREGUNTA o GUÍA (Se debe formular con base en el requisito)	TIPO[1]	Cumple/ No Cumple	OBSERVACIONES o EVIDENCIA
A 9.1.1	¿La organización cuenta con una política de control de acceso?			
A 9.1.2	¿Se han establecido mecanismos de acceso a redes y a servicios de red?			
A 9.2.1	¿La organización cuenta con una metodología clara de registro y cancelación de usuarios?			
A 9.2.2	¿Se han desarrollado e implementado perfiles de usuario para garantizar un acceso normal para todo tipo de usuarios y todos los sistemas y servicios?			
A 9.2.3	¿Se tienen implementados accesos privilegiados y quien los concede?			
A 9.2.4	¿Se utiliza algún método para controlar o gestionar la información de autenticación secreta de los usuarios?			
A 9.2.5	¿Se revisan los derechos de acceso de los usuarios?			
A 9.2.6	¿La organización cuenta con una metodología para el retiro o ajuste de los derechos de acceso de los usuarios?			
A 9.3.1	¿La organización cuenta con una política, instructivo, guía u otra para exigir a los usuarios que cumplan con las practicas sobre el uso de la información de autenticación			
A 9.4.1	¿El acceso a la información y a las funciones de los sistemas de las aplicaciones se restringe?			
A 9.4.2	¿Para el ingreso a las aplicaciones y los sistemas de información se utilizan técnicas de ingreso seguro?			
A 9.4.3	¿Es posible que el usuario final pueda interactuar con el sistema de gestión de contraseñas?			

A 9.4.4	¿La organización bloquea el uso de utilitarios privilegiados?			
A 9.4.5	¿Está prohibido el uso de ingeniería inversa sobre el software propio o licenciado?			

Clausula 10. CRIPTOGRAFÍA

Numeral	PREGUNTA o GUÍA (Se debe formular con base en el requisito)	TIPO[1]	Cumple/ No Cumple	OBSERVACIONES o EVIDENCIA
A 10.1.1	¿La organización tiene una política sobre el uso de controles criptográficos para la protección de la información y además ha sido implementada?			
A 10.1.2	¿En caso de utilizar firmas digitales y certificados digitales, como la organización usa, protege y controla el tiempo de vida de las llaves criptográficas?			

Clausula 11. ÁREAS SEGURAS

Numeral	PREGUNTA o GUÍA (Se debe formular con base en el requisito)	TIPO[1]	Cumple/ No Cumple	OBSERVACIONES o EVIDENCIA
A 11.1.1	¿La organización define y usa perímetros de seguridad física para proteger las instalaciones que procesan información crítica?			
A 11.1.2	¿Las áreas seguras de la organización tienen implementados controles de acceso físico apropiados y solo se permite el acceso a personal autorizado?			
A 11.1.3	¿Qué tipo de seguridad física esta implementada en oficinas, recintos e instalaciones?			
A 11.1.4	¿Se ha diseñado e implementado algún tipo de seguridad física como protección contra desastres naturales, ataques maliciosos o accidentes?			
A 11.1.5	¿La organización tiene guías, instructivos o procedimientos para trabajar en las áreas seguras?			
A 11.2.1	¿Se protegen los equipos de amenazas y peligros del entorno y se ubican de tal modo para evitar el riesgo de acceso no autorizado?			
A 11.2.2	¿Los equipos están protegidos contra fallas en el suministro de energía?			
A 11.2.3	¿El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información, están protegidos contra interceptación, interferencia o daño?			
A 11.2.4	¿Se cuenta con un programa de mantenimiento preventivo y correctivo para las estaciones de trabajo?			
A 11.2.5	¿La organización controla el retiro no autorizado de los equipos, el software o la información?			
A 11.2.6	¿Fuera de las instalaciones de la organización se aplican medidas de seguridad a los activos?			
A 11.2.7	¿Se hace disposición segura de medios de almacenamiento antes de su reúso?			
A 11.2.8	¿Los equipos desatendidos se bloquean para impedir el uso no autorizado?			
A 11.2.9	¿La organización tiene implementada una política de pantalla limpia en las estaciones de trabajo?			

Clausula 12. EQUIPOS

Numeral	PREGUNTA o GUÍA (Se debe formular con base en el requisito)	TIPO[1]	Cumple/ No Cumple	OBSERVACIONES o EVIDENCIA
A 12.1.1	¿La organización cuenta con procedimientos de la operación documentados y disponibles para cuando se necesiten?			
A 12.1.2	¿Se tiene implementado en la organización un proceso, política o procedimiento de gestión de cambios?			
A 12.1.3	¿Se tiene implementado en la organización un proceso, política o procedimiento de gestión de capacidad?			
A 12.1.4	¿Se ha implementado en la organización ambientes de redes lógicos para desarrollo, pruebas y producción?			
A 12.2.1	¿La organización tiene implementada una solución de control de códigos maliciosos?			
A 12.3.1	¿Se tiene implementado el respaldo de la información para los aplicativos?			
A 12.4.1	¿La organización conserva y revisa los registros de las actividades (logs) de los usuarios en las aplicaciones así como excepciones, fallas o eventos en el directorio activo?			
A 12.4.2	¿Se protege los registros de actividades (logs) contra alteración y uso no autorizado?			
A 12.4.3	¿Las actividades (logs) del administrador y de los operadores del: directorio activo, sistemas operativos de servidor, bases de datos, aplicaciones; se protegen y revisan con regularidad?			
A 12.4.4	¿La organización tiene implementado el protocolo NTP y la sincronización de relojes?			
A 12.5.1	¿Cómo controla la organización la instalación de software en las estaciones de trabajo?			
A 12.6.1	¿La organización obtiene oportunamente información acerca de las vulnerabilidades técnicas de su infraestructura tecnológica?			
A 12.6.2	¿Qué política, procedimiento, guía o instructivo tiene la organización para restringir la instalación de software por parte de los usuarios?			
A 12.7.1	¿Las auditorias son planeadas y acordada cuidadosamente con el fin de minimizar las interrupciones en los procesos del negocio?			

Clausula 13. SEGURIDAD EN LAS COMUNICACIONES

Numeral	PREGUNTA o GUÍA (Se debe formular con base en el requisito)	TIPO[1]	Cumple/ No Cumple	OBSERVACIONES o EVIDENCIA
A 13.1.1	¿De qué manera se gestionan y controlan las redes para proteger la información de las aplicaciones?			
A 13.1.2	¿Qué controles de seguridad y niveles de servicio están acordados para los servicios que actualmente se prestan en la red ya sean prestados internamente o contratados externamente?			

A 13.1.3	¿Los servicios de red, los usuarios y las aplicaciones tienen redes separadas para el préstamo de sus servicios?			
A 13.2.1	¿La organización cuenta con políticas o procedimientos para la transferencia de información?			
A 13.2.2	¿Actualmente la organización tiene directrices para acuerdos con terceras partes sobre transferencia de información?			
A 13.2.3	¿La organización cuenta con un servicio de mensajería electrónica?			
A 13.2.4	¿La organización tiene firmados con sus funcionarios, contratistas o proveedores acuerdos de confidencialidad o de no divulgación?			

Clausula 14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Numeral	PREGUNTA o GUÍA (Se debe formular con base en el requisito)	TIPO[1]	Cumple/ No Cumple	OBSERVACIONES o EVIDENCIA
A 14.1.1	¿En los requisitos no funcionales se establecen requisitos asociados a la seguridad de la			
A 14.1.2	¿Las aplicaciones se protegen de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizada en las redes públicas?			
A 14.1.3	¿Las transacciones de las aplicaciones son protegidas para evitar transmisión incompleta, enrutamiento errado, alteración de información no autorizada, divulgación no autorizada y duplicación o reproducción de información no autorizada?			
A 14.2.1	¿La organización cuenta con una política de desarrollo seguro?			
A 14.2.2	¿La organización cuenta con un procedimiento de control de cambios para las aplicaciones			
A 14.2.3	¿Cuándo se actualizan los sistemas operativos (patch management) se revisan las aplicaciones desde el punto de vista técnico para garantizar su funcionalidad?			
A 14.2.4	¿Se pueden modificar las aplicaciones sin restricciones?			
A 14.2.5	¿Se cuenta con una metodología de desarrollo de sistemas basada en las mejores prácticas asociadas a la seguridad de la información?			
A 14.2.6	¿La organización tiene un ambiente para el desarrollo seguro para las aplicaciones?			
A 14.2.7	¿La organización tiene contratado externamente el desarrollo de software?			
A 14.2.8	¿Para las aplicaciones se realizan pruebas de la funcionalidad de la seguridad?			
A 14.2.9	¿La organización ha establecido criterios y pruebas para la aceptación de las aplicaciones?			
A 14.3.1	¿Cómo seleccionan, protegen y controlan los datos usados para las pruebas			

Clausula 15. RELACIÓN CON LOS PROVEEDORES

Numeral	PREGUNTA o GUÍA (Se debe formular con base en el requisito)	TIPO[1]	Cumple/ No Cumple	OBSERVACIONES o EVIDENCIA
A 15.1.1	¿La organización ha definido una política donde incluya una valoración de riesgos asociados con el acceso de los proveedores a los activos de la organización y que haya sido documentada y comunicada entre las partes?			
A 15.1.2	¿La organización ha exigido contractualmente acuerdos de niveles de servicios (ANS) para la Prestación de servicios a través de terceras partes para las aplicaciones?			
A 15.1.3	¿Se valoran los riesgos de los proveedores asociados a la cadena de suministro de productos			
A 15.2.1	¿La organización hace seguimiento, revisa y audita la prestación de servicios de los proveedores?			
A 15.2.2	¿La organización gestiona los cambios en la prestación del servicio por parte de los proveedores?			

Clausula 16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Numeral	PREGUNTA o GUÍA (Se debe formular con base en el requisito)	TIPO[1]	Cumple/ No Cumple	OBSERVACIONES o EVIDENCIA
A 16.1.1	¿La organización ha definido responsabilidades y procedimientos de gestión de incidentes de seguridad de la información?			
A 16.1.2	¿La organización tiene provistos canales de comunicación para reportar eventos de seguridad de la información?			
A 16.1.3	¿La organización tiene provistos canales de comunicación para reportar debilidades de seguridad de la información?			
A 16.1.4	¿La organización evalúa los eventos de seguridad de la información y toma decisiones para clasificarlos como incidentes de seguridad de la información?			
A 16.1.5	¿La organización da respuesta a los incidentes de seguridad de la información a través de procedimientos documentados?			
A 16.1.6	¿El conocimiento adquirido al resolver los incidentes de seguridad de la información son documentados para reducir la probabilidad o impacto de incidentes futuros?			
A 16.1.7	¿La organización tiene un procedimiento para la recolección de evidencias?			

Clausula 17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN

Numeral	PREGUNTA o GUÍA (Se debe formular con base en el requisito)	TIPO[1]	Cumple/ No Cumple	OBSERVACIONES o EVIDENCIA
A 17.1.1	¿La organización ha determinado los requisitos para la continuidad de la seguridad de la información en situaciones adversas como una crisis o desastre?			
A 17.1.2	¿La organización he definido procedimientos y controles para asegurar la continuidad de la seguridad de la información durante una situación adversa?			
A 17.1.3	¿La organización revisa a intervalos planificados los controles implementados para la continuidad de la seguridad de la información con el fin de garantizar que son eficaces ante una situación adversa?			
A 17.2.1	¿La organización cuenta con redundancias suficientes para sus diferentes servicios?			

Clausula 18. CUMPLIMIENTO

Numeral	PREGUNTA o GUÍA (Se debe formular con base en el requisito)	TIPO[1]	Cumple/ No Cumple	OBSERVACIONES o EVIDENCIA
A 18.1.1	¿La organización ha identificado y documentado explícitamente los requisitos legales, regulatorios, estatutarios y contractuales aplicables a los sistemas de información y a la propia organización?			
A 18.1.2	¿La organización he implementado procedimientos para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales con relación a los derechos de propiedad intelectual y el uso de software patentado?			
A 18.1.3	¿Se ha establecido un proceso formal para proteger los registros de la organización?			
A 18.1.4	¿La organización asegura la privacidad y la protección de los datos personales como exige la legislación?			
A 18.1.5	¿La organización cumple los acuerdos de uso de los controles criptográficos identificados y su			
A 18.21	¿La organización ha revisado de manera independiente el SGSI?			
A 18.2.2	¿Se verifica periódicamente el cumplimiento de las políticas de seguridad de la información en los procesos que están dentro del alcance del SGSI?			
A 18.2.3	¿Se verifican periódicamente los sistemas de información que están dentro del alcance del SGSI para determinar el cumplimiento de las políticas de seguridad de la información?			

[1] C: Crítica; NM: No Conformidad Mayor; Nm: No Conformidad Menor; OBS: Observación

ANEXO B INFORME ACCIÓN DE MEJORA

CÓDIGO HALLAZGO:

TIPO ACCIÓN		NO CONFORMIDAD		ORIGEN		INFORMACIÓN AUDITORIA	
CORRECTIVA		CRÍTICA		REPORTE INTERNO		AUDITOR	
PREVENTIVA		MAYOR		AUDITORIA / AUTO INSPECCIÓN		FECHA	
		MENOR		REVISIÓN POR LA DIRECCIÓN		PROCESO	
		OBSERVACIÓN		REPORTE EXTERNO		AUDITADO	

HALLAZGO - NO CONFORMIDAD

RESPONSABLE DEL PROCESO

ANÁLISIS DE CAUSAS
Describa la conclusión del análisis

PLAN DE ACCIÓN PROPUESTO			
N°	**Actividades Propuestas**	**Responsable**	**Fecha Máxima Implementación**

SEGUIMIENTO A LA EJECUCIÓN DE ACTIVIDADES					
N° Actividad	**¿Se Implementó?**		**Fecha**	**Auditor**	**Observaciones**
	SI	NO			
	SI	NO			
	SI	NO			
	SI	NO			

EFICACIA DE LAS ACTIVIDADES					
N° Acción	**¿Fue Eficaz?**		**Auditor**	**Fecha**	**Observaciones**
	SI	NO			
	SI	NO			

	SI	NO			
	SI	NO			

EFICACIA DEL PLAN DE ACCIÓN					
¿El Plan de Acción fue eficaz para el cierre del hallazgo?	SI NO	**Firma Auditor**		**Fecha Cierre Acción**	

ANEXO C FORMATO PLAN DE AUDITORIA

OBJETIVO	ALCANCE

CRITERIOS Y DOCUMENTOS DE	EQUIPO AUDITOR		INICIALES
	Auditor Líder		
	Auditor(es) Acompañante(s)		

PROCESO A AUDITAR	RESPONSABLE EQUIPO AUDITOR	RECIBE AUDITORIA	FECHA	LUGAR	HORA

FECHA APERTURA	LUGAR APERTURA	HORA APERTURA
FECHA CIERRE	**LUGAR CIERRE**	**HORA CIERRE**

LISTA DE ASISTENTES

NOMBRE	CARGO	FIRMA APERTURA	FIRMA CIERRE

ANEXO D FORMATO INFORME DE AUDITORIA

OBJETIVO	ALCANCE

PROCESO AUDITADO	RECIBE AUDITORIA	FECHA	LUGAR	NO CONFORMIDADES	
				Tipo	Cantidad
				Crítica	
				Mayores	
				Menores	
				Observaciones	

CRITERIOS Y DOCUMENTOS DE REFERENCIA	EQUIPO AUDITOR	
	Auditor Líder	
	Auditor(es) Acompañante(s)	

ELEMENTO/DOCUMENTO/ACCIÓN AUDITADOS
FORTALEZAS

TIPO	HALLAZGO

APRECIACIÓN DEL EQUIPO AUDITOR SOBRE GRADO DE CUMPLIMIENTO

GRUPO AUDITOR

NOMBRE	CARGO	FIRMA	FECHA

ACEPTADO Y RECIBIDO RESPONSABLE DEL PROCESO

NOMBRE	CARGO	FIRMA	FECHA

ANEXO E INFORME DE GESTIÓN DE INCIDENCIAS DE SEGURIDAD

CÓDIGO INCIDENCIA:

FECHA DE INCIDENCIA	FECHA DE REPORTE INCIDENCIA	HORA DE REPORTE INCIDENCIA

DATOS DEL PERSONAL QUE REPORTA LA INCIDENCIA

NOMBRES Y APELLIDOS	
DOCUMENTO DE IDENTIFICACIÓN	
ÁREA	
CORREO ELECTRÓNICO	
TELÉFONO/EXTENSIÓN	

INFORMACIÓN DEL INCIDENTE
Descripción de los hechos
RESPONSABLE DEL REPORTE

DATOS DEL PERSONAL QUE GESTIONA LA INCIDENCIA

NOMBRES Y APELLIDOS	
DOCUMENTO DE IDENTIFICACIÓN	
ÁREA	
CORREO ELECTRÓNICO	
TELÉFONO/EXTENSIÓN	

ANÁLISIS DE CAUSAS
Descripción del análisis
RESPONSABLE DE LA GESTIÓN DEL INCIDENTE

FECHA DE ACCIÓN IMPLEMENTADA	
MECANISMOS Y ACCIONES IMPLEMENTADOS **(Diligenciar el informe acción de mejora)**	
FECHA DE CIERRE DEL INCIDENTE	

ANEXO F RESUMEN ANALÍTICO RAE

Título de Documento	Diseño del sistema de gestión de seguridad informática y de la información (SGSI) para la empresa Belisario Ltda. de la ciudad de Bogotá D.C
Autor	BOTERO VEGA, David Humberto
Palabras Claves	Sistemas de Gestión de Seguridad de la Información, MAGERIT, confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad, activo, amenaza, riesgo, impacto, salvaguarda, política
Descripción El presente documento es un proyecto de grado aplicado, desarrollado en una organización que tiene como actividad la prestación en servicios y asesorías en derecho laboral y seguridad y salud en el trabajo a diferentes entidades privadas y estatales. El objetivo de dicho proyecto es disminuir la perdida de información en la organización y lo que afecte a la protección de la confidencialidad, integridad y disponibilidad de la misma, por medio del diseño de un Sistema de Gestión de Seguridad de la Información (SGSI), aplicado a la plataforma tecnológica de la compañía y los activos y recursos que componen dicha infraestructura.	
Fuentes Bibliográficas	Alexandra Parco, P. (2008). *Sistema de gestión de seguridad de la información (SGSI) en el comando provincial de policía Imbabura Nro. 12.* (Tesis de grado ingeniero electrónico). Recuperado de http://repositorio.utn.edu.ec/handle/123456789/1888 Bolivar Leon, Y. (2015). *Diseño de un sistema de gestión de seguridad de la información en la intranet del Policlínico del sur Olaya Bogotá, bajo la norma ISO 27001.* (Tesis de grado especialista en seguridad informática). Recuperado de http://hdl.handle.net/10596/5513 Garavito Robles, H. (2015). *Análisis y gestión del riesgo de la información en los sistemas de una entidad del estado, enfocado en un sistema de seguridad de la información.* (Tesis de grado especialista en seguridad informática). Recuperado de http://repository.unad.edu.co/bitstream/10596/3423/1/37511933.pdf Guzmán García, A. y Taborda Bedoya, C. *Diseño*

	de un sistema de gestión de la seguridad informática -SGSI-, para empresas del área textil en las ciudades de Itagui, Medellin y Bogotá D.C. a través de la auditoria. (2015). (Tesis de grado especialista en seguridad informática). Recuperado de http://hdl.handle.net/10596/3448 Guzmán Silva, C. (2015). *Diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso.* (Tesis de grado especialista en seguridad de la información). Recuperado de http://repository.poligran.edu.co/bitstream/10823/746/1/Proyecto%20de%20Grado%20SGSI%20-%20IGM-%20CarlosGuzman%20(FINAL).pdf Sarria, M. (2015). *Diseño de un modelo de un Sistema de Gestión de Seguridad de la Información para la empresa social del estado Fabio Jaramillo Londoño mediante la norma ISO/IEC 27001:2013.* (Tesis de grado especialista en seguridad informática). Recuperado de http://repository.unad.edu.co/bitstream/10596/3631/1/40774057.pdf

Contenido

Belisario Ltda. es una empresa de consultoría y asesoría en derecho laboral y seguridad y salud en el trabajo, que maneja información muy importante en la que se encuentran títulos de valores, documentación confidencial de clientes, datos de procesos, entre otros. Para la alta dirección de la organización cobra una real importancia garantizar la custodia y reserva de dicha información, siendo esta el pilar del desarrollo de la actividad económica de la compañía y la base de sus procesos organizacionales.

La organización se ha visto envuelta en perdida de información relevante, esto a causa de errores atribuibles a su personal en la manipulación de la información, fraude a sus cuentas bancarias y daños ocasionados por ejecución de software y código malicioso.

Con el fin de abordar la problemática identificada, se propone el diseño e implementación de un Sistema de Gestión de Seguridad de la Información con el fin de garantizar la protección de la confidenciad, integridad y disponibilidad de su activo más importante, la información. Para la consecución y construcción de este proceso, se definen una serie de objetivos representados en la identificación y clasificación de los activos de la información susceptibles a ser atacados deliberada o accidentalmente con consecuencias para la compañía, análisis de riesgos basado

en las amenazas que puedan materializarse y afectar los activos identificados, verificar la existencia de controles para evaluar el nivel de mitigación ante amenazas, vulnerabilidades y riesgos, y el diseño del Sistema de Gestión de Seguridad de la Información que abarca las políticas, procedimientos y controles acordes al análisis anteriormente desarrollado y a las necesidades de la organización.

La identificación y clasificación de los activos de información se lleva a cabo como establece la metodología de análisis y gestión de riesgos de los sistemas de información, MAGERIT. En la identificación de los diferentes activos de información que define la metodología, se encuentran datos e información, claves criptográficas, servicios, software, hardware, redes de comunicaciones, soportes de información, equipamiento auxiliar, instalaciones y personal.

La valoración de los activos de información se realiza a través de las dimensiones, o propiedades definidas como: disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad. De acuerdo a una escala cuantitativa se asigna un valor para cada uno de los activos en las diferentes dimensiones. La valoración que recibe un activo en una determinada dimensión representa para la organización una medida de perjuicio ante la afectación en dicha característica.

Cada activo dependiendo de su clasificación es susceptible a un conjunto de amenazas, la metodología MAGERIT establece una categorización por desastres naturales, origen industrial, errores y fallos no intencionados y ataques intencionados. Con la identificación de las amenazas para cada activo de información, se procede a valorar la influencia de dicha amenaza en el valor del activo, para esto se tiene en cuenta la degradación, el grado de perjuicio en el activo y la probabilidad, la medida de ocurrencia de materialización de dicha amenaza.

Teniendo la información referente al valor del activo en sus diferentes dimensiones y la degradación que producen las amenazas, se calcula la medida del daño sobre los activos de información al materializarse dichas amenazas, esta variable es denominada impacto y al no considerarse los controles o mecanismos establecidos por la organización, se considera un impacto potencial. Con este criterio se calcula el riesgo potencial, una medida referente al daño probable sobre el sistema, basado en la probabilidad de ocurrencia.

El análisis del impacto y riesgo potencial se efectúa sin tener presente los controles o mecanismos dispuestos en la organización, es por eso que se identifican y valoran las salvaguardas implementadas por la organización con base en la tipificación que ofrece la metodología de gestión y análisis de riesgos, MAGERIT, en la que de manera general se identifican las salvaguardas preventivas, disuasorias, eliminatorias, minimizadoras, correctivas, recuperativas, de monitorización, de detección, de concienciación y administrativas, asociadas a su nivel de eficiencia. Con ese grado de evaluación se realiza el cálculo del impacto y riesgo residual.

Un documento obligatorio en el Sistema de Gestión de Seguridad de la Información es la declaración de aplicabilidad, un instrumento que acorde a la norma 27001 versión 2013, agrupa un conjunto de 114 controles distribuidos en 14 objetivos de control: políticas de seguridad, organización de la información, seguridad en recursos humanos, gestión de activos, control de accesos, criptografía, seguridad física y ambiental, seguridad en las operaciones, transferencia de la información, adquisición de sistemas, desarrollo y mantenimiento, relación con los proveedores, gestión de los incidentes de seguridad, continuidad del negocio, cumplimiento con requerimientos legales y contractuales.

En el diseño del SGSI se definen los objetivos, alcance, la política y aplicabilidad del Sistema de Gestión de Seguridad de la Información. Se establecen las políticas de seguridad de la información con base en los dominios anteriormente descritos y que corresponden a la norma ISO 27001 en su anexo A, referencia de objetivos y controles. Se definen los procedimientos de apoyo a la gestión de seguridad de la información en los que se describen acciones de mejora, control de documentos, control de registros y gestión de incidentes de seguridad de la información.

Se incluyen como anexos al proyecto una serie de instrumentos y elementos de apoyo a la gestión, operación, administración y mantenimiento del Sistema de Gestión de Seguridad de la Información en la organización. Se aporta una lista de verificación o chequeo según la norma ISO 27001 versión 2013, informe de acción de mejora, plan de auditoria, informe de auditoría, informe de gestión de incidentes de seguridad.

Metodología

El marco metodológico del proyecto se enmarca bajo las siguientes etapas que comprenden una serie de actividades encaminadas al desarrollo de cada una de las fases:

Etapa 1: Identificar y clasificar los activos de información de la organización con el fin de establecer que elementos son susceptibles a ser atacados deliberada o accidentalmente con consecuencias para la compañía.

Actividades:

- Efectuar visitas a las instalaciones de la organización con el fin de identificar los activos con los que se dispone.
- Solicitar y revisar el inventario de equipos y hojas de vida de los mismos.
- Realizar entrevistas con los miembros del área de tecnología con el fin de conocer el estado actual de los equipos soportados y administrados en la infraestructura tecnológica.

Etapa 2: Realizar un análisis de riesgos basado en amenazas y vulnerabilidades que permita determinar el estado actual de la seguridad informática en la

organización.

Actividades:

- Valoración de los activos bajo las dimensiones de disponibilidad, integridad de los datos, confidencialidad de la información, autenticidad y trazabilidad.
- Determinar bajo que amenazas y vulnerabilidades están expuestas estos activos.
- Estimar el impacto y riesgo del activo bajo la materialización de una amenaza.

Etapa 3: Verificar la existencia de controles para evaluar el nivel de mitigación ante amenazas, vulnerabilidades y riesgos.

Actividades:

- Revisión del sistema de gestión de calidad en donde se encuentran caracterizados los diferentes procedimientos correspondientes al área de tecnología.
- Inspección y auditoria a la infraestructura tecnológica de la empresa.
- Entrevistas con el personal del área de tecnología que permita establecer controles que no estén documentados.

Etapa 4: Diseñar el SGSI de la empresa Belisario Ltda garantizando la continuidad y disponibilidad del negocio acorde a su objeto social.
Actividades:

- Definir el objetivo del SGSI.
- Definir el alcance del SGSI.
- Definir las políticas, procedimientos y controles.

Conclusiones

La metodología de análisis y gestión de riesgos MAGERIT, permite identificar los activos a proteger y que hacen parte fundamental en la ejecución de los diferentes procesos organizacionales, además permite determinar el impacto y riesgo derivado de la posible materialización de amenazas, obteniendo como resultado la declaración de aplicabilidad, que expone una relación de mecanismos y controles aplicables a la organización.

La declaración de aplicabilidad es un instrumento adaptable a los cambios y necesidades que surjan dentro de la compañía, sin ser este un elemento restrictivo para la inclusión de mecanismos y controles que no estén contemplados dentro de su estructura.

La compañía ha dispuesto salvaguardas como resultado a sucesos que han generado indisponibilidad en su plataforma tecnológica y afectado su operación, dichos eventos no cuentan con un análisis de causas, lo que conlleva a establecer medidas correctivas y no acciones preventivas.

Recomendaciones

Ampliar el alcance del Sistema de Gestión de Seguridad de la Información con el fin de contemplar las diferentes áreas o procesos que componen la organización.

Establecer un plan estratégico de inversión que contemple la adquisición y mantenimiento de los diferentes mecanismos y controles dispuestos para la protección de la seguridad de la información.

La empresa debe iniciar un proceso de capacitación al personal de la organización en aspectos relevantes de la seguridad de la información.

Es importante que la organización inicie un proceso de formación en la gestión y operación del Sistema de Gestión de Seguridad de la Información aplicable al área de gestión tecnológica.

Se sugiere que la organización realice auditorias de seguimiento al Sistema de Gestión de Seguridad de la Información, como minino una vez al año.

ANEXO F MATRIZ DE TRATAMIENTO DE RIESGOS

TIPO DE ACTIVO	IDENTIFICACIÓN	RIESGO	PROBABILIDAD			IMPACTO			TRATAMIENTO	OBSERVACIÓN	CONTROL
			A	M	B	L	M	C			
DATOS E INFORMACIÓN	1	El personal divulga información confidencial de la organización esperando beneficiarse de dicha situación ante la competencia		SI			SI		Establecer un control	La organización se ve en situación de desventaja ante la competencia por fugas de información confidencial que afectan el core del negocio	Establecer acuerdos de confidencial entre empleado y empleador donde se especifique las consecuencias legales ante un posible acto de divulgación
SERVICIOS	2	Los usuarios modifican información contenida en el servidor de archivos de manera involuntaria			SI		SI		Establecer un control	Información sensible de las diferentes áreas se puede ver comprometida por errores de los usuarios en su manipulación	Establecer un plan de backup y limitar el acceso a información sensible de la organización a personal de las diferentes áreas
SOFTWARE	3	El sistema ERP de la organización es susceptible a los cambios realizados por los usuarios y administradores de la plataforma		SI			SI		Establecer un control	El ERP sustenta los diferentes procesos de la organización y ante una posible falla se ve afectado el flujo normal sus operaciones	Definición y revisión de los diferentes perfiles de usuarios. Generar planes de contingencia y recuperación
	4	Las diferentes herramientas se encuentras expuestas a vulnerabilidades y errores de actualización			SI		SI		Establecer un control	La existencia de vulnerabilidades dentro de un activo permiten la materialización de amenazas	Actualización periódica para las diferentes aplicaciones y generar un entorno de prueba para gestionar las posibles consecuencias de los cambios realizados
HARDWARE	5	Los funcionarios de la organización usan los equipos de computo para actividades que no han sido dispuestas por la compañía	SI				SI		Establecer un control	El uso indebido de los equipos afecta gradualmente la productividad de los funcionarios y en consecuencia, los servicios que presta la organización	Definir políticas sobre el uso de los dispositivos y monitorear de forma periódica el uso de los recursos
	6	Una incorrecta configuración del firewall acarrea indisponibilidad para los diferentes servicios que soporta la infraestructura tecnológica de la organización		SI			SI		Establecer un control	Un error en la configuración repercute en la indisponibilidad de servicios y posibles ataques sobre la infraestructura	Documentar los cambios realizados sobre el dispositivo y generar un backup periódico sobre dicha configuración
EQUIPAMIENTO AUXILIAR	7	El sistema de alimentacón ininterrumpida presenta fallas en la prestación del servicio			SI			SI	Establecer un control	Ante un corte en el fluido eléctrico, permite generar una disponibilidad cercana a los 15 minutos donde se apagan los equipos de una manera segura	Establecer un contrato de mantenimiento con un proveedor de servicio especializado en el tratamiento de dicho dispositivo
REDES DE COMUNICACIONES	8	Interrupción en el servicio de internet y telefonía		SI			SI		Aceptación	Son servicios de apoyo para las diferentes áreas de la organización, pero no afectan directamente el core del negocio	No aplica
PERSONAL	9	La indisponibilidad del personal genera traumatismos en los diferentes procesos de la organización ante incidencias o novedades		SI			SI		Establecer un control	La respuesta ante cualquier incidencia debe ser gestionada de manera oportuna sin importar la disponibilidad del personal a cargo de la infraestructura tecnológica	Documentar los diferentes procesos de administración de la plataforma tecnológica