PROPUESTA DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA INSTITUCIÓN EDUCATIVA DE EDUCACIÓN BÁSICA Y MEDIA DEL DEPARTAMENTO DE BOYACÁ, BASADAS EN LA NORMA ISO 27001:2013

NOHORA ESTHER MALAGÓN SÁENZ
OMAIRA FIGUEROA PÉREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
TUNJA
2016

PROPUESTA DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA INSTITUCIÓN EDUCATIVA DE EDUCACIÓN BÁSICA Y MEDIA DEL DEPARTAMENTO DE BOYACÁ, BASADAS EN LA NORMA ISO 27001:2013

OMAIRA FIGUEROA PÉREZ
NOHORA ESTHER MALAGÓN SÁENZ

Monografía de grado para optar al título de
Especialista en Seguridad Informática

Director de Proyecto
Esp. Ing. FREDDY ENRIQUE ACOSTA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
TUNJA
2016

Nota de aceptación

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Tunja, 26 de Noviembre de 2016

NOHORA ESTHER MALAGÓN SÁENZ

A Dios por ser mi guía y fortaleza en cada paso que emprendo.

A mis padres y hermanas por su apoyo y comprensión.

A mi compañera de tesis por su valioso apoyo y esfuerzo para poder terminar este proyecto

OMAIRA FIGUEROA PÉREZ

A Dios por su infinita bondad y amor, por permitirnos culminar con esta etapa de nuestras vidas.

A mi familia: mis padres, hermanos y primos tener su apoyo incondicional.

A mi compañera de tesis por su compromiso y constancia para sacar adelante este proyecto.

AGRADECIMIENTOS

Las autoras expresan sus agradecimientos a:

Ingeniero José Miguel Herrán, por su orientación y apoyo para el direccionamiento en el proceso de culminación del proyecto.

Ingeniero Ramses Ríos, por su valiosa e incondicional gestión académica para la culminación de este proyecto.

Ingeniero Freddy Enrique Acosta, director de proyecto, por sus conocimientos y su valiosa colaboración.

Ingeniera Erika Villamizar por su conocimiento y aporte al proyecto.

CONTENIDO

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

RESUMEN

La información que se maneja en una empresa o entidad es muy valiosa y esta requiere que se proteja de eventuales amenazas que pueden ocurrir en la entidad.

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

Al no tener buenas prácticas de seguridad informática y no ver la necesidad de implementarlas se está vulnerando las dimensiones de seguridad de los activos conllevando a generar daños y pérdidas económicas para la entidad.

Es por eso que en esta monografía lo que se pretende es diseñar unas políticas de seguridad de información para la institución educativa de educación básica y media del departamento de Boyacá, basadas en la norma ISO 27001:2013, para minimizar los riegos que pueden llegar a tener los activos de esta Institución.

Para el diseño de las Políticas de Seguridad Informática se hizo a través de unas fases o etapas utilizando la metodología Magerit: identificación de activos, clasificación de los activos, identificación de parámetros, clasificación de amenazas, valoración del impacto de forma cualitativa, identificación de controles y diseño de propuesta de políticas de seguridad.

En la primera etapa se realiza un diagnóstico a la institución educativa con el objeto de identificar los tipos de activos más relevantes, según metodología Magerit y de acuerdo a ello se clasifico según su tipo de Información: publica, reservada - uso interno y confidencial; con finalidad de valorar las dimensiones de seguridad informática en estos activos.

En la segunda etapa se identifica las amenazas internas y externas que pueden tener los activos de la institución y el riesgo que pueden sufrir si se materializa unas amenazas; esto se realiza de forma cualitativa.

En la tercera etapa se identifica los controles que pueden salvaguardar o contrarrestar el impacto que puede ocasionar en un activo cuando se materialice una amenaza.

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

Las políticas de seguridad están estructuradas con un objetivo, una aplicabilidad y unas directrices básicas, donde se especifican unas normas de cómo se podría utilizar adecuadamente un determinado activo para proteger su información de posibles amenazas a que están expuestos.

Palabras clave: Activos, información, seguridad informática, confidencialidad, integridad, disponibilidad, trazabilidad, salvaguardar.

ABSTRACT

The information that is handled in a company or entity is very valuable and this requires that it is protected from any threats that may occur in the entity.

Computer viruses, hacking or denial of service attacks are some common and well-known examples, but also the risks of security incidents caused voluntarily or involuntarily from within the organization itself or those caused by catastrophes Natural and technical failures.

By not having good practices of computer security and not seeing the need to implement them, the security dimensions of the assets are being violated, leading to generate damages and economic losses for the entity.

That is why in this monograph what is intended is to design information security policies for the educational institution of basic and secondary education in the department of Boyacá, based on the standard ISO 27001: 2013, to minimize the risks that can reach Have the assets of this Institution.

For the design of the IT Security Policy was done through a phases or stages using the Magerit methodology: identification of assets, classification of assets, identification of parameters, classification of threats, qualitative impact assessment, identification of controls and design of proposed security policies.

In the first stage a diagnosis is made to the educational institution in order to identify the most relevant types of assets, according to Magerit methodology and according to it is classified according to its type of Information: public, reserved - internal and confidential use; In order to assess the dimensions of computer security in these assets.

The second stage identifies the internal and external threats that may have the assets of the institution and the risk they may suffer if threats materialize; This is done qualitatively.

The third stage identifies the controls that can safeguard or counteract the impact it can have on an asset when a threat materializes.

In the fourth stage, IT security policies based on ISO 27001: 2013 are generally designed; With the purpose of protecting the assets of the Educational Institution to avoid its loss, modification, or inappropriate use of its content.

Security policies are structured with a purpose, applicability and basic guidelines, which specify rules on how a particular asset could be used properly to protect its information from potential threats to which it is exposed.

Keywords: Assets, threats, information, informatics security, confidentiality, integrity, availability, traceability, safeguard.

GLOSARIO

ACTIVO: Se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización[1].

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

ANÁLISIS DE RIESGOS: Proceso para comprender la naturaleza del riesgo y determinar el nivel del riesgo[2].

CONFIDENCIALIDAD: Es una propiedad de la información mediante la cual se garantiza el acceso a la misma solo por parte de las personas que estén autorizadas[3].

CONTROL: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

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

DISPONIBILIDAD: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada[4].

ESTÁNDARES DE SEGURIDAD: Los estándares proporcionan una base importante para llegar a crear un modelo de seguridad, esta se basa en las políticas de seguridad de la organización, las cuales determinan los procedimientos, los estándares y las herramientas que ayudan a estas labores[5].

GESTIÓN DE ACTIVOS: Es aplicar un control responsablemente al activo teniendo en cuenta el nivel adecuado de seguridad de acuerdo al proceso en la organización.

---

[1] ISO 27000.ES. Glosario [en línea]. Madrid: El autor, s.f. [citado el 22-04-16]. Disponible en: http://www.iso27000.es/glosario.html

[2] Ibid. Disponible en: http://www.iso27000.es/glosario.html

[3] DEFINICIÓNABC. Definición de confidencialidad [en línea]. s.l.: El autor, s.f. [citado el 14-04-16]. Disponible en: http://www.definicionabc.com/comunicacion/confidencialidad.php

[4] ISO 27000.ES, Op. Cit. Disponible en: http://www.iso27000.es/glosario.html

[5] GÓMEZ G., Yessica. Seguridad de la información [en línea]. s.l.: Slideshare, 2013. [citado el 28-04-16]. Disponible en: http://www.slideshare.net/hvillas/seguridaddela-informacion-17506228

INFORMACIÓN: Conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. La información, ya sea impresa, almacenada digitalmente, o hablada. Actualmente se considera como un activo importante dentro de la compañía y que se debe proteger[6].

INTEGRIDAD: Propiedad de la información relativa a su exactitud y completitud[7].

ISO: Organización Internacional de Normalización. Es una agrupación de entidades nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares, (normas)[8].

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

MAGERIT: Metodología de análisis y de Gestión de Riesgos de sistemas de información.

MEJORA CONTINUA: Es el motor impulsor de cualquier sistema de gestión, incluyéndose, como no, los Sistemas de Gestión de Seguridad de la Información[9].

POLÍTICA DE SEGURIDAD: Son una serie de instrucciones documentadas que indican la forma en que se llevan a cabo determinados procesos dentro de una organización[10].

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

SALVAGUARDAS O CONTRAMEDIDA: Son los procedimientos y controles que aplican a los activos para minimizar los riesgos que pueden tener en una organización.

---

[6] ISO 27000.ES. El portal de ISO 27001 en español [en línea]. Madrid: El autor, s.f. [citado el 22-04-16]. Disponible en: http://www.iso27000.es/iso27000.html

[7] ISO 27000.ES, Glosario, Op. Cit. Disponible en: http://www.iso27000.es/glosario.html

[8] Ibid. Disponible en: http://www.iso27000.es/glosario.html

[9] SEGUINFO. Mejora continua de un SGSI según ISO 27001 [en línea]. s.l.: El autor, 2006. [citado el 14-04-16]. Disponible en: https://seguinfo.wordpress.com/2006/11/19/mejora-continua-de-un-sgsi-segun-iso-27001/

[10] UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO. Políticas de seguridad informática de la organización [en línea]. México: UNAM, s.f. [citado el 14-04-16]. Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap4.html

RIESGO: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias[11].

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

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

VULNERABILIDAD: Es el grado de pérdida de un elemento o grupo de elementos bajo riesgo, resultado de la probable ocurrencia de un suceso desastroso expresada en una escala[14].

[11] ISO 27000.ES. Glosario, Op. Cit. Disponible en: http://www.iso27000.es/glosario.html
[12] Ibid. Disponible en: http://www.iso27000.es/glosario.html
[13] Ibid. Disponible en: http://www.iso27000.es/glosario.html
[14] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Lección 1: Conceptos de vulnerabilidad, riesgo y amenaza [en línea]. s.l.: UNAD, s.f. [citado el 20-04-16]. Disponible en: http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_1_conceptos_de_vulnerabilidad_riesgo_y_amenaza.html

INTRODUCCIÓN

Las organizaciones empresariales soportan su actividad de negocio en tecnologías de la información y de la comunicación por lo que necesitan dotar a sus sistemas e infraestructuras informáticas en red de las políticas y medidas de protección que garanticen el desarrollo y sostenibilidad de su actividad de negocio. Mantener la confidencialidad la integridad, la disponibilidad y la usabilidad autorizada de la información cobra especial importancia y plantea la necesidad de disponer de profesionales capaces de asegurar, gestionar y mantener la seguridad de las informaciones en sus sistemas presentes y futuras[15].

Debido al avance de la tecnología informática y su influencia en diversas áreas de la vida cotidiana, emergen comportamientos ilícitos. Es por ello que Royer J. (2008) afirma: "La Seguridad de la información es un proceso en el que se da cabida a un creciente número de elementos: aspectos tecnológicos, de gestión organizacionales, de recursos humanos, de índole económica de negocios, de tipo legal, de cumplimiento, etc.; abarcando no solo aspectos informáticos y de telecomunicaciones sino también aspectos físicos, medio ambientales y humanos"[16].

Por otra parte el desconocimiento de las medidas de seguridad por los funcionarios de la institución educativa y la comunidad en general pueden traer problemas potenciales de seguridad, debido al uso inadecuado que se le pueda dar a la información que se manipule, más aún cuando no se han establecido parámetros para el tratamiento y uso de la información.

Al no tener políticas establecidas se puede llegar a exponer la información a diferentes tipos de amenazas, lo que conlleva a generar que la información pierda su integridad y disponibilidad.

Es una problemática que se tiene en cualquier organización, y donde se debe involucrar a la alta dirección, haciéndole notar la importancia con el manejo y uso de la información, la cual deberá comprometerse en llevar a cabo la implementación, esto involucra la asignación de recursos, el apoyo con el conocimiento, la agilidad con que se llegue a realizar la implementación, la inversión en nueva tecnología la cual le permitirá salvaguardar la información.

Por lo tanto en el desarrollo de la monografía se podrá evidenciar la clasificación de los activos de la información mediante la metodología de análisis del riesgo MAGERIT con que cuenta la institución educativa de educación básica y media del departamento de Boyacá; lo que permite identificar las posibles amenazas que

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

puedan ocurrir, con base en esto se pueden proponer unos salvaguardas o medidas preventivas para la protección de dichos activos, lo que permitirá mitigar la perdida de información dentro y fuera de institución educativa.

1. DEFINICIÓN DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el "hacking" o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos[17].

Todas estas amenazas están en continuo proceso de expansión, lo que, unido al progresivo aumento de los sistemas de información y dependencia del negocio, hace que todos los sistemas y aplicaciones estén expuestos a riesgos cada vez mayores, que sin una adecuada gestión de los mismos, pueden ocasionar que su vulnerabilidad se incremente y consiguientemente los activos se vean afectados[18].

Por consiguiente, la institución educativa para el caso de estudio no cuenta con políticas de seguridad informática para el adecuado manejo y protección de los activos; debido a esto, muchas veces se pierde información valiosa y confidencial, por falta de un plan estratégico de seguridad informática que permita contrarrestar vulnerabilidades y posibles amenazas a que están expuestos los activos informáticos con que cuenta la institución educativa.

1.2 FORMULACIÓN DEL PROBLEMA

¿Al plantear políticas de seguridad, basados en la Norma ISO 27001:2013, se logrará reducir los riesgos a que están expuestos los activos de información de la institución educativa del departamento de Boyacá?.

1.3 OBJETIVOS

1.3.1 Objetivo general

Proponer políticas de seguridad de la información para la institucion de educación básica y media del departamento de Boyacá, basadas en la norma ISO 27001:2013.

---

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

[18] BENÍTEZ, Moisés. Políticas de seguridad informática [en línea]. En: Gestión integral. 2013. no. 1, p. 8. [citado el 16-04-16]. Disponible en: http://www.gestionintegral.com.co/wp-content/uploads/2013/05/Pol%C3%ADticas-de-Seguridad-Inform%C3%A1tica-2013-GI.pdf

1.3.2 Objetivos específicos

- Clasificar los activos de la información de la institución de educación básica y media del departamento de Boyacá, basados en la metodología de MAGERIT.

- Identificar las amenazas y vulnerabilidades de los activos de la información de la institución de educación básica y media del departamento de Boyacá, basados en la metodología de MAGERIT.

- Definir los controles acordes para la institución de educación básica y media del departamento de Boyacá, de acuerdo al anexo A de la norma ISO 27001:2013 y formular recomendaciones de implementación.

- Diseñar políticas de seguridad de la información para la institución de educación básica y media del departamento de Boyacá, basadas en la norma ISO 27001:2013.

1.4 JUSTIFICACIÓN

La sofisticación del uso y estrategia de Tecnología de Información conlleva la necesidad y obligación de mejorar las herramientas de seguridad. En todo el mundo los ataques cibernéticos se han incrementado con métodos innovadores. En Colombia, las instituciones de seguridad se están vinculando a la Estrategia TI para aumentar la capacidad del Estado de enfrentar las amenazas informáticas, pues en el momento presenta grandes debilidades, pese a que existen iniciativas gubernamentales, privadas y de la sociedad civil que buscan contrarrestar sus efectos, no hay una coordinación interinstitucional apropiada. En 2011 en Colombia hubo más de 550 ataques exitosos a entidades del Estado, para 2013 los ataques se disminuyeron a +130[19].

Es por esto que la información es el activo más valioso de cualquier organización, no precisamente por su valor en los libros de contabilidad (puesto que no está contabilizada), sino por lo que representa. Como sistema nervioso de cualquier organización, la información es indispensable para soportar la toma de decisiones, el control y el manejo de las operaciones de negocio de las organizaciones y como tal debe protegerse. Sin la información sería imposible el funcionamiento y la operación de las empresas[20].

---

[19] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Fortalecimiento de la gestión TI en el estado [en línea]. Bogotá: El autor, s.f. [citado el 30-10-16]. Disponible en: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-6206.html

[20] AUDISIS. Sistema de gestión de seguridad de la información - SCSI ISO 27001:2013 - Implantación y auditoría. [en línea]. Bogotá: El autor, s.f. [citado el 15-04-16]. Disponible en: http://www.audisis.com/BROCHURE_Sem_Implementaci%C3%B3n_SGSI.pdf

Es por esto que se hace necesario que en la institución educativa de educación básica y media del departamento de Boyacá para el caso de estudio se adopte políticas de seguridad informática para garantizar el buen uso de la información que allí se utiliza, con el objetivo de mitigar posibles amenazas y vulnerabilidades de tipo humano o natural.

Por lo tanto la implementación de políticas de seguridad en la institución educativa caso de estudio, deberá estar apoyada por la alta dirección, debido que al no existir el apoyo como tal, las medidas que se tomen no tendrán la fuerza necesaria, es de aclarar que al realizar la implementación de políticas de seguridad, traerá consigo una serie de problemas a la institución debido a que muchos funcionarios chocaran al cambio, debido a que se restringirán muchas actividades que colocan en peligro la información que allí se maneja.

Finalmente, para el levantamiento de la información se utilizará la metodología MAGERIT, la cual permite la identificación de los activos, identificación de las amenazas, riesgos, entre otros, para el diseño de la políticas de seguridad se aplicara los controles propuestos por la Norma ISO 27001:2013.

1.5 ALCANCES Y LIMITACIONES

1.5.1 Alcances

La presente monografía se encuentra enmarcada en de gestión de seguridad de la información, y lo que pretende es proponer políticas de seguridad de la información para la institución educativa de educación básica y media del departamento de Boyacá, basadas en la norma ISO 27001:2013.

1.5.2 Limitaciones

Es conveniente resaltar que el desarrollo del presente proyecto no abarcará los siguientes temas como los que se definen a continuación:

- No revelar la razón social de la institución educativa donde se realizó el levantamiento de la información, por políticas de confidencialidad.
- No verificar Política de Seguridad a los activos de la entidad.
- No utilizar la herramienta PILAR para verificar la valoración de los riesgos que pueden tener los activos.
- No se implementarán políticas de seguridad.
- No se realizará plan de gestión de riesgos.

1.6 DISEÑO METODOLÓGICO

1.6.1 Unidad de análisis

Se tomará como unidad de análisis los colegios públicos y privados de educación básica y media del departamento de Boyacá.

1.6.2 Población

Instituciones educativas del municipio de Tunja.

1.6.3 Muestra

Colegio Privado del Norte de la Ciudad.

1.6.4 Enfoque metodológico

1.6.4.1 Nivel perceptual. Indica una aproximación inicial al evento en la cual apenas se alcanza a percibir los aspectos más evidentes del mismo; por eso, los objetivos que corresponden a este nivel son: "explorar" y "describir"[21].

- **Investigación descriptiva.** Tiene como objetivo central, lograr la descripción o caracterización de un evento de estudio dentro de un contexto particular. Consiste en identificar las características del evento estudiado[22].

- **Investigación exploratoria.** Tiene como objetivo básicamente aproximarse a un evento poco conocido para familiarizarse con él, abriendo camino hacia otro tipo de investigación más compleja. Para que una investigación sea exploratoria no basta con que el tema sea poco conocido (esa es una condición necesaria pero no suficiente), se requiere además que el objetivo sea realmente explorar, es decir, que no se llegue a descripciones, ni comparaciones, ni cualquier otro grado de conocimiento[23].

1.6.4.2 Nivel compresivo. Se estudia el evento en su relación con otros eventos, dentro de un holos mayor, enfatizando por lo general las relaciones de causalidad, aunque no exclusivamente[24].

- **Investigación proyectiva.** Consiste en la elaboración de una propuesta, un plan, un programa o un modelo, como solución a un problema o necesidad de tipo práctico, ya sea de un grupo social, o de una institución, o de una región geográfica, en un área particular del conocimiento, a partir de un diagnóstico preciso de las necesidades del momento, los procesos explicativos o generadores

[21] HURTADO DE BARRERA, Jacqueline. Metodología de la investigación holística. Caracas: SYPAL-IUTC, 2000. p. 18.
[22] Ibid.
[23] HURTADO DE BARRERA, Jacqueline. Guía para la comprensión holística de la ciencia. 3a ed. Caracas: Fundación Sypal, 2010. p. 132.
[24] HURTADO DE BARRERA, Jacqueline. Metodología de la investigación holística, op. cit., p. 19.

involucrados y de las tendencias futuras, es decir, con base en los resultados de un proceso investigativo[25].

[25] HURTADO DE BARRERA, Jacqueline. La investigación proyectiva [en línea]. s.l.: Blogspot.com, 2008. [citado el 13-10-16]. Disponible en: http://investigacionholistica.blogspot.com.co/2008/02/la-investigacin-proyectiva.html

2. MARCO DE REFERENCIA

2.1 MARCO TEÓRICO

2.1.1 Activo de información

Las organizaciones poseen información importante que se desea proteger frente a cualquier riesgo o amenaza.

Los activos de información son ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, material de formación, aplicaciones, software del sistema, equipos informáticos, equipo de comunicaciones, servicios informáticos y de comunicaciones, utilidades generales como por ejemplo calefacción, iluminación, energía y aire acondicionado y las personas, que son al fin y al cabo las que en última instancia generan, transmiten y destruyen información, es decir dentro de un organización se han de considerar todos los tipos de activos de información[26].

2.1.2 Amenazas

Una amenaza se representa a través de una persona, una circunstancia o evento, un fenómeno o una idea maliciosa, las cuales pueden provocar daño en los sistemas de información, produciendo pérdidas materiales, financieras o de otro tipo. Las amenazas son múltiples desde una inundación, un fallo eléctrico o una organización criminal o terrorista. Así, una amenaza es todo aquello que intenta o pretende destruir[27].

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

Las amenazas se clasifican en:

- De origen natural: son eventos naturales que son peligrosos al hombre y que están causados por fuerzas extrañas a el. Como por ejemplo inundaciones, terremotos.
- Origen industrial: son eventos industriales que pueden ocurrir de forma

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

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

accidental, o por la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.
- Errores y fallos no intencionados: son eventos que pueden ocurrir por errores humanos no intencionados. Por ejemplo no saber utilizar una base de datos pueden ocasionar la pérdida de algún registro por no saber utilizar el sistema.
- Ataques intencionados: son eventos que pueden ocurrir con el hombre ya que estos pueden provocar intencionalmente que se dañe un sistema.

2.1.3 Seguridad de la información

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

La información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades (véase también OECD Guía para la seguridad redes sistemas de información). La información puede existir en muchas formas. Puede estar impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en películas o hablada en una conversación. Cualquiera que sea la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre debiera estar apropiadamente protegida[28].

La seguridad de la información maneja tres principios básicos:

- Confidencialidad: Consiste en asegurar la “privacidad” de los datos. Solamente los individuos, procesos o dispositivos autorizados deben poder acceder a los datos.
- Integridad. Consiste en asegurar que la información esta completa y no ha sido alterada desde el origen hasta su recepción.
- Disponibilidad: Consiste en asegurar que la información o los recursos requeridos están disponibles para todos los usuarios autorizados en el momento en que se necesitan.

La seguridad de la información se alcanza implementando un conjunto adecuado de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos. Esto se debiera realizar en conjunción con otros procesos de gestión del negocio[29].

---

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

[29] Ibid. Disponible en: https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

2.1.4 Familia de las normas ISO/IEC 27000

Es un conjunto de normas de gestión de la seguridad de la información con la IEC (International Electrotechnical Commission), comisión internacional de electrotecnia, tiene algunas similitudes a la familia de las normas de gestión de la calidad ISO 9000. Cada una de las normas de la familia 27000, define y centra todos los aspectos importantes en el contexto de la gestión de la seguridad de la información en cualquier empresa pequeña, mediana o grande, así como públicas y privadas[30].

2.1.4.1 Alcance de la norma ISO/IEC 27000. ISO 27001 propone un marco de gestión de la seguridad de toda la información de la empresa, incluso si es información perteneciente al propio conocimiento y experiencia de las personas o sea tratada en reuniones etc.

No se debe centrar la atención solamente en los sistemas informáticos por mucho que tengan hoy en día una importancia más que relevante en el tratamiento de la información ya que de otra forma, se podría dejar sin proteger información que puede ser esencial para la actividad de la empresa[31].

A continuación se exponen las Normas relacionadas con la ISO 2700:

- ISO/IEC 27000. Publicada 1 de Mayo de 2009, revisada con una segunda edición de 01 de Diciembre de 2012 y una tercera edición de 14 de Enero de 2014. Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI (la última edición no aborda ya el ciclo Plan-Do-Check-Act para evitar convertirlo en el único marco de referencia para la mejora continua). Existen versiones traducidas al español.

- ISO/IEC 27001. Publicada el 15 de Octubre de 2005, revisada el 25 de Septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones.

---

[30] ISO 27000.ES, El portal de ISO 27001 en español, Op. Cit. Disponible en: http://www.iso27000.es/iso27000.html

[31] VARGAS, Ana Cecilia y CASTRO MATTEI, Alonso. Sistemas de gestión de seguridad de la información [en línea]. San José Costa Rica: Universidad de Costa Rica, s.f. [citado el 22-04-16]. Disponible en: http://archivo.ucr.ac.cr/docum/ISOEIC27000.pdf

- **ISO/IEC 27002.** Publicada desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

Actualmente, la última edición de 2013 de este estándar ha sido actualizada a un total de 14 Dominios, 35 Objetivos de Control y 114 Controles publicándose inicialmente en inglés y en francés tras su acuerdo de publicación el 25 de Septiembre de 2013.

- **ISO/IEC 27003.** Publicada el 01 de Febrero de 2010. No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001:2005. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI.

- **ISO/IEC 27004.** Publicada el 15 de Diciembre de 2009. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.

- **ISO/IEC 27005.** Publicada en segunda edición el 1 de Junio de 2011 (primera edición del 15 de Junio de 2008). No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información.

- **ISO/IEC 27006.** Publicada en segunda edición el 1 de Diciembre de 2011 (primera edición del 1 de Marzo de 2007) y revisada el 30 de Septiembre de 2015. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

- **ISO/IEC 27007.** Publicada el 14 de Noviembre de 2011. No certificable. Es una guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011. En España, esta norma no está traducida.

- **ISO/IEC TR 27008.** Publicada el 15 de Octubre de 2011. No certificable. Es una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI. En España, esta norma no está traducida[32].

[32] ISO 27000.ES, El portal de ISO 27001 en español, Op. Cit. Disponible en: http://www.iso27000.es/iso27000.html

2.1.5 Teoría del ciclo PHVA (ciclo Deming o ODCA)

Comprende, como principal objetivo, caracterizar una metodología que genere conciencia sobre la importancia de la seguridad de la información y la aplicabilidad de la misma en pequeñas empresas, que garantice un tratamiento seguro de la integridad, disponibilidad y confidencialidad para evitar que dicha información se vuelva pública de una manera no autorizada.

La norma ISO 27001 adopta el ciclo de Deming como metodología, la cual se puede aplicar a todos los procesos que abarca el SGSI. Esta metodología es conocida por sus siglas en inglés PDCA: Plan- Do- Check-Act.

El ciclo PDCA (o PHVA en español) (figura 1) es una herramienta para la mejora continua, diseñada por el Dr. Walter Shewhart en el año 1920 y presentada por Edwards Deming a partir del año 1950, la cual se basa en un ciclo de cuatro pasos (Díaz, 2010). Plan (planificar), Do (hacer), Check (verificar) y Act(actuar). A continuación, se describirán brevemente los pasos que se siguen en el ciclo de Deming[33].

Figura 1. Ciclo PDCA (PHVA) para la implantación de SGSI.

Fuente: UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Ciclo PDCA (Eduard Deming) [en línea]. s.l.: UNAD, s.f. [citado el 20-04-16] http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/151_ciclo_pdca__edward_deming.html

[33] BUSTAMANTE, G. y CANO, J. Metodología de la seguridad de la información como medida de protección en pequeñas empresas. En: Cuaderno Activa. 2016. no. 6, p. 74-75.

- Planear: Es una fase inicial donde se realiza un análisis y estudio de la situación actual de los riesgos de los activos de la entidad.
- Hacer: Implementar y operar el sistema de Gestión de seguridad de la Información. Es una fase donde se realiza el análisis y evaluación de riesgos. En esta fase se hace el plan de tratamientos de riegos y se implementa.
- Verificar: En esta fase se efectúa el control de todos los procedimientos implementados en el Sistema de gestión de Seguridad informática.
- Actuar: Mantener y mejorar el sistema de gestión de seguridad de la información. En esta fase se realizan las acciones correcciones y preventivas de la organización.

El principal objetivo de esta metodología, es hacer ver la importancia de la seguridad de la información y su uso en las organizaciones para garantizar los pilares de la seguridad informática como lo es la integridad, disponibilidad y confidencialidad; con éste se evita que los activos estén protegidos.

2.2 MARCO CONCEPTUAL

2.2.1 Política de seguridad

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

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

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

El documento de políticas de seguridad está dirigido principalmente al personal interno de la organización, aunque hay casos en que también personas externas quedan sujetas al alcance de las políticas[34].

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

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

2.2.2 Seguridad de la información

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

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

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

Figura 2. Seguridad de la Información.

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

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

Adicionalmente, deberán considerarse los conceptos de:

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

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

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

- **No repudio:** se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

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

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

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

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

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

- **Tecnología de la información:** se refiere al hardware y software operados por el Colegio o por un tercero que procese información en su nombre, para llevar a cabo[35].

2.2.3 Metodología Magerit

Implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información[36].

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

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

---

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

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

Esta metodología contempla 3 libros:

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

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

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

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza[37].

2.3 MARCO LEGAL

2.3.1 Ley 57 de 5 de junio de 1985

"Por la cual se ordena la publicidad de los actos y documentos oficiales"[38].

2.3.2 Ley 527 de 18 de agosto 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"[39].

2.3.3 Ley 1273 de 2009

"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"[40].

---

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

[38] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 57 de 1985 (julio 5 de 1985). Bogotá. Diario Oficial 05 de julio de 1985. p. 1-6.

[39] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 527 (18 de agosto de 1999). Bogotá. Diario Oficial 43.673 de 21 de agosto de 1999. p 1-2.

[40] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 (05 de enero de 2009). Bogota. Diario

2.3.4 Decreto 1727 de 15 de mayo de 2009

"Por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información"[41].

2.3.5 Ley Estatutaria 1266 del 31 de diciembre de 2008

"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"[42].

2.3.6 Ley Estatutaria 1581 de 2012

"Por la cual se dictan disposiciones generales para la protección de datos personales"[43].

2.3.7 Decreto 1377 de 2013

"Por el cual se reglamenta parcialmente la Ley 1581 de 2012"[44].

2.3.8 Ley 1341 de 2009

"Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones"[45].

2.3.9 Real Decreto 3 de 2010

"Por el que se regula el Esquema Nacional de Seguridad en el ámbito de la

---

Oficial 47.223 de enero 5 de 2009. p. 1-15.

[41] COLOMBIA. CONGRESO DE LA REPÚBLICA. Decreto 1727 (15 de mayo de 2009). Bogotá. Diario Oficial 47.350 de mayo 15 de 2009. p. 1-5.

[42] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1266 (diciembre 31 de 2008 Bogotá. Diario Oficial 47.219 de 31 de diciembre de 2008. p. 1-19.

[43] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1581 (octubre 17 de 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial 48.587 de octubre 18 de 2012. p. 1-15.

[44] COLOMBIA. CONGRESO DE LA REPÚBLICA. Decreto 1377 (27 de junio de 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Diario Oficial 48.834 de 27 de junio de 2013. p. 1-11.

[45] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1266 (julio 30 de 2009). Bogotá. Diario Oficial 47.426 de julio 30 de 2009. p. 1-34.

Administración Electrónica"[46].

[46] ESPAÑA. MINISTERIO DE LA PRESIDENCIA. Real Decreto 3 del 2010 (enero 8 de 2010). Por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Boletín Oficial del Estado de enero 29 de 2010. p. 1-50.

3. CLASIFICACIÓN DE LOS ACTIVOS DE LA INFORMACIÓN DE LA INSTITUCIÓN DE EDUCACIÓN BÁSICA Y MEDIA DEL DEPARTAMENTO DE BOYACÁ, BASADOS EN LA METODOLOGÍA DE MAGERIT

Para la clasificación de los activos está monografía se basa en la metodología MAGERIT, activos que fueron evidenciados en la institución educativa de educación básica y media del departamento de Boyacá seleccionada para el caso de estudio, los cuales se clasificaron de la siguiente forma:

3.1 CLASIFICACIÓN DE LA INFORMACIÓN

Para la clasificación de la información, se evalúan las tres características básicas como son: confidencialidad, integridad y disponibilidad.

En la tabla 1 se puede observar los criterios de clasificación de la información.

Tabla 1. Criterios de clasificación de información.

Criterios	Descripción
Secreta	Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección de la institución educativa, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo, al Sector Público Nacional o a terceros.
Confidencial	Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a la institución educativa, al Sector Público Nacional o a terceros.
Reservada - Uso interno	Información que puede ser conocida y utilizada por todos los empleados del Colegio y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para la institución educativa, el Sector Público Nacional o terceros.
Público	Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado de la institución educativa o no.

Fuente: SECRETARÍA DE PLANIFICACIÓN Y GESTIÓN INSTITUCIONAL. Disposición 3/2013: Apruébase la "Política de Seguridad de la Información Modelo" [en línea]. Argentina: Universidad Nacional de Córdoba, 2013. [citado el 13-10-16]. Disponible en: http://www.unc.edu.ar/gestion/unidades/ciciservicio-de-informacion-tecnica-legal/novedades-en-legislacion/archivos-gladys/disposicion-3-2013-onti

3.2 ACTIVOS INFORMÁTICOS

Para la identificación de los activos de está monografía se basa en la metodología de análisis de riesgo MAGERIT.

En la tabla 2 se indican los activos más relevantes de la institución educativa de educación básica y media del departamento de Boyacá.

Tabla 2. Inventario de activos.

Tipo de activo	Código de activo	Activos más relevantes en la entidad
[info] Información	[adm]	Archivo de contratos y acuerdos
	Datos de interés para la administración pública	
	[vr] datos vitales	Base de datos de Notas
	[per] datos de carácter personal	Bases de datos de estudiantes
		Base de datos de docentes
		Base de datos de Personal administrativo
		Contabilidad de la empresa
	[classified] Datos clasificados	[classified]
		Datos históricos de Estudiantes
[D]datos / información	[Files] Ficheros	Archivos de notas
		Archivos de contabilidad
		Archivos de actas, resoluciones (actos administrativos y académicos)
	[backup]. Copias de Respaldo	Copias de seguridad de la Información del colegio como notas de estudiante, datos de estudiante, actas resoluciones
	[conf] datos de configuración	Datos de configuración de equipos de cómputo y servidores.
	[password] Contraseñas	Contraseñas de equipos de cómputo
[S] Servicios son los servicios prestados a la entidad	[www] world wide web	Internet proveedor punto vive digital. Es el servicio que ofrece el colegio a comunidad educativa
	[edi] intercambio electrónico de datos	Intercambio de datos en SIMAT
[SW] Software - Aplicaciones informáticas	[os] sistema operativo	Sistema operativo Windows XP, Windows 7, Windows 8
	[sub] Desarrollo a medida	Aplicación para el manejo de notas y reportes de los estudiantes
	[www] servidor de presentación	Servidor de paginas web
	[email_server] servidor de correo electrónico	Servidor de correos electrónicos
	[dbms] sistema de gestión de bases de datos	Gestor de base de datos para almacenar las notas de los estudiantes

Tipo de activo	Código de activo	Activos más relevantes en la entidad
[SW] Software - Aplicaciones informáticas (continuación)	[office] ofimática	Office 2010, office 2013, winrar, Adobe Acrobat Reader
	[av] antivirus	Avast security, eset 32
	[hypervisor] gestor de máquinas virtuales	Winware, virtualbox
	[std] estándar	Visual basic 6, visual basic . NET, NEtbeet
	[std] estándar	macromedia dreamweaver
	[app] servidor de aplicaciones	Apache, WANserver, XAMPP
[HW] Equipamiento informático	[mic] equipos medios	Equipos de mesa
	[pc] equipos portátiles	Equipos portátiles de computadores para educar Lenovo.
	[print] equipos de impresión	Impresoras de multifunción Impresora Epson. impresora lexmark
	[modem] módems	Modems para acceso a internet.
[COM] Redes de comunicaciones	[PSTN] red telefónica	Acceso telefónico
	[wifi] red inalámbrica	Red inalámbrica
	[Internet] Internet	Internet
[Media] Soportes de información	[DVD]	Manuales de usuario
		Archivos de documentos como resoluciones, actas tanto administrativas como académicas, proyecto educativo institucional
	[usb] memorias USB	Documentos varios
	[printed] material impreso	Carpetas varias. Observador del alumno, manuales de usuario, reglamento del aprendiz, resoluciones
		Soportes de contabilidad, facturas.
[AUX] Equipamiento auxiliar	[router] enrutadores	Router
	[furniture] mobiliario: armarios	Mobiliario: Armarios, archivadores, estantes, mesas.
	[ups] sistemas de alimentación ininterrumpida	Ups de computadores de soporte y sala de informática.
	[power] fuentes de alimentación	Fuentes de alimentación de equipos de cómputo
	Access point	Punto de acceso
[L] Instalaciones	[building] edificio	Edificio donde está ubicado el colegio.
[P] Personal	[adm] administradores de sistemas	Docente de informática
	[ui] usuarios internos	Personal administrativo, comunidad educativa
	[ue] usuarios externos	Padres de familia
	[prov] proveedores	Personas que proveen algún servicio a la institución educativa

Fuente: Propiedad de las autoras.

3.3 CLASIFICACIÓN DE LOS ACTIVOS DE ACUERDO A LOS CRITERIOS DE LA INFORMACIÓN

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen, o bien de acuerdo a las funciones que cumplen en la institución educativa de educación básica y media de departamento de Boyacá, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

A continuación en la tabla 3 se establece el criterio de clasificación de la información

Tabla 3. Clasificación de los activos según criterios de información.

Tipo de activo	Código de activo	Nombre del Activo	Clasificación de la información
[D]datos / información	[adm]. Datos de interés para la administración pública	Archivo de contratos y acuerdos	Pública
	[vr] datos vitales	Base de datos de notas	Confidencial
	[per] datos de carácter personal	Bases de datos de estudiantes	Confidencial
		Base de datos de docentes	Confidencial
		Base de datos de Personal administrativo	Confidencial
		Contabilidad de la empresa	Reservada de uso interno
	[classified] Datos clasificados	[classified]	
		Datos históricos de estudiantes	Confidencial
	[Files] Ficheros	Archivos de notas	Confidencial
		Archivos de contabilidad	Reservada de uso interno
		Archivos de actas, resoluciones (actos administrativos y académicos)	Pública
	[backup]. Copias de Respaldo	Copias de seguridad de la Información del colegio como notas de estudiante, datos de estudiante, actas resoluciones.	Secreta
	[conf] datos de configuración	Datos de configuración de equipos de cómputo y servidores	Confidencial
	[password] contraseñas	Contraseñas de equipos de cómputo	Reservada de uso interno
[S] Servicios son los servicios prestados a la entidad	[www] world wide web	Internet proveedor punto vive digital. Es el servicio que ofrece el colegio a comunidad educativa	Pública
	[edi] intercambio electrónico de datos	Intercambio de datos en SIMAT	Confidencial

Tipo de activo	Código de activo	Nombre del Activo	Clasificación de la información
[SW] Software - Aplicaciones informáticas	[os] sistema operativo	Sistema operativo Windows XP, Windows 7, Windows 8	Pública
	[sub] Desarrollo a medida	Aplicación para el manejo de notas y reportes de los estudiantes	Reservada de uso interno
	[www] servidor de presentación	Servidor de paginas web	Pública
	[email_server] servidor de correo electrónico	Servidor de correos electrónicos	Confidencial
	[dbms] sistema de gestión de bases de datos	Gestor de base de datos para almacenar las notas de los estudiantes	Confidencial
	[office] ofimática	Office 2010, office 2013, winrar, Adobe Acrobat Reader	Pública
	[av] antivirus	Avast security, eset 32	Pública
	[hypervisor] gestor de máquinas virtuales	Winware, virtualbox	Pública
	[std] estándar	Visual basic 6, visual basic. NET, NEtbeet	Pública
	[std] estándar	macromedia dreamweaver	Pública
	[app] servidor de aplicaciones	Apache, WANserver, XAMPP	Pública
[HW] Equipamiento informático	[mic] equipos medios	Equipos de mesa	Pública
	[pc] equipos portátiles	Equipos portátiles de Computadores para educar Lenovo.	Pública
	[print] equipos de impresión	Impresoras de multifunción Impresora Epson. impresora lexmark	Pública
	[modem] módems	Modems para acceso a internet.	Pública
[COM] Redes de comunicaciones	[PSTN] red telefónica	Acceso telefónico	Reservada de uso interno
	[wifi] red inalámbrica	Red inalámbrica	Reservada de uso interno
	[Internet] Internet	Internet	Pública
[Media] Soportes de información	[DVD]	Manuales de usuario	Reservada de uso interno
		Archivos de documentos como resoluciones, actas tanto admi-nistrativas como académicas, proyecto educativo institucional.	Reservada de uso interno
	[usb] memorias USB	Documentos varios	Reservada de uso interno
	[printed] material impreso	Carpetas varias. Observador del alumno, manuales de usuario, regla-mento del aprendiz, resoluciones.	Confidencial
		Soportes de contabilidad, facturas	Secreta

Tipo de activo	Código de activo	Nombre del Activo	Clasificación de la información
[AUX] Equipamiento auxiliar	[router] enrutadores	Router	Pública
	[furniture] mobiliario: armarios	Mobiliario: Armarios, archivadores, estantes, mesas	Pública
	[ups] sistemas de alimentación ininterrumpida	Ups de computadores de soporte y sala de informática.	Pública
	[power] fuentes de alimentación	Fuentes de alimentación de equipos de cómputo.	Pública
	Access point	Punto de acceso	Pública
[L] Instalaciones	[building] edificio	Edificio donde está ubicado el colegio	Pública
[P] Personal	[adm] administradores de sistemas	Docente de informática	Confidencial
	[ui] usuarios internos	Personal administrativo, comunidad educativa	Confidencial
	[ue] usuarios externos	Padres de familia	Pública
	[prov] proveedores	Personas que proveen algún servicio a la institución educativa	Pública

Fuente: Propiedad de las autoras.

3.4 DIMENSIONES DE VALORACIÓN

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

En el inventario de activos encontrados en la institución educativa de educación básica y media de departamento de Boyacá, se evalúan los activos teniendo en cuenta el criterio de valoración cualitativo de acuerdo a su impacto y a las dimensiones de seguridad.

3.4.1 De acuerdo al impacto

De acuerdo a los activos más relevantes encontrados en la institución educativa de educación básica y media del departamento de Boyacá, se realiza una valoración cualitativa según su impacto que este puede tener en la entidad al sufrir un daño leve o grave.

3.4.1.1 Criterios de valoración. Se toma como escala de 0% a 100%, donde el 0% equivale a un valor despreciable (el activo no sufre daños) y al llegar al nivel 100% equivale a un valor extremo (el activo sufre daños extremadamente graves).

A continuación se indica la escala de criterios de valoración (ver tabla 4).

Tabla 4. Criterios de valoración.

Valor		Criterio
90 - 100 %	Muy alto	Daño extremadamente grave
61 - 89%	Alto	Daño muy grave
40% - 60%	Medio	Daño importante
20 - 39 %	Bajo	Irrelevante a efectos prácticos
0 - 19 %	Muy bajo	Daño menor

Fuente: GOBIERNO DE ESPAÑA. 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.

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

En la tabla 5 se relaciona la valoración de los activos.

Tabla 5. Valoración de los activos según impacto.

Tipo de activo	Código de activo	Nombre del Activo de la información	Impacto	Descripción
[D]datos / información	[adm]. Datos de interés para la administración pública	Archivo de contratos y acuerdos	MA [90%]	**5.adm**, probablemente impediría la operación efectiva de más de una parte de la Organización.
				3.p1, probablemente afecte a un individuo
	[vr] datos vitales	Base de datos de Notas	MA [100%]	**5adm**, probablemente impediría la operación efectiva de más de una parte de la Organización
	[per] datos de carácter personal	Bases de datos de estudiantes	MA [100%]	**5.adm,** probablemente impediría la operación efectiva de más de una parte de la Organización
		Base de datos de docentes		**3.pi2,** probablemente suponga el incumplimiento de una ley o regulación
	[Files] Ficheros	Archivos de notas	MA [100%]	**5.adm**, probablemente impediría la operación efectiva de más de una parte de la Organización
		Archivos de contabilidad		
		Archivos de actas, resolu-ciones (actos administra-tivos y académicos)		
	[backup]. Copias de Respaldo	Copias de seguridad de la Información del colegio como notas de estudiante, datos de estudiante, actas resoluciones	MA [100%]	**5.adm**, probablemente impediría la operación efectiva de más de una parte de la Organización
				3.adm, probablemente impediría la operación efectiva de una parte de la Organización
	[conf] datos de configuración	Datos de configuración de equipos de cómputo y servidores.	MA [100%]	**9.olm,** Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
				7.adm, probablemente impediría la operación efectiva de la Organización
	[password] Contraseñas	Contraseñas de equipos de computo	MA [100%]	**5.adm**, probablemente impediría la operación efectiva de más de una parte de la Organización
				6.pi1, Probablemente afecte grave-mente a un grupo de individuos

Tipo de activo	Código de activo	Nombre del Activo de la información	Impacto	Descripción
[S] Servicios son los servicios prestados a la entidad	[www] world wide web	Internet proveedor punto vive digital. Es el servicio que ofrece el colegio a comunidad educativa	MA [100%]	**5.da,** Probablemente cause la interrupción de actividades propias de la Organización.
	[edi] intercambio electrónico de datos	Intercambio de datos en SIMAT	MA [100%]	**5.da**, Probablemente cause la interrupción de actividades propias de la Organización
				4.pi1, Probablemente afecte gravemente a un grupo de individuos
[SW] Software - Aplicaciones informáticas	[os] sistema operativo	Sistema operativo Windows XP, Windows 7, Windows 8	B[20%]	**3.lro**, probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
				3.da, Probablemente cause la interrupción de actividades propias de la Organización
	[sub] Desarrollo a medida	Aplicación para el manejo de notas y reportes de los estudiantes	MA[100%]	**3.lro**, probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
				3,da, Probablemente cause la interrupción de actividades propias de la Organización
	[www] servidor de presentación	Servidor de páginas web	M [50%]	**3.da**, Probablemente cause la interrupción de actividades propias de la Organización
				6.pi, Probablemente afecte grave-mente a un grupo de individuos
	[email_server] servidor de correo electrónico	Servidor de correos electrónicos	M [50%]	**5.da**, Probablemente cause la interrupción de actividades propias de la Organización
				6.pi, Probablemente afecte grave-mente a un grupo de individuos
	[dbms] sistema de gestión de bases de datos	Gestor de base de datos para almacenar las notas de los estudiantes.	M[50%]	**5.adm**, probablemente impediría la operación efectiva de más de una parte de la Organización
			M[50%]	**3.pi2**, probablemente suponga el incumplimiento de una ley o regulación
	[office] ofimática	Office 2010, office 2013, winrar, Adobe Acrobat Reader	B[20%]	**3.lro,** probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
	[av] antivirus	Avast security, eset 32	B[20%]	**3.lro,** probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
	[hypervisor] gestor de máquinas virtuales	Winware, virtualbox	B[20%]	**3.lro**, probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
	[std] estándar	Visual basic 6, visual basic . NET, NEtbeet	B[20%]	**3.lro**, probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
	[std] estándar	Macromedia Dreamweaver	B[20%]	**3.lro**, probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
	[app] servidor de aplicaciones	Apache, WANserver, XAMPP	B[20%]	**3.lro**, probablemente sea causa de incumplimiento leve o técnico de una ley o regulación

Tipo de activo	Código de activo	Nombre del Activo de la información	Impacto	Descripción
[HW] Equipamiento informático	[mic] equipos medios	Equipos de mesa	M [50%]	**1.adm**, pudiera impedir la operación efectiva de una parte de la Organización
				7.cei.c, causa de graves pérdidas económicas
	[pc] equipos portátiles	Equipos portátiles de Computadores para educar Lenovo.	M [50%]	**1.adm**, pudiera impedir la operación efectiva de una parte de la Organización
				7.cei.c, causa de graves pérdidas económicas
	[print] equipos de impresión	Impresoras de multifunción Impresora Epson. impresora lexmark	B[20%]	**7.cei**, causa de graves pérdidas económicas
				1.adm, pudiera impedir la operación efectiva de una parte de la Organización
	[modem] módems	Modems para acceso a internet.	B[20%]	**1.adm**, pudiera impedir la operación efectiva de una parte de la Organización
[COM] Redes de comunicaciones	[PSTN] red telefónica	Acceso telefónico	B[20%]	**5.da**, Probablemente cause la interrupción de actividades propias de la Organización.
	[wifi] red inalámbrica	Red inalámbrica	B[20%]	**5.da**, Probablemente cause la interrupción de actividades propias de la Organización.
	[Internet] Internet	Internet	B[20%]	**5.da**, Probablemente cause la interrupción de actividades propias de la Organización.
[Media] Soportes de información	[DVD]	Manuales de usuario	B[50%]	**6.pi2**, probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
		Archivos de documen-tos como resoluciones, actas tanto administra-tivas como académicas, proyecto educativo institucional		**6.pi2**, probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
	[usb] memorias USB	Documentos varios	MB [5%]	**6.pi2**, probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
	[printed] material impreso	Carpetas varias. Observador del alumno, manuales de usuario, reglamento del aprendiz, resoluciones.	M[50%]	**6.pi2**, probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
		Soportes de contabilidad, facturas.	MA [100%]	**9.lro**, probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
[AUX] Equipamiento auxiliar	[router] enrutadores	Router	A[80%]	**1.adm**, pudiera impedir la operación efectiva de una parte de la Organización
	[furniture] mobiliario: armarios	Mobiliario: Armarios, archivadores, estantes, mesas	A[80%]	**7.cei**, causa de graves pérdidas económicas
	[ups] sistemas de alimentación ininterrumpida	Ups de computadores de soporte y sala de informática	A[80%]	**7.cei**, causa de graves pérdidas económicas
	[power] fuentes de alimentación	Fuentes de alimentación de equipos de cómputo	M[50%]	**1.cei**, de pequeño valor comercial
	Access Point	Punto de acceso	B[20%]	**3.da**, Probablemente cause la interrupción de actividades propias de la Organización.

Tipo de activo	Código de activo	Nombre del Activo de la información	Impacto	Descripción
[L] Instalaciones	[building] edificio	Edificio donde está ubicado el colegio.	B[20%]	**7.da**, Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
			B[20%]	**7.olm**, Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[P] Personal	[adm] administradores de sistemas	Docente de informática	M[50%]	**6.pi1**, probablemente afecte gravemente a un grupo de individuos
	[ui] usuarios internos	Personal administrativo, comunidad educativa	M[50%]	**6.pi1**, probablemente afecte gravemente a un grupo de individuos
	[ue] usuarios externos	Padres de familia	M[50%]	**6.pi1**, probablemente afecte gravemente a un grupo de individuos
	[prov] proveedores	Personas que proveen algún servicio a la institución educativa	M[50%]	**6.pi2**, probablemente quebrante seriamente la ley o algún reglamento de protección de información personal

Fuente: Propiedad de las autoras.

3.4.2 De acuerdo a las dimensiones de seguridad

Las dimensiones de seguridad informática son atributos o cualidades esenciales en la seguridad de la información; ellos son: disponibilidad [D], confidencialidad [C], integridad [I] y trazabilidad [T].

La tabla 6 muestra las dimensiones de valoración informática.

Tabla 6. Dimensiones de valoración informática.

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

Fuente: Propiedad de las autoras.

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.

A continuación se da el concepto de cada dimensión para poderla identificar en cada uno de los activos del inventario realizado.

Disponibilidad [D]: Es el aseguramiento de los activos que los usuarios autorizados tienen acceso cuando requieran la información y sus activos asociados.

Integridad [I]: Es la garantía de información cuando se crea y no sufre ninguna alteración.

Confidencialidad [C]: Es el aseguramiento de la información, no se pone a disposición de todos sino únicamente a personas autorizadas.

Autenticidad [A]: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008].

Trazabilidad [T]: Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad [UNE 71504:2008].

3.4.2.1 Criterios de valoración. Se describe los criterios de valoración según el riesgo que los activos pueden presentar en la institución educativa, de acuerdo al nivel de seguridad, teniendo en cuenta su escala valoración cualitativa según MAGERIT.

En la tabla 7 se indica el valor del nivel de seguridad.

Tabla 7. Dimensiones de seguridad.

Nivel de seguridad requerido	Valor				
	Muy Alto	Alto	Medio	Bajo	Muy bajo
Confidencialidad	90 - 100 %	61 - 89%	40% - 60%	20 - 39 %	0 - 19 %
Integridad					
Autenticidad					
Trazabilidad					
Disponibilidad					

Fuente: Propiedad de la autoras.

3.4.2.2 Valoración de activos. Describe cada uno de los activos y las dimensiones de valoraciones de seguridad informática, donde éstas se avalúan dependiendo las dimensiones de seguridad de la tabla 7. La valoración que se da a cada activo en determinada dimensión depende del daño o perjuicio que pueda ocasionar a las instituciones educativas del departamento de Boyacá.

La siguiente tabla indica la valoración de activos según el nivel de seguridad que estos tienen en la institución (ver tabla 8).

Tabla 8. Valoración de activos-dimensiones.

Tipos de activos	Nombre de activos	Clasificación de Información	Valoración de los activos					
			[D]	[C]	[I]	[A]	[T]	PROM
[D]datos / información	Base de datos de Notas	Confidencial	0%	100%	100%	100%	100%	80%
	Bases de datos de estudiantes	Confidencial	0%	100%	100%	100%	100%	80%
	Base de datos de docentes	Confidencial	0%	100%	100%	100%	100%	80%
	Base de datos de Personal administrativo	Confidencial	0%	100%	100%	100%	100%	100%
	Contabilidad de la empresa	Reservada de uso interno	0%	100%	0%	0%	0%	20%
	Archivos de notas	Confidencial	100%	100%	0%	0%	0%	40%
	Archivos de contabilidad	Reservada de uso interno	0%	100%	0%	0%	0%	20%
	Archivos de actas, resoluciones	Pública	100%	0%	0%	0%	0%	20%
	Copias de seguridad de la Información del colegio	Secreta	0%	100%	100%	100%	100%	80%
	datos de configuración	Confidencial	0%	0%	100%	0%	100%	40%
[SW] Software - Aplicaciones informáticas	Sistemas Operativos: windows XP, Windows 7 home, Windows 7 ultimate , Windows 8	Pública	100%	0%	100%	0%	100%	60%
	Aplicación para el manejo de notas y reportes de los estudiantes	Reservada de uso interno	0%	0%	100%	100%	100%	60%
	Gestor de base de datos para almacenar las notas de los estudiantes	Confidencial	0%	100%	100%	100%	100%	80%
	Ofimática: Office 2010, office 2013	Pública	100%	0%	0%	50%	50%	40%
	Antivirus: Avast security, eset 32	Pública	100%	0%	0%	50%	0%	30%
	Máquinas virtuales: Winware, virtualbox	Pública	100%	0%	0%	50%	50%	40%
	Visual Basic 6, Visual Basic. NET, Netbeet - macromedia dreamweaver	Pública	100%	0%	0%	80%	0%	36%
	Apache, WANserver, XAMPP	Pública	100%	0%	0%	80%	0%	36%
[HW] Equipamiento informático	Equipos de mesa	Pública	100%	0%	0%	0%	0%	20%
	Equipos portátiles de Computadores para educar Lenovo	Pública	100%	0%	0%	0%	0%	20%
	Impresoras de multifunción	Pública	100%	0%	0%	0%	0%	20%
	Módems para acceso a internet	Pública	100%	0%	0%	0%	0%	20%

Tipos de activos	Nombre de activos	Clasificación de Información	Valoración de los activos					
			[D]	[C]	[I]	[A]	[T]	PROM
[COM] Redes de comunicaciones	Acceso telefónico	Reservada de uso interno	0%	100%	0%	0%	0%	20%
	Red inalámbrica	Reservada de uso interno	%	100%	0%	0%	0%	20%
	Internet	Pública	100%	0%	0%	0%	0%	20%
	Manuales de usuario	Reservada de uso interno	100%	0%	0%	0%	0%	20%
	Archivos de documentos como resoluciones, actas tanto administrativas como académicas, proyecto educativo institucional.	Reservada de uso interno	100%	0%	0%	0%	100%	40%
	Documentos varios	Reservada de uso interno	100%	0%	0%	0%	100%	40%
	Carpetas varias. Observador del alumno, manuales de usuario, reglamento del aprendiz, resoluciones.	Confidencial	0%	0%	0%	0%	100%	20%
[AUX] Equipamiento auxiliar	Router	Pública	100%	0%	0%	0%	0%	20%
	Mobiliario: Armarios, archivadores, estantes, mesas.	Pública	100%	0%	0%	0%	0%	20%
	Ups de computadores de soporte y sala de informática.	Pública	100%	0%	0%	0%	0%	20%
	Fuentes de alimentación de equipos de cómputo.	Pública	100%	0%	0%	0%	0%	20%
	Punto de acceso	Pública	100%	0%	0%	0%	0%	20%
[L] Instalaciones	Edificio donde está ubicado el colegio.	Pública	100%	0%	0%	0%	0%	20%
[P] Personal	Docente de informática	Pública	100%	0%	0%	0%	0%	20%
	Personal administrativo, comunidad educativa	Confidencial	100%	0%	0%	0%	0%	20%
	Padres de familia	Pública	100%	0%	0%	0%	0%	20%
	Personas que proveen algún servicio a la institución educativa	Pública	100%	0%	0%	0%	0%	20%

Fuente: Propiedad de las autoras.

4. IDENTIFICACIÓN DE AMENAZAS DE LOS ACTIVOS DE LA INFORMACIÓN DE LA INSTITUCIÓN DE EDUCACIÓN BÁSICA Y MEDIA DEL DEPARTAMENTO DE BOYACÁ, BASADOS EN LA METODOLOGÍA DE MAGERIT

4.1 IDENTIFICACIÓN Y VALORACIÓN DE AMENAZAS

Teniendo en cuenta los tipos de amenazas propuestas por la metodología Magerit, se procede a hacer el análisis de identificación y valoración de amenazas a los activos encontrados en la institución educativa de educación básica media del departamento de Boyacá. En la tabla 9 se encuentran los tipos de amenazas a que puede estar expuesto un activo.

Tabla 9. Tipos de amenazas.

Nomenclatura	Tipos de amenazas
[N]	Desastres naturales
[I]	De origen industrial
[E]	Errores y fallos no intencionados
[A]	Ataques intencionados

Fuente: propiedad de las autoras.

De origen natural [N]. Son los eventos ocurridos sin intervención de los seres humanos[47].

De origen industrial [I]. Son los eventos ocurridos de forma accidental derivados de actividades generados por el hombre[48].

Errores y Fallos no intencionados [E]. Son eventos ocasionados accidentalmente por las personas[49].

Ataques [A]. Son eventos ocurridos intencionalmente por las personas[50].

Para valorar las amenazas, es necesario que se estime una escala de valores que permita determinar el rango de frecuencia en que se puede presentar la amenaza, la cual se realiza mediante estimaciones anuales, mensuales y semanales, asignando un número de veces[51].

---

[47] GOBIERNO DE ESPAÑA, Op. Cit., p. 25.
[48] Ibid, p. 27.
[49] Ibid, p. 33.
[50] Ibid, p. 40.
[51] SUÁREZ, Lorena. Valoración de amenazas [en línea]. s.l.: Universidad Nacional Abierta y a Distancia, 2013. [citado el 28-05-16]. Disponible en: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/3232_valoracin_de_amenazas.html

En la tabla 10 se indica el valor del criterio según la frecuencia con que ocurre una amenaza.

Tabla 10. Escala de rango de frecuencia de amenazas.

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

Fuente: Propiedad de las autoras.

4.1.1 Evaluación de las amenazas a los activos

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

La tabla 11 muestra la valoración de amenazas de los activos de la institución educativa.

Tabla 11. Valoración de amenazas.

Tipos de activos	Nombre de activos	Amenaza	Frecuencia	[D]	[C]	[I]	[A]	[T]
[D]datos / información	Archivos de Documentación legal	[E.1] Errores de los usuarios	70		80%	80%		
		[E.18] Destrucción de información	70		80%	80%		
		[E.19] Fugas de información	70		80%	80%		
		[A.18] Destrucción de información	70		80%	80%		
	Base de datos de Notas - Base de datos estudiantes - Archivos de notas	[E.1] Errores de los usuarios	100	100%	100%	100%	100%	100%
		[E.2] Errores del administrador	100	100%	100%	100%	100%	100%
		[E.19] Fugas de información	100	100%	100%	100%	100%	100%
		[A.5] Suplantación de la identidad del usuario	100	100%	100%	100%	100%	100%
		[A.11] Acceso no autorizado	100	100%	100%	100%	100%	100%
		[A.15] Modificación deliberada de la información	100	100%	100%	100%	100%	100%
		[A.18] Destrucción de información	100	100%	100%	100%	100%	100%
	Base de datos de docentes - Base de datos de Personal administrativo	[E.1] Errores de los usuarios	70					
		[E.2] Errores del administrador	70	80%	80%	80%	80%	80%
		[A.11] Acceso no autorizado	100	100%	100%	100%		
		[A.18] Destrucción de información	100	100%	100%	100%	100%	100%
		[A.19] Revelación de información	100	100%	100%	100%	100%	100%
	Contabilidad de la empresa - Archivos de contabilidad	[E.1] Errores de los usuarios	100		100%	100%		
		[E.18] Destrucción de información	100		100%	100%		
		[E.19] Fugas de información	70		80%	80%		
		[A.19] Revelación de información	50	50%		80%		
	Archivos de actas, resoluciones	[E.1] Errores de los usuarios	50	50%				
		[E.18] Destrucción de información	50	50%				
		[E.19] Fugas de información	50	50%				
		[A.18] Destrucción de información	50	50%				

Tipos de activos	Nombre de activos	Amenaza	Frecuencia	[D]	[C]	[I]	[A]	[T]
[D]datos / información (continuación)	Copias de seguridad de la Información del colegio	[E.1] Errores de los usuarios	50	100%	100%	100%		
		[E.2] Errores del administrador	50	100%	100%	100%		
		[A.18] Destrucción de información	70	100%	80%			
	datos de configuración	E2. Errores del administrador	70		80%			
		E15. Alteración accidental de la información	70		80%			
		E18. Destrucción de la información	70		80%			
		A6. Abuso de privilegios de acceso	70		80%			
		A11. Acceso no autorizado	70		80%			
		A19. Revelación de información	70		80%			
[S] Servicios son los servicios prestados a la entidad	[www] world wide web - Punto vive digital - [edi] intercambio electrónico de datos	E1. Errores de usuarios	100	7,5				
		E9. Errores de re-encaminamiento	100	100%				
		E15. Alteración accidental de la información	5	10%				
		E19. Fugas de información	70	80%				
		A7. Uso no previsto	70	80%				
		A13. Repudio	70	80%				
		A15. Modificación deliberada de información	5	10%				
		A24. Denegación del servicio	100	100%				
[SW] Software - Aplicaciones informáticas	Sistemas Operativos: windows XP, Windows 7 home, Windows 7 ultimate , Windows 8 -- Ofimática: Office 2010, office 2013 -- Antivirus: Avast security, eset 32 -- Apache, WANserver, XAMPP	[I.5] avería de origen físico o lógico	100	100%				100%
		[E.1] errores de usuario	100	100%				100%
		[E.2] errores del administrador	70	80%				80%
		[E.15] Alteración accidental de la información	70	80%				80%
		[E.18] Destrucción de información	70	80%				80%
		[E.19] Fugas de información	70	80%				80%
		[E.20] vulnerabilidad de los programas.	70	100%				100%
		E21. Errores de mantenimiento, actualización de programas(software)	70	100%				100%
		[A.8] difusión de software dañino	100	100%				100%
		[A.11] Acceso no autorizado al software.	100	100%				100%
		[A.19] Software Ilegal	100	100%				100%
		[A.22] manipulación de programas	100	100%				100%
	Visual Basic 6, Visual Basic. NET, Netbeet - macromedia dreamweaver - Máquinas virtuales: Winware, virtualbox	[I.5] avería de origen físico o lógico	100	100%				100%
		[E.1] errores de usuario	100	100%				100%
		[E.2] errores del administrador	100	100%				100%
		[E.20] vulnerabilidad de los programas.	100	100%				100%
		E21. Errores de mantenimiento, actualización de programas(software)	100	100%				100%
		[A.8] difusión de software dañino	100	100%				
		[A.11] Acceso no autorizado al software.	100	100%				
		[A.19] Software Ilegal	100	100%				
		[A.22] manipulación de programas	100	100%	100%	100%	100%	100%
	- Aplicación para el manejo de notas y reportes de los estudiantes -- Gestor de base de datos para almacenar las notas de los estudiantes	[I.5] avería de origen físico o lógico	100	100%	100%	100%	100%	100%
		[E.2] errores del administrador	100	100%	100%	100%	100%	100%
		[E.15] Alteración accidental de la información	100	100%	100%	100%	100%	100%
		[E.18] Destrucción de información	100	100%	100%	100%	100%	100%
		[E.19] Fugas de información	100	100%	100%	100%	100%	100%
		[E.20] vulnerabilidad de los programas.	100	100%	100%	100%	100%	100%
		E21. Errores de mantenimiento, actualización de programas(software)	70	80%	80%	80%	80%	80%
		[A.8] difusión de software dañino	100	100%	100%	100%	100%	100%
		[A.11] Acceso no autorizado al software.	100	100%				
		[A.19] Software Ilegal	100	100%				

Tipos de activos	Nombre de activos	Amenaza	Frecuencia	[D]	[C]	[I]	[A]	[T]
[HW] Equipamiento informático	Equipos de mesa - Equipos portátiles de Computadores para educar Lenovo - Impresoras de multifunción - Módems para acceso a internet	N*. Desastre natural	100	100%				
		I1.fuego origen industrial	100	100%				
		[I.4] contaminación electromecánica	100	100%				
		[I.5] avería de origen físico o lógico	100	100%				
		[I.6] corte de suministro eléctrico	100	100%				
		[I.7]condiciones inadecuadas de temperatura humedad	100	100%				
		[E.2] errores del administrador	100	100%				
		[E.23] error de mantenimiento en los equipos	100	100%				
		[E.24] carencia de recursos físicos del computadores	100	100%				
		[A.6] Abuso de privilegios de acceso	100	100%				
		[A.7] Utilización del equipo para usos no autorizados	100	100%				
		[A.11] Acceso no autorizado al hardware.	100	100%				
		[A.25] Robo	100	100%				
[COM] Redes de comunicaciones	Acceso telefónico - red inalámbrica - internet	I.8. Fallo de servicios de comunicaciones	100	100%				100%
		[E.2] Error de usuario en la instalación y operación	100	100%				100%
		[E.9] Error de enrutamiento	100	100%				100%
		[E.18] perdida accidental de información	100	100%				100%
		[E.19] codificación de información para fines mal intencionados	100	100%				100%
		[E.24] caída del sistema por agotamiento de recursos	100	100%				100%
		[A.5] vulnerabilidad del sistema	100	100%				100%
		[A.6] Abuso de privilegios de acceso	100	100%				100%
		[A.7] abuso de los privilegios para ingreso al sistema no autorizado.	100	100%				100%
		[A.9] desvío de información	100	100%				100%
		[A.11] Acceso no autorizado al hardware	100	100%				100%
		[A.12] análisis de tráfico	100	100%				100%
		[A.14] intercepción de las comunicaciones	100	100%				100%
		[A.19] divulgación de información	100	100%				100%
		[A.24] Denegación de servicio	100	100%				100%
[Media] Soportes de información	Manuales de usuario - Archivos de documentos como académicas, proyecto educativo institucional. - Observador del alumno, reglamento del aprendiz, resoluciones. - Soportes de contabilidad, facturas.	[N.*] Desastres naturales	50	50%				
		[I.3] Otros desastres industriales	50	50%				
		[I.3] contaminación mecánica	50	50%				
		[I.7] condiciones inadecuadas de temperatura o humedad	50	50%				
		[I.10] Degradación de la vida útil del soporte de almacenamiento	50	50%				
		[E.2] errores del administrador	50	50%				
		[E.15] alteración de la información	50	50%				
		[E.18] destrucción del soporte de almacenamiento	50	50%				
		[E.25] pérdida de equipos	70	80%				
		[A.11] acceso no autorizado.	70	80%				
		[A.18] destrucción de la información	70	80%				
		[A.23] manipulación de quipos	70	80%				
		[A.25] Robo	70	80%				
[AUX] Equipamiento auxiliar	Router - Access Point	[N.*] Desastres naturales	70	80%				
		[I.4] contaminación electromecánica	5	10%				
		[I.5] avería de origen físico o lógico	5	10%				
		[I.6] corte de suministro eléctrico	5	10%				
		[I.E] condiciones de temperatura y humedad	5	10%				
		[E.2] errores del administrador	5	10%				
		[E.23] errores de mantenimiento de equipos de hardware	100	100%				

Tipos de activos	Nombre de activos	Amenaza	Frecuencia	[D]	[C]	[I]	[A]	[T]
[AUX] Equipamiento auxiliar (continuación)	Router - Access Point (continuación)	[E.25] perdida de equipos	100	100%				
		[A.23] manipulación de quipos	100	100%				
		[A.24] Denegación de servicio	100	100%				
		[A.25] Robo	70	80%				
		[A.26] Ataque destructivo	70	80%				
	Mobiliario: Armarios, archivadores, estantes, mesas.	[N.*] Desastres naturales	70	80%				
		[I.E] condiciones de temperatura y humedad	70	80%				
		[A.25] Robo	70	80%				
	Ups - Fuentes de alimentación de equipos de cómputo	[N.*] Desastres naturales	100	100%				
		[I.5] Avería de origen físico o lógico	100	100%				
		físico o lógico						
[L] Instalaciones	Edificio	N*. Desastres naturales	100	100%				
		I*. desastres industriales	100	100%				
		A11. Acceso no autorizado	100	100%				
[P] Personal	administradores de sistemas - Usuarios - proveedores	[E.7] deficiencias en el perfil del personal	70	80%				
		[E.28] indisponibilidad del personal	70	80%				
		[A.29] Extorsión	70	80%				
		[A.30] ingeniería social (picaresca)	100	100%				

Fuente: Propiedad de las autoras.

4.2 RIESGO POTENCIAL

El riesgo potencial se valora de acuerdo al impacto que llegue a materializarse la amenaza en dicho activo, y qué daño probable pueda causar a la entidad.

4.2.1 Criterios de evaluación

Los criterios de valoración se muestran en una escala cualitativa para la estimación del Riesgo que puede tener una entidad.

En la tabla 12 se presentan las escalas de impacto, probabilidad y riesgo de los activos.

Tabla 12. Escalas.

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

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

4.2.2 Evaluación del riesgo potencial a los activos

Se evalúa el riesgo potencial que tienen los activos, de acuerdo al impacto producido por amenazas que se pueden llegar a materializar y causar daños a la entidad. Esta valoración se realiza de manera cualitativa.

La tabla 13 muestra la valoración de riesgo potencial.

Tabla 13. Valoración del riesgo potencial.

Tipos de activos	Nombre de activos	Impacto	Probabilidad	Riesgo
[D]datos / información	Archivos de Documentación legal	Alto	Probable	Importante
	Base de datos de Notas - Base de datos estudiantes - Archivos de notas	Muy alto	Prácticamente inseguro	Critico
	Base de datos de docentes - Base de datos de Personal administrativo	Alto	Posible	Importante
	Contabilidad de la empresa - Archivos de contabilidad	Alto	Posible	Importante
	Archivos de actas, resoluciones	Alto	Posible	Importante
	Copias de seguridad de la Información del colegio	Alto	Posible	Importante
	datos de configuración	Alto	Probable	Importante
[S] Servicios son los servicios prestados a la entidad	[www] world wide web - Punto vive digital - [edi] intercambio electrónico de datos	Alto	Prácticamente inseguro	Importante
[SW] Software - Aplicaciones informáticas	Sistemas Operativos: windows XP, Windows 7 home, Windows 7 ultimate, Windows 8 - Ofimática: Office 2010, office 2013 - Antivirus: Avast security, eset 32 -A pache, WANserver, XAMPP	Muy alto	Posible	Muy critico
	Visual Basic 6, Visual Basic. NET, Netbeet - macromedia dreamweaver - Máquinas virtuales: Winware, virtualbox	Medio	Probable	Bajo
	Aplicación para el manejo de notas y reportes de los estudiantes -- Gestor de base de datos para almacenar las notas de los estudiantes	Muy alto	Prácticamente inseguro	Muy critico
[HW] Equipamiento informático	Equipos de mesa - Equipos portátiles de Computadores para educar Lenovo - Impresoras de multifunción - Módems para acceso a internet	Muy alto	Prácticamente inseguro	Muy critico
[COM] Redes de comunicaciones	Acceso telefónico - red inalámbrica - internet	Muy alto	Prácticamente inseguro	Apreciable
[Media] Soportes de información	Manuales de usuario - observador del alumno, reglamento del aprendiz, resoluciones. - Soportes de contabilidad, facturas.	Media	Probable	Importante

Tipos de activos	Nombre de activos	Impacto	Probabilidad	Riesgo
[AUX] Equipamiento auxiliar	Router - Access Point	Medio	Poco probable	Bajo
	Mobiliario: Armarios, archivadores, estantes, mesas.	Alto	Poco probable	Bajo
	Ups - Fuentes de alimentación de equipos de cómputo.			
[L] Instalaciones	Edificio	Bajo	Muy raro	Bajo
[P] Personal	Administradores de sistemas - Usuarios - proveedores	Medio	Posible	Apreciable

Fuente: Propiedad de las autoras.

5. DEFINICIÓN DE CONTROLES DE ACUERDO AL ANEXO A DE LA NORMA ISO 27001:2013 PARA LA INSTITUCIÓN EDUCATIVA Y RECOMENDACIONES DE IMPLEMENTACIÓN

Se definen de manera general salvaguardas o controles, para contrarrestar el impacto cuando se materialice una amenaza en los activos encontrados en la institución educativa de educación media y básica del departamento de Boyacá, para que ayuden.

En la tabla 14 se relacionan los controles, especificando si en la institución educativa cumple con la aplicación de los mismos.

Tabla 14. Controles.

Control ISO	Controles	Cumple		Control / descripción
		Si	No	
5.1	5.1.1 Políticas para la seguridad de la información		x	Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes
	5.1.2 Revisión de la política de seguridad de la información		x	Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.
6.1	6.1.1 Roles y responsabili-dades para la seguridad de información		x	Se deberían definir y asignar todas las responsabilidades de la seguridad de la información
7.1	7.1.1 Investigación de antecedentes	x		Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían 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
	7.2.1 Responsabilidades de la dirección		x	La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
8.2	8.2.1. Clasificación de la información	x		La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
	8.2.3 Manejo de activos		x	Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización
9.1	9.1.1 Política de control de acceso		x	Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información
	.9.1.2 Política sobre el uso de los servicios de red		x	Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente
	9.2.3 Gestión de derechos de acceso privilegiado		x	Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado
9.4	9.4.1 Restricción de acceso Información	x		El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.
	9.4.2 Procedimiento de ingreso seguro		x	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.
	9.4.3 Sistema de gestión de contraseñas		x	Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.
	9.4.4 Uso de programas utilitarios privilegiados		x	Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones

Control ISO	Controles	Cumple		Control / descripción
		Si	No	
11	11.1.3. Seguridad de oficinas, recintos e instalaciones	x		Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
	11.1.4. Protección contra amenazas externas y ambientales	x		Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
	11.2.2 Servicios de suministro	x		Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro
	11..2.4 Mantenimiento de equipos	x		Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.
12	12.2.1 Controles contra códigos maliciosos		x	Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
	12.3.1 Respaldo de información	x		Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.
	12.4.1 Registro de eventos		x	Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
	12.4.2 Protección de la información de registro	x		Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado
	12.5.1 Instalación de software en sistemas operativos		x	Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos
	12.6.2 Restricciones sobre la instalación de software		x	Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios
13	13.1.1 Controles de redes	x		Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.
	13.2.3 Mensajería electrónica	x		Se debería proteger adecuadamente la información incluida en la mensajería electrónica
15	15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores	x		Se deberían 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.
	15.2.1 Seguimiento y revisión de los servicios de los proveedores	x		Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
16	16.1.3 Reporte de debilidades de seguridad de la información	x		Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
	16.1.7 Recolección de evidencia		x	La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
17	17.1.2 Implementación de la continuidad de la seguridad de la información	x		La organización debería 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.
18	18.1 3 Protección de registros	x		Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
	18.1.4 Privacidad y protección de datos personales	x		Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.
	18.2.2 Cumplimiento con las políticas y normas de seguridad		x	Los directores deberían 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.
	18.2.3 Revisión del cumplimiento técnico		x	Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

Fuente: Propiedad de las autoras.

6. DISEÑO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA INSTITUCIÓN DE EDUCACIÓN BÁSICA Y MEDIA DEL DEPARTAMENTO DE BOYACÁ, BASADAS EN LA NORMA ISO 27001:2013

6.1 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

6.1.1 Políticas de clasificación de la información

La clasificación de la información de un activo se realiza de acuerdo a sus características fundamentales: confidencialidad, integridad y disponibilidad, y la función que éste tenga en la institución.

Cada área debe elaborar y mantener un inventario de los activos de información que poseen (procesada y producida). Estos activos se clasifican de acuerdo a una valoración, ubicación y acceso de la información.

- Objetivo. Clasificar los activos conforme a su nivel de criticidad en la institución educativa.

- Aplicabilidad. La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de la institución educativa, entes externos como contratistas o proveedores y cualquiera que sea el nivel de actividades que desempeñen.

- Directrices. A continuación se establece el criterio de clasificación de la información, en función a cada una de las mencionadas características:

En la clasificación de la información se tiene en cuenta los siguientes niveles: Publica - Privada - Reservada (Uso Interno) y Confidencial. Para ello se aplica las tres dimensiones fundamentales de seguridad informática.

- Confidencialidad. Información que puede ser conocida y utilizada sin autorización por cualquier usuario, sea empleado de la institución o no. PÚBLICO.

* Información que puede ser conocida y utilizada por toda la comunidad educativa de la institución y algunas entidades externas debidamente autorizadas, cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para la institución, el Sector Público Nacional o terceros. RESERVADA - USO INTERNO.
* Información que sólo puede ser conocida y utilizada por un grupo de la comunidad educativa, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a la institución, al Sector Público Nacional o a terceros. RESERVADA - CONFIDENCIAL.
* Información que sólo puede ser conocida y utilizada por un grupo muy reducido

de la comunidad educativa, generalmente los directivos, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo, al Sector Público Nacional o a terceros. RESERVADA SECRETA.

- **Integridad**

* Información cuya modificación no autorizada puede repararse fácilmente, y no afecta la operación normal de la institución.
* Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para la institución, el Sector Público Nacional o terceros.

- **Disponibilidad**

* La información es accesible y utilizada en tiempo determinado por la institución educativa.
* La Información no afecta las actividades normales de la institución educativa.

6.1.2 Políticas de seguridad para los recursos humanos

Toda la comunidad educativa debe tener sus perfiles definidos para el uso de los recursos de los activos de información, con el fin de organizar y orientar una adecuada Política de Seguridad.

- **Objetivo.** Definir las responsabilidades a cada uno de los funcionarios de acuerdo al área de trabajo.

- **Aplicabilidad.** La Política de Seguridad de recurso humano es de aplicación obligatoria para todo el personal de la institución educativa, entes externos como contratistas o proveedores y cualquiera que sea el nivel de actividades que desempeñen.

- **Directrices**

* Teniendo en cuenta el perfil del funcionario se definirá el nivel de seguridad de acuerdo a sus funciones establecidas.
* El funcionario debe ser responsable con la información y equipos que tiene asignados para el desempeño de sus actividades.
* El funcionario es responsable de solicitar capacitación necesaria de acuerdo a su perfil y su área desempeño para el adecuado desarrollo de sus actividades.
* Los funcionarios deben reportar cualquier anomalía que se presente en el área de trabajo.

6.1.3 Política de seguridad de control de acceso

Esta Política de Seguridad contempla los controles de acceso que se deben tener en cuenta de acuerdo a los perfiles de cada funcionario de la institución educativa.

- **Objetivo.** Asignar el nivel de control de acceso de acuerdo a las funciones desempeñadas de cada funcionario.

- **Aplicabilidad.** La Políticas de seguridad para usuarios

La comunidad educativa, usuarios externos y proveedores que desempeñen alguna función en la institución educativa recibirán una adecuada capacitación y actualización periódica en políticas de seguridad, normas y procedimientos de la misma.

- **Objetivo.** Especificar funciones y reglamento de seguridad de la información para los Usuarios.

- **Aplicabilidad.** La Política de Seguridad de los usuarios es de aplicación obligatoria para todo el personal de la institución educativa, entes externos como contratistas o proveedores y cualquiera que sea el nivel de actividades que desempeñen.

- **Directrices**

* El usuario debe tener en cuenta las normas establecidas de seguridad de los activos.
* Los usuario según su privilegio tendrán unas reglas que cumplir de acuerdo a los activos de información que vaya a manejar
* Los usuarios no podrán suministrar información sin previa autorización.
* La clave del usuario será asignada por el administrador del área de informática.
* La clave del usuario será cambiada periódicamente.
* Los usuarios no deben revelar las claves dadas por la Institución educativa.

6.1.4 Políticas de seguridad para contratistas

Las políticas de seguridad aplicadas a los contratistas, corresponden a personas externas a la institución educativa que realizan convenios o prestan un servicio deben cumplir las normas establecidas jurídicamente por la Institución educativa.

- **Objetivo.** Garantizar que los activos informáticos manejados por terceros, disponga de los requerimientos de seguridad de la información con el objeto de no incurrir en riesgos de los recursos de las Instituciones educativas.

- Aplicabilidad. La Política de Seguridad para contratistas es de aplicación obligatoria para contratistas, sus jefes inmediatos y sus interventores.

- Directrices

* Firma de documentos de un acuerdo oficial entre las partes.
* Legalidad de los recursos suministrados a la institución Educativa.

El suministro de los activos de la institución educativa a los contratistas debe tener la aprobación y certificación del responsable de la institución educativa. La política de seguridad de control de acceso es de aplicación obligatoria para todo el personal de la institución educativa, entes externos como contratistas o proveedores y cualquiera que sea el nivel de actividades que desempeñen.

- Directrices

* Únicamente los funcionarios autorizados por las directivas de la institución educativa serán responsables de instalar y manipular software o hardware de los equipos de la institución educativa.
* Los funcionarios deben tener su respectivo usuario y contraseña de acuerdo a su perfil en la institución educativa.
* Las contraseñas de los funcionarios son de uso personal e intransferible y es responsabilidad del funcionario el adecuado manejo que le da a la misma.

6.1.5 Política de seguridad mantenimiento de sistemas de información

Las políticas de Seguridad aplicadas al mantenimiento de sistemas de información (aplicaciones a la medida) deben tener una correcta administración de funcionamiento, manejo y protección tanto de aplicaciones a la medida (bases de datos), sistemas operativos y aplicativos en general que se requieran.

- Objetivo. Especificar las reglas generales para tener una apropiada protección de los sistemas de información por parte de la comunidad educativa y contratistas.

- Aplicabilidad. La Política de Seguridad de mantenimiento de sistemas de información es de aplicación obligatoria para todo el personal de la institución educativa, entes externos como contratistas o proveedores y cualquiera que sea el nivel de actividades que desempeñen.

- Directrices

* Las aplicaciones adquiridas por parte de terceros deben cumplir requerimientos legales de uso comercial.
* Las contraseñas de las aplicaciones deben ser manejas exclusivamente por los funcionarios que están a cargo de dicha área.

* Las aplicaciones que se instalen en la institución educativa deben tener la licencia y deben ser aprobados y autorizados por los directivos de la institución.
* Al realizar el mantenimiento de los aplicativos se deben hacer copias de seguridad, previo aviso a las directivas de la institución.
* El área encarga de la instalación de aplicativos debe verificar que se instale o actualice en los equipos destinados únicamente para tal fin.
* Se debe verificar que el aplicativo se instale o actualice únicamente en los equipos destinados para tal fin.
* Las copias de los aplicativos y su documentación correspondiente debe tener la aprobación de las directivas de la institución educativa y del proveedor.

6.1.6 Políticas de seguridad para backup de información

Las Políticas de seguridad para backup de Información se refieren a copias de respaldo de la información de los activos que maneja la institución educativa; ya que estos pueden estar expuestos a desastres naturales o de origen Industrial.

- **Objetivo.** Establecer reglas para hacer copias de seguridad de información con el objeto de proteger la información a eventuales amenazas tanto físicas como lógicas.

- **Aplicabilidad.** La Política de Seguridad de Backup de Información es de aplicación obligatoria para todo el personal de la institución educativa y cualquiera que sea el nivel de actividades que desempeñen.

- **Directrices**

* Definir y programar los procedimientos de copias de respaldo de la Información de la institución educativa.
* Se debe establecer un cronograma para realizar las copias de seguridad.
* Se debe elegir el medio o dispositivo donde se va almacenar la copia de respaldo de la información.
* Se debe revisar, periódicamente, la integridad de las copias de respaldo de la información que se está almacenando.
* Se debe elegir que usuarios pueden realizar las copias de seguridad y/o respaldo de la información.

6.1.7 Políticas de seguridad para estaciones de trabajo

- **Objetivo.** Proteger las estaciones de trabajo mediante el uso de control de acceso (usuario y contraseña) de acuerdo al perfil.

- **Aplicabilidad.** La Política de Seguridad de estaciones de trabajo es de aplicación obligatoria para todo el personal de la institución educativa, entes

externos como contratistas o proveedores y cualquiera que sea el nivel de actividades que desempeñen.

- **Directrices**

* Definir los perfiles de usuario según el nivel de servicio.
* Instalar Software adecuado para la protección de las estaciones de trabajo.
* Instalar hardware adecuado según el servicio que ofrecen las estaciones de trabajo.
* Realizar adecuadamente el mantenimiento preventivo y correctivo de las estaciones de trabajo aplicando las políticas de seguridad de mantenimiento de Equipos de cómputo.
* Informar ante cualquier eventualidad que presente una estación de trabajo a la persona responsable.
* Se debe llevar una bitácora donde se registre las eventualidades que puedan ocurrir.
* Instalar un firewall en la puerta de enlace en cada una de las estaciones de trabajo.

6.1.8 Política de seguridad de redes sociales

Esta política de seguridad de Redes sociales se refiere a la protección del manejo adecuado de las redes sociales en la institución educativa.

- **Objetivo.** Definir normas de seguridad para el ingreso a las redes sociales según los diferentes niveles de usuarios de la institución educativa.

- **Aplicabilidad.** La Política de Seguridad de redes sociales es de aplicación obligatoria para todo el personal de la institución educativa, entes externos como contratistas o proveedores y cualquiera que sea el nivel de actividades que desempeñen.

- **Directrices**

* No publicar información confidencial de la institución educativa.
* Instalar aplicaciones de redes sociales que sean solo de uso educativo.
* Bloquear las redes sociales que no sean de uso educativo.

6.1.9 Política de seguridad de uso de Internet

Las instituciones educativas deben administrar el uso de la red de internet de acuerdo a sus necesidades en cada dependencia haciendo buen uso; teniendo en cuenta las normas de seguridad que exigirán en cada área.

- Objetivo. Cumplir con las políticas de acceso establecidas para el uso adecuado de la red de Internet para mantener la privacidad de los datos.

- Aplicabilidad. La Política de Seguridad de uso de internet es de aplicación obligatoria para todo el personal de la institución educativa, entes externos como contratistas o proveedores y cualquiera que sea el nivel de actividades que desempeñen.

- Directrices

* El uso adecuado del internet.
* De acuerdo al nivel de perfil de usuarios se debe restringir el acceso a información privilegiada desde el navegador.
* Se restriegue a los usuarios descargar cualquier software de Internet sin la debida autorización de la persona responsable.
* Se debe colocar una aplicación para restringir el uso de algunas páginas de internet que no sean competentes para la educación.
* El acceso a la información tanto de la parte administrativa, docentes y estudiantes es restringida de acuerdo al perfil asignado.
* Instalar y configurar aplicaciones de seguridad a los navegadores.
* Instalar y configurar aplicaciones para controlar la navegación de los usuarios.
* Tener el software adecuado para la protección y control de la navegación de los usuarios.
* Bloquear servicios que no se requieran en la institución educativa.

6.1.10 Política de seguridad de uso de carpetas compartidas y discos externos

La institución educativa debe cumplir con las normas de seguridad del uso de carpetas compartidas y sus discos externos.

- Objetivo. Proteger Carpetas compartidas y Discos (dispositivos) externos.

- Aplicabilidad. La Política de Seguridad de protección de carpetas compartidas y discos externos es de aplicación obligatoria para todo el personal de la institución educativa, entes externos como contratistas o proveedores y cualquiera que sea el nivel de actividades que desempeñen.

- Directrices

* Definir control, de acceso y protección a las carpetas compartidas y discos externos.
* Instalar y aplicar herramientas para los permisos de carpetas compartidas y discos externos.
* Definir control de usuario de las carpetas compartidas y discos externos.

6.1.11 Política de seguridad de Impresora y servicios de Impresión

La institución educativa debe cumplir con las normas de seguridad del uso de la impresora.

- **Objetivo.** Administrar adecuadamente el uso del servicio de impresora.

- **Aplicabilidad.** La Política de Seguridad de impresora y servicios de impresión es de aplicación obligatoria para todo el personal de la institución educativa, entes externos como contratistas o proveedores y cualquiera que sea el nivel de actividades que desempeñen.

- **Directrices**

* Hacer uso adecuado del servicio de impresión.
* Únicamente el recurso de impresión se utilizara para la institución educativa.
* La impresora únicamente debe estar conectada a la red y/o equipos de la institución educativa.
* Únicamente el personal autorizado por la institución educativa podrá hacer mantenimiento de impresoras.
* Se llevar una bitácora con el registro de los eventos ocurridos de la impresora.

6.1.12 Política de seguridad de uso de correo electrónico institucional

La política de uso de seguridad del correo electrónico institucional es establecer normas para el acceso y uso del correo, cuya función será intercambiar información de ámbito laboral.

- **Objetivo.** Establecer las buenas prácticas para el acceso y uso adecuado del correo electrónico institucional.

- **Aplicabilidad.** La Política de Seguridad de uso de correo electrónico institucional es de aplicación obligatoria para todo el personal de la institución educativa, entes externos como contratistas o proveedores y cualquiera que sea el nivel de actividades que desempeñen.

- **Directrices**

* La cuenta de correo electrónico institucional debe ser utilizada para uso laboral e informativo únicamente a la comunidad educativa.
* Únicamente la cuenta de correo electrónico institucional estará activa mientras en funcionario esté vinculado a la institución.
* Cada funcionario será responsable de salvaguardar su usuario y contraseña.
* Instalar herramientas que permitan el control del correo institucional.

6.1.13 Políticas de seguridad de uso de puntos de red de datos

La institución educativa debe cumplir con las normas de seguridad para el uso de puntos de acceso a la red de datos.

- **Objetivo.** Aplicar y administrar mecanismos adecuados para la protección de la red de datos.

- **Aplicabilidad.** La Política de Seguridad de uso de puntos de red de datos es de aplicación obligatoria para todo el personal de la institución educativa, entes externos como contratistas o proveedores y cualquiera que sea el nivel de actividades que desempeñen.

- **Directrices**

* Hacer uso adecuado del acceso de la red.
* Únicamente el personal autorizado por la institución educativa se encargara del mantenimiento a la red de Datos.
* Utilizar siempre usuario y contraseña para el acceso a la red.
* Mantener actualizados los protocolos de seguridad de la red de datos.
* Únicamente deben estar conectados dispositivos y equipos que sean de la institución educativa.
* Adoptar mecanismos de seguridad tanto para la red física como lógica.
* Para conexión de equipos se debe contar con previa autorización de la persona responsable.
* Instalar un firewall en la puerta de enlace de la red de la institución educativa.

6.1.14 Políticas de seguridad de instalación de software

La institución educativa debe tener en cuenta que para la instalación de software debe cumplir con normas y requisitos de acuerdo a cada dependencia.

- **Objetivo.** Definir e instalar software con licencia según lo requiera cada dependencia de la institución educativa.

- **Aplicabilidad.** La Política de Seguridad de instalación de software es de aplicación obligatoria para el responsable de los activos informáticos de la institución educativa.

- **Directrices**

* El responsable de los activos informáticos debe contar con las licencias adecuadas para el proceso de instalación de software.
* Únicamente se instalará software de acuerdo a los requisitos solicitados por

cada dependencia previo análisis del responsable de los activos informáticos de la institución educativa.

6.1.15 Políticas de seguridad de actualización de antivirus

La Política de Seguridad de actualización de antivirus es una norma para contrarrestar y salvaguardar los posibles virus informáticos a que puede estar expuesta la información de la institución educativa.

- Objetivo. Establecer normas de seguridad con el fin de actualizar periódicamente el Antivirus para proteger la información que se encuentra en los equipos de la institución educativa.

- Aplicabilidad. La Política de Seguridad de uso de puntos de red de datos es de aplicación obligatoria para todo el personal de la institución educativa, entes externos como contratistas o proveedores y cualquiera que sea el nivel de actividades que desempeñen.

- Directrices

* Instalar antivirus licenciado.
* Actualizar el antivirus periódicamente.
* Programar el antivirus para escanear los equipos de cómputo.
* Cuando se detecte alguna amenaza informática se debe proceder a su eliminación.
* Adquirir Antivirus licenciado para actualizarlo periódicamente en las estaciones de trabajo.

6.1.16 Políticas de seguridad de actualización de computadores

- Objetivo. Establecer normas de seguridad para la actualización (robustez) de equipos de cómputo.

- Aplicabilidad. La Política de Seguridad de actualización de computadores es de aplicación obligatoria para todo el personal de la institución educativa, entes externos como contratistas o proveedores y cualquiera que sea el nivel de actividades que desempeñen.

- Directrices

* Tener debidamente registrados todas las fallas técnicas que presenta cada equipo de cómputo.
* Revisar periódicamente el estado de operación de los equipos de cómputo, para determinar su posible actualización.
* Cualquier cambio en la actualización de equipos de cómputo debe estar

debidamente documentada y autorizada por la persona responsable de la institución educativa.

6.1.17 Políticas para el administrador de sistemas

Es el responsable de la administración del sistema que funcione correcta y adecuadamente.

- Objetivo. Garantizar que el sistema funcione correctamente y que los funcionarios puedan utilizar el sistema sin problemas.

- Aplicabilidad. Esta política aplica para el administrador del sistema

- Directrices

* Mantener adecuadamente el funcionamiento del sistema
* Administración de usuarios (registro de cuentas)
* Monitoreo de la comunicaciones
* Tener debidamente registrados todas las fallas técnicas que presenta cada equipo de cómputo.
* Revisar periódicamente el estado de operación de los equipos de cómputo, para determinar su posible actualización.
* Instalación de todo el software necesario en institución
* Cualquier cambio en la actualización de equipos de cómputo debe estar debidamente documentada y autorizada por la persona responsable de la institución educativa.

6.1.18 Políticas para los outsoursing o tercerización de procesos

Es un proceso en el cual un proveedor externo realiza algunas actividades en los procesos que realiza la institución educativa.

- Objetivo. Salvaguardad la información de la Institución educativa ante los proveedores externos.

- Aplicabilidad. Esta política se aplica a proveedores externos, contratistas, consultores, personal temporal entre otros que tengan acceso a activo de la información de la institución educativa.

- Directrices

* Selección de los proveedores que van a manejar los procesos de la Institución educativa.
* Formalizar un acuerdo de confidencialidad entre las partes.

* Se debe mantener actualizados los controles en los activos que sean usados por terceras personas.

6.1.19 Políticas de uso de los activos de la Información

Esta política se refiere a las normas que se deben tener en cuenta para la protección de los activos ante eventuales amenazas.

- **Objetivo.** Resguardar apropiadamente los activos de la Información de la institución educativa.

- **Aplicabilidad.** La política de uso de los activos de información es de aplicación obligatoria para todo el personal de la institución educativa, entes externos como contratistas o proveedores y cualquiera que sea el nivel de actividades que desempeñen.

- **Directrices**

* Los activos de la institución educativa deben ser utilizados únicamente con fines laborales.
* Los usuarios únicamente manejaran los programas y equipos que desarrollan procesos que se realizan en la Institución educativa.
* Cada activo de información debe estar debidamente registrado en la bitácora y además sus modificaciones que este tenga.
* No se puede realizar actividades que no estén autorizadas por el personal de área tecnología como: - instalar software ilegal - descargar software en línea - No se podrá alterar, ni actualizar el software de la institución educativa.

6.1.20 Política de cableado de red de datos

Esta política de uso de cableado de red de datos se refiere a las normas que se deben tener en cuenta en la estructura física del cableado de red de datos instalado en la Institución educativa.

- **Objetivo.** Proteger el cableado estructurado de la institución educativa.

- **Aplicabilidad.** Esta política de seguridad de cableado de red de datos aplica para el administrador del sistema.

- **Directrices**

* Los puntos de acceso del cableado estructurado ya sea horizontal y/o vertical deben cumplir con el estándar ISO.
* Se deben utilizar las herramientas apropiadas para la certificación de cableados modificados y nuevos en la Institución educativa.

* Se debe llevar una bitácora donde se registren inconvenientes presentados y sus posibles soluciones.

6.1.21 Política de escritorio y pantalla limpia

Esta política de escritorios y pantallas limpias se refiere a las normas que se deben tener para protección de la información de fácil acceso que se maneja en las estaciones de trabajo.

- Objetivo. Especificar pautas de normas de seguridad para los escritorios y pantallas limpias de la institución educativa con el fin de evitar pérdidas y daños de la información tanto física como digital.

- Aplicabilidad. La política de seguridad de escritorios y pantallas limpias es de aplicación obligatoria para todo el personal de la institución educativa, entes externos como contratistas o proveedores y cualquiera que sea el nivel de actividades que desempeñen.

- Directrices

* Los funcionarios de la institución educativa no deben tener información importante de la entidad sobre el escritorio.
* Los equipos deben tener un protector de pantalla de seguridad (bloquear pantalla) en caso de que el funcionario se ausente de su puesto de trabajo.
* Al tener documentos ya sean impresos, copias o escaneados que son confidenciales para la entidad, estos deben ser retirados de la impresora y del escritorio y deben ser guardados debidamente.
* Proteger con claves el acceso a los Equipos de Cómputo.

6.1.22 Política de mantenimiento de equipos de cómputo

Esta política de mantenimiento de equipos de cómputo se refiere a las normas que se deben tener en cuenta para proteger el mantenimiento y configuración de los equipos de cómputo de la institución educativa.

- Objetivo. Garantizar la protección adecuada del mantenimiento de Equipos de cómputo.

- Aplicabilidad. La política de seguridad de mantenimiento de equipos de cómputo es de aplicación obligatoria para todo el personal de la institución educativa, entes externos como contratistas o proveedores y cualquiera que sea el nivel de actividades que desempeñen.

- **Directrices**

* Solamente el personal autorizado será el encargado de realizar mantenimiento a los equipos de cómputo.
* Se debe tener la hoja de vida de cada equipo de cómputo donde se especifique como mínimo: - características de hardware y software, - aplicaciones a la medida - el responsable del equipo - y la función del equipo.
* La configuración de los equipos debe estar protegida para que los funcionarios y/ o personal externo no puedan instalar y desinstalar hardware y software.
* Se debe llevar una bitácora de cada equipo de cómputo de la Institución educativa donde se registre todas las eventualidades de mantenimiento preventivo y correctivo.
* Se debe realizar el mantenimiento a los equipos de cómputo en fechas programadas por el responsable de sistemas.
* Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.

6.1.23 Política de uso de claves

Esta política de seguridad de uso de claves hace referencia a las normas para creación de una contraseña segura en la Institución educativa.

- **Objetivo.** Especificar adecuadamente las contraseñas que sean utilizadas en la Institución educativa para mantener salvaguardados los activos de información.

- **Aplicabilidad.** La política de creación y uso de claves es de aplicación obligatoria para todo el personal de la institución educativa, entes externos como contratistas o proveedores y cualquiera que sea el nivel de actividades que desempeñen.

- **Directrices**

* La contraseña es de uso personal.
* Únicamente el administrador del sistema será el único que tiene el perfil de restablecer contraseñas.
* La contraseña debe poseer las siguientes característica: para no ser descifrada Debe poseer: números, letras mayúsculas y minúsculas, símbolos especiales, no debe poseer espacios en blanco, fechas de nacimiento, documento de identidad, número telefónico.
* La contraseña debe tener como mínimo 8 caracteres
* Las contraseñas deben ser cambiadas al menos cada mes.
* Las contraseñas no deben ser expuestas a través de ningún medio de comunicación.

7. CONCLUSIONES

- En el diagnóstico realizado a los activos de información aplicando la metodología MAGERIT se pudo verificar con que activos cuenta la institución educativa, mencionados activos fueron clasificados de acuerdo a los criterios de la información (público, reservado, confidencial, secreto).

- En la institución educativa no cuenta con unas políticas de seguridad adecuadas para la seguridad de la información. Cuando debería ser importante este proceso tanto para usuarios administrativos como académicos porque ellos deben tener claro el concepto de seguridad informática y como aplicarlo debidamente a sus actividades diarias para evitar errores y así minimizar los costos elevados que se presentarían al llegar a ocurrir algún riesgo en los activos de información.

- Se utilizó la metodología Magerit teniendo en cuenta las siguientes fases: identificación de activos, clasificación de los activos, identificación de parámetros, clasificación de amenazas, valoración del impacto de forma cualitativa; con el fin de realizar un análisis de las amenazas y sus posibles riesgos si estas se llegaran a presentar.

- Al determinar las amenazas a que están expuestos los activos en la Institución Educativa nos permitió hacer el análisis para identificar los problemas de seguridad que existe en la institución y así mismo poder aplicar los controles necesarios para salvaguardarlos de los posibles riesgos.

- Al identificar las vulnerabilidades que se encontraron en los activos, se procede a la identificación de los controles, con el objetivo para reducir o disminuir el riesgo a que un activo puede estar expuesto; por consiguiente con los salvaguardas se pretende proteger la información que posee cada activo.

- El diseño de una Política de Seguridad informática es un proceso sencillo, lo difícil es su viabilidad y ejecución en una entidad.

- Las políticas de seguridad propuestas en esta monografía tiene como objetivo: reducir y mejorar la seguridad de la información, para mejorar la productividad en procesos de dichos activos en la Institución Educativa.

- Todos los activos de información que se encuentra en las entidades institucionales tiene un valor importante ya que son indispensables para sus

diferentes procesos. Es por esto que se deben tomar las medidas necesarias para proteger los activos informáticos de las amenazas y riesgos a que están expuestos diariamente. Por este motivo se aplicó la norma ISO 27001 para proponer las políticas de seguridad donde se establece unas directrices básicas para su aplicación.

8. RECOMENDACIONES

- Es importante contar con un manual de políticas de seguridad informática en una entidad con el objetivo de minimizar riesgos en los diferentes procesos de determinada entidad.

- Las políticas de seguridad descritas en este documento son a nivel general, que pueden ser aplicadas en cualquier institución educativa teniendo en cuenta sus activos.

- En la institución educativa es indispensable la capacitación a todos los usuarios que hacen parte de la comunidad educativa debido a que la seguridad informática depende de todos.

- La institución educativa debe tener el perfil del profesional adecuado para el área determinada, con el fin de administrar adecuadamente el área.

- Se recomienda que las Instituciones Educativas deben mejorar su tecnología teniendo en cuenta sus activos físicos y lógicos como por ejemplo: firewall, licencias de software, actualización de antivirus, instalación de sistemas operativos licenciados. Lo anteriormente expuesto con el fin de respetar los derechos de autor.

BIBLIOGRAFÍA

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

BUSTAMANTE, G. y CANO, J. Metodología de la seguridad de la información como medida de protección en pequeñas empresas. En: Cuaderno Activa. 2016. no. 6, p. 74-75.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Decreto 1727 (15 de mayo de 2009).Bogotá. Diario Oficial 47.350 de mayo 15 de 2009. p. 1-5.

_____. Decreto 1377 (27 de junio de 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Diario Oficial 48.834 de 27 de junio de 2013. p. 1-11.

_____. Ley 57 de 1985 (julio 5 de 1985). Por la cual se ordena la publicidad de los actos y documentos oficiales. Diario Oficial 05 de julio de 1985. p. 1-6.

_____. Ley 527 (18 de agosto de 1999).Bogotá. Diario Oficial 43.673 de 21 de agosto de 1999. p 1-2.

_____. Ley Estatutaria 1266 (diciembre 31 de 2008). Bogotá. Diario Oficial 47.219 de 31 de diciembre de 2008. p. 1-19.

_____. Ley 1273 (05 de enero de 2009). Bogotá. Diario Oficial 47.223 de enero 5 de 2009. p. 1-15.

_____. Ley Estatutaria 1266 (julio 30 de 2009). Bogotá. Diario Oficial 47.426 de julio 30 de 2009. p. 1-34.

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

ESPAÑA. MINISTERIO DE LA PRESIDENCIA. Real Decreto 3 del 2010 (enero 8 de 2010). Por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Boletín Oficial del Estado de enero 29 de 2010. p. 1-50.

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

HURTADO DE BARRERA, Jacqueline. Guía para la comprensión holística de la ciencia. 3ª ed. Caracas: Fundación Sypal, 2010.

_____. Metodología de la investigación holística. Caracas: SYPAL-IUTC, 2000.

WEBGRAFÍA

AUDISIS. Sistema de gestión de seguridad de la información - SCSI ISO 27001:2013 - Implantación y auditoría. [en línea]. Bogotá: El autor, s.f. [citado el 15-04-16]. Disponible en: http://www.audisis.com/BROCHURE_Sem_Implementaci%C3%B3n_SGSI.pdf

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

BENÍTEZ, Moisés. Políticas de seguridad informática [en línea]. En: Gestión integral. 2013. no. 1, p. 8. [citado el 16-04-16]. Disponible en: http://www.gestionintegral.com.co/wp-content/uploads/2013/05/Pol%C3%ADticas-de-Seguridad-Inform%C3%A1tica-2013-GI.pdf

CONGRESO DE COLOMBIA. Ley 1273 de 2009 [en línea]. Bogotá: Secretaría General del Senado, 2009. [citado el 21-04-16]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

_____. Ley estatutaria 1581 de 2012 [en línea]. Bogotá: Secretaría General de la Alcaldía Mayor, 2012. [citado el 15-05-16]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley estatutaria 1266 de 2008 [en línea]. Bogotá: Secretaría General del Senado, 2016. [citado el 14-05-16]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

DEFINICIÓNABC. Definición de confidencialidad [en línea]. s.l.: El autor, s.f. [citado el 14-04-16]. Disponible en: http://www.definicionabc.com/comunicacion/confidencialidad.php

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

GÓMEZ G., Yessica. Seguridad de la información [en línea]. s.l.: Slideshare, 2013. [citado el 28-04-16]. Disponible en: http://www.slideshare.net/hvillas/seguridaddela-informacion-17506228

HURTADO DE BARRERA, Jacqueline. La investigación proyectiva [en línea]. s.l.: Blogspot.com, 2008. [citado el 13-10-16]. Disponible en: http://investigacion holistica.blogspot.com.co/2008/02/la-investigacin-proyectiva.html

ISO27000.ES. Ciclo Deming (2005) - mejora continua [en línea]. Madrid: El autor, s.f. [citado el 16-04-16]. Disponible en: http://www.iso27000.es/sgsi_implantar.html#seccion1

_____. El portal de ISO 27001 en español [en línea]. Madrid: El autor, s.f. [citado el 22-04-16]. Disponible en: http://www.iso27000.es/iso27000.html

_____. Glosario [en línea]. Madrid: El autor, s.f. [citado el 22-04-16]. Disponible en: http://www.iso27000.es/glosario.html

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

IURIS TANTUM. Tipos de conectores lingüístico-argumentativos [en línea]. s.l.: Blogspot, 2011. [citado el 06-04-16]. Disponible en: http://iuristantums.blogspot.com.co/2011/06/tipos-de-conectores-linguistico_20.html

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

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. Decreto número 1317 de 2013 [en línea]. Bogotá: Ministerio de Tecnologías de la Información y las Comunicaciones, 2013. [citado el 15-05-16]. Disponible en: http://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Fortalecimiento de la gestión TI en el estado [en línea]. Bogotá: El autor, s.f. [citado el 30-10-16]. Disponible en: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-6206.html

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Seguridad y privacidad de la información: Elaboración de la política general de seguridad y privacidad de la información [en línea]. Bogotá: El autor, 2016. [citado el 12-10-16]. Disponible en: http://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

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

SECRETARÍA DE PLANIFICACIÓN Y GESTIÓN INSTITUCIONAL. Disposición

3/2013: Apruébase la “Política de Seguridad de la Información Modelo” [en línea]. Argentina: Universidad Nacional de Córdoba, 2013. [citado el 13-10-16]. Disponible en: http://www.unc.edu.ar/gestion/unidades/cici/servicio-de-informacion-tecnica-legal/novedades-en-legislacion/archivos-gladys/disposicion-3-2013-onti

SEGUINFO. Mejora continua de un SGSI según ISO 27001 [en línea]. s.l.: El autor, 2006. [citado el 14-04-16]. Disponible en: https://seguinfo.wordpress.com/2006/11/19/mejora-continua-de-un-sgsi-segun-iso-27001/

SUÁREZ, Lorena. Valoración de amenazas [en línea]. s.l.: Universidad Nacional Abierta y a Distancia, 2013. [citado el 28-05-16]. Disponible en: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/3232_valoracin_de_amenazas.html

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Ciclo PDCA (Eduard Deming) [en línea]. s.l.: UNAD, s.f. [citado el 20-04-16] http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/151_ciclo_pdca__edward_deming.html

_____. Lección 1: Conceptos de vulnerabilidad, riesgo y amenaza [en línea]. s.l.: UNAD, s.f. [citado el 20-04-16]. Disponible en: http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_1_conceptos_de_vulnerabilidad_riesgo_y_amenaza.html

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

_____. Valoración de amenazas [en línea]. s.l.: El autor, s.f. [citado el 05-05-16]. Disponible en: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/3232_valoracin_de_amenazas.html

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

_____. Fundamentos de seguridad informática: vulnerabilidades [en línea]. México: UNAM, s.f. [citado el 30-04-16]. Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/Vulnerabilidades.php

_____. Políticas de Seguridad [en línea]. México: UNAM, s.f. [citado el 06-04-16]. Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/DefinicionPolitica.php

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO. Políticas de seguridad informática de la organización [en línea]. México: UNAM, s.f. [citado el 14-04-16]. Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap4.html

VARGAS, Ana Cecilia y CASTRO MATTEI, Alonso. Sistemas de gestión de seguridad de la información [en línea]. San José Costa Rica: Universidad de Costa Rica, s.f. [citado el 22-04-16]. Disponible en: http://archivo.ucr.ac.cr/docum/ISOEIC27000.pdf

PRESIDENCIA DE LA NACIÓN. (2005). Modelo de política de seguridad de la información para organismos de la administración pública nacional [en línea]. Argentina: Oficina Nacional de Tecnologías de Información, 2005. [citado el 10-07-14]. Disponible en: http://www.sgp.gov.ar/sitio/PSI_Modelo-v1_200507.pdf