ANÁLISIS DE ACTIVOS DE LA INFORMACIÓN DEL APLICATIVO MISIONAL DE LA EMPRESA CASO DE ESTUDIO

BERCY YAQUELIN AVILA GUERRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2018

ANÁLISIS DE ACTIVOS DE LA INFORMACIÓN DEL APLICATIVO MISIONAL DE LA EMPRESA CASO DE ESTUDIO

BERCY YAQUELIN AVILA GUERRA

Monografía de Grado para optar el título de Especialista en Seguridad Informática

Ing. Esp. Freddy Enrique Acosta
Director del Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2018

Nota de Aceptación

_____
_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

Bogotá D.C., octubre 03 de 2018

AGRADECIMIENTO

Bercy Yaquelin expresa sus agradecimientos a:

Ing.Esp. Freddy Enrique Acosta, por su excelente asesoría y transferencia de conocimiento durante el desarrollo del proyecto.

Esp. Ing. Bercy Yaquelin por su interés en el desarrollo de este proyecto. Dedicado a Dios por darme la capacidad, sabiduría para poder desarrollar este proyecto, a mi familia por el apoyo que me brindaron y a la Universidad Nacional Abierta y a Distancia.

CONTENIDO

LISTA DE TABLAS

LISTA DE IMÁGENES

GLOSARIO

AUTENTICACIÓN: es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.[1]

ACTIVO: Se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización[2]

AMENAZA: Hecho que puede producir un daño provocado por un evento natural.[3]

ANÁLISIS DE RIESGOS: Proceso para comprender la naturaleza del riesgo y determinar el nivel del riesgo.[4]

DESASTRE: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.[5]

DISPONIBILIDAD: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada[6]

INTEGRIDAD: es la protección de la exactitud y estado completo de los activos.[7]

SOFTWARE: es todo programa o aplicación programada para realizar tareas específicas.[8]

VULNERABILIDADES: son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la entidad (amenazas), las cuales se constituyen en fuentes de riesgo[9]

---

[1] 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
[2] SO 27000.ES. Glosario [en línea]. Madrid: El autor, s.f. [citado el 22-04-16]. Disponible en: http://www.iso27000.es/glosario.html
[3] Ibid., p. 27.
[4] Ibid. Disponible en: http://www.iso27000.es/glosario.html
[5] Ibid. Disponible en: http://www.iso27000.es/glosario.html
[6] Ibid. Disponible en: http://www.iso27000.es/glosario.html
[7] ISO 27000.ES, Glosario, Op. Cit. Disponible en: http://www.iso27000.es/glosario.html
[8] MIERES, Jorge. Fundamentos sobre Seguridad de la Información. Disponible en internet:< http://www.segu-info.com.ar/terceros/>. p. 5.
[9] MIERES. Op. cit., p. 5.

MAGERIT: Metodología de análisis y de Gestión de Riesgos de sistemas de información[10]

ISO/IEC 27001: Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial[11]

ISO: Organización Internacional de Normalización. Es una agrupación de entidades nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares, (normas)

TRAZABILIDAD: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad[13]

SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, integridad y disponibilidad de la información[12]

RIESGO: (Inglés: Risk). Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias[13]

[10] WIKIPEDIA La enciclopedia libre. [En línea]. Actualizada el 26 marzo 2014 a las 15:58. Disponible en Internet https://es.wikipedia.org/wiki/Magerit_(metodolog%C3%ADa).
[11] Ibid. Disponible en: http://www.iso27000.es/glosario.html
[12] Ibid. Disponible en: http://www.iso27000.es/glosario.html
[13] Ibid. Disponible en: http://www.iso27000.es/glosario.html

RESUMEN

Este trabajo tiene como propósito identificar el escenario actual de la entidad, donde se evidencie los activos de la información mediante la metodología MAGERIT, identificando las amenazas y vulnerabilidades a los activos

En la monografía, se tomó como base el estado actual de lo ya dispuesto en la empresa caso de estudio bajo la norma ISO 27001:2005, lo que nos permitió determinar las fortalezas y debilidades que se tienen frente a los activos de información.

Esta información nos ayuda a generar estrategias y planes que minimizan las amenazas que puedan impactar las vulnerabilidades de la organización, dando a conocer los controles y políticas que deben ser implementadas, las cuales son producto del análisis de lo que posee implementado la empresa en mención, lo que aportara al fortalecimiento del sistema de seguridad de la información de la organización, como un proceso de mejora continua que requiere la actualización permanente.

En la primera etapa se realiza un análisis en la entidad caso de estudio con el objeto de identificar los tipos de activos más relevantes, según metodología Magerit y de acuerdo a ello se clasifico según su tipo de Información: publica, reservada, clasificada y confidencial; con el fin de valorar las dimensiones de seguridad informática en estos activos.

En la segunda etapa se identifica las amenazas de los activos de la de la entidad caso de estudio y el riesgo que pueden sufrir si se materializa unas amenazas.

En la tercera etapa se determinan los controles para cada uno de los activos previamente identificados y clasificados.

En la cuarta etapa se plantea de manera general unas políticas de seguridad informática basadas en la Norma ISO 27001:2013; con la finalidad de proteger los activos de la entidad caso de estudio para evitar su perdida, modificación, o el uso inadecuado de su contenido.

ABSTRACT

The purpose of this work is to identify the current scenario of the entity, where information assets are evidenced through the MAGERIT methodology, identifying threats and vulnerabilities to the assets

In the monograph, the current status of what was already in the company case study under ISO 27001: 2005 was taken as a basis, which allowed us to determine the strengths and weaknesses that are faced with information assets.

This information helps us to generate strategies and plans that minimize threats that may impact the vulnerabilities of the organization, making known the controls and policies that must be implemented, which are the product of the analysis of what the company in question has implemented. what will contribute to the strengthening of the information security system of the organization, as a continuous improvement process that requires permanent updating.

In the first stage, an analysis is carried out in the case study entity in order to identify the most relevant types of assets, according to the Magerit methodology and according to this, it is classified according to its type of information: public, reserved, classified and confidential; in order to assess the dimensions of computer security in these assets.

In the second stage, the threats of the assets of the case study entity are identified and the risk they may suffer if threats are materialized.

In the third stage, the controls for each of the previously identified and classified assets are determined.

In the fourth stage, computer security policies based on the ISO 27001: 2013 standard are generally considered; with the purpose of protecting the assets of the case study entity to avoid its loss, modification, or inappropriate use of its content.

INTRODUCCIÓN

Las organizaciones empresariales soportan su actividad de negocio en tecnologías de la información y de la comunicación por lo que necesitan dotar a sus sistemas e infraestructuras informáticas en red de las políticas y medidas de protección que garanticen el desarrollo y sostenibilidad de su actividad de negocio. Mantener la confidencialidad la integridad, la disponibilidad y la usabilidad autorizada de la información cobra especial importancia y plantea la necesidad de disponer de profesionales capaces de asegurar, gestionar y mantener la seguridad de las informaciones en sus sistemas presentes y futuras[14].

Debido al avance de la tecnología informática y su influencia en diversas áreas de la vida cotidiana, emergen comportamientos ilícitos. Es por ello que Royer J. (2008) afirma: “La Seguridad de la información es un proceso en el que se da cabida a un creciente número de elementos: aspectos tecnológicos, de gestión organizacionales, de recursos humanos, de índole económica de negocios, de tipo legal, de cumplimiento, etc.; abarcando no solo aspectos informáticos y de telecomunicaciones sino también aspectos físicos, medio ambientales y humanos”[15].

Garantizar que los recursos informáticos de una compañía estén disponibles para cumplir sus propósitos, es decir, que no estén dañados o alterados por circunstancias o factores externos, es una definición útil para conocer lo que implica el concepto de seguridad informática. En términos generales, la seguridad puede entenderse como aquellas reglas técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial. En este sentido, es la información el elemento principal a proteger, resguardar y recuperar dentro de las redes empresariales[16]

Actualmente no es un secreto que las tecnologías de la información están en todos los procesos que desarrollamos a diario, Al utilizar la metodología que incluye el análisis de riesgos y vulnerabilidades del manejo de la información, se pueden establecer controles y políticas para mejorar el nivel de seguridad de la información manejada por la entidad, un conjunto de reglas bien definidas, para denegar el acceso a los datos de los usuarios a personas mal intencionadas que puedan buscar hacer mal uso de esa misma información.

---

[14] AREITIO BERTOLÍN, Javier. Seguridad de la información. Redes, informática y sistemas de información. Madrid: Cengage Learning Paraninfo, 2008. Prólogo.

[15] Ibid, Prólogo.

[16] WHITTEN, Jeffrey. Seguridad Informática. [online]. 1994. [citado el citado 01-06-2017]. Disponible: http://problema.blogcindario.com/2008/10/00014-marco-teorico.html

La entidad caso de estudio permite consolidar la información financiera de las entidades que conforman el presupuesto general de la organización y ejercer el control de la ejecución presupuestal y financiera de las entidades pertenecientes a la Administración Central y Descentralizada, con el fin de propiciar una mayor eficiencia en el uso de los recursos y de brindar información oportuna y confiable.

El sistema permite la creación de una infraestructura de información para las decisiones del manejo de los recursos, mejorar el funcionamiento de los subsistemas estratégicos del ciclo financiero y apoyar a las entidades para que cumplan sus responsabilidades constitucionales.

1. DEFINICION DEL PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

Es importante tener una política de seguridad de red bien concebida y efectiva que pueda proteger la inversión y los recursos de información de la compañía. Vale la pena implementar una política de seguridad si los recursos y la información que la organización tiene en sus redes merecen protegerse. La mayoría de las organizaciones tienen en sus redes información delicada y secretos importantes; esto debe protegerse del acceso indebido del modo que los bienes valiosos como la propiedad corporativa y los edificios de oficinas.[17]

Con la norma ISO 27001:2013, se puede demostrar a clientes existentes y potenciales, proveedores y accionistas la integridad de sus datos y sistemas, así como su compromiso con la seguridad de la información. También puede dar lugar a nuevas oportunidades de negocio con clientes preocupados por la seguridad; puede mejorar la ética de los empleados y fortalecer la noción de confidencialidad en todo el lugar de trabajo. Además, le permite reforzar la seguridad de la información y reducir el posible riesgo de fraude, pérdida de información y divulgación[18].

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 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 o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos[19].

La entidad caso de estudio, es una herramienta modular automatizada que integra y estandariza el registro de la gestión financiera con el fin de propiciar una mayor eficiencia en el uso de los recursos y así poder brindar información oportuna y confiable, es por esto que se debe crear y establecer políticas de seguridad que permitan mitigar el riesgo de vulnerabilidades y amenazas a las que normalmente

[17] ALVAREZ, Daniel. Seguridad en Informática. [en línea]. En: Maestro en Ingeniería de sistemas empresariales. p.7. [citado el 24-05-17].Disponible en http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf

[18] ISO 27001. Sistema de gestión de la seguridad de la información [en línea]. Colombia 1995. [citado el 24-05-17]. Disponible en: http://www.sgs.co/es-ES/Health-Safety/Quality-Health-Safety-and-Environment/Risk-Assessment-and-Management/Security-Management/ISO-27001-2013-Information-Security-Management-Systems.aspx

[19] ISO 27000.ES. Sistema de gestión de la seguridad de la información [en línea]. Madrid: El autor, s.f. [citado el 16-04-16]. Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

se ve expuesta la información presente en cada uno de los procesos existentes dentro del aplicativo.

Las amenazas de seguridad de la información son globales, afectan tanto a individuos como organizaciones y los datos están expuestos a un sinnúmero de riesgos que pueden existir, estos pueden ser derivados de factores internos y externos.

1.2. FORMULACIÓN DEL PROBLEMA

¿De qué manera se pueden identificar y analizar los riesgos que pueden afectar la seguridad de la información a los que está expuesto el sistema de información de la empresa caso de estudio?

1.3. OBJETIVOS

1.3.1. Objetivo General

Realizar el análisis a los activos de la información para determinar los posibles riesgos que se presentan en el aplicativo misional y poder generar controles basados en la norma ISO 27001:2013.

1.3.2. Objetivos Específicos

- Clasificar los activos de información de la infraestructura tecnológica donde se encuentra en funcionamiento el aplicativo misional de la empresa caso de estudio mediante la metodología MAGERIT V3

- Identificar las amenazas de los activos de información de la infraestructura tecnológica donde se encuentra en funcionamiento el aplicativo misional de la empresa caso de estudio mediante la metodología MAGERIT V3

- Elaborar la Declaración de aplicabilidad de los controles del anexo A de la ISO 27001:2013

- Proponer políticas de seguridad de la información para el aplicativo misional de la empresa caso de estudio

1.4. JUSTIFICACION

La información es el activo más importante en toda organización, y en este mundo digital en el que vivimos y en especial en el ámbito empresarial, esta debe ser

protegida ante las crecientes y constantes amenazas a las que está expuesta por parte de delincuentes informáticos, los cuales tratan de apoderarse de esta ya sea para sacar beneficio económico al venderla o al apoderarse de números de cuentas y claves de usuarios bancarios, sacar provecho de esta información para apropiarse del dinero de los clientes[20].

Pero no solo se debe proteger la información del ataque de delincuentes externos a las organizaciones, también lo directivos de esta entidad deben mirar hacia el interior, en especial hacia sus empleados ya sea que estos manipulen o no información confidencial pues estos son los que tienen disponibles de primera mano este activo tan fundamental denominado información[21].

El control interno informático siendo un conjunto de principios, procesos, procedimientos, políticas, basándose en las políticas preestablecidas, garantiza que se minimice la ocurrencia de riesgos y sus posibles consecuencias, lo que conlleva mediante la presentación de informes que presenten oportunidades de mejora, mejorar la eficiencia y eficacia de los procesos para prevenir la ocurrencia de riesgos, fortaleciendo los procesos al realizar la gestión adecuada de los riesgos identificados[22].

Por lo tanto, por ser un sistema muy importante representa un cambio significativo en las entidades que han contribuido a la obtención de metas y objetivos planteados, es por esto que en el trascurso de los años se ha logrado el fortalecimiento con todos los macroprocesos que tienen el aplicativo, los cuales que funcionan de manera integral, lo que ha permitido la disminución de los tiempos de procesamiento, mejorar el control y flujo de la información y por consiguiente aumentar el porcentaje de satisfacción y lo más importante la seguridad de la información que se le brinde a los usuarios internos y externos.

Para lo cual es necesario identificar las amenazas y vulnerabilidades a las que puede estar expuesta la organización, para esto es preciso identificar los riesgos que pueden existir para el empresa caso de estudio, con la finalidad de garantizar mayor efectividad y eficiencia dentro de cada uno de los procesos, teniendo en cuenta que al conocer las fortalezas y debilidades se mejora el control y administración de la herramienta, lo que permitirá adoptar buenas prácticas de seguridad y de esta forma se logran los objetivos institucionales.

---

[20] AUDISIS. Sistema de gestión de seguridad de la información - SCSI ISO 27001:2013 - Implantación y auditoría. [en línea]. Bogotá. Disponible en: http://www.audisis.com/BROCHURE_Sem_Implementaci%C3%B3n_SGSI.pdf

[21] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Fortalecimiento de la gestión TI en el estado [en línea]. Bogotá. http://colnodo.apc.org/apropiacionTecnologias.shtml

[22] ISO 27000.ES. Sistema de gestión de la seguridad de la información [en línea]. Madrid. Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

1.5. ALCANCES Y LIMITACIONES

1.5.1. Alcance

La presente monografía se encuentra entre los proyectos de gestión de seguridad y lo que pretende es realizar el análisis de riesgos relacionados con la empresa caso de estudio y recomendaciones en los niveles de seguridad, que permita generar controles para minimizar la probabilidad de riesgos asociados con las vulnerabilidades.

1.5.2. Limitaciones

Es conveniente resaltar que el desarrollo de la presente monografía no abarcara temas como los que se definen a continuación:

- No se realiza la implementación y proceso de gestión de riesgos en la entidad.
- Que la entidad impida la publicación de los resultados en un repositorio.
- El área de tecnología de la información de la organización impida el acceso a la información y la instalación de software de escaneo.

1.6. DISEÑO METODOLOGICO

El mecanismo de análisis de esta monografía corresponde a los posibles riesgos y vulnerabilidades a los cuales pueden estar sometidos los activos de la entidad.

Utiliza variedad de instrumentos para recoger información, en los que se describen las rutinas y las situaciones problemáticas.

Se toma este rumbo, porque se estudia un sistema funcional, se pretende dar una respuesta a una situación problema que tiene en su ejecución.

1.6.1. Estudio metodológico

Esta monografía consiste en la elaboración de una propuesta o de un modelo, para solucionar problemas o necesidades de tipo práctico, partiendo de un diagnóstico preciso de las necesidades del momento, los procesos explicativos o generadores involucrados y las tendencias futuras

En el desarrollo del proyecto se usarán diferentes técnicas para recolección de información:

- Investigación en fuentes bibliográficas, textos y manuales impresos y recopilados de Internet referentes al tema de seguridad informática y de la información, norma ISO 27001 y SGSI.

- Se revisaron las instalaciones de la entidad para conocer de primera mano el estado de sus oficinas, equipos, documentación y controles de seguridad.

- identificación y análisis de amenazas y vulnerabilidades que impactan a los activos de la entidad.

- Evaluación de los controles y/o herramientas actuales utilizadas por la entidad para garantizar la seguridad de los sistemas informáticos y de la información.

- Uso de una metodología para el análisis y gestión de riesgos.

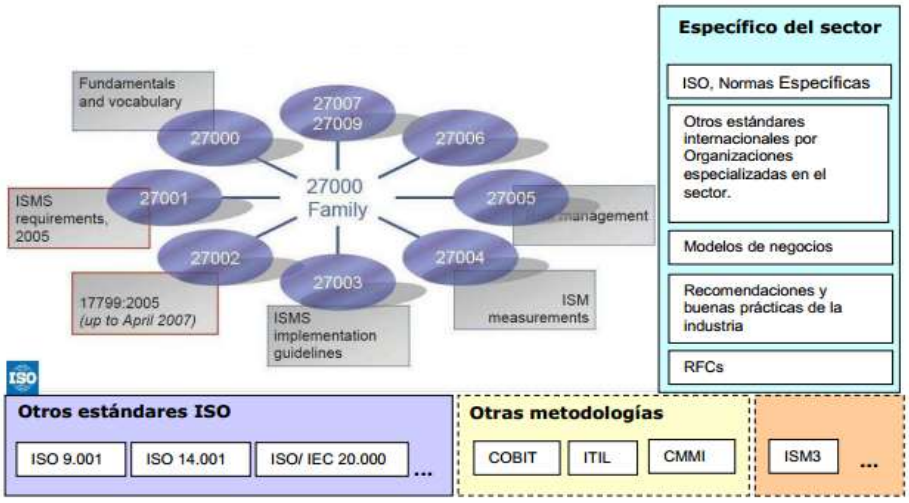
2. MARCO DE REFERENCIA

2.1. MARCO TEÓRICO

En la Figura 1 se ilustra el marco normativo de los diferentes estándares que, de una u otra manera, están vinculados a un Sistema de Gestión de la Seguridad de la Información, en este se ven representados estándares internacionales de diferente naturaleza y con diferente alcance. Algunos de ellos, como por ejemplo la serie ISO/IEC 27000 e ISM3, son específicos de la gestión de seguridad de la información, generales y aplicables a cualquier sector de actividad. Pero también deben tenerse en cuenta otros estándares y recomendaciones que son específicas del sector[23].

Figura 1 Contexto Normativo de un SGSI

[23] PALLAS, Gustavo M. Metodología de Implantación de un SGSI en un grupo empresarial jerárquico. [online][citado en marzo de 2016]. Disponible en internet: <https://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf> Pág 6.



Fuente: Alan Bryden, COPANT Seminar on Security Standards, La Paz, 25 de abril de 2006. Pág. 33. Disponible en internet <http://www.iso.org/iso/livelinkgetfile?llNodeId=21657&llVolId=-2000> (marzo de 2016).

Un SGSI, como sistema de gestión que es, de una disciplina específica como lo es la seguridad de la información, debe relacionarse con otros sistemas de gestión, por ejemplo, de Gestión de Calidad entre otros. Es así que también deben considerarse en el contexto, estos otros sistemas y los respectivos estándares metodológicos en los que se apoyan[24].

2.1.1 Activos de Información

Los activos de información son ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, material de formación, aplicaciones, software del sistema, equipos informáticos, equipo de comunicaciones, servicios informáticos y de comunicaciones, utilidades generales como por ejemplo calefacción, iluminación, energía y aire acondicionado y las personas, que son al fin y al cabo las que en última instancia generan, transmiten y destruyen información, es decir dentro de un organización se han de considerar todos los tipos de activos de información[25]

2.1.2 Activos de Información

Una amenaza se representa a través de una persona, una circunstancia o evento, un fenómeno o una idea maliciosa, las cuales pueden provocar daño en los sistemas de información, produciendo pérdidas materiales, financieras o de otro tipo. Las

[24] Ibíd,. Pág. 7.
[25] POVEDA, José Manuel. Los activos de seguridad de la información [en línea]. Chile: World Visión, s.f. [citado el 28-04-16]. Disponible en: http://www.worldvisioncapacitacion.cl/wp-content/uploads/cursos_adjuntos/f52e0bd4c6c2c203413952826f916237.pdf

amenazas son múltiples desde una inundación, un fallo eléctrico o una organización criminal o terrorista. Así, una amenaza es todo aquello que intenta o pretende destruir[26]

Se considera una amenaza, a cualquier situación que pueda dañar o deteriorar un activo, impactando directamente cualquiera de las cuatro dimensiones de seguridad. La ISO/IEC 13335-1:2004 define que una "amenaza es la causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización

2.1.3 Activos de Información

Es la protección de la información que hay en una entidad o que un individuo maneja. Esta información representa un activo valioso para la organización.

La información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades (véase también OECD Guía para la seguridad redes sistemas de información). La información puede existir en muchas formas. Puede estar impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en películas o hablada en una conversación. Cualquiera que sea la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre debiera estar apropiadamente protegida[27]

2.1.4 Serie ISO/IEC 27.000[28]

Las normas de la familia ISO 27.000, destacando fundamentalmente la ISO/IEC 27.001 e ISO/IEC 27.002, tienen como principales objetivos:

a. Establecer un marco metodológico para un SGSI.
b. La adopción de controles proporcionales a los riesgos percibidos.
c. La documentación de políticas, procedimientos, controles y tratamiento de riegos.
d. Identificación y asignación de responsabilidades al nivel adecuado.

---

[26] UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO. Fundamentos de seguridad informática: amenazas [en línea]. México: UNAM, s.f. [citado el 30-04-16]. Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/Amenazas.php

[27] ESTÁNDAR INTERNACIONAL ISO/IEC 17779. Tecnología de la información - Técnicas de seguridad - Código para la práctica de la gestión de la seguridad de la información [en línea]. s.l.: s.n., 2005. [citado el 19-04-16]. Disponible en: https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

[28] NEIRA, Agustín y SPOHR, Javier. ISO27000.es. "Sistema de Gestión de la Seguridad de la Información". [online] [citado febrero 2016].Disponible en internet: http://www.iso27000.es/doc_sgsi_all.htm

e. Formalización, seguimiento y revisión de los controles y riesgos, de forma sistemática (periódica) y metodológica.
f. Generación y preservación de evidencias.
g. Tratamiento de los incidentes de seguridad.
h. Revisión y mejora continua del SGSI.
i. Gestión de Riesgos
j. Uso de métricas para evaluar efectividad y eficiencia de los controles y del propio SGSI.

Los lineamientos metodológicos y los requerimientos de la norma ISO/IEC 27.001 son propuestos bajo el enfoque metodológico del Ciclo de Deming: Planificar – Hacer – Verificar – Actuar (PHVA)[29].

Entre ellas existen normas que son básicamente una especificación de Requerimientos como la ISO/IEC 27.001 e ISO/IEC 27006. Otras son guías de implementación o lineamientos guía que son soporte del ciclo PHVA para los sistemas de gestión de la seguridad de la información, como la ISO/IEC 27003 o ISO/IEC 27.005.

A continuación, se describen brevemente los más relevantes para este trabajo[30]:

a. "*ISO/IEC 27000 - Information technology - Security techniques - Information security management systems - Overview and vocabulary"*, provee información introductoria a seguridad de la información y a la gestión de la seguridad de la información, el estado y la relación de las normas de la familia de estándares para un SGSI.

b. *"ISO/IEC 27001:2005 - Information technology - Security techniques - Information Security Management Systems - Requirements*", es una norma que admite certificación y especifica los requerimientos para la definición, implementación, implantación, mantenimiento y mejora de un SGSI.

c. *"ISO/IEC 27002:2005 - Information technology - Security techniques - Code of practice for information security management"* - provee una guía de implementación de los controles aplicables a la seguridad de la información. Presenta once (11) cláusulas de control de la seguridad que contienen un total de treinta y nueve (39) categorías de seguridad y por lo tanto igual número de indicaciones de Objetivos de Control, con varios Controles por cada uno de ellos. Estas cláusulas, objetivos de control y controles, son incorporados en el Anexo A de la norma ISO/IEC 27.001.

[29] O la correspondiente sigla en inglés PDCA (Plan, Do, Check, Act)
[30] ISO/IEC 27000, «Information technology -Security techniques -Information security management systems - Overview and vocabulary" International Organization for Standarization (ISO),» de Information security management systems, p. [online], Disponible en internet <http://www.iso.org>.

d. *“ISO/IEC 27003 - Information technology - Security techniques - Information security management system implementation guidance”* - provee información práctica y una guía de implementación de la norma ISO/IEC 27001.

e. *“ISO/IEC 27004 - Information technology - Security techniques - Information security management measurements”* provee una guía y consejos para el desarrollo y uso de métricas para evaluar la efectividad de un SGSI, los objetivos de control y controles utilizados para implementar y gestionar la Seguridad de la Información, de acuerdo con la norma ISO/IEC 27001.

f. *“ISO/IEC 27005:2008 - Information technology - Security techniques - Information security risk management”* – provee una guía metodológica para la Gestión de Riesgos de una Organización, alineada con los requerimientos de la norma ISO/IEC 27001.

g. *“ISO/IEC 27006:2007 - Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems”* – establece los requerimientos para Organismos que prestan servicios de auditoría y certificación.

h. *“ISO/IEC 27007 Information technology - Security techniques - Information security management systems - Auditor guidelines”* - provee una guía para la realización de las auditorías de un SGSI y la competencia de los auditores, de acuerdo a la norma ISO/IEC 27001.

2.1.5 Norma ISO/IEC 27.001 y el ciclo de Deming.

La norma ISO/IEC 27.001 es un estándar que especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Especifica además los requerimientos para la implementación de controles de seguridad para las necesidades de una organización, un sector de la misma, o un proceso, según el alcance del SGSI. Establece entre otras cosas, la documentación exigida para su certificación en el caso del cumplimiento de todos los requisitos.

Sin embargo, si bien sugiere un enfoque para su cumplimiento, no establece una metodología concreta para lograr los productos y esa documentación requerida, ni especifica un flujo de trabajo (workflow) con procesos bien definidos.

Se establece un mapeo de las etapas del ciclo de Deming y los productos o entregables exigidos por la norma.

En la tabla 1, se especifican los principales procesos que indica la referida norma, mapeados con las etapas del ciclo PHVA[31].

Tabla 1 Ciclo de Deming (PHVA) aplicado a la norma ISO/IEC 2700

Ciclo PHVA	Procesos
Planificar (*Plan*)	• Establecer el contexto. • Alcance y Limites. • Definir Política del SGSI. • Definir Enfoque de Evaluación de Riesgos. • Identificación de riesgos. • Análisis y Evaluación de riesgos. • Evaluar alternativas para el Plan de tratamiento de riesgos. • Aceptación de riesgos. • Declaración de Aplicabilidad.
Hacer (*Do*)	• Implementar plan de tratamiento de riesgos. • Implementar los controles seleccionados. • Definir las métricas. • Implementar programas de formación y sensibilización. • Gestionar la operación del SGSI. • Gestionar recursos. • Implementar procedimientos y controles para la gestión de incidentes de seguridad.
Verificar (*Check*)	• Ejecutar procedimientos de seguimiento y revisión de controles. • Realizar revisiones regulares de cumplimiento y eficacia de los controles y del SGSI. • Medir la eficacia de los controles y verificación de satisfacción de los requerimientos de seguridad. • Revisión de la evaluación de riesgos periódicamente. Realizar auditorías internas. • Revisión de alcance y líneas de mejoras del SGSI por la Dirección. Actualizar los planes de seguridad. • Registrar acciones que podrían impactar la eficacia y/o eficiencia del SGSI del SGSI. • Medir la eficacia de los controles y verificación de satisfacción de los requerimientos de seguridad. • Revisión de la evaluación de riesgos periódicamente. • Realizar auditorías internas. • Revisión de alcance y líneas de mejoras del SGSI por la Dirección. Actualizar los planes de

[31] PALLAS, Gustavo M. Op. Cit., Pág. 19

Ciclo PHVA	Procesos
	seguridad. • Registrar acciones que podrían impactar la eficacia y/o eficiencia del SGSI.
Actuar ***(Act)***	• Implementar las mejoras identificadas para el SGSI. • Implementar las acciones correctivas y preventivas pertinentes. • Comunicar acciones y mejoras a todas las partes involucradas. • Asegurarse que las mejoras logren los objetivos previstos.

Fuente: PALLAS, Gustavo M. Tesis de Maestría "Metodología de Implantación de un SGSI en un grupo empresarial jerárquico". Pág. 19, [online] [citado febrero 2016].Disponible en internet: http://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf

Para el caso de la implantación de Sistemas de Gestión de la Seguridad informática, el ciclo PDCA es una estrategia efectiva para la organización y documentación que se requiere en este proceso. La figura 2 enseña el modelo basado en los procedimientos esenciales para un SGSI[32] (Ver figura 2).

Figura 2 Ciclo PDCA (PHVA) para la implantación de SGSI

[32] Universidad Nacional Abierta y A Distancia. Sistema de Gestión de la Seguridad de la Información SGSI. Unidad I. Capítulo 1 Seguridad Informática. Lección 1.5.1 Ciclo PDCA (Edward Deming). [Online] [Citado en abril 2016]. Disponible en Internet en < http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/151_ciclo_pdca__edward_deming.html

Fuente: Universidad Nacional Abierta y A Distancia. Sistema de Gestión de la Seguridad de la Información SGSI. Unidad I. Capítulo 1 Seguridad Informática. Lección 1.5.1 Ciclo PDCA (Edward Deming). [Online] [Citado en abril 2016]. Disponible en Internet en: < http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/151_ciclo_pdca__edward_deming.html

2.1.5.1 Planear

En esta etapa se enmarca todo el proceso de análisis de la situación en que actualmente se encuentra la entidad respecto a los mecanismos de seguridad implementados y la normativa ISO/IEC 17799:2005, la cual se pretende implantar para evaluación y certificación. Así mismo en la etapa de planeación se organizan fases relevantes como son:

- Establecer el compromiso con los directivos de la entidad para el inicio, proceso y ejecución
- Fase de análisis de información de la organización, En esta fase se comprueba cuáles son los sistemas informáticos de hardware y los sistemas de información que actualmente utiliza la entidad para el cumplimiento de su misión u objeto social.
- Fase de evaluación del riesgo; En esta fase se evalúa los riesgos, se tratan y se seleccionan los controles a implementar[33].

2.1.5.2 Hacer

En esta etapa se implementan todos los controles necesarios de acuerdo a una previa selección en la etapa de planeación, teniendo en cuenta el tipo de empresa. También se formula y se implementa un plan de riesgo[34].

2.1.5.3 Verificar

Consiste en efectuar el control de todos los procedimientos implementados en el SGSI. En este sentido, se realizan exámenes periódicos para asegurar la eficacia del SGSI implementado, se revisan los niveles de riesgos aceptables y residuales y se realicen periódicamente auditorías internas para el SGSI[35].

2.1.5.4 Actuar

[33] Universidad Nacional Abierta y A Distancia. Sistema de Gestión de la Seguridad de la Información SGSI. Unidad I. Capítulo 1 Seguridad Informática. Lección 1.5.1 Ciclo PDCA (Edward Deming). [Online] [Citado abril 2016]. Disponible en Internet en < http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/151_ciclo_pdca__edward_deming.html

[34] Universidad Nacional Abierta y A Distancia. Sistema de Gestión de la Seguridad de la Información SGSI. Unidad I Ibíd.

[35] Universidad Nacional Abierta y A Distancia. Sistema de Gestión de la Seguridad de la Información SGSI. Unidad I Ibíd.

Desarrollar mejoras a los hallazgos identificadas al SGSI y validarlas, realizar las acciones correctivas y preventivas, mantener comunicación con el personal de la organización relevante[36].

El estándar ISO/IEC 27001:2013 especifica los requisitos para la creación, implementación, funcionamiento, supervisión, revisión, mantenimiento y mejora de un SGSI documentado, teniendo en cuenta los riesgos empresariales generales de la organización. Es decir, explica cómo diseñar un SGSI y establecer los controles de seguridad, de acuerdo con las necesidades de una organización o de partes de la misma, pero no aclara mediante qué procedimientos se ponen en práctica. Como todo sistema de gestión, el estándar ISO/IEC 27001:2013 emplea el ciclo PDCA para el mejoramiento continuo[37].

2.2. MARCO CONCEPTUAL

2.2.1 Política de seguridad

Se pueden considerar como un conjunto de normas obligatorias propias de una organización, que regulan la manera de dirigir, proteger y distribuir los activos en una organización para llevar a cabo los objetivos de seguridad informática dentro de la misma.

Las políticas de seguridad definen lo que está permitido y lo que está prohibido, permiten definir los procedimientos y herramientas necesarias, expresan el consenso de los “dueños” y permiten adoptar una buena actitud dentro de la organización.

Las políticas son una serie de instrucciones documentadas que indican la forma en que se llevan a cabo determinados procesos dentro de una organización, también describen cómo se debe tratar un determinado problema o situación.

El documento de políticas de seguridad está dirigido principalmente al personal interno de la organización, aunque hay casos en que también personas externas quedan sujetas al alcance de las políticas[38].

Las políticas pueden y son dirigidas a un público mayor que las normas pues las políticas proporcionan las instrucciones generales, mientras que las normas indican requisitos técnicos específicos.

---

[36] Universidad Nacional Abierta y A Distancia. Op. Cit.

[37] GÓMEZ, L., ANDRÉS, A. Guía de Aplicación de la Norma UNE-ISO/IEC 27001 Sobre Seguridad en Sistemas de Información para PYMES. España: Asociación Española de Normalización y Certificación. 2012. p. 17

[38] UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO. Políticas de seguridad informática de la organización, Op. Cit. Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/ Cap4.html

2.2.2 Seguridad de la información

La seguridad de la información se entiende como la preservación de las siguientes características como se puede ver en la figura 2.

- **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

- **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Figura 3 Seguridad de la información

Fuente: BELT IBÉRICA. Seguridad informática. ¿Objetivos de la seguridad informática, que tenemos que tener en cuenta? [en línea]. España: El autor, 2012. [citado el 10-08-15]. Disponible en: http://www.belt.es/noticiasmdb/HOME2_noticias.asp?id=13451

- **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, deberán considerarse los conceptos de:

- **Autenticidad:** busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

- **Auditabilidad:** define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

- **Protección a la duplicación:** consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

- **No repudio:** se refiere a evitar que una entidad que haya enviado o recibido

información alegue ante terceros que no la envió o recibió.

- **Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el colegio.

- **Confiabilidad de la información:** es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

A los efectos de una correcta interpretación de la presente política, se realizan las siguientes definiciones:

- **Información:** se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

- **Sistema de información:** se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

- **Tecnología de la información:** se refiere al hardware y software operados por el Colegio o por un tercero que procese información en su nombre, para llevar a cabo[39].

2.2.3 Metodología Magerit

Implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información[40].

Es esencial en la entidad ya que en ella se puede llevar a cabo una serie de etapas donde se pueden hacer análisis detallado de los activos de la entidad y que amenazas pueden ocurrir dentro de ella. De acuerdo a este análisis se puede minimizar los riesgos y estandarizar normas de seguridad para controlar las amenazas que pueden tener los activos de determinada entidad.

---

[39] JEFATURA DE GABINETE DE MINISTROS. Modelo de política de seguridad de la información para organismos de la administración pública nacional [en línea]. Argentina: Oficina Nacional de Tecnologías de Información, 2005. [citado el 11-06-15]. Disponible en: http://www.sgp.gov.ar/sitio/PSI_Modelo-v1_200507.pdf

[40] GOBIERNO DE ESPAÑA. Magerit - versión 3.0: Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I - Método. Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012. p. 7.

Esta metodología contempla diferentes actividades enmarcadas a los activos que una organización posee para el tratamiento de la información.
Esta metodología contempla 3 libros:

- Método (Libro 1): Enumera los pasos y actividades para realizar un proyecto de análisis y gestión de riesgos, y proporciona una serie de aspectos prácticos.

- Catálogo de elementos (Libro 2). Clasifica los tipos de activos, dimensiones de valoración de los activos, criterios de valoración de los activos, amenazas típicas sobre los sistemas de información y salvaguardas a considerar para proteger sistemas de información en una organización.

- Guía de técnicas (Libro 3). Proporciona técnicas que se emplean habitualmente para llevar a cabo proyectos de análisis y gestión de riesgos.

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza[41].

[41] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Lección 8: Estándar Magerit para análisis de riesgos informáticos [en línea]. s.l.: UNAD, s.f. [citado el 20-04-16]. Disponible en: http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_8_estndar_magerit_para_anlisis_de_riesgos_informticos.html

Figura 4 Metodología MAGERIT

Fuente: ABRIL Ana, Pulido Jarol y BOHADA Jhon A., Análisis de Riesgos en Seguridad de la Información Fundación Universitaria Juan D Castellanos Colombia 2013.

Tabla 2 Criterios de valoración 1

[pi] Información de carácter personal		
6	6.pi1	probablemente afecte gravemente a un grupo de individuos
	6.pi2	probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
5	5.pi1	probablemente afecte gravemente a un individuo
	5.pi2	probablemente quebrante seriamente leyes o regulaciones
4	4.pi1	probablemente afecte a un grupo de individuos
	4.pi2	probablemente quebrante leyes o regulaciones
3	3.pi1	probablemente afecte a un individuo
	3.pi2	probablemente suponga el incumplimiento de una ley o regulación
2	2.pi1	pudiera causar molestias a un individuo
	2.pi2	pudiera quebrantar de forma leve leyes o regulaciones
1	1.pi1	pudiera causar molestias a un individuo

Fuente: MAGERIT V.3 – Libro II – Catálogo de Elementos

Tabla 3 Criterios de valoración 2

[lpo] Obligaciones legales		
9	9.lro	probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
7	7.lro	probablemente cause un incumplimiento grave de una ley o regulación
5	5.lro	probablemente sea causa de incumplimiento de una ley o regulación
3	3.lro	probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
1	1.lro	pudiera causar el incumplimiento leve o técnico de una ley o regulación

Fuente: MAGERIT V.3 – Libro II – Catálogo de Elementos

Tabla 4 Criterios de valoración 3

[si] Seguridad		
10	10.Si	probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
9	9.Si	probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
7	7.Si	probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
3	3.Si	probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
1	1.Si	pudiera causar una merma en la seguridad o dificultar la investigación de un incidente

Fuente: MAGERIT V.3 – Libro II – Catálogo de Elementos

Tabla 5 Criterios de valoración 4

[cei] Intereses comerciales o económicos		
9	10.Ci.a	de enorme interés para la competencia
	10.Ci.b	de muy elevado valor comercial
	10.Ci.c	causa de pérdidas económicas excepcionalmente elevadas
	10.Ci.d	causa de muy significativas ganancias o ventajas para individuos u organizaciones
	10.Ci.e	constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
7	7.cei.a	de alto interés para la competencia
	7.cei.b	de elevado valor comercial
	7.cei.c	causa de graves pérdidas económicas
	7.cei.d	proporciona ganancias o ventajas desmedidas a individuos u organizaciones

	7.cei.d	constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
3	3.cei.a	de cierto interés para la competencia
	3.cei.b	de cierto valor comercial
	3.cei.c	causa de pérdidas financieras o merma de ingresos
	3.cei.d	facilita ventajas desproporcionadas a individuos u organizaciones
	3.cei.e	constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
2	2.cei.a	de bajo interés para la competencia
	2.cei.b	de bajo valor comercial
1	1.cei.a	de pequeño interés para la competencia
	1.cei.b	de pequeño valor comercial
0	0.3	supondría pérdidas económicas mínimas

Fuente: MAGERIT V.3 – Libro II – Catálogo de Elementos

Tabla 6 Criterios de valoración 5

[da] Interrupción del servicio		
9	9.da	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
	9.da2	Probablemente tenga un serio impacto en otras organizaciones
7	7.da	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
	7.da2	Probablemente tenga un gran impacto en otras organizaciones
5	5.da	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	5.da2	Probablemente cause un cierto impacto en otras organizaciones
3	3.da	Probablemente cause la interrupción de actividades propias de la Organización
1	1.da	Pudiera causar la interrupción de actividades propias de la Organización

Fuente: MAGERIT V.3 – Libro II – Catálogo de Elementos

Tabla 7 Criterios de valoración 6

[po] Orden público		
9	9.po	alteración sería del orden público
6	6.po	probablemente cause manifestaciones, o presiones significativas
3	3.po	causa de protestas puntuales
1	1.po	pudiera causar protestas puntuales

Fuente: MAGERIT V.3 – Libro II – Catálogo de Elementos

Tabla 8 Criterios de valoración 7

[olm] Operaciones		
10	10.olm	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
9	9.olm	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
7	7.olm	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
3	3.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
1	1.olm	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)

Fuente: MAGERIT V.3 – Libro II – Catálogo de Elementos

Tabla 9 Criterios de valoración 8

[adm] Administración y gestión		
9	9.adm	probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
7	7.adm	probablemente impediría la operación efectiva de la Organización
5	5.adm	probablemente impediría la operación efectiva de más de una parte de la Organización
3	3.adm	probablemente impediría la operación efectiva de una parte de la Organización
1	1.adm	pudiera impedir la operación efectiva de una parte de la Organización

Fuente: MAGERIT V.3 – Libro II – Catálogo de Elementos

Tabla 10 Criterios de valoración 9

[lg] Pérdida de confianza (reputación)		
9	9.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
	9.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
7	7.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar grave mente a las relaciones con otras organizaciones
	7.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar grave mente a las relaciones con el público en general
5	5.lg.a	Probablemente sea causa una cierta publicidad negativa por afectar negativamente te a las relaciones con otras organizaciones
	5.lg.b	Probablemente sea causa una cierta publicidad negativa por afectar negativamente te a las relaciones con el público

3	3.lg	Probablemente afecte negativamente a las relaciones internas de la Organización
2	2.lg	Probablemente cause una pérdida menor de la confianza dentro de la Organización
1	1.lg	Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	0.4	no supondría daño a la reputación o buena imagen de las personas u organizaciones

Fuente: MAGERIT V.3 – Libro II – Catálogo de Elementos

Tabla 11 Criterios de valoración 10

[crm] Persecución de delitos		
8	8.crm	Impida la investigación de delitos graves o facilite su comisión
4	4.crm	Dificulte la investigación o facilite la comisión de delitos

Fuente: MAGERIT V.3 – Libro II – Catálogo de Elementos

Tabla 12 Criterios de valoración 11

[rto] Tiempo de recuperación del servicio		
7	7.rto	RTO < 4 horas
4	4.rto	4 horas < RTO < 1 día
1	1.rto	1 día < RTO < 5 días
0	0.rto	5 días < RTO

Fuente: MAGERIT V.3 – Libro II – Catálogo de Elementos

Tabla 13 Criterios de valoración 12

[lbl.nat] Información clasificada (nacional)		
10	10.lbl	Secreto
9	9.lbl	Reservado
8	8.lbl	Confidencial
7	7.lbl	Confidencial
6	6.lbl	Difusión limitada
5	5.lbl	Difusión limitada
4	4.lbl	Difusión limitada
3	3.lbl	Difusión limitada
2	2.lbl	Sin clasificar
1	1.lbl	Sin clasificar

Fuente: MAGERIT V.3 – Libro II – Catálogo de Elementos

MAGERIT presenta en el capítulo número 4, los criterios de valoración para los activos determinadas por las siguientes escalas como se observa en las siguientes tablas:

2.3. ANTECEDENTES

La monografía “análisis y gestión del riesgo de la información en los sistemas de información misionales de una entidad, enfocado en un sistema de seguridad de la información” presentado por Wilson Sandino, para la entidad Ministerio de Hacienda Bogotá (Colombia). Su desarrollo aporta conocimientos importantes en la gestión de riesgos que sirven de punto de referencia para el proyecto planteado en el presente documento.

2.4. MARCO LEGAL

2.4.1. Ley Estatutaria 1266[42]

“Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”.

2.4.2. Ley 527[43]

“Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”

2.4.3. Ley 1712[44]

“Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”

2.4.4 Ley Estatutaria 1581[45]

“Por la cual se dictan disposiciones generales para la protección de datos personales”.

2.4.5 Ley 1341 de 2009[46]

[42] CONGRESO DE LA REPUBLICA. Ley 1266. Bogotá. (Diciembre 31 de 2008). Colombia. Diario Oficial 47.219 de diciembre 31 de 2008. p. 1-15.

43 CONGRESO DE LA REPUBLICA. Ley 527. Bogotá. (Agosto 18 de 1999). Colombia. Diario Oficial 43.673 del 21 de agosrto de 1999 p. 1-14.

44 CONGRESO DE LA REPUBLICA. Ley 1712. Bogotá. (Marzo 06 de 2014). Colombia. Diario Oficial 49084 de marzo 6 de 2014. p. 1-15.

45 CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1581 (17 de octubre de 2012). Bogotá. Diario Oficial 48.587 de octubre 18 de 2012. p. 1-15.

46 COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1341 (30 de julio de 2009). Bogotá. Diario Oficial 47.426 de 30 de julio de 2009.

“Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones”.

2.4.6 Decreto 1151 de abril 14 de 2008[47]

Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones

2.4.7 Decreto 1360 de 1989[48]

Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor

2.4.8 Ley 1273 de 2009[49]

La cual modifica el Código Penal, creando un nuevo bien jurídico tutelado -denominado “de la protección de la información y de los datos”-, cuyo objetivo principal es preservar los sistemas que utilicen las tecnologías de la información y las comunicaciones”.

[47] CONGRESO DE LA REPUBLICA. Decreto 1151. (14, abril, 2008). Bogotá, D.C., Colombia. Diario Oficial. 46960 de abril 14 de 2008.p. 1-4.

[48] COLOMBIA, CONGRESO DE LA REPUBLICA. Decreto 1360. Bogotá. (Junio 23 de 1989). Diario Oficial 38.871 de junio 23 de 1989.

[49] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1273. Bogotá. (5 de enero de 2009). Diario Oficial 47.223 de enero 5 de 2009.

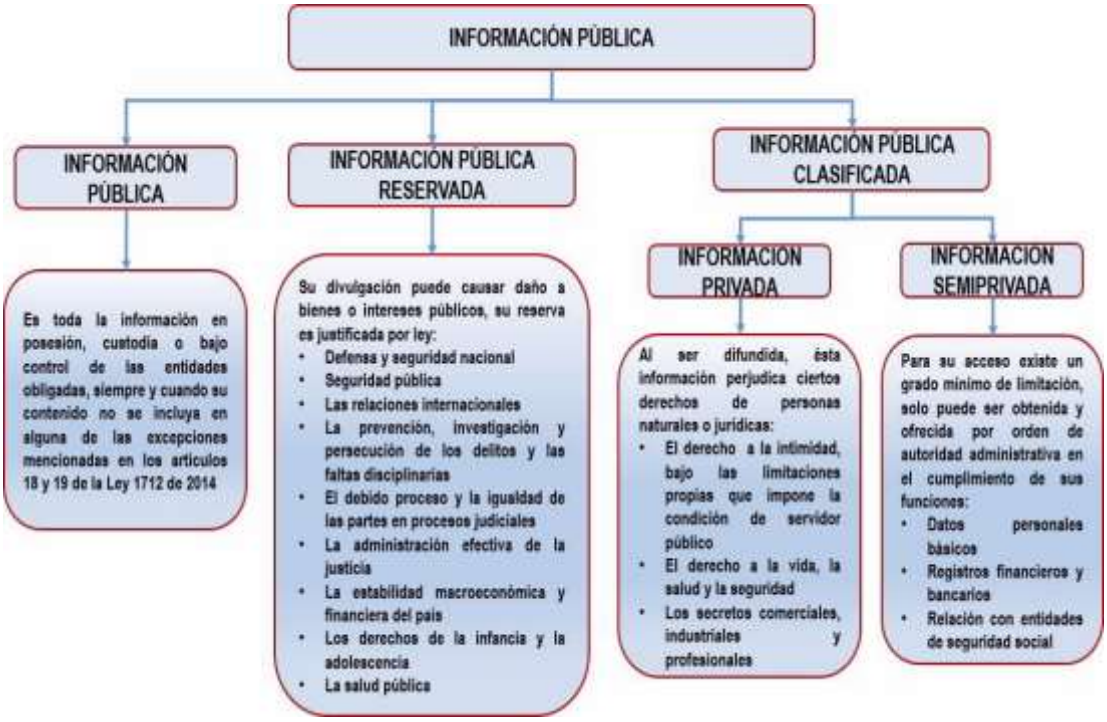
3. IDENTIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN PARA EL SISTEMA INTEGRADO DE INFORMACIÓN FINANCIERA GENERAL

3.1. INTRODUCCIÓN

Haciendo uso de la metodología de análisis y gestión de riesgos, basados en la metodología MAGERIT, se acuerdan los activos con los que cuenta la entidad caso estudio, esta identificación permite asemejar diferentes análisis de riesgos, determinando criterios que permitan analizar los diferentes activos con los que cuenta la entidad.

3.2. CLASIFICACIÓN DE LA INFORMACIÒN[50]

Figura 5 Calificación de la Información



Fuente: http://es.presidencia.gov.co/dapre/DocumentosSIGEPRE/G-GD-02-calificacion-informacion.pdf,

En la figura 5 se muestra la clasificación de la información, la cual determinará los controles requeridos para su custodia, almacenamiento y acceso además es importante asumir la calificación que manifieste su productor ya sea una persona, una empresa u otra entidad y debe contemplarse de acuerdo a:

[50] http://es.presidencia.gov.co/dapre/DocumentosSIGEPRE/G-GD-02-calificacion-informacion.pdf

3.2.1. Información pública

Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal. *(Artículo 5 Ley 1712 de 2014)* [51]

3.2.2. Información clasificada

Es toda aquella que al ser divulgada puede llegar a causar daño a algunos derechos individuales de personas naturales o jurídicas por contener información relacionada con la intimidad y privacidad de éstas. (*Artículo 18 Ley 1712 de 2014)*[52]

3.2.3. Información reservada

Su divulgación indebida puede afectar bienes o intereses públicos. *(Artículo 19 Ley 1712 de 2014).* Es necesario establecer el plazo para la clasificación de la reserva, es decir el tiempo en que se considera debe limitarse el acceso a la información el cual según la Ley solo puede durar un máximo de 15 años desde la creación del documento[53]

Así mismo se destaca que existen categorías de información (series y subseries documentales) cuyo contenido puede involucrar información pública y reservada o clasificada en forma mixta, en éstos casos se asigna la calificación más alta a toda la categoría es decir Privada, semiprivada o reservada, aclarando la parte o partes que reúnen tales requisitos de excepción, de igual manera definir controles específicos[54].

3.3. ACTIVOS INFORMATICOS

Cada metodología utiliza diferentes técnicas y métricas para identificarlos, MAGERIT en su metodología los clasifica y agrupa de la siguiente forma para que su análisis sea más eficaz.

Nomenclatura en el método MAGERIT

- Inventario de Información [D]
- Servicios [S]
- Software [SW]
- Hardware [HW]
- Comunicaciones [COM]
- Personal [P]i

[51] https://www.mintic.gov.co/portal/604/articles-7147_documento.pdf
[52] Ibid. mintic.gov.co pag.3
[53] Ibid. mintic.gov.co pag.3
[54] De acuerdo a la ley 1712 toda información en posesión, bajo control o custodia de un sujeto obligado es pública y no puede ser reservada o limitada sino por disposición constitucional o legal

- Claves criptográficas [keys]
- instalaciones [L]
- equipamiento auxiliar [AUX]
- Soportes de información [Media]
- registros de actividad [D.log]

En la tabla 14 se indican los activos más relevantes de la entidad caso de estudio.

Tabla 14 Inventario de activos

Tipo de activo	Código de activo	Activos más relevantes en la entidad
[essential] Activos esenciales	[info]	Información financiera
		Acuerdos
		Licencias, Convenios, Actas
		Informes, Autorizaciones
		Resoluciones Memorias
[arch] Arquitectura del sistema	[ext]	ETB
[D] Datos / Información	[files]	Archivos de actas Resoluciones actos administrativos
	[backup]	Copias de respaldo de seguridad de los del sistema (Ambientes, Producción Preproducción, Hallazgos y correo institucional), servidor, base de datos y los equipos de cómputo
	[conf]	Datos de configuración de los equipos
	[log]	Archivos de registros de actividad de los Sistemas de Información
[S] Servicios	[ext]	Informática / Soporte técnico Call Center
	[int]	Página Web interna (Intranet)
	[www]	Acceso transaccional a través de URL
	[email]	Envío de login de usuario y clave de acceso
	[telnet]	VPN Juniper
	[dir]	Directorio Activo
	[ipm]	Módulo de administración
	[pki]	Token
[SW] Aplicaciones (software)	[prp]	Macroprocesos o módulos Financieros
	[std]	Visual basic 6, NET, NEtbeet, dreamweaver, Java, Macromedia_Flash_8_(Portable)
	[browser]	Internet Explorer, Chrome, Firefox
	web [www]	Servidor de páginas web

Tipo de activo	Código de activo	Activos más relevantes en la entidad
	[av]	Mcafee
	[email_client]	Programas de comunicación (correo electrónico, chat, llamadas telefónicas.
	[email_server]	Correo electrónico
	[office]	Office 2013, 2016 winrar, Adobe Acrobat Reader
	[sub]	Aplicaciones para manejo informacion hallazgos y reportes
	[os]	Sistema operativo Windows 7, Windows 8, Windows 10
	[hypervisor]	Virtualbox, Winware
[HW] Equipos informáticos (hardware)	[host]	Servidor de producción Servprod HP Proliant DL380 G9, Datacenter. IBM Power System S814 Servidores aplicaciones IBM Power System S822LC
	[mid]	HP Z238, Intel Core i7-7700 3.60GHz, 8GB, 1TB, Windows 10 Pro 64-bit, HP Allin-One 200-5030 y Intel (R) Core (TM) i5
	[pc]	Dell Core i3, i5 Equipos de escritorio salas de sistemas equipos de escritorio equipo administración
	[mobile]	Portátiles DELL y HP
	[pda]	MyPAL A730W - Asus
	[vhost]	MSA Store HP 2040 SAN Con hyper-v sistemas operativos Centos, Windows server 2012 y equipos cliente Windows 7
	[backup]	Dell PowerVault Network Attached Storage (PV701N, PV705N, PV735N)
	[print]	Impresoras de multifunción Impresora Epson y lexmark
	[network]	routers Cisco 1811 y 1812 de servicios, Switch core. IBM System Networking RackSwitch G8264 Equipos (router, Cisco MDS 9718 Multilayer Director for IBM Storage Networking
	[modem]	Integrados
	[switch]	Catalyst 2960 Plus Capa 2
	[router]	Catalyst 9400 4 switch 24
	[router]	Puertos Router CISCO 2900 Series.
	[firewall]	WAN, 1 OPT, 4 LAN /DMZ ZYWALL110
	[wap]	Cisco WAP351 Wireless-N
	[pabx]	Central Telefonica Ip Pbx Grandstream 6208
	[ipphone]	Telefono IP Cisco SPA942
[COM] Redes de comunicaciones	[PSTN]	Acceso telefónico ETB
	[ISDN]	Cisco 2600 y 3700
	[[ADSL] ADSL	Cisco 2600

Tipo de activo	Código de activo	Activos más relevantes en la entidad
	[wifi]	Red inalámbrica ETB
	[Internet]	Internet ETB
	[LAN]	Cableado estructurado
[Media] Soportes de información	[disk]	Discos duros externos para almacenamiento de información
	[cd] cederrón (CD-ROM)	Manuales de usuario, Archivos documentos, resoluciones, actas administrativas. Copia de seguridad, documentos
	[usb]	Documentos varios
	[dvd] DVD	Proyecto, actas y documentos institucionales.
	[printed]	Carpetas, reglamentos, acuerdos actas, planillas, proyectos y resoluciones.
[AUX] Equipamiento auxiliar	[power]	Fuentes de alimentación UPS. IBM SmartUPS DE 1400 VA 2 U 230 V PARA RACK
	[ups]	Ups de computadores energía temporal a los Servidores y demás dispositivos vitales en caso de fallas eléctricas inesperadas
	[gen]	Generador de energía AVR
	[ac]	Compu-aire
	[cabling]	Red interna
	[wire]	Instalaciones para el suministro de energía
	[furniture]	rack, armarios, mesas, archivadores, muebles,
[L] Instalaciones	[building]	Edificación propia de la entidad
[P] Personal	[ue]	Entidades usuarias
	[ui]	Funcionarios
	[op]	Call Center
	[adm]	Administrador aplicativo misional
	[com]	Director de TI
	[dba]	Gestor de Bases de Datos
	[sec]	Director/Coordinadores aplicativo misional
	[des]	Ingenieros de Software
	[sub]	Contratistas
	[prov]	Personal ETB, Soporte Técnico

Fuente: Propiedad de Autor

3.4. CLASIFICACION DE LOS ACTIVOS DE LA INFOMACIÓN

Para la clasificación de los activos de la información de acuerdo a los criterios de la información se tomará los criterios establecidos en el numeral 3.2.

En la tabla 15 se establece el criterio de clasificación de la información

Tabla 15 Clasificación de los activos según criterios de información

Tipo de activo	Código de activo	Activos más relevantes en la entidad	Clasificación de la información
[essential] Activos esenciales	[info]	Información financiera	Pública
		Acuerdos	Pública
		Licencias, Convenios, Actas	Pública
		Informes, Autorizaciones	Pública
		Resoluciones Memorias	Pública
[arch] Arquitectura del sistema	[ext]	ETB	Reservada
[D] Datos / Información	[files]	Archivos de actas Resoluciones actos administrativos	Pública
	[backup]	Copias de respaldo de seguridad de los del sistema (Ambientes, Producción Preproducción, Hallazgos y correo institucional), servidor, base de datos y los equipos de cómputo	Reservada
	[conf]	Datos de configuración de los equipos	Reservada
	[log]	Archivos de registros de actividad de los Sistemas de Información	Reservada
[S] Servicios	[ext]	Informática / Soporte técnico Call Center	Pública
	[int]	Página Web interna (Intranet)	Reservada
	[www]	Acceso transaccional a través de URL	Pública
	[email]	Envío de login de usuario y clave de acceso	Clasificada
	[telnet]	VPN Juniper	Clasificada
	[dir]	Directorio Activo	Reservada
	[ipm]	Módulo de administración	Clasificada
	[pki]	Token	Pública
[SW] Aplicaciones (software)	[prp]	Macroprocesos o módulos Financieros	Pública
	[std]	Visual basic 6, NET, NEtbeet, dreamweaver, Java, Macromedia_Flash_8_(Portable)	Clasificada

Tipo de activo	Código de activo	Activos más relevantes en la entidad	Clasificación de la información
	[browser]	Internet Explorer, Chrome, Firefox	Pública
	web [www]	Servidor de páginas web	Pública
	[av]	Mcafee	Clasificada
	[email_client]	Programas de comunicación (correo electrónico, chat, llamadas telefónicas.	Clasificada
	[email_server]	Correo electrónico	Reservada
	[office]	Office 2013, 2016 winrar, Adobe Acrobat Reader	Clasificada
	[sub]	Aplicaciones para manejo informacion hallazgos y reportes	Pública
	[os]	Sistema operativo Windows 7, Windows 8, Windows 10	Pública
	[hypervisor]	Virtualbox, Winware	Pública
[HW] Equipos informáticos (hardware)	[host]	Servidor de producción Servprod HP Proliant DL380 G9, Datacenter. IBM Power System S814 Servidores aplicaciones IBM Power System S822LC	Reservada
	[mid]	HP Z238, Intel Core i7-7700 3.60GHz, 8GB, 1TB, Windows 10 Pro 64-bit, HP Allin-One 200-5030 y Intel (R) Core (TM) i5	Reservada
	[pc]	Dell Core i3, i5 Equipos de escritorio salas de sistemas equipos de escritorio equipo administración	Reservada
	[mobile]	Portátiles DELL y HP	Reservada
	[pda]	MyPAL A730W - Asus	Reservada
	[vhost]	MSA Store HP 2040 SAN Con hyper-v sistemas operativos Centos, Windows server 2012 y equipos cliente Windows 7	Reservada
	[backup]	Dell PowerVault Network Attached Storage (PV701N, PV705N, PV735N)	Reservada
	[print]	Impresoras de multifunción Impresora Epson y lexmark	Reservada
	[network]	routers Cisco 1811 y 1812 de servicios, Switch core. IBM System Networking RackSwitch G8264 Equipos (router, Cisco MDS 9718 Multilayer Director for IBM Storage Networking	Reservada
	[modem]	Integrados	Reservada
	[switch]	Catalyst 2960 Plus Capa 2	Reservada
	[router]	Catalyst 9400 4 switch 24	Reservada
	[router]	Puertos Router CISCO 2900 Series.	Reservada
	[firewall]	WAN, 1 OPT, 4 LAN /DMZ ZYWALL110	Reservada
	[wap]	Cisco WAP351 Wireless-N	Reservada

Tipo de activo	Código de activo	Activos más relevantes en la entidad	Clasificación de la información
	[pabx]	Central Telefonica Ip Pbx Grandstream 6208	Reservada
	[ipphone]	Telefono IP Cisco SPA942	Reservada
[COM] Redes de comunicaciones	[PSTN]	Acceso telefónico ETB	Reservada
	[ISDN]	Cisco 2600 y 3700	Reservada
	[[ADSL] ADSL	Cisco 2600	Reservada
	[wifi]	Red inalámbrica ETB	Reservada
	[Internet]	Internet ETB	Reservada
	[LAN]	Cableado estructurado	Reservada
[Media] Soportes de información	[disk]	Discos duros externos para almacenamiento de información	Clasificada
	[cd] cederrón (CD-ROM)	Manuales de usuario, Archivos documentos, resoluciones, actas administrativas. Copia de seguridad, documentos	Clasificada
	[usb]	Documentos varios	Clasificada
	[dvd] DVD	Proyecto, actas y documentos institucionales.	Clasificada
	[printed]	Carpetas, reglamentos, acuerdos actas, planillas, proyectos y resoluciones.	Clasificada
[AUX] Equipamiento auxiliar	[power]	Fuentes de alimentación UPS. IBM SmartUPS DE 1400 VA 2 U 230 V PARA RACK	Reservada
	[ups]	Ups de computadores energía temporal a los Servidores y demás dispositivos vitales en caso de fallas eléctricas inesperadas	Reservada
	[gen]	Generador de energía AVR	Reservada
	[ac]	Compu-aire	Reservada
	[cabling]	Red interna	Reservada
	[wire]	Instalaciones para el suministro de energía	Reservada
	[furniture]	rack, armarios, mesas, archivadores, muebles,	Reservada
[L] Instalaciones	[building]	Edificación propia de la entidad	Pública
[P] Personal	[ue]	Entidades usuarias	Pública
	[ui]	Funcionarios	Clasificada
	[op]	Call Center	Clasificada

Tipo de activo	Código de activo	Activos más relevantes en la entidad	Clasificación de la información
	[adm]	Administrador aplicativo misional	Clasificada
	[com]	Director de TI	Pública
	[dba]	Gestor de Bases de Datos	Pública
	[sec]	Director/Coordinadores aplicativo misional	Pública
	[des]	Ingenieros de Software	Pública
	[sub]	Contratistas	Pública
	[prov]	Personal ETB, Soporte Técnico	Pública

Fuente: Propiedad de Autor

3.5. DIMENSIONES DE VALORACIÓN

Las dimensiones de valoración se aplican para dar un valor al activo de acuerdo a su función y nivel de importancia que este tenga en la entidad.

Se evalúan los activos teniendo en cuenta el criterio de valoración cualitativo de acuerdo a su impacto y a las dimensiones de seguridad.

La metodología MAGERIT clasifican los activos de acuerdo a su valoración por dimensiones

3.5.1 De acuerdo al impacto

Es importante que cada uno de los activos sea valorado incluyendo cada uno de los procesos con los que cuentan las áreas.

3.5.2 Criterios de valoración

En la tabla 4, podemos observar las escalas de valoración, donde se evidencia que el valor de 0 corresponde a un valor Irrelevante a efectos prácticos y el máximo valor (10) corresponde a un Daño muy grave.

Tabla 16 criterios de valoración

IMPACTO	NOMENCLATURA	VALOR	DESCRIPCIÓN
MUY ALTO	**[MA]**	**10**	Daño muy grave
ALTO	**[A]**	**7-9**	Daño grave

MEDIO	**[M]**	**4-6**	Daño importante
BAJO	**[B]**	**1-3**	Daño menor
MUY BAJO	**[MB]**	**0**	Irrelevante a efectos prácticos

Fuente: MAGERIT V.3 – Libro II – Catálogo de Elementos

3.5.3 Valoración de los activos

Se describe la valoración de activos, de acuerdo al impacto que éste tiene sobre los criterios que se han tenido en cuenta en el inventario.

Para la valoración de los activos de acuerdo al impacto se tendrán en cuentas las tablas del numeral 02 al 13, criterios de valoración, que nos proporciona la valoración de los activos de información según la tabla.

Tabla 17 Valoración de Activos de acuerdo al impacto

Tipo de activo	Código de activo	Nombre del Activo de la información	Impacto	Descripción
[essential] Activos esenciales	[info]	Información financiera	MA	9.adm probablemente impediría seriamente la operación efectiva de la organización, pudiendo llegar a su cierre.
		Acuerdos	A	1.adm pudiera impedir la operación efectiva de una parte de la Organización
		Licencias, Convenios, Actas	M	5.adm probablemente impediría la operación efectiva de más de una parte de la Organización
		Informes, Autorizaciones	M	5.adm probablemente impediría la operación efectiva de más de una parte de la Organización
		Resoluciones Memorias	M	5.adm probablemente impediría la operación efectiva de más de una parte de la Organización
[arch] Arquitectura del sistema	[ext]	ETB	MA	9.da Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
[D] Datos / Información	[files]	Archivos de actas Resoluciones actos administrativos	MA	9.adm probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
	[backup]	Copias de respaldo de seguridad de los del sistema (Ambientes, Producción Preproducción, Hallazgos y correo institucional), servidor,	MA	9.da2 Probablemente tenga un serio impacto en otras organizaciones

Tipo de activo	Código de activo	Nombre del Activo de la información	Impacto	Descripción
		base de datos y los equipos de cómputo		
	[conf]	Datos de configuración de los equipos	MA	9.olm, Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
	[log]	Archivos de registros de actividad de los Sistemas de Información	MA	10.si probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
[S] Servicios	[ext]	Informática / Soporte técnico Call Center	MA	9.da Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
	[int] interno (a usuarios de la propia organización)	Página Web interna (Intranet)	MA	9.da2 Probablemente tenga un serio impacto en otras organizaciones
	[www]	Acceso transaccional a través de URL	M	5.da Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	[email]	Envío de login de usuario y clave de acceso	M	5.da2 Probablemente cause un cierto impacto en otras organizaciones
	[telnet]	VPN Juniper	B	3.da Probablemente cause la interrupción de actividades propias de la Organización
	[dir]	Directorio Activo	B	9.da Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
	[ipm]	Módulo de administración	M	9.da Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
	[pki] PKI -	Token	MA	9.da Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
[SW] Aplicaciones (software)	[prp])	Macroprocesos o módulos Financieros	MA	9.da Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la

Tipo de activo	Código de activo	Nombre del Activo de la información	Impacto	Descripción
				Organización con un serio impacto en otras organizaciones
	[std]	Visual basic 6, NET, NEtbeet, dreamweaver, Java, Macromedia_Flash_8_(Portable)	B	3.lro, probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
	[browser]	Internet Explorer, Chrome, Firefox	B	3.lro, probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
	web [www]	Servidor de páginas web	B	3.lro, probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
	[av]	Mcafee	B	3.lro, probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
	[email_cli ent]	Programas de comunicación (correo electrónico, chat, llamadas telefónicas.	B	3.lro, probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
	[email_se rver]	Correo electrónico	B	3.da Probablemente cause la interrupción de actividades propias de la Organización
	[office]	Office 2013, 2016 winrar, Adobe Acrobat Reader	B	3.lro, probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
	[sub]	Aplicaciones para manejo informacion hallazgos y reportes	B	3.lro, probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
	[os]	Sistema operativo Windows 7, Windows 8, Windows 10	B	3.lro, probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
	[hypervis or]	Virtualbox, Winware	B	3.lro, probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
[HW] Equipos informáticos (hardware)	[host]	Servidor de producción Servprod HP Proliant DL380 G9, Datacenter. IBM Power System S814 Servidores aplicaciones IBM Power System S822LC	MA	9.adm probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
	[mid]	HP Z238, Intel Core i7-7700 3.60GHz, 8GB, 1TB, Windows 10 Pro 64-bit, HP Allin-One 200-5030 y Intel (R) Core (TM) i5	A	7.adm probablemente impediría la operación efectiva de la Organización
	[pc] i	Dell Core i3, i5 Equipos de escritorio salas de sistemas equipos de escritorio equipo administración	M	5.adm probablemente impediría la operación efectiva de más de una parte de la Organización
	[mobile]	Portátiles DELL y HP	B	3.adm probablemente impediría la operación efectiva de una parte de la Organización

Tipo de activo	Código de activo	Nombre del Activo de la información	Impacto	Descripción
	[pda]	MyPAL A730W - Asus	B	3.adm probablemente impediría la operación efectiva de una parte de la Organización
	[vhost]	MSA Store HP 2040 SAN Con hyper-v sistemas operativos Centos, Windows server 2012 y equipos cliente Windows 7	M	7.da2 Probablemente tenga un gran impacto en otras organizaciones
	[backup]	Dell PowerVault Network Attached Storage (PV701N, PV705N, PV735N)	MA	9.da Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
	[print]	Impresoras de multifunción Impresora Epson y lexmark	B	1.adm pudiera impedir la operación efectiva de una parte de la Organización
	[network]	routers Cisco 1811 y 1812 de servicios, Switch core. IBM System Networking RackSwitch G8264 Equipos (router, Cisco MDS 9718 Multilayer Director for IBM Storage Networking	A	7.da Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
	[modem]	Integrados	A	7.da Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
	[switch]	Catalyst 2960 Plus Capa 2	A	7.da Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
	[router]	Catalyst 9400 4 switch 24	M	5.daProbablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	[router]	Puertos Router CISCO 2900 Series.	M	5.daProbablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	[firewall]	WAN, 1 OPT, 4 LAN /DMZ ZYWALL110	M	5.daProbablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones

Tipo de activo	Código de activo	Nombre del Activo de la información	Impacto	Descripción
	[wap]	Cisco WAP351 Wireless-N	M	5.daProbablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	[pabx]	Central Telefonica Ip Pbx Grandstream 6208	A	7.da Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
	[ipphone]	Telefono IP Cisco SPA942	M	5.daProbablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
[COM] Redes de comunicaciones	[PSTN]	Acceso telefónico ETB	M	5.daProbablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	[ISDN]	Cisco 2600 y 3700	M	5.daProbablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	[[ADSL] ADSL	Cisco 2600	M	5.daProbablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	[wifi]	Red inalámbrica ETB	M	7.si probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
	[Internet]	Internet ETB	MA	9.da Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
	[LAN]	Cableado estructurado	MA	9.da Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
[Media] Soportes de información	[disk]	Discos duros externos para almacenamiento de información	B	6.pi2, probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
	[cd]	Manuales de usuario, Archivos documentos, resoluciones, actas administrativas. Copia de seguridad, documentos	B	6.pi2, probablemente quebrante seriamente la ley o algún reglamento de protección de información personal

Tipo de activo	Código de activo	Nombre del Activo de la información	Impacto	Descripción
	[usb]	Documentos varios	B	6.pi2, probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
	[dvd] DVD	Proyecto, actas y documentos institucionales.	B	6.pi2, probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
	[printed]	Carpetas, reglamentos, acuerdos actas, planillas, proyectos y resoluciones.	MB	6.pi2, probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
[AUX] Equipamiento auxiliar	[power]	Fuentes de alimentación UPS. IBM SmartUPS DE 1400 VA 2 U 230 V PARA RACK	MA	9.da Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
	[ups]	Ups de computadores energía temporal a los Servidores y demás dispositivos vitales en caso de fallas eléctricas inesperadas	MA	9.da Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
	[gen]	Generador de energía AVR	M	5.adm probablemente impediría la operación efectiva de más de una parte de la Organización
	[ac]	Compu-aire	MA	9.da Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
	[cabling]	Red interna	MA	9.da Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
	[wire]	Instalaciones para el suministro de energía	A	9.da Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
	[furniture]	rack, armarios, mesas, archivadores, muebles,	A	7.cei.c causa de graves pérdidas económicas
[L] Instalaciones	[building]	Edificación propia de la entidad	M	7.da, Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones

Tipo de activo	Código de activo	Nombre del Activo de la información	Impacto	Descripción
[P] Personal	[ue]	Entidades usuarias	A	6.pi1, probablemente afecte gravemente a un grupo de individuos
	[ui]	Funcionarios	A	4.pi1 probablemente afecte a un grupo de individuos
	[op]	Call Center	A	6.pi1, probablemente afecte gravemente a un grupo de individuos
	[adm]	Administrador aplicativo misional	A	6.pi1, probablemente afecte gravemente a un grupo de individuos
	[com]	Director de TI	A	5.pi1 probablemente afecte gravemente a un individuo
	[dba]	Gestor de Bases de Datos	A	6.pi1, probablemente afecte gravemente a un grupo de individuos
	[sec]	Director/Coordinadores aplicativo misional	A	6.pi2, probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
	[des]	Ingenieros de Software	M	4.pi1 probablemente afecte a un grupo de individuos
	[sub]	Contratistas	M	3.pi1 probablemente afecte a un individuo
	[prov]	Personal ETB, Soporte Técnico	A	6.pi1, probablemente afecte gravemente a un grupo de individuos

Fuente: Propiedad de Autor

3.5.4. De acuerdo a las dimensiones de seguridad

Las dimensiones se utilizan para dar un valor a las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión

La tabla 18 muestra las dimensiones de valoración informática

Tabla 18 Dimensiones de valoración informática

[D]	Disponibilidad
[C]	Confidencialidad
[I]	Integridad
[A]	Autenticidad
[T]	Trazabilidad

Fuente: autor

[D] Disponibilidad
Se refiere al valor que se le otorga a un activo desde el punto de vista de disponibilidad si una amenaza la afectara.

[I] Integridad de los datos
Se asigna una valoración alta frente a la integridad cuando esta sufre algún tipo de alteración, conllevando a tener graves daños en los activos de la entidad.

[C] Confidencialidad de la información
Determina el cómo la información no se divulga o entrega a personas ajenas a la organización.

[A] Autenticidad
El garantizar que la información proviene de fuentes fiables, brindando seguridad a los usuarios de la misma.

[T] Trazabilidad
Característica de la información que refiere a la conservación e historial de la misma.

En la tabla 19 indica el valor del nivel de seguridad

Tabla 19 Criterios de Valoración de acuerdo a las dimensiones de seguridad.

Valor			**Crit erio**
90 - 100 %	Muy alto	[MA]	Daño muy grave
61 - 89%	Alto	[A]	Daño grave
40% - 60%	Medio	[M]	Daño importante
20 - 39 %	Bajo	[B]	Daño menor
0 - 19 %	Muy Bajo	[MB]	Irrelevante a efectos prácticos

Fuente: MAGERIT V.3 – Libro II – Catálogo de Elementos

3.5.5 Valoración

Se representa los criterios de valoración según el riesgo que los activos pueden presentar en la entidad, de acuerdo al nivel de seguridad, teniendo en cuenta su escala valoración cualitativa según MAGERIT.

La siguiente tabla indica la valoración de activos según el nivel de seguridad que estos tienen en la institución (ver tabla 20).

Tabla 20 Criterios de Valoración de acuerdo a las dimensiones de seguridad

Tipo de activo	Nombre de activos	Clasificación de la información	[D]	[C]	[I]	[A]	[T]	PROM
[essential] Activos esenciales	Información financiera	Pública	100%	100%	100%	100%	100%	100%
	Acuerdos	Pública	100%	100%	0%	100%	0%	60%
	Licencias, Convenios, Actas	Pública	100%	100%	0%	100%	0%	60%
	Informes, Autorizaciones	Pública	100%	100%	0%	100%	0%	60%
	Resoluciones Memorias	Pública	100%	100%	0%	100%	0%	60%
[arch] Arquitectura del sistema	ETB	Reservada	100%	0%	100%	100%	0%	60%
[D] Datos / Información	Archivos de actas Resoluciones actos administrativos	Pública	100%	0%	100%	0%	100%	60%
	Copias de respaldo de seguridad de los del sistema (Ambientes, Producción Preproducción, Hallazgos y correo institucional), servidor, base de datos y los equipos de cómputo	Reservada	0%	100%	0%	0%	0%	20%
	Datos de configuración de los equipos	Reservada	0%	100%	0%	0%	0%	20%
	Archivos de registros de actividad de los Sistemas de Información	Reservada	0%	100%	0%	0%	0%	20%
[S] Servicios	Informática / Soporte técnico Call Center	Pública	100%	0%	0%	0%	0%	20%
	Página Web interna (Intranet)	Reservada	100%	0%	0%	0%	0%	20%
	Acceso transaccional a través de URL	Pública	100%	0%	0%	0%	0%	20%
	Envío de login de usuario y clave de acceso	Clasificada	100%	0%	0%	0%	0%	20%
	VPN Juniper	Clasificada	100%	0%	0%	0%	0%	20%
	Directorio Activo	Reservada	100%	0%	0%	0%	0%	20%
	Módulo de administración	Clasificada	100%	0%	0%	0%	0%	20%
	Token	Pública	100%	0%	0%	0%	0%	20%
[SW] Aplicaciones (software)	Macroprocesos o módulos Financieros	Pública	100%	0%	100%	50%	100%	70%
	Visual basic 6, NET, NEtbeet, dreamweaver, Java, Macromedia_Flash_8_(Portable)	Clasificada	100%	50%	100%	50%	50%	70%

Tipo de activo	Nombre de activos	Clasificación de la información	[D]	[C]	[I]	[A]	[T]	PROM
	Internet Explorer, Chrome, Firefox	Pública	100%	100%	80%	50%	100%	86%
	Servidor de páginas web	Pública	100%	100%	100%	100%	100%	100%
	Mcafee	Clasificada	100%	0%	0%	50%	0%	30%
	Programas de comunicación (correo electrónico, chat, llamadas telefónicas.	Clasificada	0%	100%	100%	100%	100%	80%
	Correo electrónico	Reservada	100%	0%	0%	50%	50%	40%
	Office 2013, 2016 winrar, Adobe Acrobat Reader	Clasificada	100%	0%	100%	50%	50%	60%
	Aplicaciones para manejo informacion hallazgos y reportes	Clasificada	0%	0%	100%	100%	50%	50%
	Sistema operativo Windows 7, Windows 8, Windows 10	Pública	100%	50%	100%	70%	100%	84%
	Virtualbox, Winware	Pública	100%	0%	0%	50%	50%	40%
[HW] Equipos informáticos (hardware)	Servidor de producción Servprod HP Proliant DL380 G9, Datacenter. IBM Power System S814 Servidores aplicaciones IBM Power System S822LC	Reservada	100%	70%	70%	100%	50%	78%
	HP Z238, Intel Core i7-7700 3.60GHz, 8GB, 1TB, Windows 10 Pro 64-bit, HP Allin-One 200-5030 y Intel (R) Core (TM) i5	Reservada	100%	600%	80%	100%	50%	78%
	Dell Core i3, i5 Equipos de escritorio salas de sistemas equipos de escritorio equipo administración	Reservada	100%	80%	100%	0%	100%	76%
	Portátiles DELL y HP	Reservada	100%	100%	50%	80%	70%	80%
	MyPAL A730W - Asus	Reservada	100%	80%	50%	100%	100%	86%
	MSA Store HP 2040 SAN Con hyper-v sistemas operativos Centos, Windows server 2012 y equipos cliente Windows 7	Reservada	100%	70%	80%	100%	100%	90%
	Dell PowerVault Network Attached Storage (PV701N, PV705N, PV735N)	Reservada	100%	0%	100%	100%	50%%	75%

Tipo de activo	Nombre de activos	Clasificación de la información	[D]	[C]	[I]	[A]	[T]	PROM
	Impresoras de multifunción Impresora Epson y lexmark	Reservada	100%	50%	80%	100%	0%	66%
	routers Cisco 1811 y 1812 de servicios, Switch core. IBM System Networking RackSwitch G8264 Equipos (router, Cisco MDS 9718 Multilayer Director for IBM Storage Networking	Reservada	100%	80%	80%	80%	80%	84%
	Integrados	Reservada	100%	80%	80%	80%	80%	84%
	Catalyst 2960 Plus Capa 2	Reservada	100%	80%	80%	80%	80%	84%
	Catalyst 9400 4 switch 24	Reservada	100%	80%	100%	70%	100%	90%
	Puertos Router CISCO 2900 Series.	Reservada	100%	70%	100%	50%	100%	84%
	WAN, 1 OPT, 4 LAN /DMZ ZYWALL110	Reservada	100%	80%	100%	70%	100%	90%
	Cisco WAP351 Wireless-N	Reservada	100%	80%	100%	80%	100%	92%
	Central Telefonica Ip Pbx Grandstream 6208	Reservada	100%	40%	10%	40%	100%	58%
	Telefono IP Cisco SPA942	Reservada	100%	50%	0%	20%	0%	34%
[COM] Redes de comunicaciones	Acceso telefónico ETB	Reservada	100%	0%	100%	20%	80%	60%
	Cisco 2600 y 3700	Reservada	10%	100%	10%	20%	0%	28%
	Cisco 2600	Reservada	100%	0%	100%	0%	0%	40%
	Red inalámbrica ETB	Reservada	100%	100%	100%	80%	50%	86%
	Internet ETB	Reservada	100%	100%	100%	80%	50%	86%
	Cableado estructurado	Reservada	100%	100%	80%	50%	100%	86%
[Media] Soportes de información	Discos duros externos para almacenamiento de información	Clasificada	0%	100%	10%	40%	100%	50%
	Manuales de usuario, Archivos documentos, resoluciones, actas administrativas. Copia de seguridad, documentos	Clasificada	0%	100%	100%	0%	80%	56%
	Documentos varios	Clasificada	100%	0%	0%	0%	0%	20%
	Proyecto, actas y documentos institucionales.	Clasificada	100%	0%	100%	0%	80%	56%
	Carpetas, reglamentos, acuerdos actas, planillas, proyectos y resoluciones.	Clasificada	100%	50%	50%	50%	0%	50%
	Fuentes de alimentación UPS.	Reservada	100%	40%	50%	100%	100%	78%

Tipo de activo	Nombre de activos	Clasificación de la información	[D]	[C]	[I]	[A]	[T]	PROM
[AUX] Equipamiento auxiliar	IBM SmartUPS DE 1400 VA 2 U 230 V PARA RACK							
	Ups de computadores energía temporal a los Servidores y demás dispositivos vitales en caso de fallas eléctricas inesperadas	Reservada	100%	50%	60%	100%	0%	62%
	Generador de energía AVR	Reservada	100%	0%	0%	100%	0%	40%
	Compu-aire	Reservada	100%	100%	50%	100%	0%	70%
	Red interna	Reservada	100%	10%	40%	100%	0%	50%
	Instalaciones para el suministro de energía	Reservada	100%	20%	50%	100%	0%	54%
	rack, armarios, mesas, archivadores, muebles,	Reservada	80%	0%	20%	20%	0%	24%
[L] Instalaciones	Edificación propia de la entidad	Pública	100%	0%	0%	0%	0%	20%
[P] Personal	Entidades usuarias	Pública	100%	0%	0%	0%	0%	20%
	Funcionarios	Clasificada	100%	0%	0%	0%	0%	20%
	Call Center	Clasificada	100%	0%	0%	0%	0%	20%
	Administrador aplicativo misional	Clasificada	100%	0%	0%	0%	0%	20%
	Director de TI	Pública	100%	0%	0%	0%	0%	20%
	Gestor de Bases de Datos	Pública	100%	30%	0%	0%	0%	20%
	Director/Coordinadores aplicativo misional	Pública	100%	40%	20%	0%	30%	26%
	Ingenieros de Software	Pública	100%	0%	0%	40%	0%	38%
	Contratistas	Pública	100%	0%	0%	30%	0%	28%
	Personal ETB, Soporte Técnico	Pública	100%	40%	0%	0%	20%	26%

Fuente: Propiedad de Autor

4. IDENTIFICACIÓN DE AMENAZAS DE LOS ACTIVOS DE INFORMACIÓN DE LA EMPRESA CASO DE ESTUDIO

4.1 IDENTIFICACIÓN Y VALORACIÓN DE LAS AMENAZAS

Los tipos de amenazas propuestas por la metodología Magerit, se procede a hacer el análisis de identificación y valoración de amenazas a los activos encontrados en la entidad.

Se podrá estimar en qué grado el activo es afectado sobre las dimensiones de seguridad que la metodología MAGERIT ha considerado como la Autenticidad (A), confidencialidad (C), integridad (I), disponibilidad (D) y la trazabilidad del servicio (T).

Se efectuará la valoración del impacto que tendrían las amenazas para los activos de la entidad en las cinco dimensiones de seguridad (Disponibilidad, I: Integridad, C: Confiabilidad, A: Autenticidad y T: Trazabilidad), teniendo en cuenta su frecuencia.
En la tabla 21 se encuentran los tipos de amenazas a que puede estar expuesto un activo

Tabla 21 tipos de amenazas

Nomenclatura	Tipos de amenazas	Definición
[N]	Desastres naturales	Hay accidentes naturales (terremotos, inundaciones). Ante esos avatares el sistema de información es víctima pasiva, pero de todas formas tendremos en cuenta lo que puede suceder
[I]	De origen industrial	Hay desastres industriales (contaminación, fallos eléctricos) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos.
[E]	Errores y fallos no intencionados	Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.
[A]	Ataques intencionados	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.

Fuente: Propiedad de Autor

En la tabla 22 se indica el valor del criterio según la frecuencia con que ocurre una amenaza.

Tabla 22 Escala de rango de frecuencia de amenazas

Valor	Criterio	
	Frecuencia	Rango de Frecuencia
100	[MF] Frecuencia muy alta	A diario
70	[F] Frecuencia alta	Una vez por semana
50	[FM] Frecuencia media	Una vez por mes
10	[FB] Frecuencia baja	Una vez cada seis meses
5	[PF] Frecuencia muy baja	Una vez cada año

Fuente: Propiedad de Autor

4.1.1 Evaluación de las amenazas a los activos:

Se representan los criterios de valoración según el riesgo que los activos pueden presentar en la entidad, de acuerdo al nivel de seguridad, teniendo en cuenta su escala valoración cualitativa según MAGERIT.

En la valoración de los activos encontrados en esta investigación se identificaron las amenazas que afectan a ellos, la valoración de frecuencia con que suceden y que dimensiones de seguridad les afectan.

La tabla 23 muestra la valoración de amenazas de los activos de la empresa caso de estudio.

Tabla 23 Valoración de amenazas

Tipo de activo	Nombre de activos	Amenaza	Frecuencia	[D]	[C]	[I]	[A]	[T]
[essential] Activos esenciales	Información financiera - Acuerdos - Licencias, Convenios, Actas - Informes, Autorizaciones Resoluciones Memorias	[E.1] Errores de los usuarios	100	-	100%	100%	100%	100%
		[E.18] Destrucción de información	70	-	50%	50%	100%	100%
		[E.19] Fugas de información	70	-	80%	80%	100%	100%
		[A.18] Destrucción de información	50		100%	100%	100%	100%
		[E.2] Errores del administrador	100	-	100%	100%	100%	100%
		[A.5] Suplantación de la identidad del usuario	100	-	100%	100%	100%	100%

Tipo de activo	Nombre de activos	Amenaza	Frecuencia	[D]	[C]	[I]	[A]	[T]
		[A.15] Modificación deliberada de la información	100	-	100%	100%	100%	100%
[arch] Arquitectura del sistema	ETB	[N.*] Desastres naturales	100	100%	-	-	-	-
		[E.1] Errores de los usuarios	10	100%	-	-	-	-
		[E.2] Errores del administrador	10	80%	-	-	-	-
		[A.11] Acceso no autorizado	100	100%	-	-	-	100%
[D] Datos / Información	Archivos de actas Resoluciones actos administrativos - Archivos de registros de actividad de los Sistemas de Información	[E.1] Errores de los usuarios	70	-	80%	80%	-	-
		[E.18] Destrucción de información	70	-	80%	80%	-	-
		[E.19] Fugas de información	70	-	80%	80%		
		[A.11] Acceso no autorizado	70	-	80%	-	-	-
	Copias de respaldo de seguridad de los del sistema (Ambientes, Producción Preproducción, Hallazgos y correo institucional), servidor, base de datos y los equipos de cómputo	[E.1] Errores de los usuarios	50	100%	100%	100%		
		[E.2] Errores del administrador	70	100%	80%	-	-	-
		[A.18] Destrucción de información	70	100%	80%	-	-	-
		[A.19] Revelación de información	50	-	80%	-	-	-
		[A.11] Acceso no autorizado	5	100%	100%	100%	100%	100%
	Datos de configuración de los equipos	[E.1] Errores de los usuarios	10	100%	100%	100%		
		[E.2] Errores del administrador	10	100%	100%	100%		
		[A.11] Acceso no autorizado	5	100%	-	-	-	-
		[A.18] Destrucción de información	50	-	80%	-	-	-
		E15. Alteración accidental de la información	70	-	80%	-	-	-
[S] Servicios	Informática / Soporte técnico Call Center - Página Web interna (Intranet) - Acceso transaccional a través de URL - Envío de login de usuario y clave de acceso	E1. Errores de usuarios	70	-	100%	100%	100%	-
		E9. Errores de re-encaminamiento	50	-	70	100%	80%	-
		E15. Alteración accidental de la información	5	-	-	-	-	-
		E19. Fugas de información	5	-	-	80%	-	-
		A7. Uso no previsto	10	-	100%	-	-	-
		A13. Repudio	70	-	-	-	-	-

Tipo de activo	Nombre de activos	Amenaza	Frecuencia	[D]	[C]	[I]	[A]	[T]
	- VPN Juniper - Directorio Activo - Módulo de administración - Token	A15. Modificación deliberada de información A24. Denegación del servicio	5	-	-	-	-	-
[SW] Aplicaciones (software)	Aplicación para el manejo de reportes - Programas de comunicación (correo electrónico, chat, llamadas telefónicas. - Aplicaciones para manejo información hallazgos y reportes	[E.19] Fugas de información	100	100%	80%	80%	100%	100%
		[E.20] vulnerabilidad de los programas.	100	100%	100%	100%	100%	100%
		[A.8] difusión de software dañino	100	100%	100%	100%	100%	100%
		[A.11] Acceso no autorizado al software.	100	100%		100%	100%	-
		[A.19] Software Ilegal	100	100%	-	-	-	-
		[E.2] errores del administrador	100	100%	-	100%	100%	-
		[E.15] Alteración accidental de la información	70	100%	100%	100%	100%	100%
		[E.18] Destrucción de información	50	100%	-	-	-	-
		[E.21] Errores de mantenimiento / actualización de programas (software)	10	70	-	-	-	-
	Visual basic 6, NET, NEtbeet, dreamweaver, Java, Macromedia_Flash_8_(Portable) - Internet Explorer, Chrome, Firefox - Servidor de páginas web - Virtualbox, Winware	[I.5] avería de origen físico o lógico	100	100%	-	-	-	100%
		[E.1] errores de Usuario	100	100%				100%
		[E.2] errores del administrador	100	100%	-	-	-	100%
		[E.20] vulnerabilidad de los programas.	100	100%	-	-	-	100%
		E21. Errores de mantenimiento, actualización de programas(software)	100	100%	-	-	-	100%
		[A. I.8] difusión de software dañino	100	100%	-	-	-	100%
		[A.11] Acceso no autorizado al software.	100	100%	-	-	-	100%
		[A.19] Software Ilegal	100	100%	-	-	-	100%
		[A.22] manipulación de programas	100	100%	-	-	-	100%
	Office 2013, 2016 winrar, Adobe Acrobat Reader – Mcafee - Correo electrónico - Sistema operativo Windows 7, Windows 8, Windows 10	[I.5] avería de origen físico o lógico	100	100%	-	-	-	100%
		[E.1] errores de usuario	100	100%	-	-	-	100%
		[E.2] errores del administrador	100	100%	-	-	-	100%
		[E.15] Alteración accidental de la información	100	100%	-	-	-	100%
		[E.18] Destrucción de información	100	100%	-	-	-	100%

Tipo de activo	Nombre de activos	Amenaza	Frecuencia	[D]	[C]	[I]	[A]	[T]
		[E.19] Fugas de información	100	100%	-	-	-	100%
		[E.20] vulnerabilidad de los programas.	100	100%	-	-	-	100%
		E21. Errores de mantenimiento, actualización de programas(software)	100	100%	-	-	-	100%
		[A.8] difusión de software dañino	100	100%	-	-	-	100%
		[A.11] Acceso no autorizado al software.	100	80%	-	-	-	100%
		[A.19] Software Ilegal	80	80%	-	-	-	100%
		[A.22] manipulación de programas	50	100%	-	-	-	100%
[HW] Equipos informáticos (hardware)	Servidor de producción Servprod HP Proliant Servidores aplicaciones - HP Z238, Intel Core i7-HP - Portátiles DELL y HP - Dell PowerVault Network Attached Storage - MyPAL A730W – Asus - Impresoras de multifunción Impresora Epson y lexmark – routers – RackSwitch - Equipos router – Integrados – Puertos - switch	N*. Desastre natural	5	100%	80%		100%	100%
		[I.4] contaminación electromecánica	10	100%	70	-	-	-
		[I.5] avería de origen físico o lógico	10	100%	100%	-	-	-
		[I.6] corte de suministro eléctrico	5	100%	80%	-	-	-
		[I.7]condiciones inadecuadas de temperatura humedad	10	100%	100%	-	-	-
		[E.2] errores del administrador	50	100%	100%	-	-	-
		[E.23] error de mantenimiento en los equipos	70	100%	80%	-	-	-
		[E.24] carencia de recursos físicos del computadores	70	80%	50%	-	-	-
		[A.6] Abuso de privilegios de acceso	10	80%	100%	-	-	-
		[A.7] Utilización del equipo para usos no autorizados [A.11] Acceso no autorizado al hardware.	10	50%	50%	-	-	-
		[A.25] Robo	5	100%	100%	100%	100%	100%
	Catalyst 2960 Plus Capa 2 - Catalyst 9400 4 switch 24 - Router CISCO 2900 Series - WAN, 1 OPT, 4 LAN /DMZ ZYWALL110 - Cisco WAP351 Wireless-N - Central Telefónica Ip Pbx	N*. Desastre natural	5	100%	100%			100%
		[I.5] avería de origen físico o lógico	10	100%	80%		100%	100%
		[I.6] corte de suministro eléctrico	10	100%	70	-	-	-
		[I.7] condiciones inadecuadas de temperatura humedad	5	100%	100%	-	-	-
		[E.2] errores del administrador	70	100%	80%	-	-	-
		[E.23] error de mantenimiento en los equipos	50	100%	50%	-	-	-

Tipo de activo	Nombre de activos	Amenaza	Frecuencia	[D]	[C]	[I]	[A]	[T]
	Grandstream 6208 - Teléfono IP Cisco SPA942	[A.6] Abuso de privilegios de acceso	70	100%	-	-	-	-
		[A.7] Utilización del equipo para usos no autorizados	100	100%	-	-	-	-
		[A.25] Robo	5	100%	100%	100%	100%	100%
[COM] Redes de comunicaciones	Acceso telefónico ETB - Red inalámbrica ETB - Internet ETB - Cableado estructurado	[A.7] abuso de los privilegios para ingreso al sistema no autorizado.	50	100%	80%	-	-	100%
		[A.9] desvío de información	10	100%	100%	-	-	100%
		[A.12] análisis de tráfico	100	100%	70	-	-	100%
		[A.14] intercepción de las comunicaciones	100	100%	50%	-	-	100%
		[A.19] divulgación de información	100	100%	-	-	-	100%
		[A.24] Denegación de servicio	10	100%	-	-	-	100%
		I.8. Fallo de servicios de comunicaciones	5	100%	-	-	-	100%
		[E.2] Error de usuario en la instalación y operación	10	100%	-	-	-	100%
		[E.9] Error de enrutamiento	5	100%	-	-	-	100%
		[E.18] perdida accidental de información	10	100%	100%	-	-	100%
		[E.19] codificación de información para fines mal intencionados	5	100%	-	-	-	100%
		[E.24] caída del sistema por agotamiento de recursos	50	100%	-	-	-	100%
		[A.5] vulnerabilidad del sistema	70	100%	-	-	-	100%
		[A.6] Abuso de privilegios de acceso	70	100%	-	-	-	100%
[Media] Soportes de información	Documentos varios - Manuales de usuario, Archivos documentos, resoluciones, actas administrativas. Copia de seguridad, documentos - Proyecto, actas	[E.25] pérdida de equipos	70	100%	-	-	-	-
		[A.11] acceso no autorizado.	50	50%	-	-	-	-
		[A.18] destrucción de la información	100	80%	-	-	-	-
		[A.23] manipulación de quipos	70	10	-	-	-	-
		[A.25] Robo	5	50%	-	-	-	-
		[N.*] Desastres naturales	10	80%	-	-	-	-
		[I.3] Otros desastres industriales	10		-	-	-	-

Tipo de activo	Nombre de activos	Amenaza	Frecuencia	[D]	[C]	[I]	[A]	[T]
	y documentos institucionales - Carpetas, reglamentos, acuerdos actas, planillas, proyectos y resoluciones - Discos duros externos para almacenamiento de información	[I.3] contaminación mecánica	70	80%	-	-	-	-
		[I.7] condiciones inadecuadas de temperatura o humedad	50	50%	-	-	-	-
		[I.10] Degradación de la vida útil del soporte de almacenamiento	50	50%	-	-	-	-
		[E.2] errores del administrador	70	80%	-	-	-	-
		[E.15] alteración de la información	50	70	-	-	-	-
		[E.18] destrucción del soporte de almacenamiento	50	-	-	-	-	100%
[AUX] Equipamiento auxiliar	Fuentes de alimentación UPS. V PARA RACK Ups de computadores energía temporal a los Servidores y demás dispositivos vitales en caso de fallas eléctricas inesperadas - Compu-aire - Generador de energía AVR	[N.*] Desastres naturales	5	100%	-	-	-	-
		[I.4] contaminación electromecánica	70	100%	80%	-	-	-
		[I.5] avería de origen físico o lógico	10	100%		-	-	-
		[I.6] corte de suministro eléctrico	50	100%	50%	-	-	-
		[I.E] condiciones de temperatura y humedad	50	100%		-	-	-
		[E.2] errores del administrador	70	100%	70	-	-	-
		[E.23] errores de mantenimiento de equipos de hardware	70	100%		-	-	-
		[E.25] pérdida de equipos	50	100%	100%	-	-	-
		[A.23] manipulación de quipos	10	100%		-	-	-
		[A.24] Denegación de servicio	10	100%	50%	-	-	-
		[A.25] Robo	10	100%		-	-	-
		[A.26] Ataque destructivo	10	100%	50%	50%		
	rack, armarios, mesas, archivadores, muebles,	N.*] Desastres naturales	5	100%	-	-	-	-
		[I.E] condiciones de temperatura y humedad	50	100%	-	-	-	-
		[A.25] Robo	5	100%	-	-	-	-
[L] Instalaciones	Edificación propia de la entidad	N*. Desastres naturales	10	100%	-	-	-	-
		I*. desastres industriales	10	100%	-	-	-	-
		A11. Acceso no autorizado	50	100%	-	-	-	-
[P] Personal	Entidades usuarias - administradores de sistemas - Usuarios – proveedores –	[E.7] deficiencias en el perfil del personal	70	100%	80%	-	-	-
		[E.28] indisponibilidad del personal	70	100%	50%	-	-	-
		[A.30] ingeniería social (picaresca)	70	100%	100%	-	-	-

Tipo de activo	Nombre de activos	Amenaza	Frecuencia	[D]	[C]	[I]	[A]	[T]
	Funcionarios - Call Center	[A.29] Extorsión	10	100%	-	-	-	-

Fuente: Propiedad de Autor

4.2 RIESGO POTENCIAL

La apreciación del riesgo potencial se toman los valores de la frecuencia de ocurrencia de cada una de las amenazas con referencia a los activos e impacto acumulado, esto porque los activos necesitan una acción urgente, de acuerdo a los valores estipulados.

En la tabla 24 se presentan las escalas de impacto, probabilidad y riesgo de los activos.

Tabla 24 Escalas

Escalas		
Impacto	**Probabilidad**	**Riesgo**
MA: muy alto	MA: prácticamente inseguro	MA: critico
A: alto	A: probable	A: importante
M: medio	M: posible	M: apreciable
B: bajo	B: poco probable	B: Bajo
MB: muy bajo	MB: muy raro	MB: despreciable

Fuente: GOBIERNO DE ESPAÑA. Magerit - versión 3.0: Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I - Método. Madrid: Ministerio de Hacienda y Administraciones Públicas

4.2.1 Evaluación del riesgo potencial de los activos:

La metodología MAGERIT nos permite identificar y valorar cada uno de los activos de información que se encuentran en una organización permitiendo identificar cuáles son los riesgos con su respectivo impacto

La tabla 25 muestra la valoración de riesgo potencial.

Tabla 25 Valoración del riesgo potencial

Tipo de activo	Nombre de activos	Impacto	Probabilidad	Riesgo
[essential] Activos esenciales	Información financiera	Muy alto	Prácticamente inseguro	Critico
	Acuerdos	Alto	Posible	Importante
	Licencias, Convenios, Actas	Alto	Posible	Importante
	Informes, Autorizaciones	Alto	Posible	Importante
	Resoluciones Memorias	Alto	Posible	Importante

Tipo de activo	Nombre de activos	Impacto	Probabilidad	Riesgo
[arch] Arquitectura del sistema	ETB	Muy alto	Posible	Critico
[D] Datos / Información	Archivos de actas Resoluciones actos administrativos	Alto	Posible	Importante
	Copias de respaldo de seguridad de los del sistema (Ambientes, Producción Preproducción, Hallazgos y correo institucional), servidor, base de datos y los equipos de cómputo	Muy alto	Prácticamente inseguro	Critico
	Datos de configuración de los equipos	Alto	Posible	Importante
	Archivos de registros de actividad de los Sistemas de Información	Alto	Posible	Importante
[S] Servicios	Informática / Soporte técnico Call Center	Alto	Prácticamente inseguro	Importante
	Página Web interna (Intranet)	Alto	Prácticamente inseguro	Importante
	Acceso transaccional a través de URL	Alto	Prácticamente inseguro	Importante
	Envío de login de usuario y clave de acceso	Alto	Prácticamente inseguro	Importante
	VPN Juniper	Medio	Poco probable	Bajo
	Directorio Activo	Muy alto	Prácticamente inseguro	Critico
	Módulo de administración	Muy alto	Prácticamente inseguro	Critico
	Token	Muy alto	Probable	Critico
[SW] Aplicaciones (software)	Macroprocesos o módulos Financieros	Muy alto	Prácticamente inseguro	Importante
	Visual basic 6, NET, NEtbeet, dreamweaver, Java, Macromedia_Flash_8_(Portable)	Alto	Prácticamente inseguro	Importante
	Internet Explorer, Chrome, Firefox	Medio	Probable	Bajo
	Servidor de páginas web	Alto	Prácticamente inseguro	Importante
	Mcafee	Alto	Prácticamente inseguro	Importante
	Programas de comunicación (correo electrónico, chat, llamadas telefónicas.	Muy alto	Posible	Critico
	Correo electrónico	Muy alto	Posible	Critico
	Office 2013, 2016 winrar, Adobe Acrobat Reader	Alto	Prácticamente inseguro	Importante
	Aplicaciones para manejo informacion hallazgos y reportes	Muy alto	Posible	Critico

Tipo de activo	Nombre de activos	Impacto	Probabilidad	Riesgo
	Sistema operativo Windows 7, Windows 8, Windows 10	Muy alto	Posible	Critico
	Virtualbox, Winware	Medio	Probable	Bajo
[HW] Equipos informáticos (hardware)	Servidor de producción Servprod HP Proliant DL380 G9, Datacenter. IBM Power System S814 Servidores aplicaciones IBM Power System S822LC	Muy alto	Posible	Critico
	HP Z238, Intel Core i7-7700 3.60GHz, 8GB, 1TB, Windows 10 Pro 64-bit, HP Allin-One 200-5030 y Intel (R) Core (TM) i5	Muy alto	Prácticamente inseguro	Critico
	Dell Core i3, i5 Equipos de escritorio salas de sistemas equipos de escritorio equipo administración	Muy alto	Prácticamente inseguro	Critico
	Portátiles DELL y HP	Alto	Prácticamente inseguro	Importante
	MyPAL A730W - Asus	Alto	Prácticamente inseguro	Importante
	MSA Store HP 2040 SAN Con hyper-v sistemas operativos Centos, Windows server 2012 y equipos cliente Windows 7	Muy alto	Prácticamente inseguro	Critico
	Dell PowerVault Network Attached Storage (PV701N, PV705N, PV735N)	Muy alto	Prácticamente inseguro	Critico
	Impresoras de multifunción Impresora Epson y lexmark	Muy alto	Prácticamente inseguro	Critico
	routers Cisco 1811 y 1812 de servicios, Switch core. IBM System Networking RackSwitch G8264 Equipos (router, Cisco MDS 9718 Multilayer Director for IBM Storage Networking	Muy alto	Prácticamente inseguro	Critico
	Catalyst 2960 Plus Capa 2	Muy alto	Prácticamente inseguro	Critico
	Catalyst 9400 4 switch 24	Muy alto	Prácticamente inseguro	Critico
	Puertos Router CISCO 2900 Series.	Muy alto	Prácticamente inseguro	Critico
	WAN, 1 OPT, 4 LAN /DMZ ZYWALL110	Alto	Prácticamente inseguro	Importante
	Cisco WAP351 Wireless-N	Alto	Prácticamente inseguro	Importante

Tipo de activo	Nombre de activos	Impacto	Probabilidad	Riesgo
	Central Telefonica Ip Pbx Grandstream 6208	Alto	Prácticamente inseguro	Importante
	Telefono IP Cisco SPA942	Alto	Prácticamente inseguro	Importante
[COM] Redes de comunicaciones	Acceso telefónico ETB	Muy alto	Prácticamente inseguro	Apreciable
	Cisco 2600 y 3700	Muy alto	Prácticamente inseguro	Apreciable
	Cisco 2600	Muy alto	Prácticamente inseguro	Critico
	Red inalámbrica ETB	Muy alto	Prácticamente inseguro	Critico
	Internet ETB	Muy alto	Prácticamente inseguro	Critico
	Cableado estructurado	Muy alto	Prácticamente inseguro	Critico
[Media] Soportes de información	Discos duros externos para almacenamiento de información	Media	Probable	Importante
	Manuales de usuario, Archivos documentos, resoluciones, actas administrativas. Copia de seguridad, documentos	Media	Probable	Importante
	Documentos varios	Medio	Poco probable	Bajo
	Proyecto, actas y documentos institucionales.	Media	Probable	Importante
	Carpetas, reglamentos, acuerdos actas, planillas, proyectos y resoluciones.	Medio	Poco probable	Bajo
[AUX] Equipamiento auxiliar	Fuentes de alimentación UPS. IBM SmartUPS DE 1400 VA 2 U 230 V PARA RACK	Muy alto	Poco probable	Bajo
	Ups de computadores energía temporal a los Servidores y demás dispositivos vitales en caso de fallas eléctricas inesperadas	Muy alto	Poco probable	Bajo
	Generador de energía AVR	Alto	Poco probable	Bajo
	Compu-aire	Alto	Poco probable	Bajo
	Red interna	Alto	Poco probable	Bajo
	Instalaciones para el suministro de energía	Alto	Poco probable	Bajo
	rack, armarios, mesas, archivadores, muebles,	Alto	Poco probable	Bajo
[L] Instalaciones	Edificación propia de la entidad	Bajo	Muy raro	Bajo
[P] Personal	Entidades usuarias	Medio	Posible	Apreciable
	Funcionarios	Medio	Posible	Apreciable
	Call Center	Medio	Posible	Apreciable
	Administrador aplicativo misional	Medio	Posible	Apreciable
	Director de TI	Alto	Probable	Importante

Tipo de activo	Nombre de activos	Impacto	Probabilidad	Riesgo
	Gestor de Bases de Datos	Medio	Posible	Apreciable
	Director/Coordinadores aplicativo misional	Alto	Probable	Importante
	Ingenieros de Software	Medio	Posible	Apreciable
	Contratistas	Medio	Posible	Apreciable
	Personal ETB, Soporte Técnico	Medio	Posible	Apreciable

Fuente: Propiedad de Autor

5 DECLARACIÓN DE APLICABILIDAD DE LOS CONTROLES DEL ANEXO A DE LA ISO 27001:2013

De acuerdo a la norma ISO 27001:2013 en cada una de las amenazas y vulnerabilidades, se determinan los controles para cada uno de los activos previamente identificados y clasificados.

5.1 DEFINICIÓN DE LOS CONTROLES

En la tabla 26 se relacionan los controles, especificando si la entidad caso de estudio cumple con la aplicación de los mismos

Tabla 26 Declaración de aplicabilidad de los controles anexo A de la norma ISO 27001:2013

A5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION**		**APLICA**		**CUMPLE**		**EVIDENCIA**
A5.1	**Orientación de la dirección para la gestión de la seguridad de la información**						
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes			**SI**	**NO**	**SI**	**NO**	
A5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	X		X		Si aplica porque para cumplir una regla de seguridad se deben definir las políticas que se usarán y se proveerán a los funcionarios para que estos entren a participar en el proceso de seguridad de la información de la entidad.
A5.1.2	Revisión de las políticas para la seguridad de la información.	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.	X		X		Si aplica porque para comprobar el cumplimiento de las políticas se debe hacer seguimiento, dependiendo de los objetivos y el alcance propuesto
A6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION**		**APLICA**		**CUMPLE**		**EVIDENCIA**
A6.1	**Organización interna**						
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.			**SI**	**NO**	**SI**	**NO**	
A6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades	X		X		Si aplica porque dependiendo del cargo que desempeñe el funcionario, se le asignará unas

		de la seguridad de la información.					funciones para llevar a cabo y dar continuidad al plan de seguridad de la información
A6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización		X		X	No aplica porque los funcionarios son responsables de la labor que se les establece y son conscientes de los resultados que puede traer un acto de imprudente o no correcto.
A6.1.3	Contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.	X		X		Si aplica porque se mantienen los contactos actualizados para incidentes de seguridad.
A6.1.4	Contacto con grupos de interés especial	Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad		X		X	No aplica porque no se tiene contacto con grupos de interés especial.
A6.1.5	Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	X		X		Si aplica la Dirección de Tecnología es la encargada de velar por la aplicación de una metodología de análisis y evaluación de riesgos en los proyectos.
A6.2	Dispositivos móviles y teletrabajo		**APLICA**		**CUMPLE**		**EVIDENCIA**
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles			**SI**	**NO**	**SI**	**NO**	
A6.2.1	Política para dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	X		X		Si aplica existen políticas de seguridad de la información específicas para los servicios móviles ya que son de gran importancia en la organización y son de uso exclusivo.
A6.2.2	Teletrabajo	Control: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	X		X		Si aplica maneja políticas de Teletrabajo dependiendo de los proyectos que requieran este trabajo

A7	SEGURIDAD DE LOS RECURSOS HUMANOS		APLICA		CUMPLE		EVIDENCIA
A7.1	Antes de asumir el empleo						
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.			SI	NO	SI	NO	
A7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.	X		X		La Entidad cuenta con los procedimientos de Selección y desvinculación de los funcionarios dentro del Proceso de Gestion de Talento Humano, con las políticas establecidas.
A7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	X		X		Si aplica se establecen políticas con la función pública para la contratación de los usuarios de planta y contratistas
A7.2	Durante la ejecución del empleo		APLICA		CUMPLE		EVIDENCIA
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.			SI	NO	SI	NO	
A7.2.1	Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	X		X		Si aplica la Entidad establece en los contratos la obligatoriedad del cumplimiento de los requisitos del SGSI
A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones	X		X		Si aplica el funcionario o contratista deben ser capacitados para el buen uso de la seguridad de la información

		regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.					
A7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	X		X		Si aplica porque existen unas sanciones para quienes infrinjan las normas y políticas establecidas.
A7.3	Terminación y cambio de empleo		**APLICA**		**CUMPLE**		**EVIDENCIA**
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo			**SI**	**NO**	**SI**	**NO**	
A7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	X		X		Si aplica la entidad cuenta con los procedimientos de Selección y desvinculación de los funcionarios dentro del proceso de Gestion de Talento Humano
A8	**GESTION DE ACTIVOS**		**APLICA**		**CUMPLE**		**EVIDENCIA**
A8.1	**Responsabilidad por los activos**						
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas.			**SI**	**NO**	**SI**	**NO**	
A8.1.1	Inventario de activos	Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	X		X		Si aplica la entidad cuenta con inventario de activos, el cual se encuentra en custodia de DT
A8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.	X		X		Si aplica la entidad cuenta con inventario de activos, el cual se encuentra en custodia de DT e indica el dueño del activo

A8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	X		X		La entidad cuenta con la política de activos de información que permitan proteger los activos relevantes en la institución
A8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	X		X		Si aplica en el momento que un funcionario, contratista o pasante salda de la entidad debe devolver todos los activos a cargo para obtener el paz y salvo.
A8.2	Clasificación de la información		**APLICA**		**CUMPLE**		**EVIDENCIA**
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización**.**			**SI**	**NO**	**SI**	**NO**	
A8.2.1	Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	X		X		Si aplica toda la información requiere de un trato y cuidado muy especial por ser muy importante
A8.2.2	Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	X		X		Si aplica la entidad cuenta con un sistema de clasificación de la información
A8.2.3	Manejo de activos	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	X		X		Si aplica existe en la entidad una clasificación de los activos
A8.3	Manejo de medios		**APLICA**		**CUMPLE**		**EVIDENCIA**

Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios			**SI**	**NO**	**SI**	**NO**	
A8.3.1	Gestión de medio removibles	Control: Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.		X		X	No aplica por la sensibilidad de la información que se maneja no se permite el uso de medios removibles
A8.3.2	Disposición de los medios	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	X		X		Si aplica porque los activos que sirven como medios se deben tener funcionando en su totalidad, para el instante que sean requeridos
A8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.		X		X	No aplica porque no se transporta información físicamente.
A9	**CONTROL DE ACCESO**		**APLICA**		**CUMPLE**		**EVIDENCIA**
A9.1	**Requisitos del negocio para el control de acceso**						
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.			**SI**	**NO**	**SI**	**NO**	
A9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	X		X		Si aplica porque los usuarios que manejan el sistema de información deben acceder a este a través de un login y un password y firma digital
A9.1.2	Acceso a redes y a servicios en red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	X		X		Si aplica existen políticas de grupos de usuarios con accesos a la red según la necesidad de su cargo.
A9.2	Gestión de acceso de usuarios		**APLICA**		**CUMPLE**		**EVIDENCIA**
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.			**SI**	**NO**	**SI**	**NO**	
A9.2.1	Registro y cancelación del registro de usuarios	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios,	X		X		Si aplica la entidad cuenta con una política de control de acceso y el procedimiento de asignación de permisos

		para posibilitar la asignación de los derechos de acceso.					
A9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	X		X		Si aplica la entidad cuenta con una política de control de acceso y el procedimiento de asignación de permisos
A9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	X		X		Si aplica porque todos los funcionarios tienen diferentes privilegios, dependiendo del rol que desempeñen.
A9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	X		X		Si aplica porque cada funcionario del sistema tiene clave de acceso
A9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	X		X		Si aplica entidad cuenta con una política de control de acceso y el procedimiento de asignación de permisos
A9.2.6	Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	X		X		No aplica porque no existen usuarios externos a las instalaciones.
A9.3	Responsabilidades de los usuarios		**APLICA**		**CUMPLE**		**EVIDENCIA**
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.			**SI**	**NO**	**SI**	**NO**	
A9.3.1	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	X		X		Si aplica porque existen políticas para los diferentes usuarios del sistema, uso de contraseñas.

A9.4	Control de acceso a sistemas y aplicaciones		APLICA		CUMPLE		EVIDENCIA
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.			SI	NO	SI	NO	
A9.4.1	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	X		X		Si aplica porque la información no está disponible para todos los usuarios sino hace una clasificación
A9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	X		X		Si aplica la entidad cuenta con una politica de control de acceso y el procedimiento de asignación de permisos
A9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	X		X		Si porque se establecen unos parámetros para tener claves con alta seguridad
A9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	X		X		Si aplica dentro de las políticas esta restringuido la instalación de cualquier software, necesitando usuarios de administrador
A9.4.5	Control de acceso a códigos fuente de programas	Control: Se debe restringir el acceso a los códigos fuente de los programas.	X		X		Si aplica el acceso a código fuente solo está habilitado para el área de desarrollo
A10	**CRIPTOGRAFIA**		APLICA		CUMPLE		EVIDENCIA
A10.1	Controles criptográficos						
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información			SI	NO	SI	NO	
A10.1.1	Política sobre el uso de controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	X		X		Si aplica existe una política de seguridad que documenta el uso de los controles criptográficos,

A10.1.2	Gestión de llaves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	X		X		Si aplica existe una política de seguridad que documenta el proceso y ciclo de vida de las llaves criptográficas, la utilización de firmas digitales para el intercambio de información con entidades.
A11	**SEGURIDAD FISICA Y DEL ENTORNO**		**APLICA**		**CUMPLE**		**EVIDENCIA**
A11.1	Áreas seguras						
Objetivo: Prevenir el acceso físico no autorizado, el daño de la interferencia a la información y a las instalaciones de procesamiento de información de la organización.			**SI**	**NO**	**SI**	**NO**	
A11.1.1	Perímetro de seguridad física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.	X		X		Si aplica la entidad garantiza la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro, en todas sus instalaciones, para el control de las amenazas físicas externas e internas y las condiciones medioambientales
A11.1.2	Controles de acceso físicos	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	X		X		Si aplica el acceso físico a la infraestructura que contiene el hardware de las operaciones críticas está controlado por medio de lectores biométricos y tarjetas de proximidad que permiten el acceso a sólo el personal autorizado y registran la fecha y hora de acceso.
A11.1.3	Seguridad de oficinas, recintos e instalaciones.	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.	X		X		Si aplica para la seguridad de oficinas e instalaciones, se cuenta con personal de seguridad y cámaras de seguridad que monitorean permanentemente el ingreso y salida de personal a las mismas.
A11.1.4	Protección contra amenazas externas y ambientales.	Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	X		X		Si aplica la entidad cuenta con un Plan de Continuidad del Negocio que le permite recuperarse de incidentes
A11.1.5	Trabajo en áreas seguras.	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.					Si aplica cuenta con áreas seguras que buscan proteger los activos de información de las

							amenazas naturales y ambientales
A11.1.6	Áreas de carga, despacho y acceso público	Control: Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	X		X		No aplica porque no se cuenta con áreas de despacho
A11.2	Equipos		**APLICA**		**CUMPLE**		**EVIDENCIA**
Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.			**SI**	**NO**	**SI**	**NO**	
A11.2.1	Ubicación y protección de los equipos	Control: Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	X		X		Si aplica los equipos de cómputo son ubicados y protegidos para reducir la exposición a riesgos ocasionados por amenazas ambientales y de acceso no autorizado, y existen políticas de seguridad de la información documentadas para su uso.
A11.2.2	Servicios de suministro	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	X		X		Si aplica los centros de procesamiento de datos están protegidos con respecto a posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía está de acuerdo con las especificaciones del fabricante o proveedor de cada equipo.
A11.2.3	Seguridad en el cableado.	Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	X		X		Si aplica el cableado eléctrico está separado del cableado de datos previniendo así interferencias y están protegidos físicamente con canaleta en caso de instalación interior, o con tubo metálico en caso de instalación tipo intemperie

A11.2.4	Mantenimiento de los equipos.	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	X		X		Si aplica el mantenimiento preventivo de los equipos se realiza de acuerdo con los intervalos de servicio y especificaciones recomendadas por el
A11.2.5	Retiro de activos	Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa	X		X		Si aplica el jefe de mesa de ayuda en concordancia con el promotor de la seguridad de la información documenta el retiro de los activos.
A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	X		X		Si aplica porque los activos si se sacan de las instalaciones
A11.2.7	Disposición segura o reutilización de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobre escrito en forma segura antes de su disposición o reúso.	X		X		Si aplica se realiza borrado seguro de la información o devolución.
A11.2.8	Equipos de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	X		X		Si aplica existe un plan de capacitación de concientización a los funcionarios sobre la seguridad de la información y los riesgos a los que están expuestos los activos. Los usuarios deberán cerrar la sesión cuando hayan terminado, de igual forma los equipos de cómputo cuentan con un mecanismo de bloqueo automático como el de protector de pantalla después de 5 minutos de inactividad.

A11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	X		X		Si aplica los funcionarios garantizan que la información confidencial física es almacenada en gabinetes de forma segura impidiendo su acceso físico a personas no autorizadas
A12	**SEGURIDAD DE LAS OPERACIONES**		**APLICA**		**CUMPLE**		**EVIDENCIA**
A12.1	Procedimientos operacionales y responsabilidades						
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.			**SI**	**NO**	**SI**	**NO**	
A12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	X		X		Si aplica los empleados documentan los procedimientos de las operaciones relativas a la seguridad de la información de cada uno de los activos.
A12.1.2	Gestión de cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	X		X		Si aplica porque se deben hacer las respectivas actualizaciones si el negocio lo requiere
A12.1.3	Gestión de capacidad	Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	X		X		Si aplica se realiza un monitoreo continuo a los recursos y la adquisición de los nuevos y se proyecta de acuerdo con las necesidades críticas de la entidad.
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	X		X		Si aplica los ambientes de desarrollo, pruebas y producción, están separados en forma física o virtualizados. La transferencia de software del ambiente de pruebas al ambiente de producción será documentada, y resguardada con un backup
A12.2	Protección contra códigos maliciosos		**APLICA**		**CUMPLE**		**EVIDENCIA**

Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.			**SI**	**NO**	**SI**	**NO**	
A12.2.1	Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.					Si aplica existe una política documentada de actualización de todo el software utilizado, antivirus y sistema operativo, implementando controles para prevenir y detectar código malicioso, lo cual se basa en software, concienciación de usuarios y gestión del cambio.
A12.3	Copias de respaldo		**APLICA**		**CUMPLE**		**EVIDENCIA**
Objetivo: Proteger contra la perdida de datos			**SI**	**NO**	**SI**	**NO**	
A12.3.1	Respaldo de la información	Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	X		X		Si aplica se realizan las copias de seguridad de toda la información a intervalos programados y de acuerdo a las políticas de seguridad. El procedimiento es documentado y se realizan pruebas de recuperación a intervalos programados.
A12.4	Registro y seguimiento		**APLICA**		**CUMPLE**		**EVIDENCIA**
Objetivo: Registrar eventos y generar evidencia			**SI**	**NO**	**SI**	**NO**	
A12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	X		X		Si aplica se revisan periódicamente los registros de los usuarios y las actividades relativas a la seguridad de la información. El proceso es auditado y documentado, Los registros de auditoría de los sistemas de información están consolidados en ambientes separados a los transaccionales.
A12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	X		X		Si aplica toda la información se debe proteger contra las alteraciones que se pueden presentar o el acceso no autorizado
A12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	X		X		Si aplica las acciones y registros de los administradores son almacenados y protegidos de cualquier modificación.

A12.4.4	Sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	X		X		No aplica ya que no es necesario la sincronización de los relojes
A12.5	Control de software operacional		**APLICA**		**CUMPLE**		**EVIDENCIA**
Objetivo: Asegurarse de la integridad de los sistemas operacionales			**SI**	**NO**	**SI**	**NO**	
A12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	X		X		Si aplica Existe una documentación sobre el procedimiento de instalación de los sistemas operativos y software, que cumple con las políticas de seguridad de la información, solo usuarios administradores pueden realizar la instalación de software.
A12.6	Gestión de la vulnerabilidad técnica		**APLICA**		**CUMPLE**		**EVIDENCIA**
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas			**SI**	**NO**	**SI**	**NO**	
A12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	X		X		Si aplica existe una metodología de análisis y evaluación de riesgos sistemática y documentada, a cargo del Área de planeación de la entidad, el cual realiza el análisis de la explotación de vulnerabilidades conocidas, que podrían poner en riesgo la plataforma tecnológica institucional y su información, por tanto, estas son adecuadamente gestionadas y remediadas.
A12.6.2	Restricciones sobre la instalación de software	Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	X		X		Si aplica la instalación de software es realizada sólo por el personal autorizado y con software probado y licenciado, el procedimiento de instalación es documentado y ningún usuario final, tiene privilegios de usuario administrador.
A12.7	Consideraciones sobre auditorias de sistemas de información		**APLICA**		**CUMPLE**		**EVIDENCIA**
Objetivo: Minimizar el impacto de las actividades de auditoria sobre los sistemas operativos			**SI**	**NO**	**SI**	**NO**	

A12.7.1	Controles de auditorías de sistemas de información	Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	X		X		Si aplica el procedimiento es documentado y se coordinan las actividades previas con el fin de no afectar la disponibilidad del servicio.
A13	**SEGURIDAD DE LAS COMUNICACIONES**		**APLICA**		**CUMPLE**		**EVIDENCIA**
A13.1	Gestión de la seguridad de las redes						
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.			**SI**	**NO**	**SI**	**NO**	
A13.1.1	Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	X		X		Si aplica través del proceso de direccionamiento tecnológico se implementan controles de seguridad de la red, para lo cual usa técnicas de seguridad de la Red, garantizando la confidencialidad e integridad de la información que se transmite a través de las redes.
A13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	X		X		Si aplica el acceso a la red de los proveedores de servicio de red es monitoreado y controlado, están documentados los procedimientos de chequeo del tráfico de la red, monitoreo de los puertos en la red, y auditoría, trazabilidad y respaldo de archivos de log's
A13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	X		X		Si aplica se utiliza dispositivos de seguridad firewalls, para controlar el acceso de una red a otra, la segmentación se realiza en equipos de enrutamiento mediante la configuración de control de acceso y configuraciones de VLAN´s, en los equipos de conmutación.
A13.2	Transferencia de información		**APLICA**		**CUMPLE**		**EVIDENCIA**
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.			**SI**	**NO**	**SI**	**NO**	

A13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	X		X		Si aplica las políticas y procedimientos para de transferencia de la información están adecuadamente documentados y se aplican los mecanismos de seguridad necesarios para garantizar la confidencialidad e integridad de la información.
A13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	X		X		Si aplica existen documentos y acuerdos para la transferencia de información que garanticen su confidencialidad e integridad, la entrega de información se realiza bajo el deber de reserva, así mismo se documentan los controles.
A13.2.3	Mensajería Electrónica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	X		X		Si aplica está asociada a los servicios de correo electrónico de sus dominios y a la plataforma de comunicaciones unificada, está regulada por los términos de uso adecuado.
A13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	X		X		Si aplica ya que se establecen los acuerdos de confidencialidad y no divulgación, dejando claro las consecuencias que esto acarrearía
A14	**Adquisición, desarrollo y mantenimiento de sistemas**		**APLICA**		**CUMPLE**		**EVIDENCIA**
A14.1	Requisitos de seguridad de los sistemas de información						
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes**.**			**SI**	**NO**	**SI**	**NO**	

A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	X		X		Si aplica existe una política que establece los requisitos relativos de la seguridad de la información, para la adquisición de productos se contemplan características de seguridad y realiza un proceso formal de pruebas, que hace parte del proceso de evaluación de las ofertas.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Control: La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	X		X		Si aplica la dirección de tecnología implementan una Infraestructura de Llave Pública PKI mediante algoritmos fuertes de cifrado que garanticen la confidencialidad e integridad de la información que se transmite a través de las redes.
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	X		X		Si aplica ya que se debe garantizar que la información enviada en cada transacción llegue de forma correcta y segura a su destino final
A14.2	Seguridad en los procesos de Desarrollo y de Soporte		**APLICA**		**CUMPLE**		**EVIDENCIA**
Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.			**SI**	**NO**	**SI**	**NO**	
A.14.2.1	Política de desarrollo seguro	Control: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	X		X		Si aplican existen metodologías para la definición de requerimientos de software y para la realización de pruebas al software desarrollado. Así mismo, asegurará que todo sistema de información adquirido, desarrollado por

							terceros o al interior de la entidad, cuente con el nivel de soporte requerido por la entidad.
A.14.2.2	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	X		X		Si aplica se encuentra documentado un procedimiento de control de cambios, en el cual todo cambio es evaluado previamente tanto en los aspectos técnicos como de seguridad.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	X		X		Si aplica existe documentación sobre la implementación de las nuevas aplicaciones, se realizan revisiones con el fin de evitar fallas que afecten la disponibilidad de los mismos.
A.14.2.4	Restricciones en los cambios a los paquetes de software	Control: Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	X		X		Si aplica está documentado un procedimiento de control de cambios, en el cual las modificaciones de paquetes de software suministrados por un proveedor se analizan, se evalúan se guarda una copia del software a modificar, documentando los cambios realizados.
A.14.2.5	Principio de Construcción de los Sistemas Seguros.	Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	X		X		Si aplica se apoya efectivamente a mejorar los estándares de seguridad dentro del proceso de construcción.
A.14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el	X		X		Si aplica se busca brindar seguridad a los aplicativos institucionales desde el momento mismo del levantamiento de requerimientos y que las necesidades de seguridad, hagan parte integral de las decisiones arquitecturales del software a construir y/o adquirir.

		ciclo de vida de desarrollo de sistemas.					
A.14.2.7	Desarrollo contratado externamente	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	X		X		Si aplica los funcionario evalúan el software desarrollado externamente y prueban que cumpla con los requisitos de seguridad establecidos en las políticas de seguridad de la información, a través de la Dirección de Tecnología
A.14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	X		X		Si aplica se realizan pruebas de seguridad a los sistemas y documentan los procedimientos.
A.14.2.9	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	X		X		Si aplica se realizan pruebas a los sistemas antes de su salida a producción.
A14.3	Datos de prueba		**APLICA**		**CUMPLE**		**EVIDENCIA**
Objetivo: Asegurar la protección de los datos usados para pruebas.			**SI**	**NO**	**SI**	**NO**	
A.14.3.1	Protección de datos de prueba	Control Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	X		X		Si aplica hay una política documentada donde se establece que las pruebas de los sistemas de información se realizan en ambientes de pruebas, coordinados con la Dirección de Tecnología
A15	**RELACIONES CON LOS PROVEEDORES**		**APLICA**		**CUMPLE**		**EVIDENCIA**
A15.1	Seguridad de la información en las relaciones con los proveedores.						
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.			**SI**	**NO**	**SI**	**NO**	
A15.1.1	Política de seguridad de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la	X		X		Si aplica existe una política de seguridad de la información relacionada con los proveedores, se debe diligenciar y firmar los acuerdos de confidencialidad y acuerdos de intercambios de

		organización se deben acordar con estos y se deben documentar.					información con personal externo, sedes y dependencias
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	X		X		Si aplica hay acuerdos documentados con cada uno de los proveedores para el tratamiento de la seguridad de la información y los riesgos asociados, los cuales son formalizados en cada uno de los contratos establecidos.
A15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	X		X		Si aplica existen los acuerdos documentados con cada uno de los proveedores para el tratamiento de la seguridad de la información y los riesgos asociados. Se deja una cláusula de firma de confidencialidad, estudios de confiabilidad, y acuerdos de nivel de servicio como acuerdos de soporte, servicio y garantías.
A15.2	Gestión de la prestación de servicios de proveedores		**APLICA**		**CUMPLE**		**EVIDENCIA**
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores			**SI**	**NO**	**SI**	**NO**	
A15.2.1	Seguimiento y revisión de los servicios de los proveedores	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	X		X		Si aplica existen los acuerdos documentados con cada uno de los proveedores para el tratamiento de la seguridad de la información y los riesgos asociados, y se asigna un supervisor por cada contrato, el cual es el encargado de hacer seguimiento y cumplimiento de las obligaciones de los proveedores que suministran algún servicio o bien a la entidad.

A15.2.2	Gestión del cambio en los servicios de los proveedores	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la revaluación de los riesgos.	X		X		Si aplica se da aplicación al procedimiento de gestión de cambios, en un comité se realiza el concepto para aprobar o denegar cambios dentro de la plataforma tecnológica de la entidad o servicios de sistemas de información, actividad que es desarrollara por la Dirección de Tecnología
A16	**GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION**		**APLICA**		**CUMPLE**		**EVIDENCIA**
A16.1	Gestión de incidentes y mejoras en la seguridad de la información						
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.			**SI**	**NO**	**SI**	**NO**	
A16.1.1	Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	X		X		Si aplica se tienen documentado los procesos y procedimientos para los incidentes de la seguridad de la información. Se tiene documentado el plan de Continuidad del negocio donde están identificados claramente los responsables de su ejecución.
A16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	X		X		Si aplica la entidad cuanta con un procedimiento de atención de incidentes y una guía para la atención de eventos e incidentes informáticos.

A16.1.3	Reporte de debilidades de seguridad de la información	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	X		X		Si aplica existen los formatos documentados disponibles en la intranet para que los empleados reporten las debilidades de la seguridad de la información, los canales para reportar debilidades de seguridad de la información
A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	X		X		Si aplica ya que al llevar registro sobre los diferentes eventos ocurridos en cuanto la seguridad va hacer más fácil de tomar decisiones y corregir errores de manera más rápida en situaciones futuras
A16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	X		X		Si aplica está compuesto por un equipo de expertos en seguridad de la información, quienes velan por la prevención, atención e investigación de incidentes que afecten la seguridad de la información. La atención de incidentes está documentada mediante el procedimiento atención a incidentes.
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.	X		X		Si aplica los incidentes de la seguridad de la información son documentados especificando las vulnerabilidades, amenazas, riesgos y los posibles controles de seguridad a implementar constituyendo así una base de conocimiento.
A16.1.7	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	X		X		Si aplica existen formatos y documentos para recoger la evidencia y emitirlos a las autoridades competentes, según corresponda.

A17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO		APLICA		CUMPLE		EVIDENCIA
A17.1	**Continuidad de Seguridad de la información**						
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.			**SI**	**NO**	**SI**	**NO**	
A17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	X		X		Si aplica ya que no se sabe cuándo se asuman problemas que no están a nuestro alcance de evitarlos por lo que se debe tener planes de continuidad, aunque ocurran dichos incidentes
A17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	X		X		Si aplica ya que durante una situación inesperada se debe saber cómo proceder y controlada dicha situación, documentando todo lo que se haga.
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	X		X		Si aplica se tienen definidos intervalos de tiempo para la respectiva revisión y prueba de la funcionalidad de los procesos, procedimientos y controles de continuidad de la seguridad de la información, para asegurar que son coherentes con los objetivos de continuidad de la seguridad de la información,
A17.2	Redundancias		**APLICA**		**CUMPLE**		**EVIDENCIA**
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.			**SI**	**NO**	**SI**	**NO**	
A17.2.1	Disponibilidad de instalaciones de procesamiento de información	Control: Las instalaciones de procesamientos de información se deben implementar con redundancia	X		X		Si cumple los requisitos contractuales están identificados y se cumplen con los requerimientos exigidos por la ley

		suficiente para cumplir los requisitos de disponibilidad.					
A18	**CUMPLIMIENTO**		**APLICA**		**CUMPLE**		**EVIDENCIA**
A18.1	Cumplimiento de requisitos legales y contractuales						
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.			**SI**	**NO**	**SI**	**NO**	
A18.1.1	Identificación de la legislación aplicable.	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	X		X		Si aplica la entidad posee procedimientos para la protección de propiedad intelectual, los cuales tienen como objetivo evitar incumplimientos de carácter legal ante el uso de material o software patentado. todos los funcionarios que hacen uso de la plataforma tecnológica institucional solo pueden utilizar software autorizado
A18.1.2	Derechos propiedad intelectual (DPI)	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	X		X		Si aplica ya que se deben tener los permisos necesarios para hacer uso tanto del software como de los procesos de la entidad
A18.1.3	Protección de registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	X		X		Si aplica los registros están protegidos físicamente contra alteración, modificación, pérdida y acceso de usuarios no autorizados,

A18.1.4	Privacidad y protección de información de datos personales	Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.	X		X		Si aplica los datos personales son almacenados y protegidos de acuerdo con la ley y regulaciones. Mediante control de acceso por usuario, y procedimiento de control de registro establecido para tal fin.
A18.1.5	Reglamentación de controles criptográficos.	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	X		X		Si aplica ya que al encriptar la información se está protegiendo los datos y cumpliendo con los acuerdos de ley
A18.2	Revisiones de seguridad de la información		**APLICA**		**CUMPLE**		**EVIDENCIA**
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.			**SI**	**NO**	**SI**	**NO**	
A18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	X		X		Si aplica existe documentación para la realización de la auditoría interna del Sistema de Gestión de la Seguridad de la Información. Control interno o un organismo auditor externo, realiza revisiones independientes sobre el cumplimiento de la política de seguridad de la información.
A18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	X		X		Si aplica existe documentación para la realización de la auditoría interna del Sistema de Gestión de la Seguridad de la Información con el fin de verificar el nivel de cumplimiento, controles y políticas de seguridad de la información.

A18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	X		X		Si cumple se verifica los sistemas de información, equipos de procesamiento, bases de datos y demás recursos tecnológicos, para que cumplan con los requisitos de seguridad esperados teniendo en cuenta las solicitudes internas.

Fuente: Propiedad de Autor

6 DISEÑO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BASADAS EN LA NORMA ISO 27001:2013

6.1. POLITICAS DE SEGURIDAD DE LA INFORMACION

6.1.1. Políticas generales de la seguridad informática

Las Políticas de Seguridad de la Información, surgen como una herramienta institucional para concienciar a cada uno de los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la entidad sobre la importancia y sensibilidad de la información y servicios críticos, de tal forma que le permitan desarrollar adecuadamente sus labores y cumplir con su propósito misional.

Objetivo

Definir las pautas de propósito general para asegurar una adecuada protección de la información de la entidad

Aplicabilidad

Estas son políticas que aplican a la Gerencia, Subgerencias, Jefes de Dependencias, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de la organización.

Directrices

- Mantener un inventario actualizado de sus activos de información, bajo la responsabilidad de cada propietario de información y centralizado por el Área Información y Sistemas.
- La política de seguridad de la información deberá ser informada a los funcionarios y usuarios externos.

6.1.2. Política para dispositivos móviles y teletrabajo

El uso de equipos asignados, fuera de la entidad, está restringido equipos portátiles y móviles, se aprueba el uso de los dispositivos móviles autorizados por la entidad por parte de los empleados de la entidad, siempre y cuando no pongan en riesgo la Seguridad de la Información.

Objetivo

Garantizar la seguridad de la información en los equipos fuera de las instalaciones de la entidad

Aplicabilidad

Está dirigida a todos los funcionarios que laboran en ella

Directrices

- No se permite almacenar en dispositivos móviles personales, información de la entidad que no esté clasificada como pública.

- El software instalado en los dispositivos móviles debe estar totalmente licenciado y autorizado por la Dirección de Tecnología.

- Es responsabilidad de los empleados garantizar el adecuado uso del medio móvil asignado, conectándolo siempre a redes confiables, que no sean de acceso público para evitar que se propague cualquier amenaza pertinente a estos dispositivos virus, troyanos, malware.

6.1.3. Política de seguridad para los recursos humanos

Todos los funcionarios deben tener sus perfiles definidos para el uso de los recursos de los activos de información, con el fin de organizar y acomodar una adecuada Política de Seguridad

Objetivo
Certificar que el personal que labora en la entidad cumpla con las políticas de seguridad de la información.

Aplicabilidad

La Política de Seguridad de recurso humano es de aplicación obligatoria para todo funcionario.

Directrices

- De acurdo a las funciones establecidas de cada funcionario se definirá el nivel de seguridad.
- Todos los funcionarios, personal de prestación de servicios o cualquier otro tipo de vinculación con la entidad, deben diligenciar los formatos Declaración de Confidencialidad y Compromiso con la Seguridad de la Información.

- El funcionario está comprometido a solicitar capacitación necesaria de acuerdo a su perfil y su área desempeño para el adecuado desarrollo de sus actividades.
- Todos los candidatos a empleados de la entidad deberán presentar una verificación de antecedentes legales.

6.1.4. Política de seguridad de control de acceso

Contempla los controles de acceso que se deben tener en cuenta de acuerdo a los perfiles de cada funcionario de la entidad, para tener acceso adecuado a los sistemas de información y recursos tecnológicos, validando su autenticación, autorización y auditoría.

Objetivo

Fijar el nivel de control de acceso a la información de acuerdo a las funciones desempeñadas de cada funcionario.

Aplicabilidad

La Políticas de seguridad para funcionarios

Directrices

- El control de acceso a la información a través del sistema de información que posee la entidad se realiza a través de roles que administran los privilegios de los usuarios dentro del sistema de información.

- Los usuarios no podrán suministrar información sin previa autorización.

- La clave del usuario será cambiada cada mes y no se puede repetir o con los requisitos mínimos.
- Los usuarios según sus privilegios tendrán unas normas que cumplir de acuerdo a los activos de información que vaya a manejar.

6.1.5. Política Gestión de activos

Salvaguardar debidamente los activos asociados a las instalaciones de procesamiento de información y de información y asegurar su uso correcto.

Objetivo

Implantar responsabilidades en el manejo y uso de los activos de información.

Aplicabilidad

Grupo de seguridad de la información Contratistas funcionarios y proveedores

Directrices

- Para verificar el inventario se debe aplicar el procedimiento establecido, en la cual se describe la metodología que permite identificar, valorar y clasificar los activos de información, servicios, medios de procesamiento que soportan la gestión de los procesos y establecer su nivel de clasificación de acuerdo con las escalas contenidas en la misma.

- Tramitar con el responsable escogido la identificación, valoración y clasificación de sus activos de información dentro del inventario, manteniendo información detallada para cada activo sobre su valoración y clasificación en confidencialidad, integridad, disponibilidad. Igualmente deberá hacer el tratamiento adecuado correspondiente a su clasificación y corrección de inconsistencias detectadas.

- Los activos asociados a procesamiento de la información deberán ser identificados y mantenerse un inventario actualizado de los mismos.

- Todos los empleados y usuarios externos deberán devolver todos los activos de la entidad en la terminación de su empleo.

6.1.6. Política de gestión de contraseñas

La identificación y autenticación de usuarios se encuentra definido en la guía de usuarios.

Objetivo

Tramitar de manera segura el acceso de los usuarios a los sistemas de información de la entidad.

Aplicabilidad

Grupo de seguridad de la información y Dirección de Tecnología

Directrices

- Permite que los usuarios seleccionen y cambien sus propias contraseñas.

- Forzar a los usuarios cambiar sus contraseñas cuando ingresan por primera vez.

- Lleva un registro de las contraseñas usadas previamente, e impide su reúso.

- Almacena y transmite las contraseñas en forma protegida.

6.1.7. Política de clasificación de la información

La información de la entidad se clasifica según la sensibilidad e importancia.

Objetivo
Clasificar la información producida por área para su respectivo acceso y almacenamiento por parte de los funcionarios.

Aplicabilidad

Grupo de seguridad de la información y todo el personal de la entidad

Directrices

Información pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad

Información clasificada: Es toda aquella que al ser divulgada puede llegar a causar daño a algunos derechos individuales de personas naturales o jurídicas por contener información relacionada con la intimidad y privacidad de éstas

Información reservada: Su divulgación indebida puede afectar bienes o intereses públicos. Es necesario establecer el plazo para la clasificación de la reserva, es decir el tiempo en que se considera debe limitarse el acceso a la información el cual según la Ley solo puede durar un máximo de 15 años desde la creación del documento

6.1.8. Política sobre el uso de controles criptográficos

Se utilizan técnicas criptográficas para la protección de la información, para análisis de riesgos sobre los activos de información con mayor nivel de clasificación, con el fin de procurar una adecuada protección de su confidencialidad e integridad.

Objetivo
Utilizar herramientas criptográficas para garantizar la confidencialidad, integridad y autenticidad de la información.

Aplicabilidad

Dirigida a todos los funcionarios de la entidad

Directrices

- Se implementarán principios sobre el uso de controles criptográficos para la protección de la información.

- Se desarrollarán e implementarán métodos para el uso, la protección y la duración de las claves criptográficas

- Firma digital de documentos, correos electrónicos y transacciones

- Protección de contraseñas de acceso a sistemas y demás servicios que requieran autenticación.

6.1.9. Política escritorio y pantalla limpia

Tiene como fin reducir los riesgos de acceso no autorizado, pérdida y/o daño de la información.

Objetivo

Minimizar peligros en la exposición de la información en escritorios y equipos de cómputo.

Aplicabilidad

Dirigido a todos los funcionarios de la entidad.

Directrices

- Guardar en un sitio seguro, los documentos en papel y los dispositivos de almacenamiento removibles, en cajones y/u otro tipo de archivos seguro cuando no están siendo utilizados, especialmente fuera del horario laboral.

- Cuando no se estén utilizando los computadores bloquearlos, el protector de pantalla se encuentra configurado, para que se active en forma automática después de cinco (5) minutos de inactividad.

6.1.10. Política Protección contra código malicioso

Tiene como fin prevenir la contaminación por parte de programas maliciosos virus, gusanos, troyanos, etc. de los equipos de la entidad, impidiendo de esta manera el acceso no autorizado, la pérdida o daño de la información.

Objetivo
Proteger los equipos de infección por parte de programas maliciosos que pongan en riesgo la operación de la entidad.

Aplicabilidad
Dirigido a los administradores de seguridad de la información y direccionamiento tecnológico.

Directrices

- No se permite el intercambio de información a través de archivos, usb o discos extraíbles.

- No compartir carpetas en los equipos se debe compartir en un servidor con los permisos debidamente aprobados.

- Instalar y actualizar software de detección y reparación de virus, antispyware examinando computadores y medios informáticos, como medida preventiva y rutinaria.

6.1.11. Política de seguridad de instalación de software

Se debe tener en cuenta que para la instalación de software debe cumplir con normas y requisitos de acuerdo a cada dependencia

Objetivo
Definir e instalar software con la debida licencia según lo requiera cada dependencia o área de la entidad.
Aplicabilidad
La Política de Seguridad de instalación de software es de aplicación obligatoria para el responsable de los activos informáticos de la entidad.

Directrices

- El administrador de los activos informáticos debe contar con las licencias adecuadas para el proceso de instalación de software, en cada equipo requerido.

- Únicamente se instalará software de acuerdo a los requisitos solicitados por cada área previo estudio del responsable de los activos informáticos de la entidad.

6.1.12. Política de desarrollo seguro

Los sistemas de información son columna importante de los procesos de la entidad, en los cuales se busca brindar seguridad desde el momento del levantamiento de requerimientos, por lo tanto, las necesidades de seguridad, hace parte integral de las decisiones de arquitectura del software a construir y/o adquirir.

Objetivo
Constituir las medidas de seguridad necesarias para el desarrollo de software.

Aplicabilidad
Dirigido a los funcionarios de desarrollo

Directrices

- Todos los sistemas cuentan con un módulo de auditoría, que permita almacenar los registros de transacciones realizadas de cada usuario.

- Todos los equipos deben tener activos los archivos de log's para las auditorias.

- Se debe asegurar la independencia entre el inicio de una actividad y su autorización, para evitar la posibilidad de fraude.

6.1.13. Política procedimiento de transferencia de información

Para el intercambio de información se utiliza una política confidencial, así mismo se documentan los controles adicionales que contemplen cada uno de ellos.

Objetivo
Salvaguardar la información de la entidad del uso indebido de la misma por parte de los empleados

Aplicabilidad
Dirigido a los funcionarios de tecnología administradores de la información

Directrices

- Ejecución de webservices con autenticación.

- Sistemas informáticos, redes, móviles, correo electrónico, comunicaciones de voz, servicio de correo, impresoras

6.1.14. Política adquisición, desarrollo y mantenimiento de sistemas.

Se refiere a las normas que se deben tener en cuenta para proteger el mantenimiento y configuración de los equipos de cómputo de la entidad.

Objetivo
Garantizar la protección adecuada del mantenimiento de Equipos de cómputo y minimizar los riesgos por fallos.

Aplicabilidad
La política es de aplicación obligatoria para todo funcionario entes externos como contratistas o proveedores y cualquiera que sea el nivel de actividades que desempeñen.

Directrices

- Se debe realizar el mantenimiento a los equipos de cómputo en fechas programadas por el responsable de tecnología.

- La información que requiera servicios de aplicaciones que pasan a través de redes públicas deberá estar protegida contra la actividad fraudulenta.

- Se debe llevar una hoja de vida de cada equipo de cómputo de la entidad donde se registre todas las eventualidades de mantenimiento preventivo y correctivo, características de hardware y software, - aplicaciones a la medida - el responsable del equipo - y la función del equipo.

6.1.15. Política de seguridad de la información para las relaciones con proveedores

Se establece los mecanismos de control en sus relaciones con personal externo que le proveen bienes o servicios, supervisar los servicios contratados con personal externo para que den cumplimiento a las políticas de seguridad de la información.

Objetivo
Mantener un nivel conforme con la seguridad de la información y de prestación de servicios por parte de terceros.

Aplicabilidad
Personal externo, contratistas y proveedores

Directrices

- Los contratos deben tener claramente definidos los acuerdos de niveles de servicios y ser contemplados en las especificaciones técnicas.

- Diligenciar y firmar el formato de confidencialidad y compromiso con la seguridad de la información contratistas o terceros y acuerdo para la revelación de información confidencial.

- Los requisitos de seguridad de la información serán establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de la infraestructura.

6.1.16. Política de Gestión de incidentes

Está compuesto por un equipo de especialistas en Seguridad de la Información, quienes velan por la prevención, atención e investigación de incidentes que afecten los activos de información.

Objetivo
Proporcionar respuesta de manera oportuna a los incidentes de seguridad que se presenten a diario.

Aplicabilidad
Encaminado al grupo que tramita los Incidentes de Seguridad Informática y personal de la entidad en general.

Directrices

- Los eventos deben ser registrados por el analista encargado de seguridad de la entidad en el sistema de Información para la gestión de incidentes.

- Se establecerán las responsabilidades y los procedimientos para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

- Los accidentes de seguridad de la información deben ser reportados por el medio adecuado tan pronto como sea posible.

- Los incidentes de seguridad de la información deberán recibir una respuesta de acuerdo con los procedimientos establecidos.

6.1.17. Política de gestión de continuidad del negocio

Se establece un plan general que identifica el impacto de posibles incidentes que amenazan de manera grave el desarrollo de las actividades de la entidad y genera un plan de respuesta efectivo para garantizar su recuperación.

Objetivo
Identificar las amenazas que pueden ocasionar interrupciones de los procesos o actividades que afecten el servicio de la entidad

Aplicabilidad
Equipo de seguridad de la Información y tecnológico.

Directrices

- Durante una situación de riesgo se establecerán procesos, procedimientos y controles, documentados, implementados y mantenidos para asegurar el nivel necesario de continuidad para la seguridad de la información.

- Los controles definidos y aplicados para garantizar la continuidad de seguridad de la información serán verificados con el fin de asegurarse de que son válidos y eficaces en situaciones de riesgo.

6.1.18. Política de cumplimiento de los requisitos legales y contractuales

Impedir el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.

Objetivo
Evitar vulnerar obligaciones legales, reglamentarias o contractuales sobre cualquier requisito de seguridad.
Aplicabilidad
Directivos y equipo de seguridad de la Información.

Directrices

- Los requisitos contractuales y normas regulatorios deberán ser identificados de forma explícita, documentados y actualizados a partir de cada sistema de información.

- Se emplearán los procedimientos adecuados para garantizar el cumplimiento de requisitos legales, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual.

- Los registros deben ser protegidos de pérdida, destrucción, falsificación, acceso no autorizado y la divulgación no autorizada.

- Toda la normativa de propiedad intelectual para proteger los productos de la entidad será gestionada de acuerdo a la política de propiedad intelectual.

- Los sistemas de información deben ser revisados periódicamente para verificar el cumplimiento de las políticas y normas de seguridad de la entidad

CONCLUCIONES

Se realizó el análisis de los activos de información, basados en la metodología MAGERIT y la norma ISO 27001:2013, permitiendo de esta forma que la entidad caso estudio pueda determinar y gestionar sus posibles riesgos.

Se logró hacer la verificación del estado actual, de la entidad caso estudio, lo que permitió conocer el tipo de sistema de información con el cual cuneta la entidad, se utilizó la metodología MAGERIT teniendo en cuenta las siguientes fases: identificación de activos, clasificación de los activos, clasificación de amenazas, valoración del impacto, con el fin de realizar un análisis de las amenazas y sus posibles riesgos si estas se llegaran a presentar.

La importancia de implantar unas políticas en el sistema SUG, permite al administrador, definir las responsabilidades y procesos que se deben llevar en la sala de monitoreo, para mejorar la productividad en procesos.

Con base a la metodología MAGERIT, se identificaron las vulnerabilidades, amenazas o riesgos a los cuales están expuestos los activos de la información de la entidad, lo cual podrá ser insumo para determinar un plan de tratamiento de riesgos garantizando de esta forma que las vulnerabilidades sean mitigadas a tiempo.

Tomando el anexo A de la norma ISO 27001:2013, se formularon controles a los activos de información

La entidad cuenta con una naturaleza de activos los cuales se clasificaron según la metodología dada por MAGERIT, posterior a su clasificación y valoración se determinaron los riesgos a los cuales se les aplico una valoración especifica permitiendo de esta forma que se pueda dar a conocer a la entidad un análisis de los mismos.

Con la aplicación de los controles de la seguridad de la información teniendo en cuenta la norma ISO 27001:2013, se logra la actualización de los ya adoptados por la entidad caso de estudio basados en la norma ISO 27001:2005, lo que nos permite adaptarnos a la evolución de los nuevos riesgos, minimizando estos de forma permanentemente, realizando las

RECOMENDACIONES

Realizar la revisión y la respectiva aprobación por parte de la entidad de las políticas y controles propuestos, para su respectiva publicación y difusión.

Aplicar las políticas y controles propuestos, con el fin de minimizar riesgos y fortalecer los controles de acceso y almacenamiento de los activos de información de la entidad.

Las políticas de seguridad definidas en este documento son a nivel general, que pueden ser aplicadas teniendo en cuenta sus activos.

En la entidad es necesario la capacitación a todos los funcionarios y usuarios debido a que la seguridad informática depende de todos.

Se propone que la entidad debe mejorar su tecnología teniendo en cuenta sus activos físicos y lógicos como, por ejemplo: firewall, licencias de software, actualización de antivirus, instalación de sistemas operativos licenciados.

Establecer perfiles de acceso a cada uno de los funcionarios teniendo en cuenta la clasificación de la información de la entidad, garantizando así la confidencialidad de la información.

BIBLIOGRAFIA

BIBLIOGRAFIA
AREITIO BERTOLÍN, Javier. Seguridad de la información. Redes, informática y sistemas de información. Madrid: Cengage Learning Paraninfo, 2008. Prólogo.

GOBIERNO DE ESPAÑA. Magerit - versión 3.0: Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I - Método. Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012. p. 7.

COLOMBIA, CONGRESO DE LA REPUBLICA. Decreto 1360. Bogotá. (Junio 23 de 1989). Diario Oficial 38.871 de junio 23 de 1989

CONGRESO DE LA REPUBLICA. Ley 527. Bogotá. (Agosto 18 de 1999). Colombia. Diario Oficial 43.673 del 21 de agosto de 1999 p. 1-14.

CONGRESO DE LA REPUBLICA. Decreto 1151. (14, abril, 2008). Bogotá, D.C., Colombia. Diario Oficial. 46960 de abril 14 de 2008.p. 1-4.

CONGRESO DE LA REPUBLICA. Ley 1266. Bogotá. (Diciembre 31 de 2008). Colombia. Diario Oficial 47.219 de diciembre 31 de 2008. p. 1-15.

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1273. Bogotá. (5 de enero de 2009). Diario Oficial 47.223 de enero 5 de 2009.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1341 (30 de julio de 2009). Bogotá. Diario Oficial 47.426 de 30 de julio de 2009.

CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1581 (17 de octubre de 2012). Bogotá. Diario Oficial 48.587 de octubre 18 de 2012. p. 1-15.

CONGRESO DE LA REPUBLICA. Ley 1712. Bogotá. (Marzo 06 de 2014). Colombia. Diario Oficial 49084 de marzo 6 de 2014. p. 1-15.

GÓMEZ, L., ANDRÉS, A. Guía de Aplicación de la Norma UNE-ISO/IEC 27001 Sobre Seguridad en Sistemas de Información para PYMES. España: Asociación Española de Normalización y Certificación. 2012. p. 17

WEBGRAFIA

Alan Bryden, COPANT Seminar on Security Standards, La Paz, 25 de abril de 2006. Pág. 33. Disponible en internet <http://www.iso.org/iso/livelinkgetfile?llNodeId=21657&llVolId=-2000> (marzo de 2016).

ALVAREZ, Daniel. Seguridad en Informática. [en línea]. En: Maestro en Ingeniería de sistemas empresariales. p.7. [citado el 24-05-17].Disponible en http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf

AUDISIS. Sistema de gestión de seguridad de la información - SCSI ISO 27001:2013 - Implantación y auditoría. [en línea]. Bogotá. Disponible en: http://www.audisis.com/BROCHURE_Sem_Implementaci%C3%B3n_SGSI.pdf

BELT IBÉRICA. Seguridad informática. ¿Objetivos de la seguridad informática, que tenemos que tener en cuenta? [en línea]. España: El autor, 2012. [citado el 10-08-15]. Disponible en: http://www.belt.es/noticiasmdb/HOME2_noticias.asp?id=13451

ESTÁNDAR INTERNACIONAL ISO/IEC 17779. Tecnología de la información - Técnicas de seguridad - Código para la práctica de la gestión de la seguridad de la información [en línea]. s.l.: s.n., 2005. [citado el 19-04-16]. Disponible en: https://mmujica.files.wordpress.com/2007/07/iso- 17799-2005-castellano.pdf

ISO/IEC 27000, «Information technology -Security techniques -Information security management systems -Overview and vocabulary" International Organization for Standarization (ISO),» de Information security management systems, p. [online], Disponible en internet <http://www.iso.org>.

ISO 27000.ES. Sistema de gestión de la seguridad de la información [en línea]. Madrid: El autor, s.f. [citado el 16-04-16]. Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

ISO 27001. Sistema de gestión de la seguridad de la información [en línea]. Colombia 1995. [citado el 24-05-17]. Disponible en: http://www.sgs.co/es-ES/Health-Safety/Quality-Health-Safety-and-Environment/Risk-Assessment-and-Management/Security-Management/ISO-27001-2013-Information-Security-Management-Systems.aspx

JEFATURA DE GABINETE DE MINISTROS. Modelo de política de seguridad de la información para organismos de la administración pública nacional [en línea]. Argentina: Oficina Nacional de Tecnologías de Información, 2005. [citado el 11-06-15]. Disponible en: http://www.sgp.gov.ar/sitio/PSI_Modelo-v1_200507.pdf

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Fortalecimiento de la gestión TI en el estado [en línea]. Bogotá. http://colnodo.apc.org/apropiacionTecnologias.shtml

NEIRA, Agustín y SPOHR, Javier. ISO27000.es. “Sistema de Gestión de la Seguridad de la Información”. [online] [citado febrero 2016].Disponible en internet: http://www.iso27000.es/doc_sgsi_all.htm

PALLAS, Gustavo M. Metodología de Implantación de un SGSI en un grupo empresarial jerárquico. [online][citado en marzo de 2016]. Disponible en internet: <https://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf> Pág 6.

POVEDA, José Manuel. Los activos de seguridad de la información [en línea]. Chile: World Visión, s.f. [citado el 28-04-16]. Disponible en: http://www.worldvisioncapacitacion.cl/wp-content/uploads/cursos_adjuntos/f52e0bd4c6c2c203413952826f916237.pdf

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Lección 8: Estándar Magerit para análisis de riesgos informáticos [en línea]. s.l.: UNAD, s.f. [citado el 20-04-16]. Disponible en: http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_8_estndar_magerit_para_anlisis_de_riesgos_informticos.html

Universidad Nacional Abierta y A Distancia. Sistema de Gestión de la Seguridad de la Información SGSI. Unidad I. Capítulo 1 Seguridad Informática. Lección 1.5.1 Ciclo PDCA (Edward Deming). [Online] [Citado en abril 2016]. Disponible en Internet en:<http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/151_ciclo_pdca__edward_deming.html

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO. Fundamentos de seguridad informática: amenazas [en línea]. México: UNAM, s.f. [citado el 30-04-16]. Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/Amenazas.php

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO. Políticas de seguridad informática de la organización, Op. Cit. Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/ Cap4.html

WHITTEN, Jeffrey. Seguridad Informática. [online]. 1994. [citado el citado 01-06-2017]. Disponible: http://problema.blogcindario.com/2008/10/00014-marco-teorico.html