ANALISIS DE ACTIVOS DE INFORMACION PARA UN SISTEMA MISIONAL BASADOS EN LA METODOLOGIA MAGERIT V3 Y LA NORMA ISO 27001:2013.

Rafael Suarez González

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
UNAD CEAD JOSE ACEVEDO Y GOMEZ
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
BOGOTA
2018

ANALISIS DE ACTIVOS DE INFORMACION PARA UN SISTEMA MISIONAL BASADOS EN LA METODOLOGIA MAGERIT V3 Y LA NORMA ISO 27001:2013.

Rafael Suarez González

Monografía para optar al título de
Especialista en Seguridad Informática

Director de proyecto
Esp. Ing. Freddy Enrique Acosta

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
UNAD CEAD JOSE ACEVEDO Y GOMEZ
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
BOGOTA
2018

Nota de Aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bogotá, 18 de Julio de 2018

Este proyecto grado está dedicado primeramente a Dios por darme cada una de las capacidades para poder desarrollar este proyecto, segundo a mis padres y esposa por el apoyo que me brindaron y por último a la Universidad Nacional Abierta y a Distancia.

Rafael Suarez González.

AGRADECIMIENTOS

Rafael expresa sus agradecimientos a:

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

TC. Javier Orlando Medrano Cortes por permitir realizar este proyecto en el grupo SILOG del Ministerio de Defensa Nacional.

Ing. Ronald Mauricio Cely por su apoyo y transferencia de conocimiento en la elaboración del proyecto.

CONTENIDO

Pág.

LISTA DE TABLAS

Pag.

LISTA DE FIGURAS

Pag.

RESUMEN

Toda información se expone a sufrir diferentes tipos de riesgos, para lo cual toda empresa u organización debe identificar cuál es el valor, su impacto y lo no menos importante su plan de tratamiento de riesgos para cada uno de los activos con los que cuenta la organización, para que una empresa pueda tener identificado estos elementos puede hacer uso de diferentes metodologías como lo son ISO 27001, OCTABE, MAGRIT, entre otras las cuales brindan pasos para realizar lo que conocemos como un análisis de riesgos.

"Un análisis de riesgo, además de facilitar su continuo monitoreo a través de procesos de auditorías y mejoras continuas"[1], también tiene como resultado un diagnostico con el cual se pueden identificar y evidenciar cuales son las debilidades y bondades que llevan a la implementación de controles y mecanismos incluidos en un sistema de gestión de seguridad de la (SGSI).

El presente documento tiene como finalidad analizar los activos de información para un sistema misional, haciendo uso de la metodología MAGERIT y la norma ISO 27001:2013, con la cual se puedan aplicar la gestión de riesgos buscando de esta forma que la entidad caso de estudio pueda establecer una política de seguridad informática.

Palabras Claves: Metodología MAGERIT, Análisis de Riesgos Informáticos, Vulnerabilidades, Activos de información, Amenazas.

[1] JOHN JAIRO Perafán Ruiz, Tesis de posgrado, Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca, Universidad Nacional Abierta y a Distancia, Popayán 2014.

ABSTRACT

All information is exposed to suffer different types of risks, for which every company or organization must identify what is the value, its impact and no less important its risk treatment plan for each of the assets with which the organization has, so that a company can have identified these elements can make use of different methodologies such as ISO 27001, OCTABE, MAGRIT, among others which provide steps to perform what we know as a risk analysis.

“A risk analysis, in addition to facilitating its continuous monitoring through ongoing audits and improvements, allows a diagnosis to be made of the internal weaknesses and strengths aimed at generating the appropriate and standardized controls within the IT security policies they are part of an Information Security Management System (ISMS)”.

The purpose of this document is to analyze information assets for a mission system, making use of the MAGERIT methodology and the ISO 27001: 2013 standard, with which risk management can be applied, thus seeking to ensure that the case study entity can establish a computer security policy **Key Words**: MAGERIT Methodology, Computer Risks Analysis, Vulnerabilities, Information Assets, Threats.

Key Words: MAGERIT Methodology, Computer Risks Analysis, Vulnerabilities, Information Assets, Threats.

INTRODUCCIÓN

La mayoría de las entidades públicas y privadas, de manera directa o indirecta dependen de las tecnologías de la información como un único instrumento que permite alcanzar los objetivos de negocio, pero sin dejar de lado que en su día a día se enfrenta a diferentes tipos de amenazas y vulnerabilidades asociadas a los diferentes medios tecnológicos e informáticos.

En la actualidad el estudio de los riesgos hace parte de los procedimientos de cada una de las entidades, al llegar nuevas tecnologías y el crecimiento constante de la información, se ha hecho que los controles se extiendan a las áreas de las Tecnologías de la Información y las Comunicaciones Tics, este concepto ha hecho que las organizaciones estén más atentas y controlen los sistemas informáticos con cada una de sus aristas, desde la arquitectura, el software y los repositorios de datos, los cuales se encuentran agrupados en cada uno de los activos de información, " la grieta pequeña más grande en la armadura corporativa es la dirección de los riesgos"[2]. Esta grieta permite que las entidades desarrollen sus actividades sobre la base de sistemas de control interno a cada uno de los activos de la organización.

Basados en el concepto en el cual se determina la información como el activo más importante que tiene una organización[3], se determinan lineamientos, técnicas y mecanismos claros los cuales brindan seguridad sin dejar de reconocer la seguridad que se aplica al hardware, que es el lugar físico donde se almacena la información.

El alcance de las tecnologías y la dependencia de esta, en cada uno de los procesos con los que cuentan las empresas, permiten que se puedan presentar diferentes tipos de situaciones que obliguen a implementar sistemas de análisis de riesgos, que conlleven preservar y velar por la confidencialidad, integridad y disponibilidad de la información que esta administra.

El presente proyecto tiene como principal finalidad analizar los activos de información de un sistema misional, el cual pude ser utilizado para la implementación del sistema de gestión de seguridad informática (SGSI) mediante un análisis actual de sus riesgos y su impacto en cada uno de los activos de una entidad.

2 R. Bernens: The biggest little in the corporate armor, Internal Auditing, 1997, p.38-46.
3 José Custodio Najar Pacheco, Nubia Esperanza Suárez, “La seguridad de la información: un activo valioso de la organización” 18 febrero 2015. [En línea]. Disponible en: https://revistas.udistrital.edu.co/ojs/index.php/vinculos/article/view/10518/11605

Esta monografía identifica y clasifica los activos de información con los que cuenta la entidad caso estudio, permite realizar la valoración de estos activos con el fin de determinar su nivel de impacto riesgo y vulnerabilidades con los cuales puede ver impactado, todo con el fin de llegar a sugerir controles que la entidad puede implementar basados en el anexo A de ISO 27001.

1. DEFINICION DEL PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

"La gestión de riesgos debe garantizarle a la empresa la tranquilidad de tener identificados sus riesgos y los controles que le van a permitir actuar ante una eventual materialización o simplemente evitar que se presenten", [4]

Cuando una entidad no cuenta con las suficientes políticas, mecanismos de control de seguridad informática, "lo más seguro es que esta entidad en un futuro cercano podría ser víctima de delitos informáticos que obstaculicen su normal funcionamiento como lo pueden ser intrusiones, modificación y/o robo de información, denegación de servicios", entre otros[5].

De acuerdo a lo anterior se puede observar que en la actualidad no todas las empresas públicas como privadas cuentan con un análisis de activos de la información, que les permita conocer e identificar cuáles son sus riesgos informáticos, lo que a través de los años lo ha llevado a que sus riesgos se materialicen, provocando que la información que administran tenga vulnerabilidades en cuanto a disponibilidad, confiablidad y accesibilidad

Y a menudo se observa que muchas empresas, cuenta con procedimientos y políticas de seguridad, pero no cuenta con un análisis de riesgos para sus activos de información, que le permita tener identificado cuáles son sus verdaderas amenazas.

1.2. FORMULACIÓN DEL PROBLEMA

¿Se pueden formular controles de seguridad, realizando el análisis a los activos de información en un sistema misional de una empresa?

[4] Camilo Gutiérrez Amaya, ¿por qué hacer un análisis de riesgos?, Welivesecurity, Bogotá, (2012).
[5] John Jairo Perafán Ruiz, Mildred Caicedo Cuchumbo Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca, Tesis especialización seguridad informática, Popayán, (2014) P.25.

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Realizar un análisis a los activos de la información para determinar y gestionar los posibles riesgos que se presenten en el sistema de información misional de la entidad caso de estudio, basados en la metodología MAGERIT V3 y la norma ISO 27001:2013.

2.2. OBJETIVOS ESPECÍFICOS

- Verificar el estado actual del sistema de información misional, de la entidad caso estudio.
- Clasificar los activos de información con los que cuenta la entidad caso estudio utilizando la metodología MAGERIT V3.
- Identificar vulnerabilidades, amenazas o riesgos a que están expuestos los activos de la información de la entidad caso estudio, basado en la metodología MAGERIT V3.
- Formular controles a los activos de información de acuerdo al anexo A de la norma ISO 27001:2013

3. JUSTIFICACIÓN

"La información es un activo que, al igual que otros activos del negocio, es esencial para la organización, y por lo tanto debe ser protegido de forma adecuada."[6]

La gestión del Riesgo en la seguridad de la información, permite tener en las entidades del sector público y privado, diferentes mecanismos y herramientas que administran los riesgos, vulnerabilidades y amenazas, teniendo como finalidad principal mostrar la importancia de implementar en las entidades, sistemas de gestión de la Seguridad Informática (SGSI) en cada uno de los procesos y políticas.

Se requiere la elaboración de un análisis de los activos de información en los sistemas misionales de las entidades que les permita la identificación de los activos informáticos sus riegos, vulnerabilidades y amenazas expuestas, así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles, mecanismos y protocolos adecuados para aceptar, disminuir, o evitar la ocurrencia del riesgo, además con el objetivo de fortalecer en la organización, cada uno de los pilares de la seguridad correspondientes a la Integridad, Confidencialidad y Disponibilidad de la información, generando de esta forma que la información que administran este siempre este protegida.

Con la medición de los activos se da el primer paso para el control y la mejora, "La medición es el primer paso para el control y la mejora. Si algo no se puede medir, no se puede entender. Si no se entiende no se puede controlar, si no se puede controlar, no se puede mejorar"[7]. Por lo cual se hace necesario realizar un análisis de los riesgos informáticos que se pueden presentar en una entidad, identificando cada uno de sus activos informáticos, clasificándolos, priorizándolos y valorizándolos para posterior identificar sus riesgos y así mismo establecer e implementar mecanismos de control que conlleven a minimizar los impactos cuando un riesgo se materialice.

Teniendo en cuenta que La inseguridad es una propiedad inherente a los recursos informáticos y la gestión es la única forma de medirla y aminorarla[8], se busca tener como referencia los análisis de los riesgos en una compañía y el nivel de impactos que estos pueden tener, generando grandes pérdidas económicas y financieras, se hace necesario que se tengan identificados todos y cada uno de los activos y sus riesgos, para así poder aplicar controles que permitan mitigarlos, siempre buscando preservar los pilares de la información,

---

[6] ISO/IEC 17799:2005, International Organization for Standardization, Disponible en: https://www.iso.org/standard/39612.html

[7] DR H James Harrington, Quality Advisor para Ernst & Young, Improving healthcare Quality and cost with six Abril, Lenders, 2017.

8 Armando Carvajal, ACIS, Análisis y gestión del riesgo, base fundamental del SGSI Bogotá, 2014.

Según lo anterior se da por entendido que el problema que presenta las entidades hace relación a que no se cuenta con un análisis actualizado que permita conocer e identificar cuáles son los riesgos informáticos a los cuales se puede exponer un activo.

3.1. ALCANCE Y LIMITACIÓNES

3.1.1. Alcance. La presente monografía se encuentra entre los proyectos de gestión de seguridad de la información y lo que pretende es analizar activos de información para un sistema misional, basado en la metodología MAGERIT y la norma ISO 27001:2013.

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

- No se establecerá o implementará salvaguardas.
- No presentara un plan de tratamiento de riesgos.
- No se elaborar ni presentara ningún diagnóstico de hallazgos.
- No se elaborará un Hacking ético a una entidad.

4. DISEÑO METODOLOGÍCO

4.1. UNIDAD DE ANÁLISIS.

La unidad de análisis de esta monografía corresponde a los posibles riesgos y vulnerabilidades a los cuales pueden estar sometidos los activos de un sistema misional de la entidad caso estudio.

4.2. POBLACIÓN Y MUESTRA

4.2.1. Población. Para el desarrollo de la presente monografía se determinó la siguiente población con las siguientes características:

- Homogeneidad: un sistema misional de una entidad.
- Tiempo: el estudio se realizó en el momento presente.
- Espacio: se realizó en la ciudad de Bogotá.
- Cantidad: corresponde a las personas que laboran en la entidad caso estudio.

4.2.2. Muestra. El tipo de muestra que se determinó para esta monografía fue aleatorio, se elaboró la entrevista al 10 % de las personas que hacen parte de la entidad casi de estudio.

4.2.3. Estudio metodológico. Dado que la investigación descriptiva implica observar y describir el comportamiento de un sujeto o situación, se tendrán como técnica el uso de levantamiento de información mediante entrevistas a personal experto en el área de las tecnologías de la información de la entidad caso estudio, para su posterior observación y análisis de la misma con el objetivo de identificar los activos los cuales serán evaluados y así poder identificar sus riesgos con el objetivo que las entidades obtengan un diagnostico que conlleven a la implementación de mecanismos, política y controles para conseguir el fortalecimiento de los sistemas de gestión de seguridad de la información basada en riesgos.

Dado que la investigación descriptiva implica observar y describir el comportamiento de un sujeto o situación, se tendrán como técnica el uso de levantamiento de información mediante entrevistas a personal experto en el área de las tecnologías de la información de la entidad caso estudio, para su posterior observación y análisis de la misma con el objetivo de identificar los activos los cuales serán evaluados y así poder identificar sus riesgos con el objetivo que las entidades obtengan un diagnostico que conlleven a la implementación de mecanismos, política y controles para conseguir el fortalecimiento de los sistemas de gestión de seguridad de la información basada en riesgos.

5. MARCO REFERENCIAL

5.1. MARCO TEÓRICO

La seguridad informática se puede definir, como la preservación de la confidencialidad, la integridad y la disponibilidad de los sistemas de información[9]. Dependiendo del entorno de la organización, se pueden tener diferentes amenazas los cales pueden comprometer a los objetivos anteriormente mencionados, la organización tiene tres alternativas: aceptar el riesgo, hacer algo para disminuir la posibilidad de ocurrencia del riesgo o transferir el riesgo. A las medidas o salvaguardas que se toman para disminuir un riesgo se les denomina controles de seguridad [10]

Los controles que se determinen deben estar integrados con el fin de que estos cumplan con la efectividad esperada[11] cada uno de estos controles deben estar alineados a los objetivos trazados en la organización, se determinara una fase de diseño de la arquitectura de la seguridad informática la cual está inmersa en la etapa de análisis de riesgos[12] para lo cual se comprende los siguientes pasos:

- Se definen los activos informáticos a analizar.
- Identificar las amenazas que pueden comprometer la seguridad de los activos. Determinar la probabilidad de ocurrencia de las amenazas.
- Determinar el impacto de las amenazas, con el objeto de establecer una priorización de las mismas.
- Recomendar controles que disminuyan la probabilidad de los riesgos.
- Documentar el proceso.

La dependencia actual de las organizaciones en las Tecnologías de la Información (TI) se hace más notoria debido a que nuestra economía se basa en la generación de conocimiento[13], en donde el uso de la tecnología basado en administrar, desarrollar y transmitir activos intangibles como la información y el conocimiento son esenciales para las estrategias de negocio.

---

[9] TIPTON, 2006 Harold F. Tipton, Micki Krause (eds.), Information Security Management Handbook, 5th Ed., CRC Press, 2006

[10] WHITMAN, Herbert J. Mattord, Management of Information Security, Course Technology, 2007
Peltier, 2005 Thomas R. Peltier, Information Security Risk Analysis, CRC Press, 2005.

[11] TUDOR, 2006 Jean Killmeyer Tudor (ed.), Information Security Architecture: An Integrated Approach to Security in the Organization, CRC Press, 2006.

12 LANDOLL, 2005 Douglas J. Landoll, The Security Risk Assesment

[13] PETERSON, R. Integration Strategies and Tactics for Information Technology Governance. En W. VAN GREMBERGEN, Strategies for Information Technology Governance (p. 37-80). IDEA Group Publishing. 2004. p. 3.

Basados en el Ministerio de las tecnologías de la Información y las comunicaciones (TIC), el Estado colombiano mediante el Decreto 1537 de 2001 estableció que todas las entidades públicas deben contar con mecanismos de administración de riesgos, con el fin de controlar las vulnerabilidades, riesgo y amenazas, se busca que estas entidades se encuentren familiarizadas con el tema de seguridad de la información basada en el análisis de riesgos

Del anterior argumento se parte para decir que los riesgos no solo se miden por la parte económica o que están asociados con entidades bancarias, sino que hacen parte de cualquier sistema de gestión que se encuentre implementado en una compañía.

5.1.1. Seguridad de la información. Cuando se habla de seguridad de la información se indica que dicha posee un estatus de alta importancia por lo cual se vela por su protección.

La Seguridad de la Información se define como conjunto de metodologías, medidas técnicas, organizativas y legales que permiten a la organización asegurar los pilares de la seguridad informática, la confidencialidad, integridad y disponibilidad de su sistema de información.

"La seguridad informática consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio."[14].

5.1.2. Análisis de riesgos informáticos. Las diferentes metodologías de análisis de riesgo varían de acuerdo a la forma de cómo se determine el impacto en cada uno de los activos en la organización, para esto se puede hacer uso de dos tipos de metodologías, la cualitativa la cual es la más utilizada y con la cual se permite una caracterización entre alta media y baja, uno de los estándar internacional más conocidos como los es ISO/IEC 27001 hace uso de este tipo de metodología[15] y la metodología cualitativa la cual es usada por el estándar NIST 800-39, con este tipo de metodologías se está sujeto a la experiencia del analista, se pueden encontrar algunas metodologías como MAGERIT con las que se pueden combinar la cuantitativa y la cualitativa.

En un Sistema de Gestión de Seguridad de la Información, se requiere que toda entidad, empresa u organización tenga dentro de sus procesos implementados un sistema de gestión de análisis de riesgos con el cual se puedan identificar

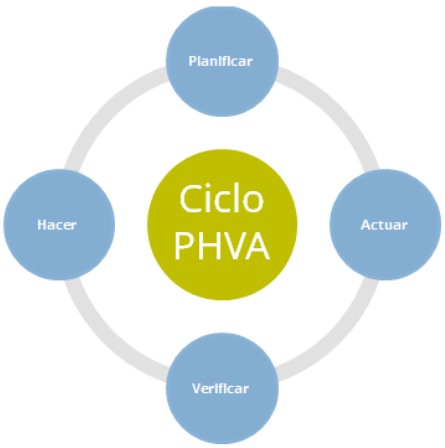
[14] MINISTERIO DE EDUCACIÓN Y DOCTRINA DE ESPAÑA, Introducción a la seguridad informática (s.f), disponible en: http://recursostic.educacion.es/observatorio/web/ ca/software/software-general/1040-introduccion-a-la-seguridad-informatica? start=1

[15] CALDER, Alan Calder, STEVE Watkins, Information Security Risk Management for ISO 27001/ISO 17799, IT Governance Publishing, 2007.

cuáles son sus principales vulnerabilidades en cada una de sus activos de información.

Como se observa en la figura No 1, en los sistemas de gestión de la seguridad de la información (SGSI), en el ciclo PHVA, podemos encontrar al análisis de riesgos dentro de las actividades de la planificación, lo que lleva a que se tomen decisiones de análisis y verificación, [16].

Figura 1. PHVA



Fuente: Blog especializado en Sistemas de Gestión de Seguridad de la Información, ISO 27001: La implementación de un Sistema de Gestión de Seguridad de la Información toma de: www.pmg-ssi.com/2015/01/iso-2700, enero 2015.

El proceso de análisis y evaluación de riesgos de acuerdo al estándar MAGERIT, nos permite realizar la valoración de los riesgos dentro de cada uno de los criterios valorados, esto nos permite definir controles de seguridad y reducir el impacto en cada una de las organizaciones, la metodología MAGERIT, realiza la clasificación de las diferentes vulnerabilidades, amenazas, riesgos y activos de información, haciendo uso de escalas de valoración y de unos criterios ya definidos para la evaluación de los activos.

Posterior a la identificación y clasificación de activos se identifica y valora los riesgos a los que estos activos pueden verse afectados, lo cual permite establecer controles los cuales se deben implementar en la organización con el fin de mitigar la exposición de riesgos en los activos

Según Fernando Izquierdo Duarte: “E R, el riesgo es un incidente o situación que ocurre en un sitio concreto durante un intervalo de tiempo determinado, con consecuencias positivas o negativas que podrían afectar el cumplimiento de los objetivos”[17]

[16] MOLINA, Miranda María Fernanda, Propuesta de un plan de gestión de riesgos de tecnología aplicada en la escuela superior politécnica del litoral, Tesis de Maestría, (2015).
[17] IZQUIERDO D, Fernando. La administración y los riesgos. EN: Maxitana C, Jennifer D. (Auditor en control de gestión). Administración de riesgos de tecnología de información de una empresa del sector informático. Tesis, Escuela Superior politécnica del Litoral, Guayaquil Ecuador. 2005. P.39. disponible en: http://www.cib.espol.edu.ec/Digipath/D_Tesis_PDF/D-33960.pdf.

5.1.3. Metodología de análisis de riesgos. Las metodologías de análisis de riesgos tienen como función principal la identificación de los controles y mecanismos en un plan de salvaguardas, se pueden encontrar dos clases, las cualitativas y las cuantitativas, la metodología es flexible en el momento de su implementación, esto quiere decir que no se requiere de su implementación total para que esta brinde resultados satisfactorios, se pude hacer una adopción a la norma de forma parcial.

5.1.4. Objetivos de la metodología MAGERIT. Dice Ana Pulido y Jhon A,[18] MAGERIT resulta ser la opción más efectiva y completa ya que protege la información en cuanto a integridad, confidencialidad, disponibilidad y otras características importantes para garantizar la seguridad de los sistemas y procesos de la organización.

La implementación de las metodologías de análisis de riesgos en una entidad permite que esta tenga un control de los riesgos permitiendo así la buena administración de los mismos, permitiendo así que la entidad implemente controles que la lleven hacer una compañía competitiva, garantizando la integridad de su información.

5.1.5. Normas ISO.

5.1.5.1. ISO 27001. Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:201319.

Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013[20].

5.1.5.2. SO/IEC 27000. Es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.[21].

[18] ABRIL Ana, Pulido Jarol y BOHADA Jhon A., Análisis de Riesgos en Seguridad de la Información (2013), Fundación Universitaria Juan D Castellanos Colombia
[19] BS 7799-2. Advisera Iso270011 {En línea} (s.f), tomado de: https://advisera.com/27001academ y/es/que-es-iso-27001/
[20] BS 7799-2. Advisera Iso270011 {En línea} (s.f), tomado de: https://advisera.com/27001academ y/es/que-es-iso-27001/
[21] PERAFÁN John Jairo Ruiz, CAICEDO Mildred Cuchimba, Análisis de riesgos de la seguridad de la información para la institución universitaria colegio mayor del cauca, (2014), tesis posgrado, Popayán 2014.

En este apartado se resumen las distintas normas que componen la serie ISO 27000 y se indica cómo puede una organización implantar un sistema de gestión de seguridad de la información (SGSI) basado en ISO 27001 en conjunto con otras normas de la serie 27k, pero también con otros sistemas de gestión[22].

5.1.5.3. ISO/IEC 27001. Es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.[23.]

los requisitos para la implementación de un SGSI (Sistema de Gestión de la Seguridad de la Información). DRI internacional.[24].

5.1.5.4. ISO/IEC 27002. (Anterior ISO 17799). Es una guía de buenas prácticas, describe los controles a seguir dentro del marco de la seguridad de la información; enmarcados en 11 dominios, 39 objetivos de control y 133 controles.[25].

5.1.5.5. ISO/IEC 27003. Es un estándar internacional que constituye una guía para la implantación de un SGSI. Se trata de una norma adaptada tanto para los que quieren lanzarse a implantar un SGSI como para los consultores en su trabajo diario, debido a que resuelve ciertas cuestiones que venían careciendo de un criterio normalizado. SGSI.[26].

5.2. MARCO CONCEPTUAL

EVENTO: Es una situación que es posible pero no certera; es siempre un evento futuro y tiene influencia directa o indirecta sobre el resultado. Un evento se trata como un suceso negativo y representa algo indeseado.

RIESGO RESIDUAL: Es el valor de riesgo tras la aplicación de uno o varios controles.

ISO: International Standard Organization. En español Organización de Estándares Internacionales.

---

[22] ISO2700 {En línea} (2015), disponible en: http://www.iso27 000.es/iso27000.html

[23] PERAFÁN John Jairo Ruiz, CAICEDO Mildred Cuchimba, Análisis de riesgos de la seguridad de la información para la institución universitaria colegio mayor del cauca, (2014), tesis posgrado, Popayán 2014.

[24] ISO 27000 {En línea} (s,f), disponible en: http://iso27000.es/iso27002.html

[25] DRI internacional, ISO 27000 {En línea} (s,f), disponible en: http://iso27000.es/iso27002.html

[26] blog especializado en sistema de gestión de seguridad, {En línea} (2014) disponible en: http://www.pmg-ssi.com/2014/01/isoiec-27003-guia-para-la-implementacion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/

ANÁLISIS DE RIESGOS: Método sistemático de recopilación, evaluación, registro y difusión de información requerida para formular recomendaciones encaminadas a la adopción de una medida en respuesta a un determinado peligro.

ESTIMACIÓN DEL RIESGO: Proceso de asignación de valores a la probabilidad e impacto de un riesgo.[27]

RIESGO INFORMÁTICO: Es la probabilidad de que una amenaza en particular expone a una vulnerabilidad que podría afectar a la organización. Es la posibilidad de que algo pueda dañar, destruir o revelar datos u otros recursos.[28]

VULNERABILIDAD: Es una falla o debilidad en los procedimientos, diseño, implementación o controles internos en un sistema de seguridad. Es cualquier ocurrencia potencial que pueda causar un resultado indeseado para una organización o para un activo en específico.[29]

INFORMACIÓN: Datos relacionados que tienen significado para la organización.

S.G.S.I: Sistema de Gestión de Seguridad de la Información

SISTEMA GESTIÓN DE SEGURIDAD INFORMÁTICA (SGSI): hace refiere al Sistema de Gestión de la Seguridad de la Información e (ISMS) siglas que equivalen en ingles a Información Security Management System.[30]

ANÁLISIS: Un análisis es un efecto que comprende diversos tipos de acciones con distintas características y en diferentes ámbitos, pero en suma es todo acto que se realiza con el propósito de estudiar, ponderar, valorar y concluir respecto de un objeto, persona o condición.[31]

USUARIOS: Son las personas que están directamente involucradas con la infraestructura tecnológica, comunicaciones y administradores de la información. La seguridad informática debe establecer normas que minimicen los riesgos tanto de información como de su infraestructura, dentro de dichas normas de debe contemplar, horarios de acceso, restricciones físicas y lógicas, permisos, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo esto debe estar regido por estándares y normas que minimicen los

27 Rodrigo Ferrer Cissp, metodología de análisis de riesgo, Bogotá, SISTESEG

28 Andrés Felipe Doria Corcho, Tesis de grado, Diseño de un sistema de gestión de seguridad de la información mediante la aplicación de la norma internacional ISO/IEC 27001:2013 en la oficina de sistemas de información y telecomunicaciones de la universidad de córdoba, Montería, 2015

29 DORIA CORCHO Andrés Felipe, Tesis de grado, Diseño de un sistema de gestión de seguridad de la información mediante la aplicación de la norma internacional ISO/IEC 27001:2013 en la oficina de sistemas de información y telecomunicaciones de la universidad de córdoba, Universidad Nacional Abierta y a Distancia, Montería, 2015

30 Blog especializado en Sistemas de Gestión de Seguridad de la Información. SGSI PMG {En línea} (s.f), disponible en: http://www.pmg-ssi.com/2015/07/que-es-sgsi/

31 Definición ABC, (s.f), http://www.definicionabc.com/ciencia/analisis.php

riesgos y el impacto en caso de llegar a presentar un siniestro.[32]

INFORMÁTICA: La informática se define como la ciencia que estudia el tratamiento de la información mediante medios automáticos, es decir la ciencia de la información automática.

ACTIVO INFORMÁTICO: Se define como todo aquello que pueda generar valor para la empresa u organización y que éstas sientan la necesidad de proteger. Un activo o recurso informático está representado por los objetos físicos (hardware, como los *routers*, *switches*, *hubs*, *firewalls*, antenas, computadoras), objetos abstractos (software, sistemas de información, bases de datos, sistemas operativos) e incluso el personal de trabajo y las oficinas.[33]

SEGURIDAD INFORMÁTICA: Permite asegurar que los recursos del sistema de información de una organización sean seguro y confiables, mediante el establecimiento de normas, métodos y técnicas.

El objetivo principal de la informática consiste en automatizar mediante equipos generalmente electrónicos todo tipo de información, de tal forma que evite la repetición de tareas arduas las cuales pueden inducir al error reduciendo a su vez el tiempo de ejecución de las mismas[34], la unión de estos dos términos permite definir la seguridad informática como la disciplina que se encarga de salvaguardar información contenida en una tecnología.

La seguridad informática se manifiesta en tres pilares básicos: confidencialidad, integridad y disponibilidad[35].

CONFIDENCIALIDAD: Los componentes del sistema serán accesibles sólo por aquellos usuarios autorizados.

INTEGRIDAD: Los componentes del sistema sólo pueden ser creados y modificados por los usuarios autorizados.

DISPONIBILIDAD: Los usuarios deben tener disponibles todos los componentes del sistema cuando así lo deseen. De nada sirve la información si se encuentra intacta en el sistema, pero los usuarios no pueden acceder a ella

---

[32] Análisis de riesgos de la seguridad de la información para la institución universitaria colegio mayor del cauca, {En línea} (2014), tesis posgrado, disponible en: http://www.academia.edu/24661883/An%C3%A1lisis_de_Riesgos_de_la_Seguridad_de_la_Informaci%C3%B3n_para_la_Instituci%C3%B3n_Universitaria_Colegio_Mayor_Del_Cauca

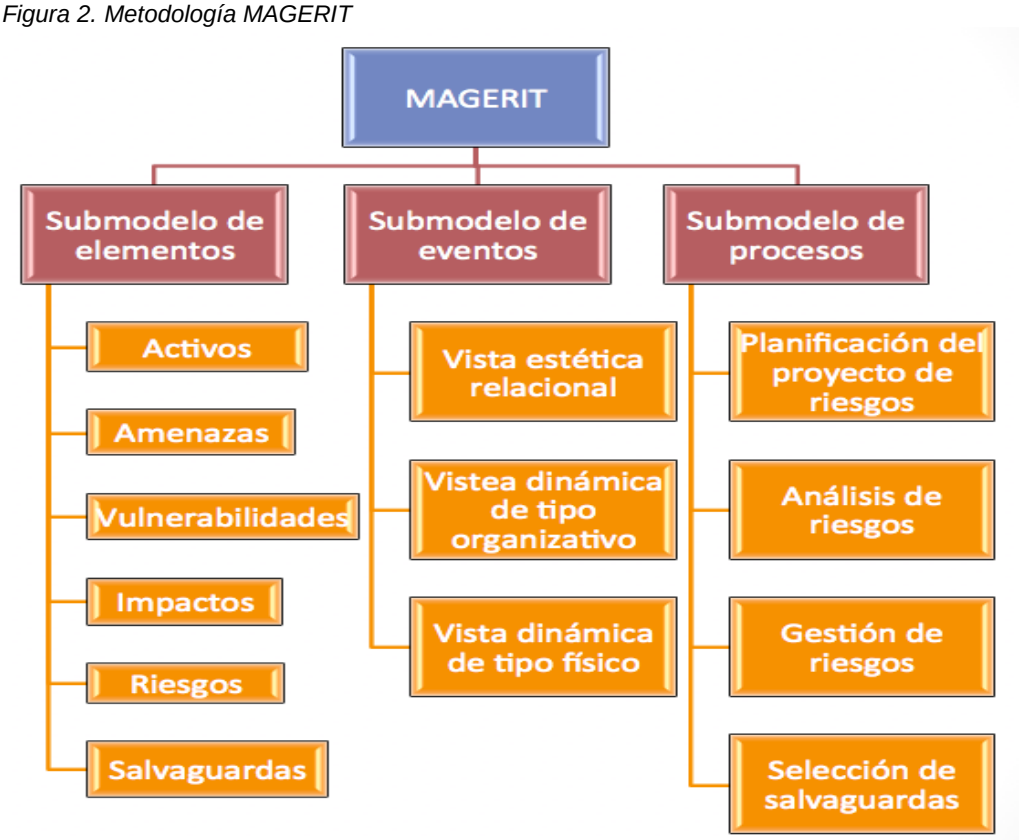
[33] Andrés Felipe Doria Corcho, Tesis de grado, Diseño de un sistema de gestión de seguridad de la información mediante la aplicación de la norma internacional ISO/IEC 27001:2013 en la oficina de sistemas de información y telecomunicaciones de la universidad de córdoba, Montería, 2015

[34] Generalidades de la informática, {En línea}, disponible en: https://sites.google.com/site/navegadorteleinformatico/navegador-teleinformatico

[35] Se le conoce como la Tríada CIA, por sus siglas en inglés Confidentiality, Integrity, Availability. KIM, D., SALOMON, M. G. Fundamentals of Information System Security. Estados Unidos de América: Jones & Bartlett Learning International. 2012. p. 10.

MAGERIT: Metodología de análisis y gestión de riesgos de los Sistemas de Información elaborada por el Consejo Superior de Administración Electrónica para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información, enfocada a las Administraciones Públicas.[36] MAGERIT hace uso de la siguiente estructura para su funcionamiento como se observa en la figura 2.

Figura 2. 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*.

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:

Tabla 1 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

[36] Portal administración Metodología de análisis {En línea} (2012), disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WRIcMEWGPIU

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

Tabla 2 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: Fuente: MAGERIT V.3 – Libro II – Catálogo de Elementos

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

Tabla 4 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: Fuente: MAGERIT V.3 – Libro II – Catálogo de Elementos

Tabla 5 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: Fuente: MAGERIT V.3 – Libro II – Catálogo de Elementos

Tabla 6 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: Fuente: MAGERIT V.3 – Libro II – Catálogo de Elementos

Tabla 7 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: Fuente: MAGERIT V.3 – Libro II – Catálogo de Elementos

Tabla 8 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: Fuente: MAGERIT V.3 – Libro II – Catálogo de Elementos

Tabla 9 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: Fuente: MAGERIT V.3 – Libro II – Catálogo de Elementos

Tabla 10 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: Fuente: MAGERIT V.3 – Libro II – Catálogo de Elementos

Tabla 11 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: Fuente: MAGERIT V.3 – Libro II – Catálogo de Elementos

Tabla 12 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: Fuente: MAGERIT V.3 – Libro II – Catálogo de Elementos

Tabla 13 Criterios de valoración 13

[lbl.ue] Información clasificada (Unión Europea)		
10	10.ue	TRES SECRET UE
9	9.ue	SECRET UE
8	8.ue	CONFIDENTIEL UE
7	7.ue	CONFIDENTIEL UE
6	6.ue	RESTREINT UE
5	5.ue	RESTREINT UE
4	4.ue	RESTREINT UE
3	3.ue	RESTREINT UE

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

ANÁLISIS DE RIESGOS: Como parte del Sistema de Gestión de Seguridad de la Información, es necesario para la empresa hacer una adecuada gestión de riesgos que le permita saber cuáles son las principales vulnerabilidades de sus activos de información y cuáles son las amenazas que podrían explotar las vulnerabilidades. En la medida que una empresa tenga clara esta identificación

de riesgos podrá establecer las medidas preventivas y correctivas viables que garanticen mayores niveles de seguridad en su información[37]

RIESGOS: es la probabilidad de que una amenaza se convierta en un desastre. La vulnerabilidad o las amenazas, por separado, no representan un peligro. Pero si se juntan, se convierten en un riesgo, o sea, en la probabilidad de que ocurra un desastre. Sin embargo, los riesgos pueden reducirse o manejarse.[38]

AMENAZA: Es el potencial que un intruso o evento explote una vulnerabilidad específica. Es cualquier probabilidad que pueda ocasionar un resultado indeseable para la organización o para un activo en específico. Son acciones que puedan causar daño, destrucción, alteración, pérdida o relevancia de activos que podrían impedir su acceso o prevenir su mantenimiento.[39], se pueden encontrar diferentes tipos de amenazas:

- De origen natural

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.

- Del entorno (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.

- Defectos de las aplicaciones

Hay problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se denominan vulnerabilidades técnicas o, simplemente, 'vulnerabilidades'13.

- Causadas por las personas de forma accidental

Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.

- Causadas por las personas de forma deliberada

Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.[40]

---

[37] Welivesecurity análisis de riesgos {En línea} (2013), disponible en: https://www.welivesecurity.com/la-es/2012/08/16/en-que-consiste-analisis-riesgos/

[38] Que es el riesgo {En línea} (2014), disponible en: https://www.unisdr.org/2004/campaign/booklet-spa/page9-spa.pdf

[39] TAMAYO, A. Auditoría en Sistemas: Una Visión Práctica. Manizales: UNAD. 2001. p. 14.

[40] MAGERIT V3.0, Metodología de análisis y gestión de riesgos y análisis de información, Libro 1, Ministerio de Hacienda y administración pública, España, 2012, p 27.

5.3. ANTECEDENTES

5.3.1. Antecedente No 1. Diseño de un sistema de gestión de seguridad de la información mediante la aplicación de la norma internacional ISO/IEC 27001:2013 en la oficina de sistemas de información y telecomunicaciones de la entidad caso estudio de córdoba.

Autor: ANDRÉS FELIPE DORIA CORCHO

Establece las bases para la posterior implementación de un Sistema de Gestión de la Seguridad de la Información, en la oficina de Sistemas y Telecomunicaciones de la entidad caso estudio de Córdoba, la cual es la unidad encargada de prestar los servicios de TI. Siguiendo las mejores prácticas de estándares de seguridad internacionales como lo es la norma ISO/IEC 27001:2013, y mediante una metodología de análisis de riesgos se identifican qué activos informáticos son los más críticos y de mayor impacto que requieren mayores controles de seguridad y así establecer un plan para la continuidad de los servicios.[41]

5.3.2. Antecedente No 2. Análisis y gestión del riesgo de la información en los sistemas de información misionales de una entidad del estado, enfocado en un sistema de seguridad de la información.

Autor: HINA LUZ GARAVITO ROBLES

Realiza un análisis de gestión del riesgo de la información en una empresa del estado la cual manifiesta la urgente necesidad de proteger su activo más valioso "la información" y esto se ve agravado con el constante incremento de la información en la entidad como también de los sistemas de información en la web que son necesarios para la gestión de información en sus diferentes centros de servicio a nivel nacional.[42]

Se realizó el análisis por medio de la metodología la cual es el primer paso para garantizar la seguridad de los activos de información y el normal funcionamiento interno de la entidad.

[41] ANDRÉS Felipe Doria Corcho, Trabajo de grado para optar por el título de: Especialista en Seguridad Informática, Universidad Nacional Abierta y a Distancia, Montería, (2015).
[42] HINA Luz Garavito Robles, Tesis de grado para optar por el título: Especialista En Seguridad Informática, Análisis y gestión del riesgo de la información en los sistemas de información misionales de una entidad del estado, enfocado en un sistema de seguridad de la información; Bogotá, (2015).

5.4. MARCO LEGAL

5.4.1. Ley Estatutaria 1266. “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”[43].

5.4.2. Ley 1273. Del 5 de enero de 2009 emitida por el Congreso de Colombia, "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"[44]

5.4.3. ley estatutaria 1581. DE 2012. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013. Por la cual se dictan disposiciones generales para la protección de datos personales, “La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma”.[45].

5.4.4. ley 527 de 1999. 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.[46].

5.4.5. ley 1343 de 2009. Por medio de la cual se aprueba el “Tratado sobre el Derecho de Marcas” y su “Reglamento”, adoptados el 27 de octubre de 1994.[47].

5.4.6. decreto 1360 de 1989. Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor".[48].

Existen otros decretos y actos administrativos relevantes que regulan diversas actividades relacionadas con el entorno digital, tales como la Circular Externa de

---

[43] CONGRESO DE LA REPUBLICA. Ley 1266. Bogotá. (diciembre 31 de 2008). Colombia, Diario Oficial. 219 de diciembre 31 de 2008. p. 1-15.

[44] CONGRESO DE LA REPÚBLICA, Ley 1273 del 5 de enero de 2009 emitida por el Congreso de la República COLOMBIA. “Ley 1273 de 2009”. Disponible en Ministerio de Tecnologías de la Información y las Comunicaciones: (http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf).

[45] ALCALDIA MAYOR DE BOGOTA, ley 1581 de 2012, Régimen Legal de Bogotá, (octubre 17 de 2012) Colombia

[46] REGIMEN LEGAL DE BOGOTA DC, Ley 527 de 1999 Nivel Nacional, Colombia, 18 de agosto de 1999

[47] SECRETARIADO DEL SENADO, Congreso De La República, LEY 1343 DE 2009, Bogotá, Colombia, 2010.

[48] ALCALDIA MAYOR DE BOGOTA, DECRETO 1360 DE 1989, Régimen Legal de Bogotá, Colombia junio 23 de 1989.

la Superintendencia Financiera de Colombia 052 de 2007 (estándares de seguridad y calidad para el manejo de la información a través de medios y canales de distribución de productos y servicios), las Resoluciones CRC 3066 y 3067 de 2011 (Régimen integral de protección de los derechos de los usuarios e indicadores de calidad para los servicios de telecomunicaciones), Decreto 1704 de 2012 (interceptación legal de comunicaciones), Decreto Ley 019 de 2012 (entidades de certificación digital), Resolución de la Superintendencia de Industria y Comercio de Colombia (SIC) No. 76434 de 2012 (protección de datos personales), Decreto 2573 de 2014 (Gobierno en línea).[49]

[49] CONPES, CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, Política Nacional De Seguridad Digital, Bogotá, 2016,

6. ESTADO ACTUAL DEL SISTEMA DE INFORMACION MISIONAL DE LA ENTIDAD CASO ESTUDIO

En la actualidad, la entidad caso estudio cuenta con funciones determinadas para el desarrollo de los procesos de seguridad informática y del análisis de riesgos y vulnerabilidades.

Cuenta con un proceso de análisis de riesgos el cual tiene como objetivo identificar las posibles vulnerabilidades técnicas de la plataforma para evitar acciones que atenten con la seguridad de la información.

6.1. DESCRIPCION DE LA ENTIDAD CASO ESTUDIO

La entidad caso estudio como empresa tiene como actividad principal administrar, soportar, capacitar e implementar la plataforma de Planificación de Recursos Empresariales (Enterprise Resource Planning -ERP) SAP en todas sus sucursales a nivel Colombia y Estados Unidos.

6.1.1. Historia. El 25 de julio de 2004 se creó la entidad caso estudio, como uno de los proyectos más grandes capaz de mostrar lo que significa realmente el trabajo conjunto interinstitucional. Esta entidad recibida apoyo efectivo de otros países para ser implementado a nivel nacional e internacional.

En esta fecha se inició la implementación del proyecto en las 185 sociedades financieras que se proyectaron las cuales están ubicadas a lo largo y ancho de la Geografía Nacional e internacional. Actualmente soporta aproximadamente más de 9000 usuarios finales.

6.1.2. Misión. Capacitar, implementar y soportar a las diferentes sucursales a nivel país y a sus sucursales internacionales**.**

6.1.3. Visión. Mantener la plataforma SAP disponible y actualizada para su uso las 24 horas del día, los 7 días de la semana, sin interrupciones.

6.2. ESTRUCTURA ORGANIZACIONAL DE LA ENTIDAD CASO ESTUDIO

Figura 3 Estructura organizacional.

Fuente: Autor.

6.2.1. Área de sistemas. El área técnica o de Tecnología de la información (TI) se encuentra conformado por:

- Infraestructura> conformado por personal profesional y experto en servidores, redes, firewall, base de datos.
- Aplicaciones> conformada por personal profesional y experto en SAP, administradores de los servidores de aplicaciones.
- Basis conformada por personal profesional y expertos en SAP en el módulo de Basis.
- Desarrollo con formada por personal profesional y expertos en desarrollo bajo el lenguaje de programación ABAP.

6.2.2. caracterización del área de sistemas.

6.2.2.1. Misión.

- Gestionar la coordinación, seguimiento y consolidación de las áreas financiera, logística, de mantenimiento, desarrolladores, mesa de ayuda, seguridades y administrativa, BASIS, Infraestructura Técnica, Seguridad de la plataforma.
- Proponer políticas de mejoramiento continuo de los procesos.
- Modelar los cambios al interior de cada una de las áreas.

- Crear los indicadores de gestión que permitan medir el rendimiento y objetivos estratégicos de cada una de las áreas acordes a los lineamientos de calidad.

- Garantizar la operatividad del sistema, canales, comunicaciones y redes

- Actualizar el inventario de software, Hardware, aplicaciones que soportan el negocio tanto internos como externos.

6.2.2.2. **Objetivos**.

- Asesorar en los aspectos relacionados con políticas y la toma de decisiones en el área de tecnología información a la Coordinación.

- Asesor al negocio respecto a sus requerimientos de sistemas, comunicaciones, redes e infraestructura tecnológica.

- Mantener informado a la coordinación de las nuevas innovaciones en el campo de la informática, telecomunicaciones y/o redes y herramientas tecnológicas que soportan el Sistema de Información.

- Liderar la definición de la arquitectura técnica total de la plataforma de tecnológica que soporta el sistema de información Evaluar los riesgos vulnerables de uso y comportamiento de las tecnologías de la Información y las Comunicaciones en coordinación con la oficina de sistema de la entidad.

- Participar en los proyectos de implementación de nuevas tecnologías.

6.2.2.3. **Descripción de cargos y funciones.**

Jefe sección técnica

- Asesorar en los aspectos relacionados con políticas y la toma de decisiones en el área de tecnologías de la información
- Asesorar a las áreas de negocio respecto a sus requerimientos de sistemas, comunicaciones redes e infraestructura tecnología
- Mantenerse informado de las innovaciones en el campo de la informática, telecomunicaciones o redes y las nuevas herramientas tecnológicas que soportan el sistema de información.
- Liderar la definición de la arquitectura táctica total de la plataforma de tecnología que soporta el sistema de información.
- Presentar informes periódicos sobre el desarrollo de las actividades de la sección

- Participar en los proyectos de implementación de nuevas tecnologías
- Administrar y desarrollar el talento humano del personal a cargo
- Ejercer las demás funciones que le sean asignadas y que correspondan a la naturaleza de la dependencia.

Jefe de seguridad

- Coordinar el cumplimiento de la política de seguridad establecidas en la entidad
- Difundir la cultura de seguridad informática entre todos los miembros de la entidad
- Participar en el desarrollo implementación y certificación del sistema de gestión de calidad
- Evaluar y controlar del riesgo de la seguridad de la información
- Avalar en conjunto con el comité de control de cambios los pasos a productivo
- Analizar propuestas para el desarrollo de las políticas de seguridad de los roles de los usuarios de la plataforma de información.
- Seguimiento a las conexiones múltiples de los usuarios activos
- Ejercer las demás funciones que le sean asignadas y que correspondan a la naturaleza de la dependencia.

Basis/Netweaver

- Administrar y monitorear el sistema de información a nivel de sistema operativo
- Realizar la administración, verificación y monitoreo de las aplicaciones y subsistemas
- Administrar el sistema SMP.
- Verificación y monitoreo del sistema para detección de consumo
- Garantizar la realización de los transportes en los ambientes disponibles
- Gestionar los recursos de soporte a la mesa de ayuda en lo relacionado con problemas técnicos.
- Participar en los proyectos de implementación de nuevas tecnologías
- Ejercer las demás funciones que le sean asignadas y que correspondan a la naturaleza de la dependencia.

Jefe infraestructura

- Coordinar el funcionamiento efectivo de los procesos operativos de la infraestructura tecnológica.
- Supervisar los procesos de licitación y contratación de productos y servicios asignados.
- Planificar procesos de planeación de capacidad y demanda de la infraestructura de la plataforma tecnológica
- Administrar los servicios de los servidores

- Desarrollar y documentar los procedimientos de administración y control de la infraestructura tecnológica
- Ejercer las demás funciones que le sean asignadas y que correspondan a la naturaleza de la dependencia.

6.2.2.4. Infraestructura tecnológica

La infraestructura tecnológica de la entidad está conformada por una red de comunicaciones WAN y LAN y sus sistemas de información.

La entidad caso estudio cuenta con una red WAN la cuneta con una cobertura en el área geográfica de Colombia con la cual se puede comunicar múltiples servicios mediante la transmisión de datos y voz.

Por medio de la red WAN (MPLS) permite cubrir áreas mayores con las cuales se consigue comunicación a nivel nacional, con una cobertura extensa y una interconexión de varias áreas metropolitana.

La estructura de la red de la entidad está compuesta por: zonas desmilitarizadas, Sucursales a nivel nacional e internacional, Data Center.

En los Data Center se pueden encontrar el Portal institucional y el sistema de información misional de la entidad.

6.2.2.5. Políticas de uso para la utilización de los PC.

- Los funcionarios que hagan uso de los equipos de cómputo de la entidad, tendrán que estar autorizados y tener diligenciado y actualizado el formato de confidencialidad.

- Los computadores no pueden estar encendidos y en modo activo sin que el funcionario se encuentre en el equipo trabajando.

- Los computadores de escritorio, computadores portátiles que sean conectados a la red corporativa de la entidad, no deben mostrar las contraseñas en pantalla.

- Las contraseñas para el acceso a la red institucional deben tener un período de vigencia y, una vez alcanzado éste, se debe exigir cambio de contraseña. De manera adicional.

- Las contraseñas deben tener una longitud mínima de 8 caracteres y deben contener por lo menos una letra mayúscula, una letra minúscula, un número y un carácter especial. Se debe solicitar el cambio de contraseña para el acceso a la red institucional, la primera vez que se haga uso del código de identificación y/o cuenta de usuario.

- Las contraseñas de los servidores deben ser cambiadas cada 6 meses, utilizando un mínimo de 12 caracteres para los servidores ambiente Windows, y máximo 8 caracteres para el ambiente UNIX – AIX.

6.2.2.6. Políticas de uso para la utilización de INTERNET

El servicio de Internet en la entidad, se hará uso del internet como una herramienta de apoyo a las funciones y responsabilidades de los funcionarios, para lo cual el uso del mismo debe estar autorizado por el coordinador de la oficina.

- El uso del Servicio de Internet está limitado exclusivamente para propósitos laborales.

- Los servicios a los que un determinado usuario pueda acceder desde la Internet dependerán del rol que desempeña el usuario en la entidad y para los cuales este formal y expresamente autorizado.

- Está expresamente prohibido el acceso a páginas web, portales, sitios web y/o aplicaciones web que no hayan sido autorizadas por la coordinación.

- Está expresamente prohibido el envío y/o descarga de cualquier tipo de software archivos de fuentes externas y/o de procedencia desconocida.

- Está expresamente prohibido acceder a páginas que agredan la ética y el buen comportamiento.

La entidad se reserva el derecho de monitorear los accesos y por tanto uso del Servicio de Internet de todos sus funcionarios, además de limitar el acceso a determinadas páginas de Internet.

6.3. SISTEMAS DE INFORMACION

La entidad caso estudio, administra y soporta el Enterprise Resource Planning, en español “sistema de planificación de recursos empresariales ERP, el cual se encuentra instalado bajo los siguientes módulos:

- PP: (Production Planning) Planificación de la producción.
- MM: (Materials Management) Gestión de Materiales.
- SD: (Sales and Distribution) Ventas y Distribución.
- FI: (Finanzas) Contabilidad Financiera
- CO: (Controlling) Control y Costos.
- BC Basis Components

6.3.1. SERVICIOS QUE PRESTAN

La entidad caso estudio como implementador y administrador de la plataforma SAP implementa, capacita y soporta en los diferentes módulos que se encuentran implementados.

7. CLASIFICACION DE LOS ACTIVOS DE INFORMACION CON LOS QUE CUENTA LA ENTIDAD CASO ESTUDIO BASADOS EN LA METODOLOGIA MAGERIT

7.1. INTRODUCCIÓN.

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

7.2. CLASIFICACIÓN DE LA INFORMACIÒN

Basados en el Departamento Administrativo de la Presidencia de la República DAPRE, Un activo de información puede tener las siguientes características, independiente del tipo de activo[50]:

- El activo de información es reconocido como valioso para el DAPRE.
- No es fácilmente reemplazable sin incurrir en costos, habilidades especiales, tiempo, recursos o combinación de los mismos.
- Forma parte de la identidad de la entidad y sin la cual el DAPRE puede estar en algún nivel de riesgo. (La determinación del nivel y tipo de riesgo se estima sobre la base del Modelo Estándar de Control Interno MECI del DAPRE).

Con base en el DAPRE y de acuerdo al riesgo y a la exposición, se puede calificar la Información en pública, información pública reservada o información pública clasificada (privada y semiprivada).

Información pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.[51]

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.[52]

[50] Presidencia de la Republica, guía para la calificación de la información de acuerdo con sus niveles de seguridad, marzo 2017
[51] Artículo 5 Ley 1712 de 2014
[52] Artículo 18 Ley 1712 de 2014

Información reservada: Su divulgación indebida puede afectar bienes o intereses públicos.[53].

7.3. ACTIVOS INFORMATICOS

Son el eslabón de información determinable e identificable, que se puede ubicar en cualquier medio, 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]

Tabla 14 Activos de información

Tipo de activo	Código de activo	Activos más relevantes en la entidad
[AUX] Equipamiento auxiliar	POWER	UPS. IBM Smart-UPS DE 1400 VA 2 U 230 V PARA RACK
[COM] Redes de comunicaciones	WIFI	Equipos de la red inalámbrica (router, Punto de acceso Cisco WAP121 Wireless-N con configuración de un solo punto
[HW] Equipamiento informático (hardware)	HOST	Datacenter. IBM Power System S814
		Servidores aplicaciones IBM Power System S822LC para Big Data
	NETWORK	Switch core. IBM System Networking RackSwitch G8264
		Equipos de la red cableada (router, Cisco MDS 9718 Multilayer Director for IBM Storage Networking)
	PC	Computadoras Desktop HP All-in-One 200-5030
		Portátiles HP 530

[53] Artículo 19 Ley 1712 de 2014

	FIREWALL	Firewall. Cortafuegos de hardware dedicado IBM
	PRINT	Servicios de Impresión Lexmark
[L] Instalaciones	BUILDING	Control de Ingreso al edificio BTX V3
		Oficinas, Recepción, Sala de espera, Sala de reunión.
[P] Personal	UE	Portafolio de servicios
		Manuales procedimentales del sistema de información
		Mesa de Servicio
		Portales Empresariales
		Planes de acción.
	COM	Canal de comunicaciones.
	OP	Empresa prestadora de servicios técnicos de sistemas
	UI	Chat interno Comuni
		Llamadas telefónicas externas
		Coordinación
		Personal técnico
		Recepción
[S] Servicios	[ext] a usuarios externos (bajo una relación contractual)	Capacitación usuarios finales
		Página Web externa
		Informática / Soporte técnico interno
		Soporte técnico externo
	[int] interno	Página Web interna (Intranet)
[SW] Software - Aplicaciones informáticas	PRP	Módulos SAP
		Sistema de información SAP ECC 6.0 EHP 8
	APP	Servidores aplicaciones IBM Power System S814, AIX Versión 6.1
	STD	VPN GlobalProtect PaloAlto
	SUB	Software gestión documental Orfeo
		Servicio de limpieza de planta
	SUBD	software suit visión
	DBMS	Base de datos Oracle Linux 6

		Base de datos de desarrollo Oracle Linux 6.
		Base de datos de pruebas Oracle Linux 6.
		Base de datos producción Oracle Linux 6.
		Base de datos B.I. Oracle Linux 6
	EMAIL_CLIENT	Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)
	EMAIL _SERVER	Correo electrónico
	BACKUP	Respaldos IBM Tivoli Directory Server Versión 6.2
	BROWSER	Navegación en Internet Google Chrome
	FILES	Planes, Documentación, Manuales, Formatos.

Fuente: Autor.

7.4. CLASIFICACION DE LOS ACTIVOS DE LA INFOMACIÒN

Tabla 15 Matriz clasificación de los activos de información

Tipo de activo	Código de activo	Activos más relevantes en la entidad	Clasificación de la información
[AUX] Equipamiento auxiliar	POWER	UPS. IBM Smart-UPS DE 1400 VA 2 U 230 V PARA RACK	Clasificada
[COM] Redes de comunicaciones	WIFI	Equipos de la red inalámbrica (router, Punto de acceso Cisco WAP121 Wireless-N con configuración de un solo punto	Reservada
[HW] Equipamiento informático (hardware)	HOST	Datacenter. IBM Power System S814	Reservada
		Servidores aplicaciones IBM Power System S822LC para Big Data	Reservada
	NETWORK	Switch core. IBM System Networking RackSwitch G8264	Reservada

		Equipos de la red cableada (router, Cisco MDS 9718 Multilayer Director for IBM Storage Networking)	Reservada
	PC	Computadoras Desktop HP All-in-One 200-5030	Clasificada
		Portátiles HP 530	Clasificada
	FIREWALL	Firewall. Cortafuegos de hardware dedicado IBM	Reservada
	PRINT	Servicios de Impresión Lexmark	Publica
[L] Instalaciones	BUILDING	Control de Ingreso al edificio BTX V3	Publica
		Oficinas, Recepción, Sala de espera, Sala de reunión.	Publica
[P] Personal	UE	Portafolio de servicios	Clasificada
		Manuales procedimentales del sistema de información	Publica
		Mesa de Servicio	Publica
		Portales Empresariales	Clasificada
		Planes de acción.	Publica
	COM	Canal de comunicaciones.	Reservada
	OP	Empresa prestadora de servicios técnicos de sistemas	Clasificada
	UI	Chat interno Comuni	Clasificada
		Llamadas telefónicas externas	Clasificada
		Coordinación	Publica
		Personal técnico	Clasificada
		Recepción	Publica
[S] Servicios	[ext] a usuarios externos (bajo una relación contractual)	Capacitación usuarios finales	Publica
		Página Web externa	Clasificada
		Informática / Soporte técnico interno	Publica
		Soporte técnico externo	Publica

	[int] interno	Página Web interna (Intranet)	Reservada
[SW] Software - Aplicaciones informáticas	PRP	Módulos SAP	Reservada
		Sistema de información SAP ECC 6.0 EHP 8	Reservada
	APP	Servidores aplicaciones IBM Power System S814, AIX Versión 6.1	Reservada
	STD	VPN GlobalProtect PaloAlto	Clasificada
	SUB	Software gestión documental Orfeo	Reservada
		Servicio de limpieza de planta	Publica
	SUBD	software suit visión	Clasificada
	DBMS	Base de datos Oracle Linux 6	Reservada
		Base de datos de desarrollo Oracle Linux 6.	Reservada
		Base de datos de pruebas Oracle Linux 6.	Reservada
		Base de datos producción Oracle Linux 6.	Reservada
		Base de datos B.I. Oracle Linux 6	Reservada
	EMAIL_CLIENT	Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	Clasificada
	EMAIL _SERVER	Correo electrónico	Reservada
	BACKUP	Respaldos IBM Tivoli Directory Server Versión 6.2	Reservada
	BROWSER	Navegación en Internet Google Chrome	Clasificada
	FILES	Planes, Documentación, Manuales, Formatos.	Reservada

Fuente: Autor.

7.5. DIMENSIONES DE VALORACION

Partiendo de las características y atributos que le dan el valor a un activo. Una dimensión es un aspecto de un activo, independiente de otros aspectos. Pueden hacerse análisis de riesgos centrados en un único aspecto, independientemente de lo que ocurra con otros.

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

- Disponibilidad [D]

¿Qué importancia tendría que el activo no estuviera disponible?

- Integridad [I]

¿Qué importancia tendría que los datos fueran modificados fuera de control?

- Confidencialidad [C]

¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?

- Trazabilidad [T]

¿Qué importancia tendría que no quedara constancia fehaciente del uso del servicio?

7.5.1. de acuerdo al impacto. La valoración de acuerdo al impacto permite comparar los diferentes riesgos permitiendo tener un análisis para cada una de las dimensiones, cuando la evaluación se hace de acuerdo al impacto y se hace de forma cualitativa su valoración se da de forma subjetiva.

El impacto Hace referencia al daño causado sobre un activo atraído por la materialización de las amenazas, el impacto sobre los activos es originado por la valoración más el porcentaje de degradación que es originado por las amenazas.

La estimación de impactos de estos porcentajes se hace en función de varios factores, como son:

- La ejecución de una amenaza puede de perjudicar a todo un recurso de información o solo a una parte del mismo.

- Ante la materialización de una amenaza perjudica a partes claves o partes dependientes del recurso de información.

- Si la amenaza, una vez perpetrada, tiene consecuencias de forma temporal o de forma permanente hacia el recurso.[54]

Se encuentran dos tipos de impactos, el acumulado y el residual, en el primero podemos determinar el impacto al cual se expone el activo, teniendo como base el valor derivado de cada uno de los activos y la valoración de las amenazas; el impacto residual es aquel resultado al termino de combinar el valor estipulado en cada uno de los activos con la valoración de las amenazas y la efectividad de las salvaguardas aplicadas.

7.5.1.1. Criterios de valoración. Es importante que cada uno de los activos sean valorados incluyendo cada uno de los procesos con los que cuentan las áreas.

La valoración consiste en asignar un valor a cada uno de los activos teniendo en cuenta cada uno de las dimensiones y su importancia a nivel de seguridad, tal como lo estipula la metodología MAGERIT: seguridad: la disponibilidad, integridad, confidencialidad y trazabilidad; para esto MAGERIT concierta dos clases de valoración, la cuantitativa y la cualitativa, "La valoración cualitativa permite calcular un valor a través de una escala cualitativa donde se valora el activo de acuerdo al impacto que puede causar en la empresa su daño o perdida".[55].

Se tiene una escala cualitativa que permite valorar el activo de acuerdo a su impacto que puede hacer daño

- **[D]: Despreciable**
- **B: bajo**
- **M: medio**
- **A: alto**
- **MA: muy alto**
- **[E]: Extremo**

La tabla N.3 de valoración de acuerdo al impacto permite tener una relación entre un valor determinado por la metodología y una escala cualitativa para medir el impacto que puede causar el daño del activo.

[54] HINA LUZ Garavito robles, tesis de grado análisis y gestión del riesgo de la información en los sistemas de seguridad de la información, UNAD, (2015), p. 53.
[55] HINA LUZ Garavito robles, tesis de grado análisis y gestión del riesgo de la información en los sistemas de seguridad de la información, UNAD, (2015), p. 55.

Tabla 16 Valoración de acuerdo al impacto.

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

7.5.1.2. Valoración de activos. Se realiza la respectiva valoración de los activos de la entidad caso estudio previamente identificados y clasificados, con el objetivo de determinar el impacto que pudieren tener y la descripción de acuerdo a la escala estándar que la metodología MAGERIT brinda para homogenizar cada uno de los activos, ver tabla 4.

Tabla 17 Valoración de Activos de acuerdo al impacto.

Tipo de activo	Código de activo	Nombre del Activo de la información	Impacto	Descripción
[AUX] Equipamiento auxiliar	POWER	UPS. IBM Smart-UPS DE 1400 VA 2 U 230 V PARA RACK	M	(7.da)
[COM] Redes de comunicaciones	WIFI	Equipos de la red inalámbrica (router, Punto de acceso Cisco WAP121 Wireless-N con configuración de un solo punto	M	(7.si)
[HW] Equipamiento informático (hardware)	HOST	Datacenter. IBM Power System S814	MA	(7.da)
		Servidores aplicaciones IBM Power System S822LC para Big Data	MA	(7.da2)
	NETWORK	Switch core. IBM System Networking RackSwitch G8264	A	(9.si)

		Equipos de la red cableada (router, Cisco MDS 9718 Multilayer director for IBM Storage Networking)	B	(7.si)
	PC	Computadoras Desktop HP All-in-One 200-5030	A	(7.si)
		Portátiles HP 530	M	(7.si)
	FIREWALL	Firewall.Cortafuegos de hardware dedicado IBM	A	(9.si)
	PRINT	Servicios de Impresión Lexmark	B	(1.oml)
[L] Instalaciones	BUILDING	Control de Ingreso al edificio BTX V3	B	0
		Oficinas, Recepción, Sala de espera, Sala de reunión.	B	(1.oml)
[P] Personal	UE	Portafolio de servicios	B	(7.lg.a)
		Manuales procedimentales del sistema de información	B	(7.lg.a)
		Mesa de Servicio	M	(3.oml)
		Portales Empresariales	A	(1.oml)
		Planes de acción.	B	(1.oml)
	COM	Canal de comunicaciones.	M	(7.da2)
	OP	Empresa prestadora de servicios técnicos de sistemas	A	(3.pi.2)
	UI	Chat interno Comuni	B	(1.oml)
		Llamadas telefónicas externas	MB	(1.oml)
		Coordinación	M	(3.pi.3)
		Personal técnico	A	(3.pi.4)
		Recepción	MB	(3.pi.2)
[S] Servicios	[ext] a usuarios externos (bajo	Capacitación usuarios finales	M	(5lg.a)
		Página Web externa	M	(1.da)

	una relación contractual)	Informática / Soporte técnico interno	M	(3.pi.3)
		Soporte técnico externo	M	(3.pi.4)
	[int] interno	Página Web interna (Intranet)	A	(1.da)
[SW] Software - Aplicaciones informáticas	PRP	Módulos SAP	MA	(7.da2)
		Sistema de información SAP ECC 6.0 EHP 8	MA	(10.olm)
	APP	Servidores aplicaciones IBM Power System S814, AIX Versión 6.1	A	(9.si)
	STD	VPN GlobalProtect PaloAlto	M	(7.da)
	SUB	Software gestión documental Orfeo	MB	(1.adm)
		Servicio de limpieza de planta	B	(3.pi.2)
	SUBD	software suite vision	B	(1.oml)
	DBMS	Base de datos Oracle Linux 6	A	(9.si)
		Base de datos de desarrollo Oracle Linux 6.	A	(10.lbl)
		Base de datos de pruebas Oracle Linux 6.	A	(10.lbl)
		Base de datos producción Oracle Linux 6.	A	(10.lbl)
		Base de datos B.I. Oracle Linux 6	A	(10.lbl)
	EMAIL_CLIENT	Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	B	(3.da)
	EMAIL _SERVER	Correo electrónico	M	(1.da)
	BACKUP	Respaldos IBM Tivoli Directory Server Versión 6.2	A	(10.lbl)

	BROWSER	Navegación en Internet Google Chrome	M	(1.da)
	FILES	Planes, Documentación, Manuales, Formatos.	A	(1.adm)

Fuente: Autor

7.5.2. 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"[56].

[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.

7.5.2.1. Criterios de Valoración. Mediante una tabla comprendida por una escala de 10 valores iniciando en 0como el valor despreciable a nivel de riesgo, hasta llegar a 10 que sería el valor que se le puede dar a un activo con un daño extremo.

[56]AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 7-13.

Tabla 18 Criterios de Valoración de acuerdo a las dimensiones de seguridad.

Valor			Criterio
10	Muy alto	[MA]	Daño muy grave
7-9	Alto	[A]	Daño grave
4-6	Medio	[M]	Daño importante
0-3	Bajo	[B]	Daño menor
0	Despreciable	[D]	Irrelevante a efectos prácticos

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

7.5.2.2. Valoración de los activos.

Tabla 19 Valoración de activos de acuerdo a la dimensión

Tipos de activos	Nombre de activos	Valoración de los activos				
		[D]	[C]	[I]	[A]	[T]
[AUX] Equipamiento auxiliar	UPS. IBM Smart-UPS DE 1400 VA 2 U 230 V PARA RACK	A	M	M	A	A
[COM] Redes de comunicaciones	Equipos de la red inalámbrica (router, Punto de acceso Cisco WAP121 Wireless-N con configuración de un solo punto	M	B	B	M	M
[HW] Equipamiento informático (hardware)	Datacenter. IBM Power System S814	A	A	MA	A	MA
	Servidores aplicaciones IBM Power System S822LC para Big Data	MA	MA	MA	MA	MA
	Switch core. IBM System Networking RackSwitch G8264	A	A	A	A	A
	Equipos de la red cableada (router, Cisco MDS 9718 Multilayer director for IBM Storage Networking)	MA	MA	MA	MA	MA
	Computadoras Desktop HP All-in-One 200-5030	MA	MA	MA	MA	MA
	Portátiles HP 530	MA	MA	MA	MA	MA
	Firewall.Cortafuegos de hardware dedicado IBM	A	A	MA	A	A

	Servicios de Impresión Lexmark	M	B	M	B	M
[L] Instalaciones	Control de Ingreso al edificio BTX V3	B	M	M	A	B
	Oficinas, Recepción, Sala de espera, Sala de reunión.	M	M	M	M	M
[P] Personal	Portafolio de servicios	M	MA	M	M	M
	Manuales procedimentales del sistema de información	B	B	B	B	A
	Mesa de Servicio	M	A	B	B	M
	Portales Empresariales	B	M	B	B	MA
	Planes de acción.	B	B	D	B	B
	Canal de comunicaciones.	MA	A	MA	A	MA
	Empresa prestadora de servicios técnicos de sistemas	M	B	B	B	M
	Chat interno Comuni	B	B	B	B	B
	Llamadas telefónicas externas	B	B	B	B	B
	Coordinación	MA	MA	MA	MA	MA
	Personal técnico	MA	MA	MA	MA	MA
	Recepción	M	M	M	M	M
[S] Servicios	Capacitación usuarios finales	M	MA	M	D	M
	Página Web externa	M	M	M	M	M
	Informática / Soporte técnico interno	M	M	M	M	M
	Soporte técnico externo	M	M	M	M	M
	Página Web interna (Intranet)	M	M	M	M	M
[SW] Software - Aplicaciones informáticas	Módulos SAP	MA	MA	MA	MA	MA
	Sistema de información SAP ECC 6.0 EHP 8	MA	A	MA	A	MA

	Servidores aplicaciones IBM Power System S814, AIX Versión 6.1	MA	A	A	A	MA
	VPN GlobalProtect PaloAlto	MA	MA	A	MA	A
	Software gestión documental Orfeo	B	B	B	B	B
	Servicio de limpieza de planta	B	B	B	B	B
	software suit visión	MA	MA	MA	MA	MA
	Base de datos Oracle Linux 6	MA	MA	A	A	MA
	Base de datos de desarrollo Oracle Linux 6.	MA	MA	A	A	MA
	Base de datos de pruebas Oracle Linux 6.	MA	M	A	M	MA
	Base de datos producción Oracle Linux 6.	MA	MA	MA	MA	MA
	Base de datos B.I. Oracle Linux 6	MA	MA	MA	MA	MA
	Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	M	M	B	M	M
	Correo electrónico	M	M	M	M	M
	Respaldos IBM Tivoli Directory Server Versión 6.2	M	M	M	M	M
	Navegación en Internet Google Chrome	M	M	M	M	M
	Planes, Documentación, Manuales, Formatos.	M	B	M	M	B

Fuente: Autor.

8. IDENTIFIACAR LAS VULNERABILIDADES, AMENAZAS O RIESGOS A QUE ESTÁN EXPUESTOS LOS ACTIVOS DE INFORMACIÓN DE LA ENTIDAD CASO ESTUDIO

8.1. INTRODUCCIÓN

En la determinación de vulnerabilidades, amenazas y riesgos se busca proporcionar todas las posibles amenazas a las cuales un activo se puede ver afectado en las diferentes dimensiones de seguridad que MAGERIT propone, con el objetivo de asignar un valor coherente se debe estimar la frecuencia de ocurrencia y el rango porcentual de impacto para los activos.

Se relacionan las posibles amenazas a las cuales se puede ver expuesto un activo, determinando su frecuencia de presencia en los activos y la dimensión de seguridad que esta está afectando, para esto se hace uso de una tabla que permite determinar la frecuencia en la que se presenta.

8.2. IDENTIFICACIÓN Y VALORACIÓN DE LAS AMENAZAS.

Para valorar el nivel o frecuencia de la amenaza en cada activo, es necesario valorar también el impacto que sería en realidad el daño causado al activo en caso de materialización de una amenaza; Así mismo 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.

Tabla 20 Tipos de amenazas.

Nomenclatura	Tipos de amenazas	Descripción
[N]	Desastres naturales	Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.
[I]	De origen industrial	Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.
[E]	Errores y fallos no intencionados	Fallos no intencionales causados por las personas.

[A]	Ataques intencionados	Fallos deliberados causados por las personas

Fuente: Autor.

Tabla 21 Definición 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: Autor.

8.2.1. Criterios de evaluación. Con el fin de medir el nivel de frecuencia de una amenaza en los activos de la organización se hace necesario tener el valor del impacto el cual es el equivalente al daño generado al activo, esto en el caso de que se materialice una amenaza, permitiendo de esta forma determinar el grado de afectación en cada una de las dimensiones de seguridad.

Tabla 22 Probabilidad de ocurrencia.

NOMENCLATURA	Valor	Criterio	
		Frecuencia	Rango de Frecuencia
MF	100	Muy frecuente	A diario
F	10	Frecuente	Mensualmente
FN	1	Normal	Una vez al año
PF	1/10	Poco frecuente	Cada varios años
MB	1/100	Muy poco frecuente	Siglos

Fuente: Autor.

8.2.2. Evaluación de las amenazas a los activos. la valoración del impacto que pueden tener cada una de las amenazas en caso de que se materialicen en cada uno de los diferentes activos para las distintas dimensiones de seguridad, teniendo en cuenta la frecuencia en que la amenaza puede impactar los activos en cada uno de las dimensiones de seguridad. Ver tabla 10.

Tabla 23 Amenazas de los activos.

Tipos de activos	Nombre de activos	Amenaza	Frecuencia	[D]	[C]	[I]	[A]	[T]
[AUX] Equipamiento auxiliar	UPS. IBM Smart-UPS DE 1400 VA 2 U 230 V PARA RACK	[E.4]	FN	A	M	M	A	A
[COM] Redes de comunicaciones	Equipos de la red inalámbrica (router, Punto de acceso Cisco WAP121 Wireless-N con configuración de un solo punto	[A.7]	FN	M	B	B	M	M
[HW] Equipamiento informático (hardware)	Datacenter. IBM Power System S814	[E.2]	FN	A	A	MA	A	MA
	Servidores aplicaciones IBM Power System S822LC para Big Data	[E.17]	FN	MA	MA	MA	MA	MA
	Switch core. IBM System Networking RackSwitch G8264	[E.19]	FN	A	A	A	A	A
	Equipos de la red cableada (router, Cisco MDS 9718 Multilayer director for IBM Storage Networking)	[E.4]	FN	MA	MA	MA	MA	MA
	Computadoras Desktop HP All-in-One 200-5030	[I.8]	FN	MA	MA	MA	MA	MA
	Portátiles HP 530	[N.*]	PF	MA	MA	MA	MA	MA
	Firewall. Cortafuegos de hardware dedicado IBM	[A.14]	FN	A	A	MA	A	A
	Servicios de Impresión Lexmark	[I.8]	FN	M	B	M	B	M
[L] Instalaciones	Control de Ingreso al edificio BTX V3	[N.*]	PF	B	M	M	A	B
	Oficinas, Recepción, Sala de espera, Sala de reunión.	[E.21]	FN	M	M	M	M	M
[P] Personal	Portafolio de servicios	[E.2]	FN	M	MA	M	M	M
	Manuales procedimentales del sistema de información	[E.2]	PF	B	B	B	B	A
	Mesa de Servicio	[E.28]	FN	M	A	B	B	M
	Portales Empresariales	[E.18]	FN	B	M	B	B	MA
	Planes de acción.	[A.7]	FN	B	B	D	B	B
	Canal de comunicaciones.	[I.8]	FN	MA	A	MA	A	MA
	Empresa prestadora de servicios técnicos de sistemas	[N.*]	PF	M	B	B	B	M
	Chat interno Comuni	[E.19]	FN	B	B	B	B	B
	Llamadas telefónicas externas	[A.8]	FN	B	B	B	B	B

	Coordinación	[E.18]	F	MA	MA	MA	MA	MA
	Personal técnico	[A.8]	FN	MA	MA	MA	MA	MA
	Recepción	[E.18]	FN	M	M	M	M	M
[S] Servicios	Capacitación usuarios finales	[A.11]	PF	M	MA	M	D	M
	Página Web externa	[E.15]	FN	M	M	M	M	M
	Informática / Soporte técnico interno	[E.18]	FN	M	M	M	M	M
	Soporte técnico externo	[A.14]	FN	M	M	M	M	M
	Página Web interna (Intranet)	[N.*]	FN	M	M	M	M	M
[SW] Software - Aplicaciones informáticas	Módulos SAP	[A.5]	F	MA	MA	MA	MA	MA
	Sistema de información SAP ECC 6.0 EHP 8	[E.4]	FN	MA	A	MA	A	MA
	Servidores aplicaciones IBM Power System S814, AIX Versión 6.1	[A.8]	FN	MA	A	A	A	MA
	VPN GlobalProtect PaloAlto	[I.7]	FN	MA	MA	A	MA	A
	Software gestión documental Orfeo	[I.7]	FN	B	B	B	B	B
	Servicio de limpieza de planta	[A.8]	FN	B	B	B	B	B
	software suit visión	[I.8]	F	MA	MA	MA	MA	MA
	Base de datos Oracle Linux 6	[A.15]	FN	MA	MA	A	A	MA
	Base de datos de desarrollo Oracle Linux 6.	[E.18]	FN	MA	MA	A	A	MA
	Base de datos de pruebas Oracle Linux 6.	[E.18]	FN	MA	M	A	M	MA
	Base de datos producción Oracle Linux 6.	[A.8]	FN	MA	MA	MA	MA	MA
	Base de datos B.I. Oracle Linux 6	[E.18]	FN	MA	MA	MA	MA	MA
	Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	[E.4]	FN	M	M	B	M	M
	Correo electrónico	[I.7]	FN	M	M	M	M	M
	Respaldos IBM Tivoli Directory Server Versión 6.2	[E.19]	FN	M	M	M	M	M
	Navegación en Internet Google Chrome	[A.5]	FN	M	M	M	M	M
	Planes, Documentación, Manuales, Formatos.	[N.*]	PF	M	B	M	M	B

Fuente: Autor.

8.3. RIESGO POTENCIAL

Para la estimación 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.

8.3.1. Criterios de evaluación. Los criterios que se utilizan para la evaluación del Impacto, probabilidad y riesgo por medio de escalas y según lo determina MAGERIT, se dan de acuerdo a una escala que va desde muy bajo hasta muy alto, permitiendo así poder identificar su nivel de impacto la probabilidad de que ocurra o materialice y el valor del riesgo en el activo, esto se conoce como evaluación cualitativa:

Tabla 24 Valoración del riesgo

	Escalas	
Impacto	**Probabilidad**	**Riesgo**
MA: muy alto	MA: prácticamente seguro	MA: crítico
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: Autor.

La tabla 13 permite evaluar de forma combinada el impacto y la frecuencia con el fin de calcular el riesgo:

Tabla 25 Valoración del riesgo 2

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

Fuente: Autor.

8.3.2. Evaluación del riesgo potencial a 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.

Tabla 26 Riesgo potencial de los activos

Tipos de activos	Nombre de activos	Amenaza	Impacto	Probabilidad	Riesgo
[AUX] Equipamiento auxiliar	UPS. IBM Smart-UPS DE 1400 VA 2 U 230 V PARA RACK	[E.4]	M	M	M
[COM] Redes de comunicaciones	Equipos de la red inalámbrica (router, Punto de acceso Cisco WAP121 Wireless-N con configuración de un solo punto	[A.7]	B	MB	B
[HW] Equipamiento informático (hardware)	Datacenter. IBM Power System S814	[E.2]	A	M	M
	Servidores aplicaciones IBM Power System S822LC para Big Data	[E.17]	B	MB	MB
	Switch core. IBM System Networking RackSwitch G8264	[E.19]	M	M	M
	Equipos de la red cableada (router, Cisco MDS 9718 Multilayer director for IBM Storage Networking)	[E.4]	M	B	B
	Computadoras Desktop HP All-in-One 200-5030	[I.8]	M	M	M
	Portátiles HP 530	[N.*]	M	M	M
	Firewall. Cortafuegos de hardware dedicado IBM	[A.14]	MA	B	M
	Servicios de Impresión Lexmark	[I.8]	M	M	M
[L] Instalaciones	Control de Ingreso al edificio BTX V3	[N.*]	MB	M	MB

	Oficinas, Recepción, Sala de espera, Sala de reunión.	[E.21]	A	M	M
[P] Personal	Portafolio de servicios	[E.2]	MA	B	M
	Manuales procedimentales del sistema de información	[E.2]	M	A	M
	Mesa de Servicio	[E.28]	A	A	A
	Portales Empresariales	[E.18]	MA	B	M
	Planes de acción.	[A.7]	MA	B	M
	Canal de comunicaciones.	[I.8]	A	M	M
	Empresa prestadora de servicios técnicos de sistemas	[N.*]	A	M	M
	Chat interno Comuni	[E.19]	M	B	B
	Llamadas telefónicas externas	[A.8]	M	M	M
	Coordinación	[E.18]	M	A	M
	Personal técnico	[A.8]	M	A	M
	Recepción	[E.18]	MA	M	A
[S] Servicios	Capacitación usuarios finales	[A.11]	B	M	B
	Página Web externa	[E.15]	M	M	M
	Informática / Soporte técnico interno	[E.18]	M	M	M
	Soporte técnico externo	[A.14]	M	B	B
	Página Web interna (Intranet)	[N.*]	M	M	M
[SW] Software - Aplicaciones informáticas	Módulos SAP	[A.5]	A	M	M
	Sistema de información SAP ECC 6.0 EHP 8	[E.4]	M	A	M
	Servidores aplicaciones IBM Power System S814, AIX Versión 6.1	[A.8]	MA	B	M
	VPN GlobalProtect PaloAlto	[I.7]	M	M	M
	Software gestión documental Orfeo	[I.7]	B	B	B

	Servicio de limpieza de planta	[A.8]	M	B	B
	software suit visión	[I.8]	M	M	M
	Base de datos Oracle Linux 6	[A.15]	A	MA	MA
	Base de datos de desarrollo Oracle Linux 6.	[E.18]	A	M	M
	Base de datos de pruebas Oracle Linux 6.	[E.18]	A	MA	MA
	Base de datos producción Oracle Linux 6.	[A.8]	M	M	M
	Base de datos B.I. Oracle Linux 6	[E.18]	A	M	M
	Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	[E.4]	A	M	M
	Correo electrónico	[I.7]	A	A	A
	Respaldos IBM Tivoli Directory Server Versión 6.2	[E.19]	M	B	B
	Navegación en Internet Google Chrome	[A.5]	M	B	B
	Planes, Documentación, Manuales, Formatos.	[N.*]	M	B	B

Fuente: Autor.

9. FORMULACIÓN DE CONTROLES A LOS ACTIVOS DE INFORMACIÓN DE ACUERDO AL ANEXO A DE LA NORMA ISO 27001:2013

Basados en el anexo A y en cada una de las amenazas y vulnerabilidades, se determinan los controles para cada uno de los activos previamente identificados y clasificados.

9.1. DEFINCIÒN DE CONTROLES

Tabla 27 Definición de controles.

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 realizar el plan de seguridad se deben definir las políticas que se usarán y se fomentarán a los empleados para que estos entren a participar en el proceso de seguridad de la información de la entidad caso estudio.
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 verificar el cumplimiento de dichas 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 de la seguridad de la información.	X		X		Si aplica porque dependiendo del cargo que desempeñe en el departamento de recursos humanos, se le asignará un rol 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 empleados son responsables de la labor que se les asigna y son conscientes de las consecuencias que puede traer un acto de imprudente o no adecuado.
A6.1.3	Contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.	X		X		Si aplica porque existe una jerarquía y un sistema de vigilancia
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 los activos del departamento no son tan sofisticados ni desconocidos de tal manera que no se requiere de un tratamiento especializado
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 porque en el área de recursos humanos se maneja el recurso económico que maneja la entidad caso estudio.
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 porque se debe prevenir el saqueo de información o envió de datos a través de los móviles
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	No aplica porque la entidad caso estudio no maneja la modalidad de teletrabajo
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		Si aplica porque el departamento debe tener políticas claras y previamente establecidas para hacer una buena elección del personal que hará parte de la entidad caso estudio.
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 porque se está trabajando con el área de recursos humanos donde se manejan los respectivos contratos de la entidad caso estudio.
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	No aplica porque los encargados de la seguridad del departamento de recursos humanos no son todos los de la entidad caso estudio
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 regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	X		X		Si porque los empleados deben ser educados para un mejor manejo de la información.
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 deben existir 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	No aplica porque en la entidad caso estudio los empleados son pocos para estar cambiando de responsabilidades.
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 porque teniendo en cuenta los activos más relevantes para el departamento se pueden aplicar las medidas necesarias para su protección
A8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.		X		X	No aplica porque es una entidad pública.
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		Si aplica porque se deben establecer reglas que permitan proteger los activos relevantes para el negocio
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	No aplica porque los activos son del departamento, no de los empleados.
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	No aplica porque toda la información requiere el mismo cuidado.

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	No aplica porque el departamento no cuenta con un esquema 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 porque si existe 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 porque no se estiman 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 momento 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.
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 porque el tráfico de los usuarios en la red se controla, bloqueando determinadas páginas web.

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, para posibilitar la asignación de los derechos de acceso.		X		X	No aplica porque los usuarios son pocos
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	No aplica porque para revocarle los derechos a los usuarios se deshabilitan del sistema.
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 usuarios tienen diferentes privilegios, dependiendo del cargo 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 usuario 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	No aplica porque la entidad es pública
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.
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	No aplica porque las aplicaciones diferentes al sistema no tienen el acceso controlado
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	No aplica porque los programas utilitarios son muy básicos
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 porque se hacen implementaciones.
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	No aplica porque los usuarios solo usan el sistema, no implementa el código de este.
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	No aplica porque no se manejan datos encriptados
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 porque cuenta con un servicio de vigilancia.
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 porque el departamento es grande y sus principales activos no están en el sistema.
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 existe un sistema de vigilantes del departamento físico
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 porque se debe tener un plan de contingencia en caso de desastres
A11.1.5	Trabajo en áreas seguras.	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	X			X	Si aplica porque los procedimientos que se manejan son complejos
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 porque se busca brindar el mejor cuidado y soporte a los equipos empleados para el desarrollo de la actividad laboral.
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 porque los equipos informáticos son activos relevantes y se debe proporcionar su adecuado funcionamiento

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 porque se debe proteger el cableado para protección de los datos.
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 porque los equipos de cómputo requieren mantenimiento y este se debe hacer de forma controlada y supervisada.
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 en caso de tener que sacar los equipos para hacerle un mantenimiento o arreglo
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 por la configuración de los equipos informáticos.
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 porque hay equipos desatendidos.
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	No aplica porque la información que se maneja no lo requiere
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	No aplica porque los procesos deben ser observados por determinados usuarios.
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 porque se hace seguimiento al sistema para solicitar sus mejoras si estas son requeridas.
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 porque, aunque no es una empresa de desarrollo de aplicaciones, si hace sus propios desarrollos.
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.	X		X		Si aplica porque se deben crear las respectivas salvaguardas en caso de la existencia de código malicioso que pueda afectar el sistema.
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 porque se deben hacer respaldos de la información para prevenir perdida de esta en caso de desastres o alteraciones.
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 ya que todo lo que se realiza registro de las actividades que realiza cada usuario, las fallas que se han presentado y como se han resuelto
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 ya que 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 ya que no solo la información generada por parte de los usuarios debe llevar su respectivo registro sino también todo lo que el administrador realiza, igualmente se debe proteger esta información
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 ya que se deben tener procedimientos específicos para realizar cualquier tipo de actividad donde se especifique lo que se debe realizar y como se debe hacer
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 ya que al realizar la gestión de las vulnerabilidades que se pueden presentar en los sistemas de información se pueden tener medidas de contingencia o medidas para tratar los riesgos que se presentan

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 ya que al establecer reglas para la instalación de software por parte de los usuarios se disminuye el riesgo de que estos puedan realizar cambios que puedan afectar el sistema
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 auditoria 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 ya que tanto en los sistemas como las organizaciones se deben realizar periódicamente auditorias para detectar fallas y minimizar interrupciones en los procesos del negocio
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 ya que las redes necesitan ser controladas para mantenerlas en las mejores condiciones y controlar la información que está siendo envía por ellas
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 ya que es buena práctica separar los servicios dependiendo de los diferentes usuarios que haya en la red y los privilegios que estos tienen, ya que se tiene un mayor control
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 ya que es mejor tener grupos por separado las redes dado un usuario o según la información como se encuentre clasificada
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 ya que siempre es mejor establecer políticas y procedimientos que especifiquen claramente cómo se va a realizar la transferencia de información y a donde se va a realizar dicha transferencia
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 ya que al establecer acuerdos con las partes externas a donde se va a realizar la transferencia y definir el tipo de seguridad que se va a implantar se disminuyen los riesgos
A13.2.3	Mensajería Electrónica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	X		X		Si aplica ya que la información es personal
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 traería
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 ya que todo sistema nuevo o mejora debe cumplir con los requisitos relacionados con la seguridad de la información ya establecidos
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	X		X		Si aplica ya que toda la información debe estar protegida ante posibles actividades fraudulentas a las que están expuestas

		divulgación y modificación no autorizadas.					
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 deben 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 aplica porque, aunque no es una empresa de desarrollo, si hace sus propios desarrollos.
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 porque, aunque no es una empresa de desarrollo, si hace sus propios desarrollos.
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 porque, aunque no es una empresa de desarrollo, si hace sus propios desarrollos.
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 porque, aunque no es una empresa de desarrollo, si hace sus propios desarrollos.

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 porque, aunque no es una empresa de desarrollo, si hace sus propios desarrollos.
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 ciclo de vida de desarrollo de sistemas.	X		X		Si aplica porque, aunque no es una empresa de desarrollo, si hace sus propios desarrollos.
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				Si aplica porque, aunque no es una empresa de desarrollo, si hace sus propios desarrollos.
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 porque, aunque no es una empresa de desarrollo, si hace sus propios desarrollos.
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 porque, aunque no es una empresa de desarrollo, si hace sus propios desarrollos.
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 porque, aunque no es una empresa de desarrollo, si hace sus propios desarrollos.
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 organización se deben acordar con estos y se deben documentar.	X		X		Si aplica porque los proveedores interactúan directamente con el sistema de información que se maneja

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 porque los proveedores interactúan directamente con el sistema de información que se maneja
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 ya que se deben establecer acuerdos con los proveedores sobre los servicios que estos nos brindan
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 ya que se debe tener un seguimiento o control sobre los servicios
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 ya que cualquier cambio que se realice debe estar debidamente documentado y registrado para llevar un control permitiendo la reevaluación de los riesgos a partir de estos cambios
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 ya que se deben asignar responsabilidades si llega a ocurrir algún incidente y se pueda solucionar de manera eficaz y rápida
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 ya que cualquier evento que ocurra en cuanto a la seguridad de la información debe ser reportado lo más pronto al encargado para que dé una solución
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 ya que, así como se deben reportar los incidentes también se deben realizar los respectivos reportes sobre las posibles debilidades a las que está expuesta la información para que el responsable tome medidas de protección antes de que estas ocurran y causen daños en los datos
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 ya que cuando se documentan los incidentes de seguridad se da respuestas más rápidas ya que se tiene la solución a la mano y que ha sido validada
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 ya que al tener registro de los incidentes ocurridos anteriormente se tiene conocimiento de los que se debe hacer o cual es el procedimiento que se debe seguir para contrarrestarlo

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 ya que se debe establecer procedimientos de cómo se va a realizar la recolección de la información que sirve como evidencia para el control y la toma de decisiones
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 tengan 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 controlar 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 ya que, aunque no se dan muy seguidas estas situaciones, siempre se debe estar preparado por lo cual es importante mantener y actualizar dichos controles y procedimientos de manera que nos asegure la 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 suficiente para cumplir los	X		X		Si aplica ya que la redundancia nos permite tener la información siempre disponible, aunque falle alguna de las redes

		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 ya que se debe tener documentado los reglamentos y requisitos para los sistemas de información y la organización
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 ya que todos los registros que se lleven tanto de los procedimientos como de la información deben estar protegida de acuerdo con los requisitos legales
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 ya que los datos son personales e intransferibles

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 están 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 ya que se debe realizar una revisión periódica de los controles, políticas, procesos y procedimientos del manejo de la información, aun cuando se realicen cambios
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 ya que los encargados del cumplimiento de las políticas y normas de seguridad deben revisar con regularidad si se cumple a cabalidad con dichas normas
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 aplica ya que todo sistema de información necesita que se le realice un mantenimiento preventivo con el fin de verificar el cumplimiento de las políticas establecidas

Fuente: NTC-ISO-IEC 27001:2013.

RECOMENDACIONES

Los resultados de este análisis de riesgos se pueden tomar como base y fundamento para la elaboración de un sistema de gestión de seguridad de la información, con el fin de promover la seguridad basada en la confiabilidad, integridad, disponibilidad y autenticidad de la información.

Se deben fortalecer los esquemas de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.

Documentar dentro del SGSI una política de administración de contraseñas formal

La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente.

Diseñar un simulacro de recuperación de un sistema de información que haya impactado la integridad o confidencialidad de la información

CONCLUCIONES

Se realizo el análisis de los activos de información de un sistema misional, 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 pudo hacer la verificación del estado actual del sistema de información misional, de la entidad caso estudio, lo que permitió conocer el tipo de sistema de información con el cual cuneta la entidad.

Se logro identificar y clasificar los activos de información con los que cuenta la entidad caso estudio haciendo uso de la metodología MAGERIT V3.

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 caso estudio.

Haciendo uso del anexo A de la norma ISO 27001:2013, se formularon controles a los activos de información.

Al término del análisis de los riesgos de la entidad caso estudio, se llegó a tener como resultados que la entidad puede contar con un diseño del análisis de riesgos con la cual se pueden administrar y controlar los activos y sus amenazas y vulnerabilidades, lo cual podrá ser insumo para determinar un plan de tratamiento de riesgos garantizando de esta forma que las vulnerabilidades sean mitigadas a tiempo.

La entidad cuenta con un universo 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.

Al final el resultado del análisis de los riesgos se entrega la matriz en la cual se dan a conocer los riesgos, amenazas y vulnerabilidades con su valor especifico, la situación de seguridad en que se encuentran los activos analizados y algunas recomendaciones de seguridad para corrección de las vulnerabilidades.

Como parte fina del análisis de los riesgos se entrega un informe de resultados para que la entidad pueda emitir un plan de tratamiento de riesgos y basados en este pueda emitir políticas, mecanismos o protocolos con el fin de salvaguardar la confidencialidad, integridad, disponibilidad y autenticidad de la información de la entidad caso estudio

BIBLIOGRAFÍA

[Tipton, 2006] Harold F. Tipton, Micki Krause (eds.), Information Security Management Handbook, 5th Ed., CRC Press, 2006. [Whitman, 2007] Michael E. (s.f.).

ABRIL Ana, PULIDO Jarol y BOHADA Jhon A., Análisis de Riesgos en Seguridad de la Información (2013), Fundación Universitaria Juan D Castellanos Colombia . (s.f.).

Análisis de riesgos de la seguridad de la información para la institución universitaria colegio mayor del cauca, (2014), tesis posgrado, disponible en:: http://www.aca demia.edu/24661883/An%C3%A1lisis_de_Riesgos_de_la_Seguridad_de_la_In formaci% C3%B3n_par. (s.f.).

Análisis de riesgos de la seguridad de la información para la institución universitaria colegio mayor del cauca, {En línea} (2014), tesis posgrado, disponible en: http://www.academia.edu/24661883/An%C3%A1lisis_ . (s.f.).

Análisis de riesgos de la seguridad de la información para la institución universitaria colegio mayor del cauca, {En línea} (2014), tesis posgrado, disponible en: http://www.academia.edu/24661883/An%C3%A1lisis_ de_Riesgos_de_la_Seguridad_de_la_Informaci%. (s.f.).

Armada Nacional, Sistema de información logístico, {En línea} (2011), disponible en: https://www.armada.mil.co/es/content/silog-%E2%80%9Csistema-de-informaci%C3%B3n-log%C3%ADstica-del-sector-defensa%E2%80%9D. (s.f.).

BISOGNO, María Victoria. Metodología para el aseguramiento de entornos informatizados – MAEI. Buenos Aires – Argentina. Universidad de Buenos Aires, 2004 P.15. (s.f.).

blog especializado en sistema de gestión de seguridad, {En línea} (2014) disponible en: http://www.pmg-ssi.com/2014/01/isoiec-27003-guia-para-la-implementacion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/. (s.f.).

Blog especializado en Sistemas de Gestión de Seguridad de la Información. SGSI PMG {En línea} (s.f), disponible en: http://www.pmg-ssi.com/2015/07/que-es-sgsi/. (s.f.).

BS 7799-2. Advisera Iso270011 {En línea} (s.f), tamado de: https://advisera.com/27001academ y/es/que-es-iso-27001/. (s.f.).

CIFUENTES Garzón, Guillermo Análisis de seguridad en base de datos: Aplicación Oracle versión. Maestría en Evaluación y Auditoría de Sistemas

Tecnológicos. Universidad de las Fuerzas Armadas ESPE. Sede Sangolquí, (2014). (s.f.).

DRI internacional, Iso 27000 {En línea} (s,f), disponible en: http://iso27000.es/iso27002.html. (s.f.).

ELVIRA Mifsud, Introducción a la seguridad informática {En línea} (2012), disponible en: http://recursostic.educacion.es/observatorio/web/en/software/software-general/1040-introduccion-a-la-seguridad-informatica?showall=1. (s.f.).

ELVIRA Mifsud, Introducción a la seguridad informática {En línea} (2012), disponible en: http://recursostic.educacion.es/observatorio/web/en/software/software-general/1040-introduccion-a-la-seguridad-informatica?showall=1. (s.f.).

Generalidades de la informática, {En línea} (s,f), disponible en: https://sites.google.com/site/navegadorteleinformatico/navegador-teleinformatico. (s.f.).

Iso 27000 {En línea} (s,f), disponible en: http://iso27000.es/iso27002.html. (s.f.).

Iso Iso2700 {En línea} (2015), disponible en: http://www.iso27000.es/iso27000.html. (s.f.).

John Jairo Perafán Ruiz, Mildred Caicedo Cuchimba Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca (2014) P.25. (s.f.).

Ministerio de educación y doctrina de España, Introducción a la seguridad informática {En línea} (s.f), disponible en: http://recursostic.educacion.es/observatorio/web/ ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1. (s.f.).

Portal administración Metodología de análisis {En línea} (2012), disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WRIcMEWGPIU. (s.f.).

Que es el riesgo {En línea} (2014), disponible en: https://www.unisdr.org/2004/campaign/booklet-spa/page9-spa.pdf. (s.f.).

Que es info {En línea} (s.f), disponible en: http://www.quees.info/que-es-la-informatica.html. (s.f.).

Welivesecurity análisis de riesgos {En línea} (2013), disponible en: https://www.welivesecurity.com/la-es/2012/08/16/en-que-consiste-analisis-riesgos/. (s.f.).