UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE ARQUITECTURA E INGENIERÍAS

**Trabajo de Fin de Carrera Titulado:**

# "DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIDAD EDUCATIVA BORJA 3 CAVANIS, BASADO EN LA NORMA ISO/IEC 27002:2013"


**Realizado por:**

Ing. Israel Alejandro Cárdenas Calderón

**Director del Proyecto:**

Ing. Verónica Elizabeth Rodríguez Arboleda, MBA.


**Como requisito para la obtención del título de**

MÁSTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGURIDAD EN REDES Y COMUNICACIÓN

## DECLARACIÓN JURAMENTADA

Yo, ISRAEL ALEJANDRO CÁRDENAS CALDERÓN, con cédula de identidad 1723886212, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

_____

**ISRAEL ALEJANDRO CÁRDENAS CALDERÓN**

**C.I.: 1723886212**

**DECLARATORIA**

**El presente trabajo de investigación titulado:**

"DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIDAD EDUCATIVA BORJA 3 CAVANIS, BASADO EN LA NORMA DE ISO/IEC 27002:2013"

**Realizado por:**

ISRAEL ALEJANDRO CÁRDENAS CALDERÓN

**Como requisito para la obtención del título de:**

MÁSTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGURIDAD EN REDES Y COMUNICACIÓN

**Ha sido dirigido por el profesor**

Ing. Verónica Elizabeth Rodríguez Arboleda, MBA.

**Quien considera que constituye un trabajo original de su autor**

_____

Ing. Verónica Elizabeth Rodríguez Arboleda, MBA.

DIRECTORA

**LOS PROFESORES INFORMANTES:**

**Los profesores informantes:**

Ing. Diego Fernando Riofrio Luzcando, PhD

Ing. Christian David Pazmiño Flores, Msc

**Después de revisar el trabajo presentado, lo han calificado como apto para su defensa oral ante el Tribunal Examinador.**

Ing. Diego Fernando Riofrio Luzcando, PhD

Ing. Christian David Pazmiño Flores, Msc.

Quito, enero del 2020

# DEDICATORIA

**Este tema de titulación lo dedico a:**

Mi divino niño al bendecirme y guiarme en mis estudios, darme la salud y el trabajo para poder culminar una más de mis metas de vida profesional y personal.

Mi esposa Maribel Velastegui, que es mi apoyo, mi compañera de toda la vida, por haberme brindado su ayuda incondicional no solo en los estudios, sino en el transcurso de la vida.

A mis dos hijas Danna y Romina, quienes son los ejes fundamentales de mi vida y el motor de lucha para ser cada día mejor.

A mis padres Carlos y Verónica, por inculcarme valores y principios, por guiarme en mi camino de la educación, por darme la mano cuando necesité y por estar a mi lado en las buenas y en las malas.

A mi hermano David, por estar en los momentos más duros de mi vida personal y profesional, por ser un padre, hermano y amigo en cada momento, su constante apoyo y confianza ha sido la motivación para terminar este trabajo.

# AGRADECIMIENTO

**Agradezco infinitamente a:**

Dios, por darme la sabiduría, el amor y la fuerza para seguir adelante sin importar los obstáculos que se presenten.

Mi familia, por estar ahí y darme su apoyo para ser el mejor.

Mi esposa Maribel, que es mi apoyo incondicional y quien me dio la fuerza para buscar ser mejor cada día.

A mi profesora, Ing. Verónica Rodríguez, al dedicarme su valioso tiempo y permitirme culminar este proyecto de titulación.

A la UNIVERSIDAD INTERNACIONAL SEK, por permitirme crecer intelectual y profesionalmente.

## RESUMEN

El presente proyecto tiene como alcance establecer lineamientos para que el Departamento de Gestión Tecnológica de la Unidad Educativa Borja 3 Cavanis pueda mitigar las vulnerabilidades y amenazas que afectan la integridad, confidencialidad y disponibilidad de su información; ya que maneja datos académicos muy importantes como calificaciones, matrículas, información de alumnos, docentes y autoridades, pese a ello la Institución no cuenta con un sistema de seguridad de la información. Como primer paso, se aplicó la matriz de riesgos basada en la metodología Magerit que permitió valorar las amenazas que existen en la Institución. Posteriormente, se realizó una encuesta al Coordinador del Departamento de Gestión Tecnológica para analizar y verificar como está el manejo de seguridad de los datos. De forma paralela, se revisó las normas ISO/IEC 27002:2013, que son un referente de buenas prácticas para la implementación de sistemas de gestión de la Seguridad de la Información, para todo tipo de organizaciones, adaptándose correctamente al área de tecnologías de la información y comunicación. Con el análisis realizado y los riesgos detectados se escogen los controles de la norma ISO/IEC 27002:2013, que permitió mitigar las amenazas encontradas en la Institución. Para finalizar, se diseñó una Política de Seguridad de la Información para la Unidad Educativa Borja 3 Cavanis, esto permitió al área de Gestión Tecnológica disponer de una guía adecuada para el manejo de los activos de la Institución



**Palabras Claves**: Gestión Tecnológica, Política de Seguridad, Vulnerabilidades, Metodología Magerit, ISO/IEC 27002:2013, Borja 3 Cavanis

## ABSTRACT

The purpose of this degree project is to establish guidelines so that the Technology Management Department of the Borja 3 Cavanis Educational Unit can mitigate vulnerabilities and threats that affect the integrity, confidentiality and availability of your information; since it handles very important academic data such as qualifications, enrollments, information of students, teachers and authorities despite this, the Institution does not have an information security system. As a first step, the risk matrix based on the Magerit methodology was applied, which allowed assessing the threats that exist in the Institution. Subsequently, a survey was conducted to the Coordinator of the Department of Technology Management to analyze and verify how the data security management is. In parallel, the ISO / IEC 27002: 2013 standards were reviewed, which are a benchmark of good practices for the implementation of information security management systems for all types of organizations, adapting correctly to the area of information technology and communication, with the analysis performed and the risks detected, the controls of the ISO / IEC 27002: 2013 standard are chosen, which allowed mitigating the threats found in the Institution, to finalize an Information Security Policy for the Educational Unit Borja 3 Cavanis, this allowed the Technology Management area to have an adequate guide for the management of the assets of the Institution



**Keywords**: Technological Management, Security Policy, Vulnerabilities, Magerit Methodology, ISO / IEC 27002: 2013, Borja 3 Cavanis

## TABLA DE CONTENIDOS

# ÍNDICE DE FIGURAS

# ÍNDICE DE TABLAS

# CAPÍTULO I

# INTRODUCCIÓN

## 1.1. El problema de investigación

### 1.1.1 Planteamiento del problema

El desarrollo constante de la tecnología ha traído múltiples beneficios a la sociedad, pero también problemas relacionados a la protección de datos sensibles y confidenciales tanto de los sujetos como de las organizaciones.

La Unidad Educativa Borja 3 Cavanis, es una entidad de educación conformada por 180 empleados y 1100 estudiantes en distintas secciones, que son: Preparatoria, Básica Elemental, Básica Media, Básica Superior y Bachillerato. Se manejan procesos críticos como: registro de información del personal docente, estudiantes y administrativos, servicios de matrícula, ingreso de notas, registro de asistencias, administración del sistema contable y financiero, portafolio digital del docente, reportes académicos de estudiantes y la base de datos de los respaldos de cada año lectivo.

Los servicios mencionados disponen de datos valiosos y confidenciales, son administrados por un software académico denominado Academium, cuyo aplicativo es manejado por el área de Gestión Tecnológica de la Unidad Educativa.

El departamento de Gestión Tecnología de la Institución educativa se encarga de las siguientes actividades:

- Mantenimiento correctivo y preventivo de los dispositivos informáticos.
- Optimización del rendimiento de los equipos tecnológicos.
- Asignación de equipos tecnológicos a usuarios, creación de sus cuentas.
- Copias de seguridad periódicas.
- Evaluación de necesidades de recursos en los dispositivos ya sean memorias, discos, etc.
- Actualizaciones de software.
- Instalación y configuración de aplicaciones en los servidores.
- Administración de las listas de correo.
- Diseño, implementación y administración de Redes de Comunicaciones.
- Administración de Sistemas Académicos.
- Administración de Bases de Datos.
- Mantenimiento de Aplicaciones.
- Soporte a usuarios y mantenimiento de equipos.
- Soporte de Aplicaciones.
- Apoyo técnico a la Dirección y áreas administrativas.
- Administración de laboratorios informáticos.
- Seguridad de los equipos tecnológicos.

Mediante la observación directa y encuesta (ANEXO 3) realizada al administrador y coordinador del área de Gestión Tecnológica, se identificaron los siguientes inconvenientes:

- La Unidad Educativa Borja 3 Cavanis no dispone de un acuerdo de no divulgación y confidencialidad de la información, que mantenga la protección de los datos.
- No existe la documentación correspondiente de los sistemas informáticos que maneja la organización como son: Manual del administrador y del usuario.

- El departamento de Gestión Tecnológica no cuenta con una normativa de uso y manejo de la información, que detalle los lineamientos y controles para el manejo seguro de los datos.
- Existen usuarios que no bloquean las pantallas de los equipos asignados en la Institución, esto ocasiona que se pueda acceder a la información cuando el responsable esté ausente.
- No existe ningún sistema de seguridad contra intrusos, como por ejemplo un firewall.
- No cuentan con un antivirus en los equipos informáticos.

La Unidad Educativa Borja 3 Cavanis como una organización que brinda servicios de educación, debe tomar acciones para conservar los tres factores importantes de su información: confidencialidad, integridad y disponibilidad; detectando las vulnerabilidades de sus aplicaciones, corrigiendo e implementando medidas para controlar los riesgos de seguridad, lo que se puede obtener con buenas prácticas y procedimientos claros alineados a estándares internacionales.

### 1.1.2 Formulación del problema

La Unidad Educativa Borja 3 Cavanis presenta inconvenientes en la Seguridad de la Información lo que afecta de una manera crítica a sus activos informáticos.

## 1.2 Objetivos

### 1.2.1 Objetivo general

Diseñar una política de seguridad para la Unidad Educativa Borja 3 Cavanis basada en la norma ISO 27002:2013, que garantice la integridad, disponibilidad y confidencialidad de los datos.

### 1.2.2 Objetivos específicos

Analizar las vulnerabilidades de los datos de la Unidad Educativa Borja 3 Cavanis, mediante una matriz de riesgos basada en la metodología Magerit, que permita que las amenazas sean identificadas.

Seleccionar las normas ISO/IEC 27002:2013 mediante un análisis de su aplicación que conlleve a la mitigación de las vulnerabilidades encontradas.

Estructurar la política de seguridad, en base a los controles seleccionados de la norma ISO/IEC 27002:2013 que garantice la seguridad de la información de la Unidad Educativa Borja 3 Cavanis.

### 1.2.3 Justificación

Después de haber observado los problemas que enfrenta la Unidad Educativa Borja 3 Cavanis, se puede decir que es necesario aprovechar al máximo los recursos tecnológicos disponibles para administración y manejo de los datos, sin embargo, la tecnología trae consigo una serie de vulnerabilidades que pueden comprometer la información que maneja, como por ejemplo: los virus, el espionaje, intrusiones y demás delitos informáticos: por tal motivo, es fundamental implementar el uso de normas y políticas de seguridad que ayuden a mitigar las amenazas a los que está expuesta.

Por lo tanto, en este tema de titulación se utiliza la familia ISO 27000, con la cual se diseñará la política de seguridad utilizando la norma ISO 27002:2013, que permite cumplir los objetivos propuestos en la institución.

Para lo cual se realiza un análisis de riesgos de los activos, utilizando la metodología que se adapte de mejor manera sus controles como se describen en la tabla 1.

**Tabla 1**: *Comparación de Metodologías*

| Metodologías | Magerit | Mehari | Octave |
|---|---|---|---|
| **Ventajas** | • Es metódica por lo que se hace fácil su comprensión<br>• Tipifican, se buscan sus dependencias, se valoran en cuanto a: disponibilidad, confidencialidad, autenticidad, integridad y trazabilidad.<br>• Comprende los procesos de análisis y gestión de riesgos.<br>• Usa un modelo de análisis de Riesgos cualitativo y cuantitativo<br>• Soporta herramientas comerciales EAR y No comerciales PILAR, así como las normas ISO/IEC 27001:2005 | • Tiene la capacidad de evaluar y simular los niveles de riesgos derivados de medidas adicionales.<br>• Soporta herramientas comerciales y no comerciales como RISICARE DE BUC S.A.<br>• Es compatible con el estándar ISO/IEC 27001:2005<br>• ISO/IEC 27005:2008<br>• Usa un modelo de análisis de riesgos cualitativo y cuantitativo.<br>• Es una metodología para la gestión de riesgos | • Cualquier metodología que aplica los criterios (principio, atributos y resultados) es considerado compatible con la metodología octave.<br>• Involucra todo el personal de la entidad.<br>• Es la más completa ya que involucra como elemento de su modelo de análisis: procesos, activos y dependencias, recursos, vulnerabilidades, amenazas y salvaguardas |
| **Desventajas** | • No toma en cuenta el principio de no repudio de la información como objetivo de seguridad<br>• No toma en cuenta un análisis de vulnerabilidades.<br>• La recomendación de los controles no la incluye dentro del análisis de riesgos sino en la gestión y evaluación<br>• Comprende como elementos del modelo de análisis solo: activos y dependencias.<br>• La estimación del impacto se realiza en el proceso de gestión y evaluación de riesgos | • Solo tomo en cuenta los principios de confidencialidad, integridad y disponibilidad de la información como objetivos de seguridad dejando a un lado el no repudio.<br>• La estimación del impacto se realiza en el proceso de gestión y evaluación de riesgos<br>• La recomendación de los controles no la incluye dentro del análisis de riesgos sino en la gestión de riesgos. | • Aplicable solo en PYME pequeñas y medianas empresas<br>• No tiene compatibilidad con estándares internacionales |

**Fuente*:*** Magerit Versión 3, Consejo Superior de Administración Electrónica (2012)

Al realizar una revisión de las metodologías de los sistemas de gestión, se llega a la conclusión de utilizar la metodología MAGERIT por las siguientes razones:

- Para implementar esta metodología contiene pasos específicos a realizar, obteniendo como resultado un estado del riesgo junto con un plan de seguridad.
- Esta metodología puede ser utilizada en cualquier tipo de institución ya sea privada o pública.
- Magerit es gratuita y puede ser utilizada en todas las organizaciones.
- Magerit colabora en la certificación de ISO 27001

Como indica las razones antes mencionadas la metodología MAGERIT, es la opción más efectiva y completa para el análisis de riesgos en la Unidad Educativa Borja 3 Cavanis, porque permite la valoración de los activos en base a su integridad, disponibilidad y confidencialidad, como también la identificación de amenazas y vulnerabilidades que pueden impactar los activos, facilitando la selección de medidas de seguridad que garanticen el éxito de los procesos, para la selección y elaboración de las medidas de seguridad para el área de Gestión Tecnológica.

### 1.2.4 Estado del arte

Se ha realizado una búsqueda en artículos científicos y tesis sobre información relacionada con el tema de investigación y se presenta algunos estudios relevantes:

Cevallos (2019) diseñó una política de seguridad de la información para el área de TI del Instituto Tecnológico Superior Central Técnico, implementando las políticas de seguridad de la información en el área de TIC mediante el uso de las normas internacionales ISO/IEC 27002: 2013.

Contero (2019) en su proyecto de titulación de maestría en la Universidad Internacional SEK realizó el diseño de una política de seguridad de la información,

usando la norma ISO 27002:2013 para el sistema de botones de seguridad del Ministerio del Interior aplicando la metodología de Magerit, para poder identificar las vulnerabilidades y los riesgos de los activos de la organización.

Contreras (2017) utilizó la Metodología de Magerit para analizar e identificar los riesgos existentes en la Gobernación de Boyacá, lo cual permite documentar el inventario de activos. A través de esta herramienta fue posible evidenciar de forma clara los activos que se encuentran en riesgo, con el fin de poder ser tratados de forma inmediata, mediante un Sistema de Gestión de Seguridad de la Información e implementación de Políticas y normativas institucionales.

Cárdenas (2018) diseñó una política de seguridad de la información basada en la norma ISO 27799 para el control de accesos a las aplicaciones médicas de la red en el Hospital Axxis. Además, realizó un análisis de riesgos completo con entrevistas al personal del Hospital, con esta revisión exhaustiva seleccionó controles según la norma ISO 27799.

Horvath y Jakub (2009) indican que en empresas o sociedades pequeñas se debe aplicar de manera obligatoria los requisitos de seguridad que cumplan con la norma ISO 27002, ya que debe ser una prioridad mantener la seguridad de la institución con la ayuda de un sistema informático.

Magerit Versión 3 analiza e identifica los riesgos existentes en las organizaciones, mediante esta metodología es posible evidenciar de forma clara los activos que se encuentran en riesgo, a fin de poder ser tratados de forma inmediata a través del Sistema de Gestión de Seguridad de la Información e Implementación de Políticas y Normas Institucionales (Consejo Superior de Administración Electrónica, 2012).

Rodríguez y Peralta (2013) señalan que la metodología de Magerit es la opción más efectiva y completa para el análisis, de igual manera facilita la identificación de amenazas y vulnerabilidades, brindando las medidas de seguridad para el sistema académico.

# CAPÍTULO II

# MARCO TEÓRICO

## 2.1 Seguridad informática

Según Tarazona (2007), en la actualidad las empresas privadas o públicas al igual que las personas dependen de la tecnología de la información como una herramienta fundamental para lograr los objetivos de los negocios o para su uso diario, al mismo tiempo las organizaciones o los usuarios que utilizan los sistemas informáticos deben enfrentarse con una gran cantidad de amenazas y vulnerabilidades.

Tarazona (2007) indica que la seguridad de la información va más allá de la seguridad de los datos en los equipos tecnológicos, ésta debe estar enfocada en proteger la propiedad intelectual y la información importante de organizaciones públicas, privadas y personales.

Los riesgos que afectan a la Seguridad de la Información son principalmente debido a amenazas y vulnerabilidades tanto de hardware como de software, estos vacíos de seguridad permiten que posibles atacantes puedan tomar ventajas de las debilidades de los sistemas académicos en las instituciones educativas.

### 2.1.1 Estándares y normas para asegurar la información

Burgos y Campos (2008) señalan que existen tres requisitos para el buen uso de la seguridad de la información como son:

- Confidencialidad.
- Integridad.

- Disponibilidad.

**Confidencialidad**

La confidencialidad indica que no se pone a disposición ni se revela la información de la organización.

**Integridad**

Este método asegura que los datos puedan ser manipulados solo por el personal autorizado, lo cual permite proteger la información del equipo y posibles modificaciones no autorizadas.

**Disponibilidad**

Garantizar la utilización de los datos y los sistemas informáticos en la organización para el uso de los usuarios.

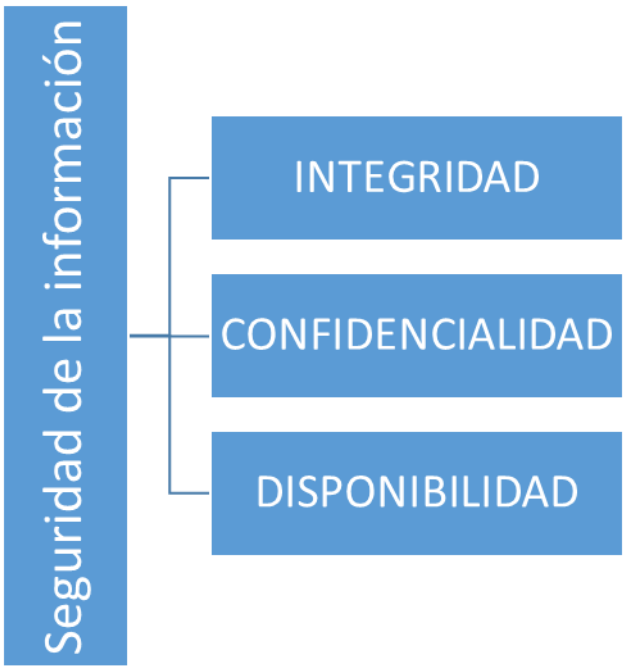


***Figura 1:*** Elementos de la seguridad

**Fuente**: Elaboración propia

## 2.2 Riesgos de los sistemas informáticos

Solarte y Benavides (2015) indican que los riesgos informáticos se pueden presentar por no tener las normas apropiadas para proteger los datos de la institución, estos se clasifican en:

- Integridad de riesgos.
- Relación de riesgo.
- Acceso de riesgo.
- Utilidad de riesgo.
- Infraestructura de riesgos.

### 2.2.1 Riesgo

Según Aguilera (2010) el riesgo consiste en la posibilidad de que una amenaza, aproveche una vulnerabilidad existente en un sistema informático. Ante un riesgo específico, una empresa puede manejar tres opciones que son: Asumirlo sin hacer nada, aplicar medidas para mitigar o eliminarlo.

### 2.2.2 Ataque

Chávez (2015) indica que se produce un ataque deliberado o accidental contra el sistema informático cuando se ha materializado una amenaza.

La clasificación de los ataques es la siguiente:

- Activos: si alteran, dañan, eliminan o aumentan información, o bloquean los canales de comunicación
- Pasivos: Solamente ingresan sin autorización a los datos almacenados en el sistema, son los más difíciles de descubrir.

### 2.2.3 Amenazas de seguridad

Según Huacanés (2016) una amenaza de seguridad puede afectar a instituciones públicas y privadas en su totalidad, ocasionando el daño a un sistema de información o a su entorno. Se pueden tener varios tipos de amenazas como las que se detallan a continuación:

- Interrupción.
- Intercepción.
- Alteración.
- Agregación.

**Interrupción**

Es cuando un sistema suspende su operatividad de forma abrupta y no planificada, Aguilera (2010) indica que este tipo de amenazas perjudican directamente al hardware y software del equipo, ocasionando daño crítico al sistema operativo y aplicaciones que se ejecutan diariamente.

**Agregación**

Es cuando se agregan registros a las bases de datos alterando la información y el desempeño de la misma (Segovia, 2009).

**Alteración**

Es la adulteración no autorizada de los registros de un sistema de activos, es una amenaza a las credenciales de acceso, lo que genera dificultad a la hora de reparar esos registros (Aguilera, 2010).

**Intercepción**

Según Mieres (2009) se lleva a cabo por personal no autorizado, que consigue tener acceso al flujo de datos; ya sea por un medio lógico o una red local, permitiendo que el intruso genere copias de la información de la organización para ocupar dicha documentación con distintos fines.

### 2.2.4 Vulnerabilidades

Según Mieres (2009), es una debilidad la cual puede ser explotada por una amenaza ya sea por medio del software o hardware, así como en los usuarios que forman parte del área de informática con el objetivo de causar daño sobre un activo o una organización.

**Principales amenazas informáticas**

Con el avance tecnológico de la computación y servicios de Internet, se explican en la siguiente tabla los tipos de ataques más comunes utilizados en la actualidad.

**Tabla 2**: *Principales amenazas informáticas*

| AMENAZAS | SIGNIFICADO |
|---|---|
| Malware | Son programas diseñados por ciberdelincuentes cuyo objetivo es alterar el funcionamiento de cualquier sistema informático. Tienen la capacidad de corromper los archivos del equipo. |
| Spyware | Es un aplicativo que tiene la capacidad de adquirir información de un dispositivo electrónico y transmitirla poniendo en peligro la seguridad del ordenador. |
| Ransomware | Tanto para ordenadores como para teléfonos móviles, es una de las amenazas con mayor crecimiento en la actualidad. |
| Phishing | Llega mediante correo electrónico. de modo que, se consiguen los datos confidenciales de forma fraudulenta |
| Troyanos | Es un programa malicioso el cual se ejecuta de manera automática en los dispositivos tecnológicos, dando el control remoto del equipo al atacante. |
| Gusanos | Son aplicaciones que se pueden presentar en distintas formas en los dispositivos tecnológicos, la afectación de estas amenazas es crear gran número de copias de sí mismo. |
| Backdoor | Algunos programadores maliciosos dejan una puerta trasera para así poder evitar los sistemas de seguridad de acceso, para poder acceder al sistema con total comodidad. |

**Fuente***:* Seguridad en los sistemas informáticos, Oceano IT, (2014)

**Amenazas lógicas**

La amenaza lógica afecta a los datos almacenados en los dispositivos.

**Amenazas estructuradas**

Como indica Tarazona (2007), en este grupo de amenazas, cabe destacar los denominados *crackers*, que tienen como principal motivación investigar y conocer las redes de las organizaciones y sus vulnerabilidades para crear e implementar códigos hacking, con la finalidad de penetrar en los sistemas tecnológicos ocasionando daños o pérdidas de información de la entidad.

**Amenazas no estructuradas**

Tarazona (2007) señala que consiste en individuos sin experiencia, que por medio de Internet consiguen herramientas que facilitan su participación como *hacker*. Algunos de quienes ejecutan estas actividades tienen como única motivación el causar daño, pero la mayoría lo considera con un desafío intelectual, a este tipo de usuarios se los conoce como *script kiddies*.

## 2.3 Seguridad de los sistemas informáticos

Aguilera (2010)**,** menciona que las amenazas, vulnerabilidades y todas las debilidades que componen los sistemas informáticos pueden comprometer la integridad, confidencialidad y disponibilidad de la información.

## 2.4 Seguridad de la información en una organización

Según Fisher (1988), una empresa debe saber que la información en un activo primordial en el proceso del negocio, por lo cual le corresponde estructurar medidas que apoyen y garanticen los datos. Sin embargo, muchas de las empresas se enfocan

únicamente en la seguridad física, dejando de lado otros aspectos que están ligados directamente al manejo y gestión de la documentación, lo cual se denomina Seguridad de la Información.

Como indica Aguilera (2010), se debe tener en cuenta que la aplicación de políticas de seguridad tiene como propósito garantizar que los riesgos sean minimizados y gestionados por la Institución de una forma sistemática, eficiente y adaptada a los cambios que se originen en los entornos y las tecnologías.

## 2.5 Esquema gubernamental de Seguridad de la Información

Establece un grupo de directrices prioritarias para la Gestión de la Seguridad de la Información e inicia una mejora continua en empresas privadas y en las instituciones de la Administración Pública. El EGSI no reemplaza la norma ISO/IEC 27002 sino que marca como prioridad la implementación de algunas directrices.

El EGSI también detalla que, de acuerdo a las necesidades de las organizaciones, se podrán especificar políticas de seguridad propias o relacionadas, así como su misión y competencia.

## 2.6 Normas ISO/IEC 27000

El Ministerio de Educación, Cultura y Deportes de España a través de Aula Mentor (2016) establece que las normas deben basarse en estándares internacionales para aplicar políticas de seguridad de la información, desarrollado según la familia de normas ISO/IEC 27000; el enfoque de buenas prácticas podrá sustentarse en la norma ISO/IEC 27002.

La Comisión Electrotécnica Internacional (IEC), se encarga de los estándares y guías de seguridad relacionadas con los sistemas de gestión, la cual permite ser aplicadas a

cualquier tipo de organización internacional o mundial, su propósito es facilitar el comercio, y apoyar la transferencia de las tecnologías (Aula Mentor, 2016).

La familia de normas ISO/IEC 27000 tiene como finalidad proporcionar un marco de referencia para la gestión de la seguridad, estas normas o políticas contienen las mejores prácticas recomendadas en el entorno de la Seguridad de la Información.

**Tabla 3**. *Familia Normas ISO 27000*

| Norma | Descripción |
|---|---|
| ISO / IEC 27000 | Normas estándar para el uso del SGSI para todas las la familia |
| ISO / IEC 27001 | Esta norma es la más importante debido a que se enfoca en la gestión de riesgos y ofrece a los procesos una mejora continua. |
| ISO/IEC 27002 | Se la conoce como ISO 17799:2005 en julio del 2005 su nombre oficial es asignado el 1 de julio del 2007 como ISO/IEC 27002:2005. |
| ISO/IEC 27003 | El sistema SGSI. es el soporte de la norma ISO/IEC 27001. En la actualidad no se encuentra certificada. |
| ISO/IEC 27004 | Es la que recomienda cuándo y cómo realizar procesos de seguridad de la información |
| ISO/IEC 27005 | Proporciona lineamientos y recomendaciones para técnicas de evaluación de riesgos en la seguridad de la información. |
| ISO/IEC 27006 | La norma ISO 27006 específica la información necesaria para la certificación de un sistema SGSI. |
| ISO/IEC 27007 | Esta norma permite realizar las respectivas auditorias al sistema SGSI de la organización. |
| ISO/IEC 27799:2008 | La norma ISO/IEC 27002 permite aplicar la seguridad de la información en la industria de la salud. |

***Fuente**:* Familia norma ISO, Ministerio de Educación, Cultura y Deporte, Aula Mentor (2016).

### 2.6.1 La norma ISO 27001

La norma ISO 27001 permite controlar y mantener en buen funcionamiento un Sistema de Gestión de Seguridad de la Información permitiendo colocar controles o normas a la medida de la institución (Aula Mentor, 2016).

El objetivo es la mejora continua y se adopta el modelo Plan o ciclo Demming para todos los procesos de la institución.


***Figura* 2**. Modelo (PDCA o ciclo Demming)

**Fuente:** Ministerio de Educación, Cultura y Deporte. Aula Mentor (2016)

Las fases de estos modelos son:

**Planificación**

Se basa en establecer procedimientos que beneficien la Seguridad de la Información de la institución, con el fin de obtener resultados de acuerdo a las normas de la organización. El proceso se detalla a continuación:

- Identificar o que se va a mejorar.
- Recopilar datos del proceso que se quiere mejorar.

- Analizar los datos recogidos.
- Constituir objetivos de mejora.
- Especificar los resultados obtenidos.
- Conseguir los objetivos, fijando los procesos adecuados.

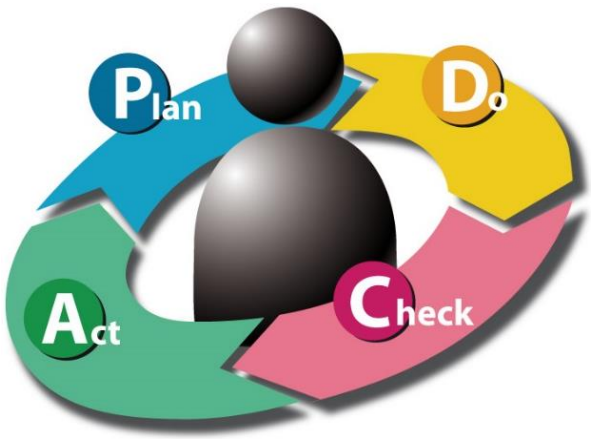


***Figura 3***. Planificación (Plan)

**Fuente:** Ministerio de Educación, Cultura y Deporte, Aula Mentor (2016).

**Ejecución**

Implementar y administrar el SGSI de acuerdo a sus políticas y procedimientos. En la medida de lo posible debería realizar un entorno de prueba para poder verificar su proceso de ejecución y resultados antes de aplicarlo en el sistema real.


***Figura 4.*** Ejecución (Do)

**Fuente:** Ministerio de Educación, Cultura y Deporte, Aula Mentor (2016)

**Seguimiento**

Medir y verificar las prestaciones de los procesos del SGSI. Comprobar que las reglas adoptadas han generado efecto, para ello se debe recopilar los datos para monitorear el comportamiento del sistema de gestión.

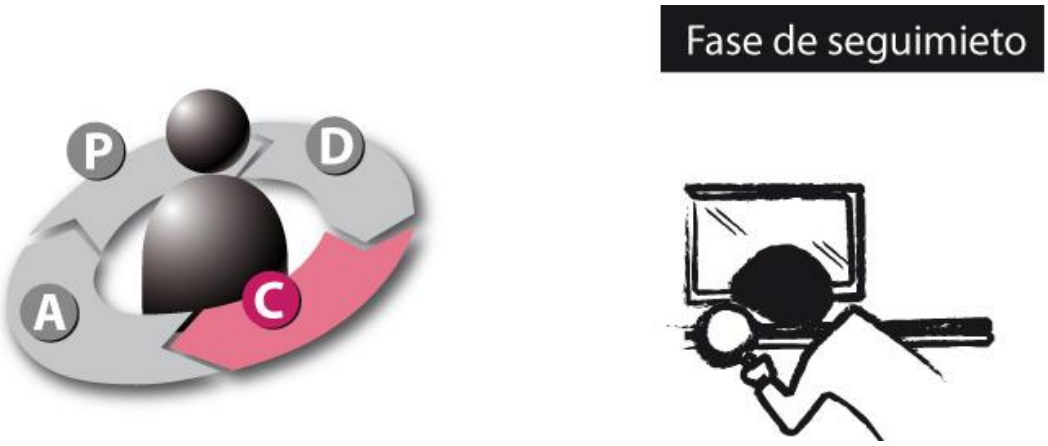


***Figura 5***. Seguimiento (Check)

**Fuente:** Ministerio de Educación, Cultura y Deporte, Aula Mentor (2016)

**Mejora**

Las acciones pueden ser preventivas y correctivas ejecutando revisiones internas para mejorar el objetivo del SGSI. En el caso de que exista un mal funcionamiento, se repetirá nuevamente el ciclo, si el funcionamiento fue exitoso, se da paso a la instalación de las modificaciones del sistema de manera definitiva.

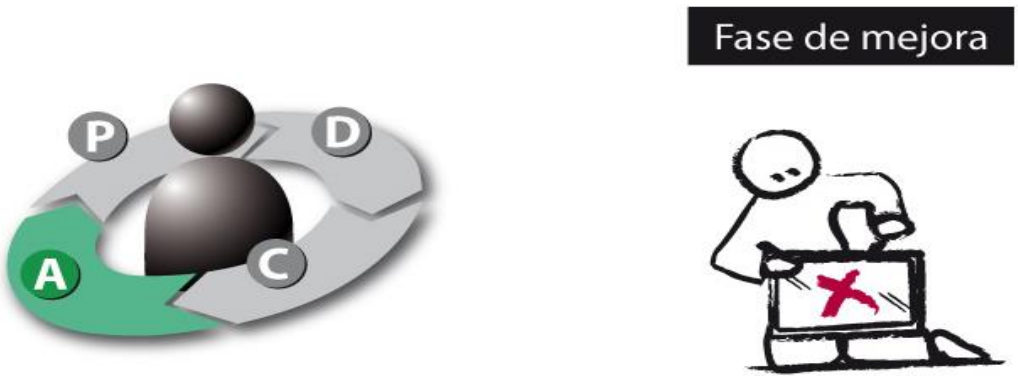


***Figura 6***. Mejora (Act)

**Fuente:** Ministerio de Educación, Cultura y Deporte, Aula Mentor (2016)

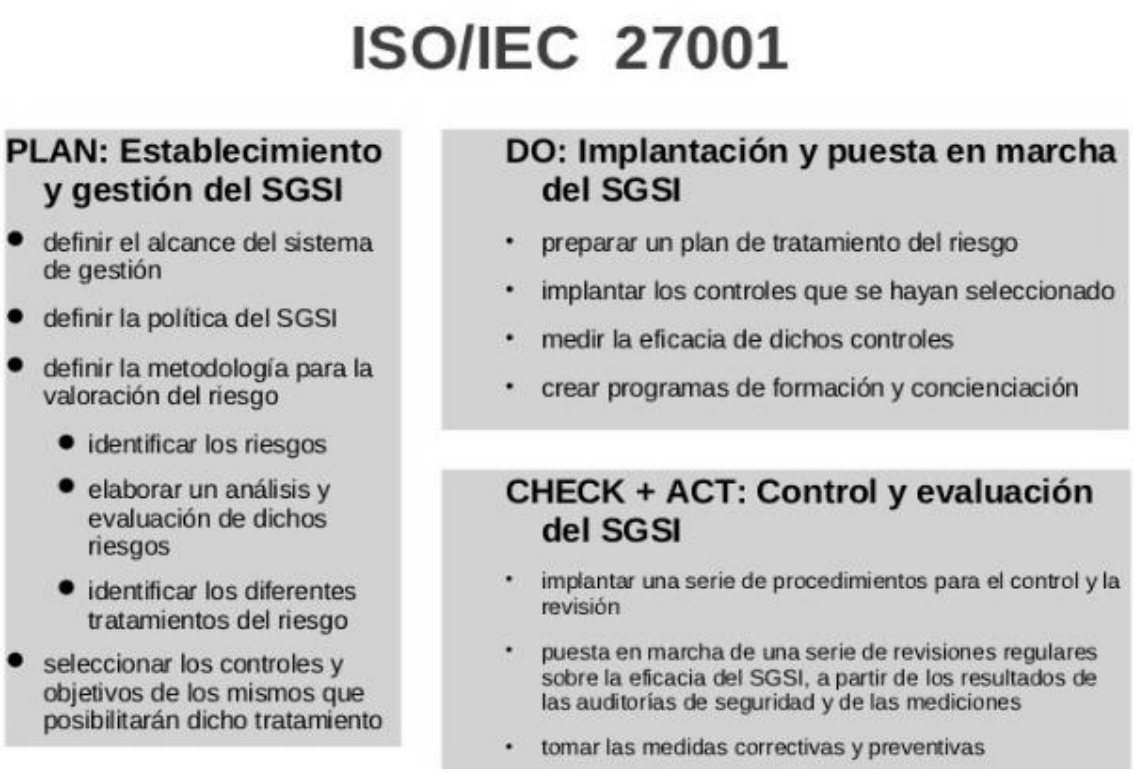


***Figura 7***. Mejora (Act)

**Fuente:** Ministerio de Educación, Cultura y Deporte, Aula Mentor (2016)

Según Segovia (2009), la norma ISO 27001:2013, especifica 10 puntos, los cuales se muestran a continuación:

**1.** Objeto y campo de aplicación: Describe la finalidad de la norma.

**2.** Referencias normativas: Estándar en el que otorgan definiciones.

**3.** Término y definiciones: Términos de la norma ISO/IEC 27000.

**4.** Contexto de la empresa: Define los requisitos para comprender cuestiones internas y externas del SGSI de cara a especificar el alcance.

**5.** Liderazgo: Se define como el establecimiento de contenido y roles de la política de alto nivel sobre Seguridad de la Información.

**6.** Planificación: Valoración y evaluación de riesgos. Adicionalmente, la organización debe identificar los objetivos de la información.

**7.** Soporte: Se debe asignar para la implementación, mantenimiento y mejora del SGSI.

**8.** Operación: Se debe planificar la operación, así como la valoración de los riesgos y su tratamiento.

**9.** Planificar, implementar y controlar: Apreciación de los riesgos y el tratamiento sobre los mismos.

**10.** Evaluación de desempeño: Monitoreo y evaluación del SGSI, auditorías dentro de la organización.

**11.** Mejora: Acciones correctivas y mejora continua.

### 2.6.2 Norma ISO 27002

Según Ladino, Villa y López (2010) esta norma es muy relevante dentro de las empresas públicas y privadas, ya que toma como base todas las amenazas a las que se enfrentan las organizaciones en su día a día, y a partir de allí tiene como objetivo principal establecer, implantar y mejorar la Seguridad de la Información de la empresa.

La norma ISO 27002 establece un catálogo de buenas prácticas que determina la importancia de disponer de una información actualizada, que es la clave para un mejor desempeño de las actividades de la organización, sin embargo, es todavía mucho más importante mantener los datos seguros para evitar pérdidas. Al fin y al cabo, la documentación que dispone la organización, es el activo más valioso que puede marcar el futuro de la Institución.

Segovia (2009) indica que la norma ISO 27002 se implementó en 14 capítulos que describen las áreas que se debe considerar para la seguridad de los datos.

**Control de acceso**

Buendía (2013) señala que se debe controlar quien accede a los datos de un sistema informático, ello implica conocer a los usuarios que ingresan con mayor y con menor

frecuencia al sistema. Además, es necesario establecer controles como registro de usuarios, gestión de los privilegios de acceso, etc.

**Criptografía**

Como indica Contreras (2017), cuando se dispone de documentación importante para la organización se debe implementar técnicas criptográficas para garantizar la integridad de la información.

**Seguridad física y del entorno**

La seguridad no es sólo a nivel tecnológico sino también físico, proteger la información de los equipos e impresoras; ya que personal externo puede manipular y poner en riesgo los datos de la organización (Contreras, 2017).

**Seguridad de las operaciones**

Manejar copias de seguridad, control de software, gestión de amenazas, etc.

**Relación de proveedores**

Se deben establecer medidas de seguridad y pudiendo ser muy recomendable e incluso necesaria la evaluación periódica.

**Gestión de incidentes de seguridad de la información**

Es necesario estar preparado para cualquier tipo de incidente, con el fin de dar una respuesta rápida y eficiente, lo que además permite prevenir problemas a futuro.

Aspectos de seguridad de la información para la gestión de la continuidad de negocio

Sufrir una pérdida de datos relevantes y no poder recuperarla de alguna forma, puede generar peligro para la organización.

**Cumplimiento**

Aplicación de la política que se encuentra relacionada con este campo y con la organización contribuyendo a mejorar la gestión de la información.

## 2.7 Definición e implantación de las políticas de seguridad

Aguilera (2010) indica que la estrategia de Seguridad de la Información puede manejar la siguiente jerarquía:

Plan de seguridad: Son las acciones futuras y los medios que se deben utilizar para ejecutar las mismas.

Procedimiento de seguridad: son pasos que deben seguirse para ejecutar tareas determinadas, los procedimientos de seguridad pueden ser como tareas y operaciones específicas y éstas pueden generar registros y evidencias.


***Figura* 8**. Jerarquía en los conceptos de Seguridad de la Información

**Fuente:** Seguridad de la Información, Aguilera López, (2010)

### 2.7.1 Definir la política

Al plantear una política de seguridad en una organización, surgen varias interrogantes como:

- ¿Quiénes son los responsables de desarrollar la política?
- ¿Qué debe abarcar la política?
- ¿Qué debe contener la política?
- ¿Cómo hacer cumplir la política?

Para ello se ocupan las siguientes etapas:

**Planeación de las políticas**

Mantener el apoyo de las directivas de la organización, conocer el giro de negocio de la empresa, identificar la problemática a través de un análisis de riesgos y definir qué se va a proteger.

**Iniciar su desarrollo**

Designar a una persona como responsable del proceso de la implementación de la norma o política y de dar el seguimiento a las áreas involucradas.

**Redacción de la política**

Hacer partícipes a los conocedores de los procesos de la empresa para saber los aspectos críticos de los sistemas tecnológicos. Se contemplan los siguientes aspectos:

- Enfocar la política al problema de la empresa.
- El documento debe tener una estructura bien definida.
- Los enunciados deben ser claros y precisos.
- Exponer de manera explícita la aplicación.

- Establecer obligaciones para los usuarios.
- Definir claramente las sanciones.
- El documento debe tener flexibilidad para realizar actualizaciones.

**Aprobación y difusión**

La política debe ser revisada y aprobada por las áreas involucradas de la organización y a su vez por el cuerpo directivo, finalmente debe ser socializada a todos los trabajadores.

## 2.8 Metodología para el análisis de riesgos (Metodología Magerit)

Magerit Versión 3, en su capítulo 1, indica que es una metodología, que implementa un análisis de riesgo en un marco de trabajo enfocado a las tecnologías de la información y sus entornos (Consejo Superior de Administración Electrónica, 2012).

Con la metodología Magerit se ejecutará un análisis ordenado de los activos de la organización, las amenazas sobre los activos, estimación del impacto y riesgo; este análisis puede ser resumido en la matriz de riesgos. A través de las normas ISO/IEC 27002:2013 se podrán identificar los riesgos encontrados.

En España, el Consejo Superior de Administración Electrónica, describe el proceso de análisis de riesgos a través de la metodología Magerit.

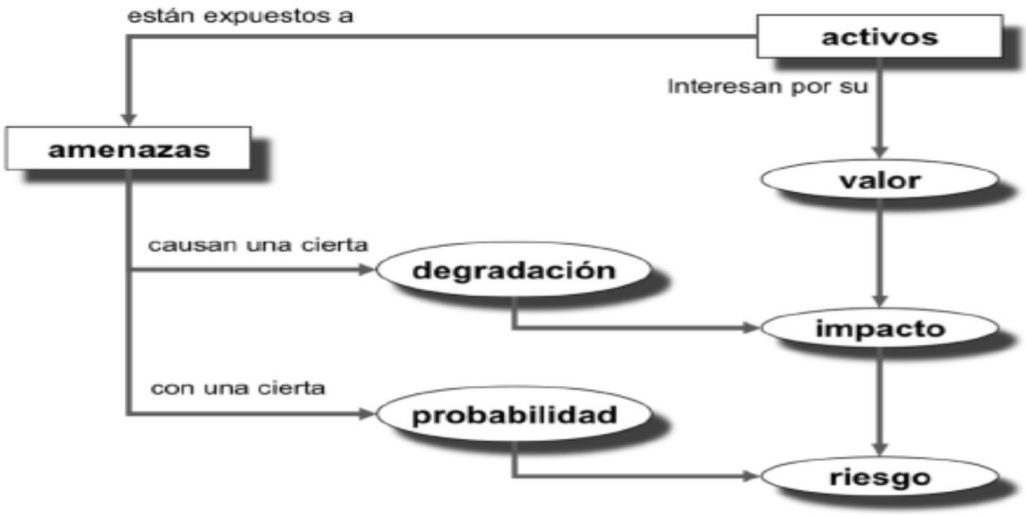


***Figura 9***. Análisis del riesgo a través de Magerit

**Fuente:** Magerit Versión 3, Consejo Superior de Administración Electrónica (2012)

### 2.8.1 Determinar los activos de la organización

El primer paso se basa en determinar los datos y equipos de la organización, para este análisis se establece un catálogo de activos relevantes, los cuales se clasificarán dentro de cada categoría:

- Datos: Información importante para la organización.
- Servicios: actividades que se ejercen en la institución.
- Software – aplicaciones informáticas: aplicaciones en donde se manejan los datos de la empresa.
- Hardware- equipos informáticos: equipos físicos que maneja el usuario de la organización.
- Las instalaciones: donde se encuentran los equipos de comunicación y el personal a cargo de los procesos.
- Recursos humanos: personas que facilitan el cumplimiento de los procesos en la organización.

Posteriormente se realiza una valoración de activos, basado en el impacto que tendría en relación a su disponibilidad, confidencialidad e integridad.

A continuación, se indica la tabla para la valoración de los activos, se deberá establecer una valoración individual para la disponibilidad, integridad y confidencialidad

**Tabla 4**. *Análisis del riesgo a través de Magerit*

| DESCRIPCIÓN | VALORACIÓN | AFECTACIÓN |
|---|---|---|
| Extremadamente grave | 5 | Extremo |
| Muy grave | 4 | Muy alto |
| Grave | 3 | Alto |
| Importante | 2 | Medio |
| Menor | 1 | Bajo |
| Irrelevante | 0 | Despreciable |

**Fuente***:* Magerit Versión 3, Consejo Superior de Administración Electrónica (2012)

### 2.8.2 Determinar las amenazas a las cuales están expuestas los activos

Según Magerit Versión 3, en el capítulo 1, menciona que la metodología identifica las típicas vulnerabilidades, que causan daños a los sistemas de información y a sus entornos, esta metodología establece un listado de amenazas de acuerdo a su origen (Consejo Superior de Administración Electrónica, 2012), las cuales se presentan a continuación:

**De origen natural**

Magerit Versión 3, en el capítulo 1, indica que son las amenazas de la naturaleza, las mismas que no son predecibles y no pueden ser controladas por sistemas informáticos ni por el humano. Por ejemplo: terremotos y otros eventos, ante cualquier situación de este tipo, el sistema de información es una víctima pasiva, estas amenazas no pueden evitarse, pero se deben tener en cuenta (Consejo Superior de Administración Electrónica, 2012).

**Del entorno**

Magerit Versión 3, en el capítulo 1 establece son desastres industriales, por ejemplo: la contaminación de químicos, entre otros. Los sistemas de información también son víctimas pasivas ante estas amenazas, pero no por eso hay que permanecer indefenso ante estos eventos (Consejo Superior de Administración Electrónica, 2012).

**Defectos de las aplicaciones**

Los sistemas informáticos no son perfectos, ya que son creados por humanos y pueden existir errores como: diseño, implementación y operación, estas pueden ser denominadas vulnerabilidades.

**Causadas por las personas de forma accidental**

Cevallos (2019) indica que estos eventos se dan cuando las personas que tienen acceso a las plataformas tecnológicas o al entorno de la organización, ocasionen problemas, típica y generalmente por error.

**Causadas por las personas de forma deliberada**

Cevallos (2019) señala que estos eventos se generan cuando el personal con acceso al sistema causa problemas intencionados, con ánimo de beneficiarse indebidamente, ocasionando daños y perjuicios a la organización.

### 2.8.3 Estimar el impacto

Magerit Versión 3, en el capítulo 3 define el impacto se conoce como daño sobre el activo (Consejo Superior de Administración Electrónica, 2012).

**Tabla 5**. *Valoración del impacto*

| IMPACTO | | DEGRADACIÓN | | |
|---|---|---|---|---|
| | | B | M | A |
| VALOR ACTIVO | MA | M | A | MA |
| | A | B | M | A |
| | M | MB | B | M |
| | B | MB | MB | B |
| | MB | MB | MB | MB |

**Fuente***:* Magerit Versión 3, Consejo Superior de Administración Electrónica (2012)

## Degradación: Públicas

Magerit Versión 3, en el capítulo 3, establece que las amenazas cuando no son intencionales pueden ser perjudiciales para un activo, pero cuando son intencionales el atacante puede generar mucho daño a la empresa (Consejo Superior de Administración Electrónica, 2012).

**Tabla 6.** *Degradación del valor*

| | | | |
|---|---|---|---|
| MA | Fácil | Casi seguro | Muy alta |
| A | Medio | Muy alto | Alta |
| M | Difícil | Posible | Media |
| B | Muy difícil | Poco probable | Baja |
| Mb | Extremadamente difícil | Muy raro | Muy baja |

**Fuente***:* Magerit Versión 3, Consejo Superior de Administración Electrónica (2012)

**Probabilidad**

Cuan probable es que la amenaza sea materializada por medio de escalas nominales.

**Tabla 7**. *Probabilidad de ocurrencia*

| | | | |
|---|---|---|---|
| MB | Muy poco frecuente | Siglos | 0,01 |
| B | Poco frecuente | Cada varios años | 0,1 |
| M | Normal | Una vez al año | 1 |
| A | Frecuente | Mensualmente | 10 |
| MA | Muy frecuente | A diario | 100 |

**Fuente*:*** Magerit Versión 3, Consejo Superior de Administración Electrónica (2012)

### 2.8.4 Determinación del riesgo potencial

Magerit Versión 3, en el capítulo 3, determina el riesgo, conforme al daño que se refleja en el activo de la institución (Consejo Superior de Administración Electrónica, 2012)

• Zona 1 – Riesgos de impacto muy alto

• Zona 2 – Cubre situaciones de impacto bajo

• Zona 3 – Riesgos de impacto menor

• Zona 4 – Riesgos de impacto moderado

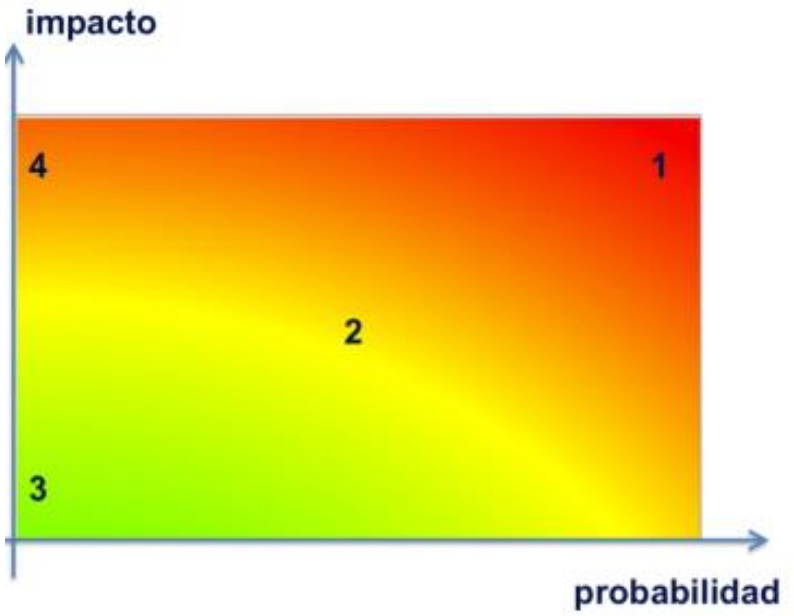


***Figura 100*.** El riesgo en función del impacto y la probabilidad

**Fuente:** Magerit Versión 3, Consejo Superior de Administración Electrónica, (2012)

### 2.8.5 Determinar las salvaguardas

Magerit Versión 3, en el capítulo 3, define que las salvaguardas conocidas también como contramedidas son los mecanismos que se utilizan para reducir el riesgo en los activos (Consejo Superior de Administración Electrónica, 2012)

- Tipo de activos se protege de una forma específica.
- Se requiere protección en las dimensiones de seguridad de los datos.
- Se debe proteger de las amenazas.

La asignación de los controles dependerá de las prioridades de la organización, para este efecto se seleccionará las Norma INEN ISO/IEC 27002:2013.

# CAPÍTULO III

# ANÁLISIS Y SITUACION ACTUAL

## 3.1 SITUACION ACTUAL

### 3.1.1 ANTECEDENTES

Pedro Pablo Borja fue el fundador de la escuela elemental Borja, un tiempo después, es adquirida por Padre Luis Tapia, el cual mantenía ideas futuristas, típico de un espíritu emprendedor en la obra educativa (Borja 3 Cavanis, 2017).

Con este emprendedor nació la Unidad Educativa Borja 3 Cavanis, su inauguración fue el 14 de septiembre de 1957, con 81 estudiantes en el área de inicia el primer año escolar, por la insistencia de los padres de familia, se fundó la Secundaria con nombre de Academia Militar Borja 3 Cavanis.

La Unidad Educativa Borja 3 Cavanis en sección matutina y Academia Militar Borja 3 Cavanis en sección vespertina, mantiene 60 años de servicio en el ámbito de la educación, sirviendo a la juventud y niñez, orientados en la religión cristiana, haciendo hincapié en la seriedad académica y en las aplicaciones prácticas, motivando la valoración del ser humano. (Borja 3 Cavanis, 2017)

En la Institución educativa Borja 3 Cavanis forma estudiantes que sean responsables de sí mismos, seres humanos capaces de trabajar por su comunidad. (Borja 3 Cavanis, 2017)

**Misión:**

> La Unidad Educativa Particular Borja N° 3 Cavanis es una institución católica basada en el Carisma de Marcos y Antonio Cavanis de ser más padres que maestros, formando niños y jóvenes con conciencia ambiental capaces de desenvolverse en el presente, con proyección hacia el futuro, mediante el fortalecimiento de la razón y el corazón, obteniendo una formación de calidad y excelencia educativa. (Borja 3 Cavanis, 2017, 1)

**Visión**:

> En el año 2021 seremos líderes e innovadores en proyectos productivos, posicionados entre los mejores colegios de la capital, por su excelencia educativa y sus resultados académicos, dotando al estudiante de conocimientos y habilidades imprescindibles para su formación integral, con altos índices de ingreso a la educación superior, preparados para el cuidado y protección del medio ambiente y actitud para enfrentar los retos de la sociedad. (Borja 3 Cavanis, 2017)

## 3.2 Área de Gestión Tecnológica de la Unidad Educativa Borja 3 Cavanis

El departamento de Gestión Tecnológica de la Unidad Educativa Borja 3 Cavanis no dispone de normas de seguridad de la información, por este motivo se plantea el trabajo de titulación basado en la norma ISO/IEC 27002:2013.

Previamente, se realizó un análisis de las vulnerabilidades de los sistemas y los riesgos a los que la organización está expuesta para lo cual se utilizó la metodología Magerit.

Es una de las metodologías con mayor aceptación a nivel empresarial, ya que es un soporte para auditorías, acreditaciones o certificaciones que puedan ser alcanzadas por las organizaciones.

## 3.3 Aplicación de la metodología Magerit para el análisis y valoración del riesgo

### 3.3.1 Determinar los activos relevantes para la organización

Con la autorización (ANEXO 1) del Msc. Fausto Loor, Rector de la Unidad Educativa Borja 3 Cavanis, se recolectaron datos. Para esto se utilizaron técnicas de visualización en las actividades que desempeña el departamento de Gestión Tecnológica, se realizó una encuesta de seguridad (ANEXO 3) al Msc. Miguel García, coordinador del departamento de Gestión Tecnológica de la Unidad Educativa Borja 3 Cavanis, del mismo modo se realizaron las inspecciones físicas de cada uno de los departamentos.

Las actividades realizadas por el departamento de Gestión Tecnológica son:

- Administración de la plataforma del sistema académico ACADEMIUM, que actualmente se encuentra en producción y los usuarios manejan los módulos de: registro de asistencia, administración de paralelos, ingreso de notas y cambios de paralelos.
- Mantenimiento preventivo y correctivo de equipos tecnológicos.
- Administración de los laboratorios informáticos.
- Administración del correo corporativo de la Institución.
- Capacitación a los usuarios de los sistemas informáticos.

De acuerdo a las funciones que desempeña el departamento de Gestión Tecnológica, con la ayuda del catálogo de elementos de Magerit y el responsable del departamento de Gestión Tecnológica, se identificaron los activos más destacados y se los clasificó de la siguiente manera:

**[D] Datos**

Los datos le permiten al área de Gestión Tecnológica prestar correctamente los servicios y usar ese conocimiento para el correcto funcionamiento de la institución.

- Base de datos del sistema académico ACADEMIUM.
- Código del sistema académico de la institución.

**[SW] Software – Aplicaciones informáticas**

Este punto hace referencia a la aplicación que desarrolló el área de Gestión Tecnológica para la Unidad Educativa Borja 3 Cavanis que es:

- Desarrollo: sistema de monitoreo de la red.

**[HW] Equipamiento informático (hardware)**

En este punto constan los medios físicos y materiales que dispone el área de Gestión Tecnológica, entre los equipos que posee el departamento se cuenta con:

- Computadoras de escritorio.
- Routers.
- Switchs.
- Routers inalámbricos.
- Computadoras Portátiles.

**[L] Instalaciones**

El lugar donde se dispone los sistemas de información y comunicación, es el área de Gestión Tecnológica de la Unidad Educativa Borja 3 Cavanis.

- Departamento de Gestión Tecnológica.

**[AUX] Equipamiento auxiliar**

El área de Gestión Tecnológica cuenta con el siguiente equipamiento auxiliar:

- Cableado estructurado.

**[PERSONAL] Personal**

Son las personas que facilitan el correcto uso y funcionamiento de los sistemas de información.

- Administración del sistema académico y financiero.
- Configuración y administración de las bases de datos.

Según Magerit Versión 3, en el capítulo 3, los activos se basan en la integridad, confidencialidad y disponibilidad, esto permite comprender el valor del activo para el área de Gestión Tecnológica. (Consejo Superior de Administración Electrónica, 2012)

Menciona que contemplan los siguientes objetivos:

**Directos:**

- Información de la aparición del riesgo y de la necesidad de gestionarlos,
- Ofrecer un método sistemático para analizar los riesgos.

**Indirectos:**

Mantener preparada la institución para procesos de evaluaciones, certificados o acreditación, según corresponda en cada caso el análisis de riesgos es una aproximación para determinar el riesgo tomando en cuenta los siguientes puntos:

- Determinar los activos relevantes para la Organización.
- Determinar a qué amenazas están expuestos aquellos activos.
- Estimar el impacto, definido como el daño sobre el activo.
- Estimar el riesgo, definido como el impacto de la amenaza.

Para la valoración de activos se utilizó una escala cuantitativa, donde los criterios van desde un nivel 5 hasta 0.

**Tabla 8**. *Criterios de valoración de activos*

| Descripción | Valor |
|---|---|
| Depreciable | 0 |
| Bajo | 1 |
| Medio | 2 |
| Alto | 3 |
| Muy alto | 4 |
| Extremo | 5 |

**Fuente*:*** Elaborado por el autor de la investigación, basado en la metodología Magerit Versión 3 (2012).

En la tabla 8 se indica la valoración de los activos bajo los criterios de Confidencialidad, Integridad y Disponibilidad.

**Tabla 9**. *Valoración de activos*

| Activo | Disponibilidad | Confidencialidad | Integridad | Promedio | Valoración |
|---|---|---|---|---|---|
| [D] Datos / Información | | | | | |
| Base de datos: Sistema académico (ACADEMIUM). | 5 | 5 | 5 | 5 | Extremo |
| [SW] Software – Aplicaciones informáticas | | | | | |
| Sistema de monitoreo de la red | 5 | 5 | 5 | 5 | Extremo |
| [HW] Equipamiento informático | | | | | |
| Computadoras de escritorio | 4 | 4 | 4 | 4 | Muy alto |
| Portátiles | 4 | 4 | 4 | 4 | Muy alto |
| Router inalámbrico | 3 | 3 | 3 | 3 | Alto |
| Routers | 2 | 2 | 2 | 2 | Medio |
| Switchs | 2 | 2 | 2 | 2 | Medio |
| [L] Instalaciones | | | | | |
| Oficina de TICS | 3 | 3 | 3 | 3 | Alto |
| [AUX] Equipamiento auxiliar | | | | | |
| Cableado | 2 | 2 | 2 | 2 | Medio |
| [PERSONAL] Personal | | | | | |
| Administrador de base de datos. | 5 | 5 | 5 | 5 | Extremo |
| Administración de sistema académico y financiero | 5 | 5 | 5 | 5 | Extremo |

**Fuente*:*** Elaborado por el autor de la investigación, basado en la encuesta realizada al coordinador de Gestión Tecnológica

Con esta valoración y clasificación se identifican los activos de importancia para la Unidad Educativa Borja 3 Cavanis, que deben mantener una mayor protección de la información.

### 3.3.2 Determinar las vulnerabilidades a las que están expuestos los activos

Fisher (1988) indica que las amenazas pueden generarse de manera accidental o meditada. Que puede ser una aplicación o un servicio.

Al identificar las amenazas en los sistemas informáticos se utiliza la metodología Magerit, la cual se encarga de organizar las amenazas para cada uno de los activos de la siguiente forma:

**Tabla 10.** *Clasificación de amenazas*

| AMENAZA | DESCRIPCIÓN |
|---|---|
| [N] Desastres Naturales | Causada directa o indirecta por accidentes naturales (terremotos, inundaciones entre otros). |
| [I] De origen industrial | Pueden darse de forma accidental o meditada<br>Sucesos derivados de la actividad humana de tipo industrial (contaminación, fallos eléctricos, entre otros). |
| [E] Errores y fallos no intencionados | Fallos causados por las personas con acceso al sistema de información. |
| [A] Ataques intencionados | Fallos deliberados causados por las personas con acceso al sistema de información. |

**Fuente:** Elaborado por el autor de la investigación, basado en la metodología Magerit Versión 3 (2012).

**[D] Datos / Información**

**Tabla 11**. *Datos / Información*

| Nro. | Código | Amenaza | Dimensión de seguridad afectada |
|---|---|---|---|
| Activo: Base de datos: Sistema académico (ACADEMIUM). | | | |
| 1 | [E.1] | Errores de los usuarios. | Confidencialidad<br>Disponibilidad<br>Integridad |
| 2 | [E.2] | Errores del administrador. | Confidencialidad<br>Disponibilidad<br>Integridad |
| 3 | [E.15] | Alteración accidental de la información. | Integridad |
| 4 | [E.18] | Destrucción de la información | Disponibilidad<br>Integridad |
| 5 | [E.19] | Fugas de información. | Confidencialidad |
| 6 | [A.5] | Suplantación de identidad del usuario | Confidencialidad<br>Integridad |
| 7 | [A.6] | Abuso de privilegios de acceso | Integridad<br>Confidencialidad<br>Disponibilidad |
| 8 | [A.11] | Acceso no autorizado | Confidencialidad<br>Disponibilidad<br>Integridad |
| 9 | [A.15] | Modificación deliberada de la información | Disponibilidad<br>Integridad |
| 10 | [A.18] | Destrucción de información | Disponibilidad |
| 11 | [A.19] | Divulgación de información | Confidencialidad |

**Fuente*:*** Elaborado por el autor de la investigación, basado en la metodología Magerit Versión 3 (2012)

En la tabla 11, se aprecia las amenazas presentes en el activo Datos/Información, que son:

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

Estas amenazas afectan al desempeño de la organización ya que son los datos de uso exclusivo de la institución.

**[SW] Software – Aplicaciones informáticas.**

**Tabla 22.** *Software – Aplicaciones informáticas*

| Nro. | Código | Amenaza | Dimensión de seguridad afectada |
|---|---|---|---|
| Activo: De desarrollo propio: Sistema de monitoreo de la red | | | |
| 1 | [I.5] | Daño de origen lógico o físico. | Disponibilidad |
| 2 | [E.1] | Error de uso. | Integridad<br>Confidencialidad<br>Disponibilidad |
| 3 | [E.20] | Vulnerabilidades de los sistemas (software). | Integridad<br>Confidencialidad<br>Disponibilidad |
| 4 | [A.6] | Ingresos no autorizados sin privilegios de acceso | Integridad<br>Disponibilidad<br>Confidencialidad |
| 5 | [A.19] | Clonación ilegal de software de la institución. | Integridad |

**Fuente***:* Elaborado por el autor de la investigación, basado en la metodología Magerit Versión 3 (2012)

En la tabla 12, se aprecia que las amenazas presentes en el activo Software – Aplicaciones informáticas son:

- De tipo Ataques intencionados [A]
- Errores y fallos no intencionados [E]
- De origen industrial [I]

Este tipo de amenazas son las que más afectan a los activos y que para reducirlas es fundamental generar un control que garantice la integridad, confidencialidad y disponibilidad del mismo.

**[HW] Equipamiento informático**

**Tabla 33**. *Equipamiento informático*

| Nro. | Código | Amenaza | Dimensión de seguridad afectada |
|---|---|---|---|
| Activo: Dispositivos tecnológicos de escritorio y portátiles | | | |
| 1 | [I.6] | Suspensión de energía eléctrica | Disponibilidad |
| 2 | [E.2] | Fallas administrativas de los dispositivos. | Integridad<br>Confidencialidad<br>Disponibilidad |
| 3 | [E.23] | Falla de coordinación en los mantenimientos. | Disponibilidad |
| 4 | [A.6] | Falla de permisos para acceder al dispositivo. | Integridad<br>Confidencialidad<br>Disponibilidad |
| 5 | [A.11] | Permisos no autorizados a los sistemas informáticos | Integridad<br>Confidencialidad |
| Activo: Routers inalámbricos y router | | | |
| 1 | [I.6] | Corte de energía eléctrica | Disponibilidad |
| 2 | [E.2] | Fallas administrativas de los dispositivos. | Integridad<br>Confidencialidad<br>Disponibilidad |
| 3 | [E.23] | Falla de coordinación en los mantenimientos. | Disponibilidad |
| 4 | [A.6] | Falla de permisos para acceder al dispositivo. | Integridad<br>Confidencialidad<br>Disponibilidad |
| 5 | [A.11] | Permisos no autorizados a los sistemas informáticos | Integridad<br>Confidencialidad |
| Activo: Switchs | | | |
| 1 | [I.6] | Corte de energía eléctrica | Disponibilidad |
| 2 | [E.2] | Fallas administrativas de los dispositivos. | Integridad<br>Confidencialidad<br>Disponibilidad |
| 3 | [E.23] | Falla de coordinación en los mantenimientos. | Disponibilidad |
| 4 | [A.11] | Permisos no autorizados a los sistemas informáticos | Integridad<br>Confidencialidad |

**Fuente:** Elaborado por el autor de la investigación, basado en la metodología Magerit Versión 3, (2012).

En la tabla 13, se evidencia que las amenazas presentes en el activo equipamiento informático son de tipo:

- Ataques intencionados [A]

- Errores y fallos no intencionados [E]

- De Origen industrial [I]

Afectando así su disponibilidad, integridad y confidencialidad en los activos para mitigar el impacto de estas amenazas se debe mantener políticas de seguridad en la organización.

**[L] Instalaciones.**

**Tabla 44**. *Instalaciones*

| Nro. | Código | Amenaza | Dimensión de seguridad afectada |
|---|---|---|---|
| Activo: Oficina de TICS | | | |
| 1 | [A.11] | Permisos no autorizados a los sistemas informáticos | Integridad<br>Confidencialidad |
| 2 | [A.26] | Destrucción de propiedad | Disponibilidad |

**Fuente***:* Elaborado por el autor de la investigación, basado en la metodología Magerit Versión 3 (2012).

En la tabla 14, se constata que la Integridad, Disponibilidad y Confidencialidad del activo es afectado por amenazas de tipo:

- Ataques intencionados [A]

Es necesario crear un protocolo e implementar normas de seguridad para lograr mitigar los ataques intencionados en el activo.

**[AUX] Equipamiento auxiliar**

**Tabla 55**. *Equipamiento auxiliar*

| Nro. | Código | Amenaza | Dimensión de seguridad afectada |
|---|---|---|---|
| Activo: Cableado | | | |
| 1 | [N.1] | Fuego | Disponibilidad |
| 2 | [N.3] | Contaminación | Disponibilidad |
| 3 | [N.6] | Fenómeno climático | Disponibilidad |
| 4 | [N.7] | Fenómeno sísmico | Disponibilidad |
| 5 | [N.10] | Inundación | Disponibilidad |
| 6 | [A.26] | Destrucción de propiedad | Disponibilidad |

**Fuente*:*** Elaborado por el autor de la investigación, basado en la metodología Magerit Versión 3 (2012).

En la tabla 15, se aprecia que las amenazas presentes en el activo Equipamiento auxiliar son de tipo:

- Desastres Naturales [N]
- Ataques intencionados [A]

En el equipamiento auxiliar se be comprometida la disponibilidad en el activo.

**[PERSONAL] Personal**

**Tabla 66**. *Personal*

| Nro. | Código | Amenaza | Dimensión de seguridad afectada |
|---|---|---|---|
| Activo: Administración de sistema académico y financiero | | | |
| 1 | [E.7] | Deficiencias en la organización | Disponibilidad |
| 2 | [E.19] | Fugas de información | Confidencialidad |
| 1 | [I.6] | Corte de energía eléctrica | Disponibilidad |
| 2 | [E.2] | Fallas administrativas de los dispositivos. | Integridad<br>Confidencialidad<br>Disponibilidad |

| Nro. | Código | Amenaza | Dimensión de seguridad afectada |
|---|---|---|---|
| 3 | [E.23] | Falla de coordinación en los mantenimientos. | Disponibilidad |
| 4 | [A.6] | Falla de permisos para acceder al dispositivo. | Integridad<br>Confidencialidad<br>Disponibilidad |
| 5 | [A.11] | Permisos no autorizados a los sistemas informáticos | Integridad<br>Confidencialidad |
| Activo: Administrador de base de datos | | | |
| 1 | [E.19] | Fugas de información | Confidencialidad |
| 2 | [A.11] | Permisos no autorizados a los sistemas informáticos | Integridad<br>Confidencialidad |
| 3 | [E.23] | Falla de coordinación en los mantenimientos. | Disponibilidad |

**Fuente*:*** Elaborado por el autor de la investigación, basado en la metodología Magerit Versión 3 (2012).

En la tabla 16, se determina que las amenazas presentes en el activo Personal son de tipo:

- Ataques intencionados [A]
- Errores y fallos no intencionados [E]
- De Origen industrial [I]

Estas tres amenazas ponen en riesgo los tres factores principales que son Disponibilidad, Confidencialidad e Integridad, para lo cual es necesario crear un protocolo de seguridad para el manejo de la información.

**Vulnerabilidades**

Magerit Versión 3, en el capítulo 2, indica que se denomina vulnerabilidad a toda debilidad que puede ser aprovechada por una amenaza a los activos que facilitan el éxito

de una amenaza potencial que puede afectar a la organización poniendo en riesgo los datos o información (Consejo Superior de Administración Electrónica, 2012).

Con el área de Gestión Tecnológica, se describen las vulnerabilidades o debilidades encontradas que amenazan a los activos.

**Tabla 77**. *Amenazas y vulnerabilidades de los activos*

| Activo | Amenaza | Vulnerabilidad |
|---|---|---|
| **Base de datos: Sistema académico (ACADEMIUM)** | Fallas de los usuarios | No hay manuales de uso o guías para los administradores. |
| | Errores del administrador. | Módulos de las bases de datos innecesarios que se encuentran habilitados. |
| | Alteración accidental de la información. | Disponer de configuraciones establecidas por defecto |
| | Sustracción de información | No mantener las normas de confidencialidad de la información. |
| | Sustracción de información | Módulos de las bases de datos innecesarios que se encuentran habilitados. |
| | Robo de identidad del usuario | Credenciales con parámetros débiles |
| | Falla de permisos para acceder al dispositivo. | Falta de seguridad en los dispositivos autorizados. |
| | Permisos no autorizados a los sistemas informáticos | Credenciales con parámetros débiles |
| **De desarrollo propio: Sistema de monitoreo de la red.** | Avería de origen lógico o físico | No se ejecuta las suficientes pruebas para los sistemas. |
| | Fallas de los usuarios | No hay manuales de uso o guías para los administradores. |
| | Falla de permisos para acceder al dispositivo. | Falta de seguridad en los dispositivos autorizados. |

| | | |
|---|---|---|
| | Copia de software ilegal | No existe un monitoreo y control de las aplicaciones propias de la institución. |
| **Computadoras de escritorio y portátiles** | Corte de energía eléctrica | No hay equipos ups que eviten la perdida de energía eléctrica. |
| | Fallas administrativas de los dispositivos. | Periféricos USB de equipos tecnológicos habilitados |
| | Fallas administrativas de los dispositivos. | Equipos informáticos sin sus respectivas configuraciones de usuarios estándar o administradores. |
| | Falla de coordinación en los mantenimientos. | No hay un procedimiento claro para realizar los mantenimientos preventivos o correctivos en (Hardware y Software). |
| | Falla de permisos para acceder al dispositivo. | Falta de seguridad en los dispositivos autorizados. |
| | Permisos no autorizados a los sistemas informáticos | Credenciales con parámetros débiles |
| **Routers inalámbricos** | Corte de energía eléctrica | No hay equipos ups que eviten la perdida de energía eléctrica. |
| | Fallas administrativas de los dispositivos. | Falta de seguridades en las redes inalámbricas, bloqueos de páginas inadecuadas. |
| | Falla de coordinación en los mantenimientos. | Mantenimiento de software de los equipos, liberación de IP´s. |
| | Falla de permisos para acceder al dispositivo. | Falta de seguridad en los dispositivos autorizados. |
| | Permisos no autorizados a los sistemas informáticos | Credenciales con parámetros débiles |

| | | |
|---|---|---|
| **Switchs** | Corte del suministro eléctrico | No hay equipos ups que eviten la perdida de energía eléctrica. |
| | Fallas administrativas de los dispositivos. | Falta de configuración y seguridad en los equipos, mantener inactivos los puertos que no se ocupen. |
| | Falla de coordinación en los mantenimientos. | Mantenimiento de software de los equipos. |
| | Permisos no autorizados a los sistemas informáticos | Credenciales con parámetros débiles |
| **Área de Gestión Tecnológica** | Permisos no autorizados a los sistemas informáticos | Credenciales con parámetros débiles |
| | Daño a la propiedad | No existen controles de seguridad adecuados en la institución. |
| | Fenómeno climático | Falta de seguridad en ductos de cableado |
| | Fenómeno sísmico | Falta de seguridad en ductos de cableado |
| | Inundación | Falta de seguridad en ductos de cableado |
| | Daño a la propiedad | Falta de seguridad en ductos de cableado |
| **Administración de sistema académico y financiero** | Deficiencias en la organización | Falta de información y capacitación a los usuarios de la organización. |
| | Sustracción de información | No mantener las normas de confidencialidad de la información. |
| | Corte de suministro eléctrica | No hay equipos ups que eviten la perdida de energía eléctrica. |

| | | |
|---|---|---|
| | Fallas administrativas de los dispositivos. | Falta monitoreo en los sistemas académicos y financieros. |
| | Falla de coordinación en los mantenimientos. | No disponer de licencias en los equipos que manejan en la organización y no se encuentran actualizados los equipos y el antivirus. |
| | Falla de permisos para acceder al sistema. | No hay procesos establecidos para desarrollar las funciones de la organización. |
| | Permisos no autorizados a los sistemas informáticos | Falta de controles de bloqueo a usuarios que estén dentro de la red. |
| **Administrador de base de datos** | Sustracción de información | Falta de controles en los procesos o políticas de seguridad para los datos de la organización. |
| | Permisos no autorizados a los sistemas informáticos | Credenciales con parámetros débiles |
| | Falla de coordinación en los mantenimientos. | No existe monitoreo en las bases de datos de la organización. |

**Fuente***:* Elaborado por el autor de la investigación, basado en la encuesta con el coordinador del área de Gestión Tecnológica y la metodología Magerit Versión 3 (2012).

### 3.3.3 Estimación del impacto

Al haber detectado que amenazas son perjudiciales para los activos, hay que verificar que influencia presenta en el activo, que pueden ser los siguientes:

Degradación: En la organización el activo se verá perjudicado.

**Tabla 88.** *Estimación del impacto - Degradación*

| | | | | |
|---|---|---|---|---|
| 100% | MA | Muy alta | Casi seguro | Fácil |
| 90% | A | Alta | Muy alto | Medio |
| 50% | M | Media | Posible | Difícil |
| 10% | B | Baja | Poco probable | Muy difícil |
| 1% | MB | Muy baja | Muy raro | Extremadamente difícil |

***Fuente**:* Elaborado por el autor de la investigación, basado en la metodología Magerit Versión 3 (2012).

Probabilidad: cuán improbable o probable seria que se materialice la amenaza del activo.

**Tabla 99**. *Estimar el impacto - Probabilidad*

| | | | |
|---|---|---|---|
| MA | 5 | Muy frecuente | A diario |
| A | 4 | Frecuente | Mensualmente |
| M | 3 | Normal | Una vez al año |
| B | 2 | Poco frecuente | Cada varios años |
| MB | 1 | Muy poco frecuente | Siglos |

***Fuente:*** Elaborado por el autor de la investigación, basado en la metodología Magerit Versión 3 (2012).

**Tabla 2010**. *Mapa de calor de estimación del impacto*

| Impacto | | Degradación | | | | |
|---|---|---|---|---|---|---|
| | | 1 | 10% | 50% | 90% | 100% |
| | | (MB) | (B) | (M) | (A) | (MA) |
| Probabilidad | MA | A | MA | MA | MA | MA |
| | A | M | A | A | MA | MA |
| | M | B | M | M | A | A |
| | B | MB | B | B | M | M |
| | MB | MB | MB | MB | B | B |

***Fuente:*** Elaborado por el autor de la investigación, basado en la metodología Magerit Versión 3 (2012).

**Tabla 111**. *Estimación del impacto*

| Activo | Código | Amenaza | Vulnerabilidad | Degradación | Probabilidad | Impacto |
|---|---|---|---|---|---|---|
| Base de datos: Sistema académico (ACADEMIUM) | [E.1] | Fallas de los usuarios | No hay manuales de uso o guías para los administradores. | M | MB | M |
| | [E.2] | Errores del administrador. | Módulos de las bases de datos innecesarios que se encuentran habilitados. | A | MB | B |
| | [E.15] | Alteración accidental de la información. | Disponer de configuraciones establecidas por defecto | MA | M | A |
| | [E.18] | Sustracción de información | No mantener las normas de confidencialidad de la información. | MA | MB | B |
| | [E.19] | Sustracción de información | Módulos de las bases de datos innecesarios que se encuentran habilitados. | A | M | A |
| | [A.5] | Robo de identidad del usuario | Credenciales con parámetros débiles | A | MB | B |
| | [A.6] | Falla de permisos para acceder al dispositivo. | Falta de seguridad en los dispositivos autorizados. | A | B | M |
| | [A.11] | Permisos no autorizados a los sistemas informáticos | Credenciales con parámetros débiles | A | MB | B |
| De desarrollo propio: Sistema | [I.5] | Avería de origen lógico o físico | No se ejecuta las suficientes pruebas para los sistemas. | A | A | MA |

| Activo | Código | Amenaza | Vulnerabilidad | Degradación | Probabilidad | Impacto |
|---|---|---|---|---|---|---|
| de monitoreo de la red. | [E.1] | Fallas de los usuarios | No hay manuales de uso o guías para los administradores. | M | M | M |
| | [A.6] | Falla de permisos para acceder al dispositivo. | Falta de seguridad en los dispositivos autorizados. | M | M | M |
| | [A.19] | Copia de software ilegal | No existe un monitoreo y control de las aplicaciones propias de la institución. | B | B | B |
| Computadoras de escritorio y portátiles | [I.6] | Corte de energía eléctrica | No hay equipos ups que eviten la perdida de energía eléctrica. | B | B | B |
| | [E.2] | Fallas administrativas de los dispositivos. | Periféricos USB de equipos tecnológicos habilitados | B | B | B |
| | [E.2] | Fallas administrativas de los dispositivos. | Equipos informáticos sin sus respectivas configuraciones de usuarios estándar o administradores. | MA | MA | MA |
| | [E.23] | Falla de coordinación en los mantenimientos. | No hay un procedimiento claro para realizar los mantenimientos preventivos o correctivos en (Hardware y Software). | M | M | M |
| | [A.6] | Falla de permisos para acceder al dispositivo. | Falta de seguridad en los dispositivos autorizados. | M | M | M |
| | [A.11] | Permisos no autorizados a los sistemas informáticos | Credenciales con parámetros débiles | M | M | M |

| Activo | Código | Amenaza | Vulnerabilidad | Degradación | Probabilidad | Impacto |
|---|---|---|---|---|---|---|
| Routers inalámbricos y routers | [I.6] | Corte de energía eléctrica | No hay equipos ups que eviten la perdida de energía eléctrica. | M | M | M |
| | [E.2] | Fallas administrativas de los dispositivos. | Falta de seguridades en las redes inalámbricas, bloqueos de páginas inadecuadas. | MA | MA | MA |
| | [E.23] | Falla de coordinación en los mantenimientos. | Mantenimiento de software de los equipos, liberación de IP´s. | M | M | M |
| | [A.6] | Falla de permisos para acceder al dispositivo. | Falta de seguridad en los dispositivos autorizados. | M | M | M |
| | [A.11] | Permisos no autorizados a los sistemas informáticos | Credenciales con parámetros débiles | M | M | M |
| Switch | [I.6] | Corte del suministro eléctrico | No hay equipos ups que eviten la perdida de energía eléctrica. | M | M | M |
| | [E.2] | Fallas administrativas de los dispositivos. | Falta de configuración y seguridad en los equipos, mantener inactivos los puertos que no se ocupen. | MA | MA | MA |
| | [E.23] | Falla de coordinación en los mantenimientos. | Mantenimiento de software de los equipos. | B | B | B |
| | [A.11] | Permisos no autorizados a los sistemas informáticos | Credenciales con parámetros débiles | M | M | M |

| Activo | Código | Amenaza | Vulnerabilidad | Degradación | Probabilidad | Impacto |
|---|---|---|---|---|---|---|
| Área de Gestión Tecnológica | [A.11] | Permisos no autorizados a los sistemas informáticos | Credenciales con parámetros débiles | M | M | M |
| | [A.26] | Daño a la propiedad | No existen controles de seguridad adecuados en la institución. | M | MA | MA |
| Cableado | [N.3] | Fenómeno climático | Falta de seguridad en ductos de cableado | M | M | M |
| | [N.6] | Fenómeno sísmico | Falta de seguridad en ductos de cableado | M | B | B |
| | [N.7] | Inundación | Falta de seguridad en ductos de cableado | M | B | B |
| | [N.10] | Daño a la propiedad | Falta de seguridad en ductos de cableado | M | B | B |
| Administración de sistema académico y financiero | [E.7] | Deficiencias en la organización | Falta de información y capacitación a los usuarios de la organización. | M | B | B |
| | [E.19] | Sustracción de información | No mantener las normas de confidencialidad de la información. | MA | MA | MA |
| | [I.6] | Corte de suministro eléctrica | No hay equipos ups que eviten la perdida de energía eléctrica. | M | M | M |
| | [E.2] | Fallas administrativas de los dispositivos. | Falta monitoreo en los sistemas académicos y financieros. | M | B | B |

| Activo | Código | Amenaza | Vulnerabilidad | Degradación | Probabilidad | Impacto |
|---|---|---|---|---|---|---|
| | [E.23] | Falla de coordinación en los mantenimientos. | No disponer de licencias en los equipos que manejan en la organización y no se encuentran actualizados los equipos y el antivirus. | MA | MA | MA |
| | [A.6] | Falla de permisos para acceder al sistema. | No hay procesos establecidos para desarrollar las funciones de la organización. | M | MA | MA |
| | [A.11] | Permisos no autorizados a los sistemas informáticos | Falta de controles de bloqueo a usuarios que estén dentro de la red. | M | M | M |
| Administrador de base de datos | [E.19] | Sustracción de información | Falta de controles en los procesos o políticas de seguridad para los datos de la organización. | M | MA | MA |
| | [A.11] | Permisos no autorizados a los sistemas informáticos | Credenciales con parámetros débiles | M | B | B |
| | [E.23] | Falla de coordinación en los mantenimientos. | No existe monitoreo en las bases de datos de la organización. | M | M | M |

**Fuente***:* Elaborado por el autor de la investigación, basado en la encuesta con el coordinador del área de Gestión Tecnológica, aplicando la metodología Magerit Versión 3 (2012).

En la tabla 21, se expone las amenazas de los activos con mayor impacto en la organización que son:

- Base de datos: Sistema académico (ACADEMIUM).
- De desarrollo propio: Sistema de monitoreo de la red.
- Oficina de TICS y computadoras de escritorio y portátiles.
- Routers inalámbricos y router.
- Switchs.
- Oficina de TIC.
- Cableado.
- Administración de sistema académico y financiero.
- Administrador de base de datos.

### 3.3.4 Estimación del riesgo

Magerit Versión 3, en el capítulo 4, define que el riesgo aumenta con la probabilidad y el impacto, permitiendo identificar varias zonas el momento de aplicar el tratamiento del riesgo: (Consejo Superior de Administración Electrónica, 2012)

- Zona 1: riesgos de muy alto impacto.
- Zona 2: franja amarilla: riesgo de impacto medio, pero de impacto bajo o muy bajo.
- Zona 3: riesgos de bajo impacto.

**Tabla 122**. *Matriz de riesgos*

| Activo | Código | Código Riesgo | Amenaza | Vulnerabilidad | Impacto | Probabilidad de ocurrencia | Evaluación del riesgo | Controles aplicables ISO/IEC27002:2013 |
|---|---|---|---|---|---|---|---|---|
| Base de datos: Sistema académico (ACADEMIUM) | [E.1] | R1 | Fallas de los usuarios | No hay manuales de uso o guías para los administradores. | M | A | A | • 12.1.1 Documentación de procedimientos de operación |
| | [E.2] | R2 | Errores del administrador. | Módulos de las bases de datos innecesarios que se encuentran habilitados. | B | A | M | • 12.1.1 Documentación de procedimientos de operación |
| | [E.15] | R3 | Alteración accidental de la información. | Disponer de configuraciones establecidas por defecto | A | B | A | • 9.1.1 Política de control de accesos |
| | [E.18] | R4 | Sustracción de información | No mantener las normas de confidencialidad de la información. | B | MB | MB | • 9.2.6 Retirada o adaptación de los derechos de acceso |
| | [E.19] | R5 | Sustracción de información | Módulos de las bases de datos innecesarios que se encuentran habilitados. | B | MB | MB | • 7.2.2 Concienciación, educación y capacitación en seguridad de la información |
| | [A.5] | R6 | Robo de identidad del usuario | Credenciales con parámetros débiles | B | MB | MB | • 9.1.1 Política de control de accesos 9.4.2 Procedimientos seguros de inicio de sesión |
| | [A.6] | R7 | Falla de permisos para acceder al dispositivo. | Falta de seguridad en los dispositivos autorizados. | M | MB | B | • 14.2.2 Procedimientos de control de cambios en los sistemas. |
| | [A.11] | R8 | Permisos no autorizados a los sistemas informáticos | Credenciales con parámetros débiles | B | MB | MB | • 9.1.1 Política de control de accesos 9.4.2 Procedimientos seguros de inicio de sesión |

| Activo | Código | Código Riesgo | Amenaza | Vulnerabilidad | Impacto | Probabilidad de ocurrencia | Evaluación del riesgo | Controles aplicables ISO/IEC27002:2013 |
|---|---|---|---|---|---|---|---|---|
| De desarrollo propio: Sistema de monitoreo de la red. | [I.5] | R9 | Avería de origen lógico o físico | No se ejecuta las suficientes pruebas para los sistemas. | MA | B | MA | • 14.2.2 Procedimientos de control de cambios en los sistemas |
| | [E.1] | R10 | Fallas de los usuarios | No hay manuales de uso o guías para los administradores. | M | A | A | • 12.1.1 Documentación de procedimientos de operación |
| | [A.6] | R11 | Falla de permisos para acceder al dispositivo. | Falta de seguridad en los dispositivos autorizados. | M | MB | B | • 7.2.2 Concienciación, educación y capacitación en seguridad de la información |
| | [A.19] | R12 | Copia de software ilegal | No existe un monitoreo y control de las aplicaciones propias de la institución. | B | MB | MB | • 14.2.1 Política de desarrollo seguro de software. 14.2.6 Seguridad en entornos de desarrollo. |
| Computadoras de escritorio y portátiles | [I.6] | R13 | Corte de energía eléctrica | No hay equipos ups que eviten la perdida de energía eléctrica. | B | B | B | • 11.2.2 Instalaciones de suministro |
| | [E.2] | R14 | Fallas administrativas de los dispositivos. | Periféricos USB de equipos tecnológicos habilitados | B | A | M | • 9.3.1 Uso de información confidencial para su autenticación 16.1.3 Notificación de puntos débiles de la seguridad 16.1.5 Respuesta a los incidentes de seguridad |
| | [E.2] | R15 | Fallas administrativas de los dispositivos. | Equipos informáticos sin sus respectivas configuraciones de usuarios estándar o administradores. | MA | A | MA | • 12.4.2 Protección de los registros de información |

| Activo | Código | Código Riesgo | Amenaza | Vulnerabilidad | Impacto | Probabilidad de ocurrencia | Evaluación del riesgo | Controles aplicables ISO/IEC27002:2013 |
|---|---|---|---|---|---|---|---|---|
| | [E.23] | R16 | Falla de coordinación en los mantenimientos. | No hay un procedimiento claro para realizar los mantenimientos preventivos o correctivos en (Hardware y Software). | M | B | M | • 11.2.4 Mantenimiento de los equipos |
| | [A.6] | R17 | Falla de permisos para acceder al dispositivo. | Falta de seguridad en los dispositivos autorizados. | M | B | M | • 7.2.2 Concienciación, educación y capacitación en seguridad de la información |
| | [A.11] | R18 | Permisos no autorizados a los sistemas informáticos | Credenciales con parámetros débiles | M | MB | B | • 9.3.1 Uso de información confidencial para su autenticación 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla |
| Routers inalámbricos y routers | [I.6] | R19 | Corte de energía eléctrica | No hay equipos ups que eviten la perdida de energía eléctrica. | M | MB | MB | • 11.2.2 Instalaciones de suministro |
| | [E.2] | R20 | Fallas administrativas de los dispositivos. | Falta de seguridades en las redes inalámbricas, bloqueos de páginas inadecuadas. | MB | B | B | • 9.3.1 Uso de información confidencial para su autenticación 16.1.3 Notificación de puntos débiles de la seguridad 16.1.5 Respuesta a los incidentes de seguridad |
| | [E.23] | R21 | Falla de coordinación en los mantenimientos. | Mantenimiento de software de los equipos, liberación de IP´s. | B | B | B | • 11.2.4 Mantenimiento de los equipos |
| | [A.6] | R22 | Falla de permisos para acceder al dispositivo. | Falta de seguridad en los dispositivos autorizados. | M | B | M | • 7.2.2 Concienciación, educación y capacitación |

| Activo | Código | Código Riesgo | Amenaza | Vulnerabilidad | Impacto | Probabilidad de ocurrencia | Evaluación del riesgo | Controles aplicables ISO/IEC27002:2013 |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | en seguridad de la información |
| | [A.11] | R23 | Permisos no autorizados a los sistemas informáticos | Credenciales con parámetros débiles | M | MB | B | • 9.3.1 Uso de información confidencial para su autenticación 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla |
| Switch | [I.6] | R24 | Corte del suministro eléctrico | No hay equipos ups que eviten la perdida de energía eléctrica. | M | MB | MB | • 11.2.2 Instalaciones de suministro |
| | [E.2] | R25 | Fallas administrativas de los dispositivos. | Falta de configuración y seguridad en los equipos, mantener inactivos los puertos que no se ocupen. | MB | B | B | • 9.3.1 Uso de información confidencial para su autenticación 16.1.3 Notificación de puntos débiles de la seguridad 16.1.5 Respuesta a los incidentes de seguridad |
| | [E.23] | R26 | Falla de coordinación en los mantenimientos. | Mantenimiento de software de los equipos. | B | A | M | • 11.2.4 Mantenimiento de los equipos |
| | [A.11] | R27 | Permisos no autorizados a los sistemas informáticos | Credenciales con parámetros débiles | M | MB | B | • 9.3.1 Uso de información confidencial para su autenticación 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla |
| Oficina de TICS | [A.11] | R28 | Permisos no autorizados a los sistemas informáticos | Credenciales con parámetros débiles | M | MA | A | • 11.1.2 Controles físicos de entrada |

| Activo | Código | Código Riesgo | Amenaza | Vulnerabilidad | Impacto | Probabilidad de ocurrencia | Evaluación del riesgo | Controles aplicables ISO/IEC27002:2013 |
|---|---|---|---|---|---|---|---|---|
| | [A.26] | R29 | Daño a la propiedad | No existen controles de seguridad adecuados en la institución. | MA | MB | A | • 11.1.4 Protección contra las amenazas externas y ambientales |
| Cableado | [N.3] | R30 | Fenómeno climático | Falta de seguridad en ductos de cableado | M | MB | MB | • 11.1.4 Protección contra las amenazas externas y ambientales |
| | [N.6] | R31 | Fenómeno sísmico | Falta de seguridad en ductos de cableado | B | MB | MB | • 11.2.3 Seguridad del cableado |
| | [N.7] | R32 | Inundación | Falta de seguridad en ductos de cableado | B | MB | MB | • 11.2.3 Seguridad del cableado |
| | [N.10] | R33 | Daño a la propiedad | Falta de seguridad en ductos de cableado | B | MB | MB | • 11.2.3 Seguridad del cableado |
| Administración de sistema académico y financiero | [E.7] | R34 | Deficiencias en la organización | Falta de información y capacitación a los usuarios de la organización. | B | B | B | • 7.2.2 Concienciación, educación y capacitación en seguridad de la información |
| | [E.19] | R35 | Sustracción de información | No mantener las normas de confidencialidad de la información. | MB | B | B | • 7.2.2 Concienciación, educación y capacitación en seguridad de la información |
| | [I.6] | R36 | Corte de suministro eléctrica | No hay equipos ups que eviten la perdida de energía eléctrica. | M | MB | B | • 11.2.2 Instalaciones de suministro |
| | [E.2] | R37 | Fallas administrativas de los dispositivos. | Falta monitoreo en los sistemas académicos y financieros. | A | A | MA | • 12.4.3 Registros de actividad del administrador y operador del sistema. |
| | [E.23] | R38 | Falla de coordinación en los mantenimientos. | No disponer de licencias en los equipos que manejan en la | MA | B | MA | • 11.2.2 Instalaciones de suministro |

| Activo | Código | Código Riesgo | Amenaza | Vulnerabilidad | Impacto | Probabilidad de ocurrencia | Evaluación del riesgo | Controles aplicables ISO/IEC27002:2013 |
|---|---|---|---|---|---|---|---|---|
| | | | | organización y no se encuentran actualizados los equipos y el antivirus. | | | | |
| | [A.6] | R39 | Falla de permisos para acceder al sistema. | No hay procesos establecidos para desarrollar las funciones de la organización. | MA | B | MA | • 12.1.1 Documentación de procedimientos de operación. |
| | [A.11] | R40 | Permisos no autorizados a los sistemas informáticos | Falta de controles de bloqueo a usuarios que estén dentro de la red. | M | B | M | • 10.1.2 Gestión de claves. |
| Administrador de base de datos | [E.19] | R41 | Sustracción de información | Falta de controles en los procesos o políticas de seguridad para los datos de la organización. | MA | B | MA | • 6.1.1 Asignación de responsabilidades para la segur. de la información. |
| | [A.11] | R42 | Permisos no autorizados a los sistemas informáticos | Credenciales con parámetros débiles | A | A | MA | • 13.1.2 Mecanismos de seguridad asociados a servicios en red. |
| | [E.23] | R43 | Falla de coordinación en los mantenimientos. | No existe monitoreo en las bases de datos de la organización. | M | MB | B | • 12.4.3 Registros de actividad del administrador y operador del sistema |

**Fuente***:* NORMA ISO/IEC 27002:2013, Elaborado por el autor de la investigación basado en la metodología Magerit Versión 3 (2012).

Este mapa de calor de riesgo permite visualiza y detallar los riesgos encontrados en la organización, con la ayuda de las categorías de probabilidad e impacto.

**Tabla 133**. *Mapa de calor*

| Riesgo | | Probabilidad | | | | |
|---|---|---|---|---|---|---|
| | | Muy baja | Baja | Media | Alta | Muy alta |
| Impacto | Muy alta | R29 | R9, R38, R39, R41 | | R15 | |
| | Alta | | R3 | | R37, R42 | |
| | Media | R7, R11, R18, R19, R23, R24, R27, R30, R36, R43 | R16, R17, R22, R40, | | R1, R10, R28 | |
| | Baja | R4, R5, R6, R8, R12, R31, R32, R33, | R13, R21, R34 | | R2, R14, R26 | |
| | Muy baja | | R20, R25, R35 | | | |

**Fuente:** Elaborado por el autor de la investigación, basado con la metodología de Magerit Versión 3 (2012).

Los resultados presentados con la metodología de Magerit en la Tabla 23, los activos que se visualiza en la tabla que tienen un riesgo extremo se debe tratar para dejarlo en moderado y los activos críticos a nivel bajo.

**Tabla 144.** *Aceptación del riesgo*

| Aceptación y Tolerancia | | | |
|---|---|---|---|
| B | Zona de riesgo | Baja | Riesgos de bajo impacto |
| M | Zona de riesgo | Moderada | Evaluar el riesgo y determinar si los controles implementados son suficientes |
| A | Zona de riesgo | Alta | Riesgos improbables, pero de muy alto impacto. |
| MA | Zona de riesgo | Extrema | Requiere atención urgente y dispone de impacto alto al activo |

**Fuente***:* Elaborado por el autor de la investigación, basado con la metodología Magerit Versión 3 (2012).

### 3.3.5 Determinar que salvaguardas hay dispuestas frente al riesgo

El objetivo de los controles es minimizar que la amenaza pueda afectar al activo y mitigar la probable degradación que un activo de la institución pueda ser afectado.

Para el análisis de esta sección, se da uso el (ANEXO 2) que indica las normas de seguridad de la información según la ISO 27002:2013, de acuerdo al activo, se establece el control respectivo que es el siguiente:

**Tabla 155**. *Norma ISO/IEC 27002:2013*

| Dominio | Objetivo de control | Controles |
|---|---|---|
| ➢ 5. POLÍTICAS DE SEGURIDAD | ✓ 5.1. Indicaciones de la dirección en seguridad de la información. | • 5.1.1 Conjunto de políticas para la seguridad de la información.<br>• 5.1.2 Revisión de las políticas para la seguridad de la información. |
| ➢ 6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN | ✓ 6.1. Organización interna. | • 6.1.1 Asignación de responsabilidades para la seguridad de la información<br>• 6.1.2 Segregación de tareas |
| ➢ 7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS | ✓ 7.2 Durante la contratación | • 7.2.2 Concienciación, educación y capacitación en seguridad de la información. |
| | ✓ 7.3 Cese o cambio de puesto de trabajo | • 7.3.1 Cese o cambio de puesto de trabajo. |
| ➢ 9. CONTROL DE ACCESOS | ✓ 9.1 Requisitos de negocio para el control de accesos. | • 9.1.1 Política de control de accesos |
| | ✓ 9.2 Gestión de acceso de usuarios | • 9.2.1 Gestión de altas/bajas en el registro de usuarios<br>• 9.2.3 Gestión de los derechos a acceso con privilegios especiales<br>• 9.2.6 Retirada o adaptación de los derechos de acceso |
| | ✓ 9.3 Responsabilidades del usuario | • 9.3.1 Uso de información confidencial para su |
| | ✓ 9.4 Control de acceso a sistemas y aplicaciones | • 9.4.2 Procedimientos seguros de inicio de sesión. |
| ➢ 11 SEGURIDAD FÍSICA Y AMBIENTAL | ✓ 11.1 Áreas seguras | • 11.1.2 Controles físicos de entrada<br>• 11.1.4 Protección contra las amenazas externas y ambientales |
| | ✓ 11.2 Seguridad en los equipos | • 11.2.2 Instalaciones de suministro<br>• 11.2.3 Seguridad del cableado.<br>• 11.2.4 Mantenimiento de los equipos.<br>• 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla |
| | ✓ 12. 1 Responsabilidades y procedimientos de operación | • 12.1.1 Documentación de procedimientos de operación. |

| Dominio | Objetivo de control | Controles |
|---|---|---|
| ➢ 5. POLÍTICAS DE SEGURIDAD | ✓ 5.1. Indicaciones de la dirección en seguridad de la información. | • 5.1.1 Conjunto de políticas para la seguridad de la información.<br>• 5.1.2 Revisión de las políticas para la seguridad de la información. |
| ➢ 12. SEGURIDAD EN LA OPERATIVA | ✓ 12.2 Protección contra código malicioso | • 12.1.4 Separación de entornos de desarrollo, prueba y producción<br>• 12.2.1 Controles contra código malicioso |
| ➢ 14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN | ✓ 14.2 Seguridad en los procesos de desarrollo y soporte | • 14.2.1 Política de desarrollo seguro de software.<br>• 14.2.2 Procedimientos de control de cambios en los sistemas.<br>• 14.2.6 Seguridad en entornos de desarrollo.<br>• 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.<br>• 14.2.9 Pruebas de aceptación. |
| ➢ 16 GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN | ✓ 16.1 Gestión de incidentes en la seguridad de la información y mejoras | • 16.1.3 Notificación de puntos débiles de la seguridad 16.1.5 Respuesta a los incidentes de seguridad |

**Fuente***:* NORMA ISO/IEC 27002:2013

# CAPÍTULO IV

# PROPUESTA

A continuación, se presenta la propuesta de la Política de Seguridad de la información basada en la norma NTE INEN ISO/IEC 27002:2013, para la Unidad Educativa Borja 3 Cavanis.

## 4.1 OBJETIVO Y CAMPO DE APLICACIÓN

La Política de Seguridad de la Información o datos establece las normativas o reglas que se aplicará a la Unidad Educativa Borja 3 Cavanis.

## 4.2 REFERENCIAS NORMATIVAS

El presente documento está basado en la Norma Ecuatoriana NTE INEN-ISO/IEC 27002:2013; Guía de buenas prácticas.

## 4.3 TÉRMINOS Y DEFINICIONES

Información del activo

Es un dato o elemento de una organización que tiene un valor importante en la empresa.

**Seguridad de la Información**

Como su nombre lo indica es proteger la información y sus activos más importantes de la organización mediante controles y normas que garanticen la confidencialidad, integridad y disponibilidad de la información permitiendo con esto la continuidad del negocio.

**Confidencialidad**

Es garantizar que los datos y la información que es utilizada por la organización tenga acceso solo personas autorizado.

**Integridad**

Garantiza que la información esté completa y no se encuentre adulterada.

**Disponibilidad**

Que la información y sus activos se encuentren disponibles siempre que el personal de la institución lo requiera.

**Usuario**

Es el personal de la empresa que usan los servicios y recursos tecnológicos para desempeñar las funciones en la organización.

**Vulnerabilidad**

Buendía (2013) menciona que una vulnerabilidad es un defecto de un sistema o falla de una aplicación que al ser explotada por un atacante puede aprovechar este inconveniente y ocasionar grandes daños.

**Amenaza**

Chávez (2015) indica que las amenazas informáticas pueden causar afectaciones a los activos y los sistemas de las organizaciones, estas amenazas están relacionas con el personal o eventos naturales.

**Incidente de Seguridad de la información**

Un incidente de seguridad presenta afectaciones negativas en la organización incluso en los activos que son de carácter crítico.

## 4.4 ABREVIATURAS

ID: Identificador de usuario

IEC: Comisión Internacional de Electrotécnica

ISO: Organización Internacional de Normalización

UEB3: Unidad Educativa Borja 3 Cavanis

LOSEP: Ley Orgánica de Servicio Público

TIC: Tecnologías de la Información y Comunicaciones

## 4.5 POLÍTICA DE SEGURIDAD

### 4.5.1 OBJETIVO

Establecer las normativas destinadas a garantizar la seguridad de la información a través de una orientación y soporte para la ejecución de los procesos de gestión.

**RESPONSABILIDADES**

Coordinador General de las Tecnologías de la Información.

Persona encargada de aprobar las políticas de seguridad, monitorear y actualizar que se cumpla estas normas en la Institución. Coordinador del área de Gestión Tecnológica de la Unidad Educativa Borja 3 Cavanis.

**Máxima autoridad o su delegado.**

Personal responsable para implementar estas políticas de seguridad en la Institución: Director General y Rector de la Unidad Educativa Borja 3 Cavanis.

**Funcionarios.**

Conocer y aplicar las normativas establecidas en la política de seguridad.

### 4.5.2 DESARROLLO DE LA POLÍTICA

#### 4.5.2.1 Política de seguridad

**Objetivo**

Implementar un proceso para el uso y manejo de los activos que permitan minimizar la pérdida de la información y permisos no autorizados a plataformas de la Institución.

#### 4.5.2.2 Directrices de la dirección en seguridad de la información

**Conjunto de políticas para la seguridad de la información.**

**Artículo 1**

El coordinador del área de Gestión Tecnológica aprobará la política de seguridad de la información y socializará con las áreas involucradas de la Unidad Educativa Borja 3 Cavanis

**Revisión de las políticas para la seguridad de la información**

**Artículo 2**

La política de seguridad debe ser actualizada y socializada en intervalos de tiempos planificados, para evitar que los usuarios que no disponen del acceso autorizado puedan ingresar al sistema académico o bases de datos, de modo que puedan poner en peligro la información de los administrativos, docentes, estudiantes y padres de familia.

#### 4.5.2.3 Aspectos organizativos de la seguridad de la información

**Objetivo**

Establecer un responsable para controlar y guiar la operación de la seguridad de la información dentro de la Unidad Educativa Borja 3 Cavanis.

**Organización interna.**

**Asignación de responsabilidades para la seguridad de la información.**

**Artículo 3**

El coordinador del departamento de Gestión Tecnológica puede asignar actividades de seguridad de la información por escrito a varios integrantes del departamento de Gestión Tecnológica, siempre y cuando los procesos estén bien establecidos y en coordinación con la organización.

**Artículo 4**

El coordinador del área de Gestión Tecnológica debe inspeccionar que las tareas asignadas se ejecuten correctamente en la Unidad Educativa Borja 3 Cavanis.

**Segregación de tareas**

**Artículo 5**

El departamento de Gestión Tecnológica debe mantener un control de monitoreo de las actividades asignadas para verificar que se cumpla adecuadamente.

#### 4.5.2.4 Seguridad ligada a los recursos humanos

**Objetivo**

Asegurar que los miembros de la Institución conozcan sobre las políticas de Seguridad de la Información para mitigar el riesgo de robos y fraudes a la Institución.

**Antes de la contratación.**

**Términos y condiciones de contratación**

**Artículo 6**

Los integrantes del área de Gestión Tecnológica deberán firmar un compromiso de confidencialidad, debido a que en esta área se maneja datos muy importantes de la organización.

**Durante la contratación**

**Concienciación, educación y capacitación en seguridad de la información**

**Artículo 7**

Antes de entregar las credenciales de acceso a los sistemas, la Unidad Educativa Borja 3 Cavanis a través del área de Gestión Tecnológica deberá capacitar a los usuarios nuevos y antiguos de la Institución, además se informarán las normas y políticas de seguridad que dispone la misma.

**Artículo 8**

El responsable del departamento tecnológico designará qué usuarios tienen un mejor dominio en el tema de seguridad de la información, para ofrecer capacitaciones y coordinar el manejo en cada área de la organización.

**Artículo 9**

Es deber de los usuarios de la Unidad Educativa Borja 3 Cavanis estar presentes en las capacitaciones, así como obedecer las disposiciones y normas que se indique en cada una de ellas.

**Artículo 10**

La capacitación programada por el personal de Gestión Tecnológica sobre la Seguridad de la Información deberá disponer de todos los materiales de apoyo, los cuales serán proporcionados a los usuarios.

**Artículo 11**

Es responsabilidad de los usuarios de la organización cumplir con las normas y políticas de Seguridad de la Información establecidas en el presente manual.

**Cese o cambio de puesto de trabajo.**

**Artículo 12**

El departamento de Recursos Humanos de la Unidad Educativa Borja 3 Cavanis tiene la obligación de informar inmediatamente la desvinculación del personal administrativo o docente al área de Gestión Tecnológica, para que este dé de baja al usuario y lo elimine del sistema.

**Artículo 13**

El departamento de Gestión Tecnológica de la Unidad Educativa Borja 3 Cavanis debe indicar que siguen vigentes las normas de seguridad después de realizar el cambio de puesto del trabajo del administrativo o docente de la organización.

**Artículo 14**

Los activos entregados al departamento de Gestión Tecnológica que dan por terminada su relación laboral, deben ser entregado al departamento de activos fijos para el control de inventarios, en las mismas condiciones que fueron entregados originalmente.

#### 4.5.2.5 Control de accesos

**Objetivo**

Limitar el acceso al sistema, de procesamiento de información de la Unidad Educativa Borja 3 Cavanis

**Requerimientos de negocios para el control de accesos**

**Política de control de accesos**

**Artículo 15**

El coordinador del departamento de Gestión Tecnológica proporcionará por medio de un acta de entrega recepción, los manuales de usuarios finales para el correcto manejo y uso de los sistemas de la Institución.

**Artículo 16**

El responsable del área de Gestión Tecnológica deberá informar a los docentes, administrativos, padres de familia y estudiantes que es fundamental realizar el cambio de la contraseña temporal la cual es entregada en el primer acceso a la aplicación de la institución.

**Artículo 17**

Evitar indicar o divulgar las contraseñas cuando son ingresadas a la aplicación de la Unidad Educativa Borja 3 Cavanis.

**Artículo 18**

Utilizar las credenciales de acceso a los sistemas con parámetros de cifrado.

**Artículo 19**

El personal de Gestión Tecnológica procurará que las credenciales ingresadas por los usuarios de la organización sean difíciles de identificar, por lo que debe cumplir con ciertos parámetros de seguridad, como:

- Las credenciales deben poseer una longitud de ocho caracteres como mínimo y de doce como máximo.

- Las contraseñas deben disponer de un periodo de vigencia, luego se cambiará por unas credenciales nuevas.

- Al colocar la contraseña deberán usar datos no personales,

- Usar una contraseña que no sean con significado obvio.

**Artículo 20**

El departamento de Gestión Tecnológica permitirá el respectivo monitoreo a cada usuario que presente una actividad sospechosa relacionada con la institución, este proceso puede llevarse dentro o fuera de la organización.

**Artículo 21**

El departamento de Gestión Tecnológica no asignará ningún acceso adicional a las aplicaciones académicas solicitadas por el usuario de la organización, sin haber cumplido con los requisitos para su respectiva autorización.

**Artículo 22**

Se considerará una falta grave, cualquier procedimiento no autorizado, esto se puede identificar mediante una auditoría y monitoreo del sistema, en la que el usuario informático que está a cargo y conoce del mismo pueda corroborar la manipulación y el mal uso de los dispositivos tecnológicos.

#### 4.5.2.6 Gestión de acceso de usuarios

**Gestión de altas/bajas en el registro de usuarios**

**Artículo 23**

El departamento de Recursos Humanos de la Unidad Educativa Borja 3 Cavanis deberá informar al responsable del departamento de Gestión Tecnológica la nómina del personal nuevo para la creación de los accesos a las aplicaciones académicas que maneja la organización.

**Artículo 24**

El acceso lógico a las aplicaciones de los usuarios que fueron desvinculados de la Unidad Educativa Borja 3 Cavanis debe ser retirado de los sistemas informáticos por el encargado del área de Gestión Tecnológica de manera inmediata, colocándoles un estado de INACTIVO a los usuarios.

**Gestión de los derechos a acceso con privilegios especiales**

**Artículo 25**

Una vez autorizado por la Unidad Educativa Borja 3 Cavanis; ya sea por escrito o correo electrónico, se asignará credenciales de accesos a los sistemas académicos a docentes y administrativos.

**Retirada o adaptación de los derechos de acceso**

**Artículo 26**

El departamento de Gestión Tecnológica verificará los privilegios de acceso a los usuarios que cambiaron sus funciones o tareas en la organización o fueren relevados de sus cargos.

#### 4.5.2.7 Responsabilidades del usuario

**Uso de información confidencial para la autenticación**

**Artículo 27**

El usuario se hará cargo de la protección del equipo de cómputo que fue entregado por el responsable del departamento de Gestión Tecnológica, mediante protectores de pantalla con contraseña cuando requiera ausentarse de su puesto de trabajo.

**Artículo 28**

Ningún usuario podrá acceder a las aplicaciones académicas con las credenciales de otro usuario.

**Artículo 29**

Es responsabilidad de los usuarios de la organización, el uso que haga de la cuenta de acceso al sistema académicos y equipos de cómputo entregados por el departamento de Gestión Tecnológica.

**Artículo 30**

Los usuarios son responsables de todas las actividades llevadas a cabo con su cuenta de acceso y contraseña.

**Artículo 31**

El personal de la institución debe reportar de urgencia al departamento de Gestión Tecnológica cualquier falla o daño al identificar una amenaza en la institución.

**Artículo 32**

El área de Gestión Tecnológica de la Unidad Educativa Borja 3 Cavanis no se hará responsable del mal uso y manejo que se den a los sistemas académico o correo corporativo de la organización.

**Artículo 33**

Las cuentas de correos corporativas que se encuentren con estado desactivado o inactivo se conservarán y se realizará el proceso de eliminación.

#### 4.5.2.8 Control de acceso a sistemas y aplicaciones

**Procedimientos seguros de inicio de sesión**

**Artículo 34**

El equipo tecnológico debe manejar un sistema de monitoreo y un mecanismo de autenticación de los usuarios de la organización.

**Artículo 35**

Las contraseñas deben cambiarse antes de colocarlas en producción.

**Artículo 36**

El departamento de Gestión Tecnológica asignará cuentas de usuario y contraseña al personal de la Institución, estas credenciales sólo las usarán en el primer inicio de sesión; ya que se solicita de manera obligada ingresar la nueva contraseña para acceder al servicio.

**Artículo 37**

Los usuarios que ocuparán el sistema académico deberán cambiar su contraseña en el momento del primer ingreso al sistema.

**Artículo 38**

Por ningún motivo deberán compartirse a usuarios distintos al originalmente asignado, las credenciales que se introducen para el acceso al sistema académico, el área de Gestión Tecnológica deberá implementar credenciales de acceso con un alto nivel de complejidad.

#### 4.5.2.9 Seguridad física y ambiental

**Controles físicos de entrada**

**Artículo 39**

Los usuarios que ingresen a las áreas restringidas donde se encuentra los sistemas de almacenamiento y procesamiento de información deben portar de manera obligatoria una credencial de manera visible.

**Protección contra las amenazas externas y ambientales**

**Artículo 40**

Los controles de acceso a las áreas de procesamiento de la información o almacenamiento deben ser revisados, actualizados o revocados, según sea el caso.

**Artículo 41**

Se prohíbe todo consumo de alimentos dentro de los laboratorios de informática.

**Artículo 42**

Se debe prohibir el ingreso del personal de limpieza con maletas.

**Artículo 43**

Se debe contar con extintores en las áreas que reposen los equipos informáticos.

**Artículo 44**

Los suministros como papelería deberán estar ubicados a una distancia considerable de los equipos informáticos.

#### 4.5.2.10 Seguridad en los equipos

**Instalaciones de suministro**

**Artículo 45**

Los equipos de almacenamiento y procesamiento de información deberán mantener equipos redundantes para evitar la pérdida de energía eléctrica.

**Artículo 46**

El cableado de la institución ya sea de red o eléctrico deberá estar correctamente etiquetado para identificar en donde se encuentra conectados los dispositivos.

**Mantenimiento de los equipos**

**Artículo 47**

El departamento de Gestión Tecnológica es el responsable de planificar los mantenimientos preventivos y correctivos de los equipos informáticos, teniendo en cuenta que no se puede obstaculizar el trabajo de los funcionarios de la organización.

**Artículo 48**

Los mantenimientos preventivos y correctivos de los equipos informáticos de la Unidad Educativa Borja 3 Cavanis serán únicamente responsabilidad del departamento de Gestión Tecnológica.

**Artículo 49**

El departamento de Gestión Tecnológica deberá llevar un control de los mantenimientos correctivos y preventivos realizados a los equipos informáticos de la organización.

**Artículo 50**

Cuando se programe realizar los mantenimientos de los equipos del personal administrativo, docente o directivos; se debe enviar el cronograma a todos los funcionarios con anticipación para poder cumplir los tiempos establecidos.

**Políticas de puesto de trabajo y bloqueo de pantalla**

**Artículo 51**

Cuando el personal de la institución debe ausentarse de su puesto de trabajo deberá colocar su equipo de cómputo con contraseña.

**Artículo 52**

Se prohíbe a los usuarios de la organización mover o reubicar los equipos sin la respectiva autorización del coordinador del departamento de Gestión Tecnológica.

**Artículo 53**

Al tener un cambio o una reubicación de un equipo tecnológico deberá ser notificado al coordinador del área de Gestión Tecnológica con anticipación.

**Artículo 54**

Al finalizar la jornada de trabajo de los usuarios; ya sean administrativos, docentes o directivos, deberán apagar los equipos de cómputo que están a su cargo para evitar acceso no autorizados de terceros.

**Artículo 55**

El responsable del área de Gestión Tecnológica asignará una persona para el control del uso del laboratorio informático.

**Artículo 56**

Los equipos tecnológicos de la institución no podrán salir sin una autorización del director general y validación del responsable del departamento de Gestión Tecnológica.

### 4.5.3 Seguridad en la operativa

**Objetivo**

Plantear normas y reglas para asegurar las operaciones en el departamento de Gestión Tecnológica.

#### 4.5.3.1 Responsabilidades y procedimientos de operación

**Documentación de procedimientos de operación**

**Artículo 57**

El departamento de Gestión Tecnológica diseñará los manuales de usuarios de los sistemas y aplicaciones que utilice la institución para el correcto funcionamiento de los mismos.

**Artículo 58**

El departamento de Gestión Tecnológica deberá mantener actualizada la información de las aplicaciones informáticas que se usa en la institución.

**Separación de entornos de desarrollo, prueba y producción**

**Artículo 59**

Se debe separar los ambientes de producción y prueba para minimizar el riesgo de accesos no autorizado a los sistemas de la organización.

#### 4.5.3.2 Protección contra código malicioso

**Controles contra código malicioso**

**Artículo 60**

El coordinador del área de Gestión Tecnológica deberá tener los equipos de cómputo de la institución con un antivirus adecuado y actualizado.

**Artículo 61**

Es obligación del usuario revisar que todo medio extraíble como memoria USB debe ser analizado por el antivirus del equipo.

#### 4.5.3.3 Copias de seguridad

**Copias de la seguridad de la información.**

**Artículo 62**

El responsable del departamento de Gestión Tecnológica es el encargado de realizar las copias de seguridad de la información de los sistemas académicos e incluso de las máquinas personales de los usuarios de la organización.

**Artículo 63**

El responsable del departamento de Gestión Tecnológica del sistema académico deberá definir el tiempo de periodicidad de las respectivas copias de seguridad de los sistemas informáticos de la Institución.

**Artículo 64**

Solamente el coordinador del área de Gestión Tecnológica podrá eliminar las copias de seguridad de los sistemas informáticos, con la autorización respectiva de la máxima autoridad de la Unidad Educativa Borja 3 Cavanis.

**Artículo 65**

Las copias de seguridad de los sistemas informáticos deberán almacenarse en dispositivos como NAS, discos externos o la nube de información.

**Artículo 66**

La eliminación de copias de seguridad de la información deberá quedar registrada con el fin de mantener trazabilidad para su auditoria.

### 4.5.4 Seguridad en las telecomunicaciones

**Objetivo**

Asegurar que la información de la organización quede protegida incluso en su infraestructura de telecomunicaciones.

#### 4.5.4.1 Gestión de la seguridad en las redes

**Controles de red**

**Artículo 67**

Únicamente el área de Gestión Tecnológica mantendrá la administración de la red de la Unidad Educativa Borja 3 Cavanis

**Artículo 68**

El personal autorizado a acceder a la red de la Unidad Educativa Borja 3 Cavanis deberán acercarse al departamento de Gestión Tecnológica con su equipo para registrar la dirección MAC, así como permisos para navegar en dicha red; previa autorización de la máxima autoridad.

**Artículo 69**

Se considera como uso aceptable de la red de la institución, la navegación para realizar actividades propias de la institución.

**Artículo 70**

El departamento de Gestión Tecnológica es responsable de la implementación de herramientas informáticas para la administración del servicio de red, para minimizar los riesgos en la organización.

**Artículo 71**

El departamento de Gestión Tecnológica bloqueará cualquier acceso que presente las siguientes actividades en la navegación a sitios o páginas web: contenidos pornográficos, comunidades de *hackers*, violación de los derechos de privacidad, confidencialidad y protección de los datos.

### 4.5.5 Adquisición, desarrollo y mantenimiento de los sistemas de información

#### 4.5.5.1 Seguridad en los procesos de desarrollo y soporte

**Política de desarrollo seguro de software**

**Artículo 72**

El departamento de Gestión Tecnológica es el único autorizado para realizar copias de seguridad de los sistemas informáticos y preservar el software original.

**Procedimientos de control de cambios en los sistemas**

**Artículo 73**

Se debe llevar un registro de todas las solicitudes de cambio de los sistemas informáticos de la organización en caso de solicitar una auditoria.

### 4.5.6 Gestión de incidentes en la Seguridad de la Información

#### 4.5.6.1 Gestión de incidentes en la Seguridad de la Información y mejoras

**Respuesta a los incidentes de seguridad**

**Artículo 74**

Se deberá disponer de un reporte detallado de todos los sucesos de Seguridad de la Información y la respuesta generada para solventar cada uno de ellos; con el respectivo detalle y de ser posible la valoración de daños del mismo, si fuere el caso.

### 4.5.7 Procedimientos de control de proveedores

**Artículo 75**

Se deben definir los requisitos en Ciberseguridad que deben cumplir los productos o servicios que sea solicitado al proveedor, dichos requisitos tendrán que cumplir con las políticas de seguridad de la información de la Institución y los extenderemos a proveedores, colaboradores, distribuidores y suministradores, etc.

**Artículo 76**

Definir cláusulas con el fin de establecer contratos con nuestros proveedores y acuerdos de confidencialidad de acceso a los datos de la organización.

**Artículo 77**

Definir los Acuerdos de Nivel de Servicio con el proveedor con el fin de concretar las características de calidad y garantías de equipos o servicios adquiridos.

# CAPÍTULO V

## Conclusiones y trabajos futuros

### 5.1 Conclusiones

Fue posible diseñar una política de seguridad de la información para el área de Gestión Tecnológica en función de la criticidad de la seguridad de la Unidad Educativa Borja 3 Cavanis, la misma que se aplicará en los procesos tecnológicos para salvaguardar la integridad, confidencialidad y disponibilidad de la información, acorde a las normas ISO/IEC 27002:2013, ya que estas políticas se pueden implementar en cualquier organización.

Al realizar la matriz de riesgos en el área de Gestión Tecnológica, se evidencia que existen vulnerabilidades y amenazas y a las cuales están expuestos los activos del sistema académico Academium, este procedimiento fue sustentado y elaborado de acuerdo a la Metodología Magerit.

Mediante los resultados desplegados en el análisis de riesgos se pudo concluir que no es necesario implementar todos los controles recomendados por la norma ISO/IEC 27001:2013; por lo cual se seleccionó los más adecuados que permitirán minimizar el riesgo que ocasiona las amenazas sobre los activos, teniendo en cuenta el presupuesto de la organización y el giro del negocio.

Al momento de finalizar el proyecto de titulación el área de Gestión Tecnológica de la Unidad Educativa Borja 3 Cavanis consideró que la política que se diseñó permitirá que personas extrañas a la Unidad Educativa no tengan accesos a la información personal de cada estudiante, administrativo, docente, de servicio, etc.

Se debe tener en cuenta que toda política de seguridad implementada en una institución educativa permitirá el bienestar y tranquilidad de sus alumnos y sus representantes.

## 5.2 Recomendaciones

Se recomienda que la política de Seguridad de la Información diseñada para el área de Gestión Tecnológica de la Unidad Educativa Borja 3 Cavanis, sea aprobada por las autoridades de la institución.

Una vez aprobada esta propuesta, se sugiere que el personal del departamento de Gestión Tecnológica implemente la política de Seguridad de la Información, ya que está servirá como guía para los usuarios sobre las acciones preventivas o correctivas que se deben aplicar para evitar o mitigar amenazas y vulnerabilidades en los sistemas informáticos de la organización.

Asimismo, que sea socializada con el personal de la organización: administrativos, directivos, docentes, estudiantes para que contribuyan con la aplicación de la misma.

Se sugiere que el área de Gestión Tecnológica realice una evaluación y revisión periódica para confirmar que los funcionaros de la organización cumplan con las normas definitivas y si los controles aplicados satisfacen las necesidades de Seguridad de la Institución.

# 6 BIBLIOGRAFÍA


Aguilera, P. (2010). *Seguridad informática*. Madrid: Editex S. A.

Aula Mentor. (2016). *Normas ISO sobre gestión de seguridad de la información*. España: Ministerio Educación, Cultura y Deporte. Obtenido de: http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/normas_iso_sobre_gestin_de_seguridad_de_la_informacin.html

Borja 3 Cavanis. (2017). *Borja 3 Cavanis*. Obtenido de: https://www.borja3cavanis.edu.ec/index.php/el-colegio/quienes-somos.html

Buendía, J. F. (2013). *Seguridad Informática*. Madrid: McGraw-Hill.

Cárdenas, G. D. (2018). *Diseño de una política de seguridad de la información basada en la norma ISO 27799 para el control de accesos a las aplicaciones médicas de la red en el Hospital* AXXIS (Tesis de Maestría). UISEK. Quito-Ecuador

Cevallos, Y. (2019). *Diseño de una política de seguridad de la información para el área de tics del Instituto Tecnológico Superior Central Técnico, basado en la norma de Seguridad ISO/IEC 27002:2013* (Tesis de Maestría). UISEK. Quito-Ecuador

Chávez, J. D. (2015). *Seguridad Informática Personal y Corporativa*. Venezuela: IEASS Editores.

Contero, W. (2019). *Diseño de una política de seguridad de la información basada en la norma ISO 27002:2013, para el sistema de botones de seguridad del Ministerio del Interior* (Tesis de Maestría). UISEK. Quito-Ecuador

Contreras, L. C. (2017). *Diseño de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 para la direccion de sistemas de la gobernación de Boyacá.* (Tesis de Maestría). UNAD. Bogotá-Colombia.

Fisher, R. P. (1988). *Seguridad en los sistemas informáticos.* Madrid: Diaz de Santos, S.A.

Gutiérrez, C. (2013). ISO/IEC 27002:2013 y los cambios en los dominios de control. Obtenido de: https://www.welivesecurity.com/la-es/2013/12/12/iso-iec-27002-2013-cambios-dominios-control/

Horvath, M., & Jakub, M. (2009). Implementation of security controls according to iso/iec 27002 in a small organisation. *Qual. Innovation Prosperity, 13*, 48-54.

Huracanes, R. (2016). *Implementación de la norma ISO-IEC 27002: 2013, sección "Control de acceso" para las aplicaciones informáticas de la Aseguradora del Sur* (Tesis de pregrado), Universidad de las Américas, Quito-Ecuador.

Ladino, M. I., Villa, P. A., & López, A. M. (2011). Fundamentos de ISO 27001 y su aplicación en las empresas. *Scientia et technica, 17*(47), 334-339.

Ledezma, N. (2015). *Desarrollo de políticas de seguridad de la información basadas en las normas ISO 27002 para una coordinación zonal del INEC* (Tesis de Maestría). PUCE, Quito-Ecuador.

Ministerio de Hacienda y Administraciones Públicas . (2012). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método.* Madrid: E.N.S.

Norma ISO/IEC 27002:2013 (2013). *Information technology - Security techniques - Information security management systems.* International Organization for Standardization.

Rodríguez, J. M., & Peralta, I. (2013). *Administración Electrónica Gestión de Riesgos Magerit.* España: Think.

Burgos, J., & Campos, P. G. (2008). Modelo para Seguridad de la Información en TIC. Concepción, Chile: Universidad del Bío-Bío.

Solarte, F. N. S., Rosero, E. R. E., & del Carmen Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica-ESPOL*, *28*(5)

Tarazona, T. (2007). Amenazas informáticas y seguridad de la información. *Derecho Penal y Criminología*, 28 (84), 137-146.

ANEXO 1: **AUTORIZACIÓN PARA EL DESARROLLO DEL PROYECTO DE TITULACIÓN**

**BORJA N 3 CAVANIS**

*"SER MÁS PADRES, QUE MAESTROS"*

**UNIDAD EDUCATIVA y ACADEMIA MILITAR**

*Educación Cristiana - formación integral* *Formación Cristiana – Disciplina militar*

**2019 - 2020**

Quito, 16 de septiembre del 2019

MSc. Fausto Gilberto Guerrero Loor

**RECTOR DE LA UNIDAD EDUCATIVA BORJA 3 CAVANIS**

**Presente.**

Yo, Israel Alejandro Cárdenas calderón, Administrador del área de gestión tecnológica de la unidad educativa Borja 3 Cavanis, con un atento saludo ante usted me dirijo respetuosamente para solicitar de la manera más cordial. me autorice diseñar una política de seguridad de la información para el área de gestión tecnológica, lo cual me servirá como proyecto de titulación de la Maestría en Tecnologías de la Información con mención en Seguridad Informática de la Universidad Internacional SEK.

Agradezco su favorable atención a la presente,

Atentamente

Ing. Israel Cárdenas
1723886212

*"Formamos seres humanos preparados en una educación de calidad Para la vida, al particular estilo de la Comunidad Cavanis"*

Página WEB: www.borja3cavanis.edu.ec

**BORJA N 3 CAVANIS**

"SEAMOS PADRES, QUE SEAMOS MAESTROS"

**UNIDAD EDUCATIVA y ACADEMIA MILITAR**

*Educación Cristiana – Formación Integral* *Formación Cristiana – Disciplina Militar*

**2019 - 2020**

Quito, 16 de septiembre del 2019

Padre Mauricio Kwiatkovski de Lima

**DIRECTOR GENERAL DE LA UNIDAD EDUCATIVA BORJA 3 CAVANIS**

**Presente.**

Yo, Israel Alejandro Cárdenas calderón, Administrador del área de gestión tecnológica de la unidad educativa Borja 3 Cavanis, con un atento saludo ante usted me dirijo respetuosamente para solicitar de la manera más cordial, me autorice diseñar una política de seguridad de la información para el área de gestión tecnológica, lo cual me servirá como proyecto de titulación de la Maestría en Tecnologías de la Información con mención en Seguridad Informática de la Universidad Internacional SEK.

Agradezco su favorable atención a la presente,

Atentamente

Ing. Israel Cárdenas
1723886217

DIRECCIÓN GENERAL
16 SEP 2019
RECIBIDO
P. Mauricio Kwiatkovski de Lima, CSCh
Director General

*"Formamos seres humanos preparados en una educación de calidad Para la vida, al particular estilo de la Comunidad Cavanis"*

Página WEB:

ANEXO2**: NORMA ISO/IEC 27002:2013**

## ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

**5. POLÍTICAS DE SEGURIDAD.**
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

**6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.**
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

**7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.**
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

**8. GESTIÓN DE ACTIVOS.**
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

**9. CONTROL DE ACCESOS.**
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

**10. CIFRADO.**
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

**11. SEGURIDAD FÍSICA Y AMBIENTAL.**
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

**12. SEGURIDAD EN LA OPERATIVA.**
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

**13. SEGURIDAD EN LAS TELECOMUNICACIONES.**
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

**ISO27002.es PATROCINADO POR:**

GES CONSULTOR
GOBIERNO T.I. · RIESGO · CUMPLIMIENTO

**14. ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.**
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

**15. RELACIONES CON SUMINISTRADORES.**
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en teonologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

**16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.**
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

**17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.**
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

**18. CUMPLIMIENTO.**
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.



Octubre-2013

## ANEXO 3: ENCUESTA COORDINADOR DE GESTIÓN TECNOLÓGICA DE LA UNIDAD EDUCATIVA BORJA 3 CAVANIS

**Entrevista para el responsable del área de gestión tecnológica de la unidad educativa Borja 3 Cavanis, que permitirá explorar los aspectos de la seguridad informática en la institución**

Nombre: Juan Miguel García
Edad: 43 Sexo: M Puesto: Coordinador de Gest. Tecnológica

**Instrucciones: Conteste las siguientes preguntas.**

1) ¿Cuándo inicio a trabajar en la Unidad Educativa Borja 3 Cavanis?
- En noviembre del 2014

2) ¿Qué tipo de problemas en seguridad informática son más comunes?
- Acceso a sitios no deseados.

3) ¿Qué tipo de herramientas informáticas utiliza para prevenir fugas o pérdidas de información?
- Windows Defender.

4) ¿Qué tipo de pérdidas de información son más comunes en la Unidad Educativa Borja 3 Cavanis?
- Registros de Notas y reportes académicos.

5) La Unidad Educativa Borja 3 Cavanis ¿tiene normas o políticas de seguridad de la información?
- Si pero son normas básicas.

6) ¿Cuáles son las áreas de la Unidad Educativa Borja 3 Cavanis en las que más cuidado se debe de tener en cuestión de la seguridad de la información?
- En secretaría docente; acceso al sistema académico y contable

7) ¿Describa cuáles son los filtros que se utiliza para que personas extrañas no puedan ver información importante en el lugar de trabajo?
- Acceso através de contraseñas protejidas y roles de usuarios

8) ¿Ha tenido problemas graves en fuga de la información de su Institución describe cuáles?
- No muy graves

9) ¿Considera que para la Unidad Educativa Borja 3 Cavanis le hace falta invertir más en seguridad informática?
- Si para poder segmentar la red y aplicar zonas específicas

10) ¿Con que frecuencia respalda la información de los usuarios de la Unidad Educativa Borja 3 Cavanis?
- Cada noche

11) ¿Cómo te proteges de la inseguridad informatica?
- A través de cortafuegos y niveles de accesos

12) ¿Has tenido problemas con la información de los usuarios de Institución a causa de virus?
- Si, pero no muy desastrozas, por la falta de actualizaciones

13) ¿Has tomado medidas para evitar qué ocurra de nuevo indique cuáles?
- Si se han tomado medidas.

14) ¿Crees que se encuentra segura la información que contiene internet?

15) ¿El área de gestión tecnológica de la Unidad educativa Borja 3 Cavanis, posee un manual de políticas de seguridad de la información?

- No

16) ¿Existen procedimientos establecidos en el área de gestión tecnológica con los respectivos responsables y estos procesos se encuentran documentados?

- En un 50%

17) ¿Tiene instalado un antivirus en los equipos de computación?

- Si el básico que trae el SO win 10

18) ¿Qué mecanismos de autenticación para los usuarios de la Institución utiliza?

- Credenciales de acceso usuarios estándar

19) ¿Mantiene un registro de fallas cuando ocurre algún evento en servidores, computadores o en la red?

- 50%

20) ¿Se utiliza mecanismo de bloqueo automatico de las estaciones de trabajo de los usuarios cuando se encuentran ausentes?

- Si pasado 20 min

MSc. Miguel García
Coordinador del área de Gestión Tecnológica
Unidad Educativa Borja 3 Cavanis

Ing. Israel Cárdenas
1723886212