# TFM SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN


**FABIO HERNÁN PORRAS NIÑO**

**DIRECTOR:**
**ANTONIO JOSÉ SEGOVIA HERNARES**

**UNIVERSIDAD OBERTA DE CATALUNYA**
**JUNIO DE 2018**

## Tabla de contenido

## Índice de Tablas

## Índice de Imágenes

**Índice de Anexos**

# 1. Introducción

Actualmente las Instituciones Educativas no son ajenas al vertiginoso crecimiento de las tecnologías de la información y las comunicaciones, y en tal sentido, realizan grandes esfuerzos económicos que les permitan un posicionamiento estratégico en el mercado que redunde en la atracción de nueva población estudiantil y en alto grado de satisfacción de los actuales alumnos y del personal que labora en torno a la Institución.

Así las cosas, los procesos actuales en un Colegio con carácter de bachillerato internacional en Colombia, son forjados, gestionados, administrados y usados gracias a sistemas informáticos, que permiten la interacción de la comunidad (estudiantes, padres de familia y colaboradores) accediendo a dichos sistemas con la posibilidad de consultar, realizar pagos y modificar información sin importar la ubicación geográfica. Lo anterior, representa grandes ventajas para quienes hacen uso de dichos sistemas de información, pero a su vez, representa grandes retos en cuento al aseguramiento de la información que se dispone ya que se debe garantizar sus atributos principales, es decir, la Confidencialidad, Integridad, Disponibilidad, Autenticidad y no repudio y la Trazabilidad de la información.

Dicho lo anterior, es necesaria la implementación de una metodología que represente la mejor opción para la consecución de un Sistema de Gestión de seguridad de la información que establezca unos niveles aceptables para el aseguramiento de la información que maneja toda la comunidad.

## 1.1. Planteamiento del Problema

La normatividad colombiana establece la regulación y el tratamiento de datos personales y por ende obliga en este caso a la Institución Educativa, a velar por su protección. Lo anterior cobra relevancia en tanto la comunidad está compuesta principalmente por menores de edad. De esta forma, es necesaria la implementación de una estrategia que permita el aseguramiento de la información.

Dicho lo anterior, y teniendo en cuenta que el Colegio ha implementado un sistema de gestión de calidad que le permitió la certificación del servicio de educación formal en todos sus niveles, bajo la norma ISO 9001:2008, la norma internacional ISO/IEC 27001:2013 sigue los estándares de calidad establecidos en la institución y constituye certificación bajo un modelo relevante para el Colegio que permita la implementación del SGSI-Sistema de Gestión de Seguridad de la Información. Dichas certificaciones otorgan un valor agregado a la Institución de cara a la competencia u otras ofertas educativas, ya que establece compromisos institucionales que, para este caso, fija en

torno a la información.

En tal caso, la implementación del SGSI debe estar concebida bajo el establecimiento inicial del estado actual en el que se encuentra el Colegio, que permita la realización de fases metódicas que conlleven a su consolidación e implementación, fijando como premisa el establecimiento de los riesgos y la fijación de estos en niveles aceptables por la Institución.

## 1.2. Alcance del Plan Director

Tomando como base el sistema de gestión de calidad certificado en la institución, se establece la necesidad de implementar el sistema de Gestión de Seguridad de la información y la consecución de la certificación ISO 27001. Así las cosas, con el Plan Director se establece la importancia de efectuar el análisis de riesgos asociados a los activos del Colegio en cuyo caso, se deberán identificar y cuantificar el impacto en caso de ser materializado. Así mismo, establecer un plan de acción que contrarreste el impacto mencionado y la evaluación del impacto residual de dicho plan. De igual forma, y basados en la ISO 27002:2013, se fijarán planes a desarrollar que permitan una posterior certificación.

Dicho lo anterior, el alcance del plan director estará ligado con el alcance del sistema de gestión de calidad existente en la institución, el cual abarca la totalidad de los procesos que enmarcan el funcionamiento diario del Colegio.

En consecuencia, la certificación ISO 27001:2013 por parte de entidad avalada para tal fin, no hace parte del presente trabajo.

## 1.3. Objetivos del Plan Director

### Objetivo General

Establecer el Plan Director de Seguridad para el Colegio, basado y alineado con los estándares ISO 27001:2013 y 27002 y la metodología de Análisis y Gestión de Riesgos MAGERIT. Así mismo, fijar las bases para la implementación del SGSI buscando la mejora continua.

### Objetivos Específicos

- Identificar el estado actual de la Seguridad de la información del Colegio en torno al cumplimiento de las normas ISO 27001 e ISO 27002 de 2013.
- Revisar la normatividad vigente en seguridad de la información aplicable al colegio y el grado de cumplimiento.

- Establecer los activos críticos del colegio en relación con la seguridad de la información.
- Revisar el grado de cumplimiento del Colegio en torno a la normatividad colombiana en relación con la seguridad de la información.
- Proponer la Política de Seguridad del Colegio.
- Realizar un análisis y gestión de Riesgos basados en la metodología MAGERIT.
- Definir los roles y responsabilidades de los activos.
- Identificar el impacto en caso de pérdida de confidencialidad, integridad y disponibilidad para cada activo.
- Identificar salvaguardas o controles que permitan establecer planes de acción para la mitigación de los riesgos identificados.
- Establecer una auditoria de cumplimiento basado en los controles de la norma ISO 27001:2013

## 1.4. Metodología

La metodología para desarrollar el plan director de seguridad que permita la posterior implementación del Sistema de Gestión de Seguridad de la Información está enmarcada en una serie de fases consecutivas que permitan la consecución de los objetivos fijados. En tal sentido, la institución es consciente de su gran responsabilidad en torno a la implementación de este tipo de medidas que le permita en un futuro recibir la certificación en la materia y constituir elementos diferenciales de cara a la competencia en el mercado.

Así las cosas, tenemos las siguientes fases:

- Fase 1: Situación actual: Contextualización, objetivos y análisis diferencial
- Fase 2: Sistema de Gestión Documental
- Fase 3: Análisis de riesgos
- Fase 4: Propuesta de Proyectos
- Fase 5: Auditoría de Cumplimiento de la ISO/IEC 27002:2013
- Fase 6: Presentación de Resultados y entrega de Informes

## 1.5. Normatividad

Como se ha mencionado previamente, la Seguridad de la Información está tomando día a día más relevancia y en tal sentido, es indispensable fijar metodologías y buenas prácticas acordes que nos permitan el óptimo aseguramiento de los sistemas de información. Dicho lo anterior, las normas ISO/IEC 27000, representan un compendio

de estándares publicados por la Organización Internacional de Estandarización ISO y la Comisión Internacional Electrotécnica IEC. Está familia de normas son principalmente:

| Normatividad | Descripción[1] |
|---|---|
| ISO/IEC 27000 | Proporciona una visión general del compendio de normas contenidas en la serie 27000. |
| ISO/IEC 27001 | Comprende los requisitos necesarios para la implementación de un SGSI. |
| ISO/IEC 27002 | Es la guía de buenas prácticas con los objetivos y controles recomendados para la seguridad de la información. |
| ISO/IEC 27003 | Representa la guía para el diseño e implementación del SGSI. |
| ISO/IEC 27004 | Guía para el desarrollo de métricas para determinar la eficacia de un SGSI. |
| ISO/IEC 27005 | Otorga directrices para le gestión del riesgo de la Seguridad de la Información. |
| ISO/IEC 27006 | Determina los requisitos para la acreditación de las diferentes entidades de auditoria y certificación de SGSI. |
| ISO/IEC 27007 | Guía para realizar auditorías de un SGSI. |
| ISO/IEC 27008 | Guía de auditoria de controles apropiados en la implantación del SGSI. |
| ISO/IEC 27016 | Guía para realizar la valoración financiera de la seguridad de la información. |
| ISO/IEC 27017 | Guía para cloud computing y controles en torno a la nube. |
| ISO/IEC 27035 | Proporciona una guía para la gestión de incidentes de seguridad de la información. |
| ISO/IEC 27040 | Concentra especificaciones para la seguridad en medios de almacenamiento. |

***Tabla 1 Principales* normas *de la familia 27000***

Visto lo anterior, la norma ISO/IEC 27002:2013 cobra especial relevancia para la elaboración del plan director de Seguridad para la Institución y para la posterior certificación a través de la ISO/IEC 27001:2013. Por lo anterior, profundizaremos un poco más en ellas.

[1] Consultado en: http://www.iso27000.es/iso27000.html, el 1 de marzo de 2018, a las 10.45 p.m.

### 1.5.1. ISO/IEC 27001:2013

La ISO/IEC 27001:2013, es una norma internacional emitida por la Organización Internacional de Normalización ISO. Esta norma fue publicada el 15 de octubre del año 2005 y posteriormente revisada el 25 de septiembre de 2013. Ésta norma, se elaboró con el fin de conceder los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información[2].

La norma, plantea 10 capítulos que promueven el mejoramiento continuo bajo el enfoque del análisis PHVA o ciclo Deming, que permite fijar la calidad de los sistemas desarrollados con el enfoque de la ISO. Así las cosas, tenemos:


***Imagen 1 ISO/IEC 27001, basada en el ciclo PHVA.***

[2] Consultado en: https://tienda.icontec.org/producto/e-book-ntc-iso-iec27001-tecnologia-de-la-informacion-tecnicas-de-seguridad-sistemas-de-gestion-de-la-seguridad-de-la-informacion-requisitos/?v=42983b05e2f2, el 10 de marzo de 2018, a las 9.35 p.m.

La ISO/IEC 27001:2013, permite a las diferentes compañías, públicas o privadas, grandes o pequeñas, a través de una Entidad certificadora, obtener la confirmación de que se ha gestionado de manera correcta a través del cumplimiento de la norma, la certificación internacional correspondiente a la ISO/IEC 27001:2013.

### 1.5.2. ISO/IEC 27002:2013

Permite establecer bases transversales para desarrollar[3]:

- Normatividad de seguridad en la organización.
- Prácticas efectivas de gestión de seguridad.
- Confianza en interacciones con terceras empresas.

La norma ISO/IEC 27002:2013, fue concebida como referencia para establecer controles a la hora de implementar un Sistema de gestión de seguridad de la información, basada en la norma ISO/IEC 27001:2013. La norma fue publicada inicialmente como un cambio a la norma ISO 17799:2005 que se estableció como estándar en el año 1995. En la versión de la norma publicada en el año 2005, la ISO/IEC 27002, compilaba 11 dominios, bajo 33 objetivos de control y 133 controles, pero con la revisión posterior del año 2013, la ISO/IEC 27002, restructuró su estrategia a un total de 14 dominios, 35 objetivos de control y 114 controles.

## 1.6. Contextualización

Para la elaboración del plan director de seguridad, se escogió una Institución Educativa, la cual posee aproximadamente 800 estudiantes, 100 docentes y cerca de 200 colaboradores en el área administrativa. El colegio cuenta con 90 años de existencia en una única sede ubicada en la ciudad de Bogotá.

El colegio cuenta con la certificación del Sistema de gestión integrado en calidad y seguridad y salud en el trabajo, ISO 9001:2008, entregada por la Entidad certificadora INCONTEC. Siendo una de las primeras instituciones educativas en Colombia en hacerse acreedora a dicha certificación. Actualmente se están adelantando las actividades pertinentes que permitan alcanzar a finales del presente año, la recertificación ISO 9001 en su versión 2015. En consecuencia, la posterior consecución de la certificación internacional ISO/IEC 27001:2013, cobra especial relevancia de cara a un futuro.

No obstante, la Seguridad de la Información está en una fase inicial, ya que no se cuenta con un plan director para tal fin, pero se cuenta con la voluntad de la alta

[3] Garre Gui S. Implementación de un Sistema de gestión de la seguridad de la información (SGSI). UOC.

dirección y el apoyo necesario para que se dé inicios en la materia. Dicho lo anterior, cabe resaltar que la infraestructura tecnológica de la Institución no cuenta con soluciones dedicadas o especializadas que permitan una óptima gestión de la Seguridad de la información, por lo que es indispensable que dicho plan director permita enfocar de la mejor manera, un plan para la consolidación de la plataforma tecnológica del Colegio.

## 1.7. Análisis Diferencial

Para la elaboración del análisis diferencial se realizó una serie de entrevistas a fin de conocer el estado actual y contrastar la información entregada por las partes, en tal sentido, se revisó la documentación pertinente con las áreas de calidad y tecnología, que permitieron realizar un análisis diferencial.

El modelo de madurez empleado para obtener los valores descritos en el análisis diferencial ISO/IEC 27001:2013 e ISO/IEC 27002:2013, son los definidos por Control Objetives for Information and related Technology COBIT, y basado a su vez en el Capability Marurity Model CMM, realizado por la Carnegie Mellon School. Así las cosas, tenemos[4]:

| Valor | Evaluación | Prácticas de Gestión IT | Impacto sobre el negocio |
|---|---|---|---|
| 5 | Optimizado | Los procesos han sido revisados hasta un nivel de “best practice”, sobre la base de una mejora continua. | Las IT son utilizadas de manera integrada para automatizar los workflows, proporcionando herramientas para mejorar la calidad y eficiencia, haciendo que la organización se adapte rápidamente. |
| 4 | Gestionado | Los procesos están en mejora continua y proporcionan mejores prácticas. Se usan herramientas automatizadas de manera aislada o fragmentada. | Es posible monitorizar y medir el cumplimiento con los procedimientos y tomar medidas cuando los procesos no funcionan de manera efectiva. |

[4] Consultado en: http://cv.uoc.edu/webapps/xwiki/wiki/matm1709/view/Main/An%C3%A1lisis+diferencial#Attachments, el 2 de marzo de 2018 a las 2.10 a.m.

| | | | |
|---|---|---|---|
| 3 | Definido | La organización asegura que control se planifica, documenta, ejecuta, monitoriza y controla. | Se deja a discreción del usuario seguir procedimientos y es probable que no se detecten desviaciones respecto a los mismos. |
| 2 | Repetible | Los procesos han evolucionado de forma que se siguen procedimientos similares para realizar la misma tarea. No existe formación ni comunicación de procedimientos estándar y la responsabilidad recae en el individuo. | Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son probables. |
| 1 | Inicial | No existen procesos estándar, aunque si planteamientos "ad hoc" que se utilizan en cada situación. | Existe evidencia de que la organización ha reconocido que debe contemplar la seguridad. |
| 0 | No existente | Ausencia total de procesos reconocibles. | La organización no es consciente de que debe gestionar la seguridad. |

**Tabla 2 Modelo de madurez para establecer la valoración de los controles.**

Así las cosas, el cumplimiento actual de la institución en torno a la norma ISO 27001:2013 es la siguiente:

| CONTROL | Evaluación | Valor | Total |
|---|---|---|---|
| 4. Contexto de la Organización | | | 0 |
| 4.1 Conocimiento de la Organización y su contexto | No existente | 0 | |
| 4.2 Comprensión de las necesidades y expectativas de las partes interesadas | No existente | 0 | |
| 4.3 Determinación del alcance del SGSI | No existente | 0 | |
| 4.4 Sistema de Gestión de Seguridad de la Información. | No existente | 0 | |
| 5. Liderazgo | | | 1 |
| 5.1 Liderazgo y compromiso | Definido | 3 | |
| 5.2 Política | Inicial | 1 | |
| 5.3 Roles, Responsabilidades y autoridades en la organización | No existente | 0 | |

| | | | | |
|---|---|---|---|---|
| 6. Planificación | | | | 0 |
| | 6.1 Acciones para tratar riesgos y oportunidades | No existente | 0 | |
| | 6.2 Objetivos de la seguridad de la información | No existente | 0 | |
| 7. Soporte | | | | 0 |
| | 7.1 Recursos | No existente | 0 | |
| | 7.2 Competencia | No existente | 0 | |
| | 7.3 Toma de conciencia | No existente | 0 | |
| | 7.4 Comunicación | No existente | 0 | |
| | 7.5 Información documentada | No existente | 0 | |
| 8. Operación | | | | 0 |
| | 8.1 Planificación y control operacional | No existente | 0 | |
| | 8.2 Evaluación de riesgos de la seguridad de la información | No existente | 0 | |
| | 8.3 Tratamiento de riesgos de seguridad de la información | No existente | 0 | |
| 9. Evaluación de desempeño | | | | 0 |
| | 9.1 Seguimiento, medición, análisis y evaluación. | No existente | 0 | |
| | 9.2 Auditoría interna | No existente | 0 | |
| | 9.3 Revisión por la dirección | No existente | 0 | |
| 10. Mejora | | | | 1 |
| | 10.1 No conformidades y acciones correctivas | Inicial | 1 | |
| | 10.2 Mejora continua | No existente | 0 | |

**Tabla 3 Cumplimiento de la norma ISO/IEC 27001:2013**

Debido a que no se cuenta con un Sistema de Gestión de Seguridad de la Información, el grado de cumplimiento es muy bajo, sin embargo, se ve que el apartado de liderazgo y de mejora, tienen algún trabajo asociado, como se observa a continuación:

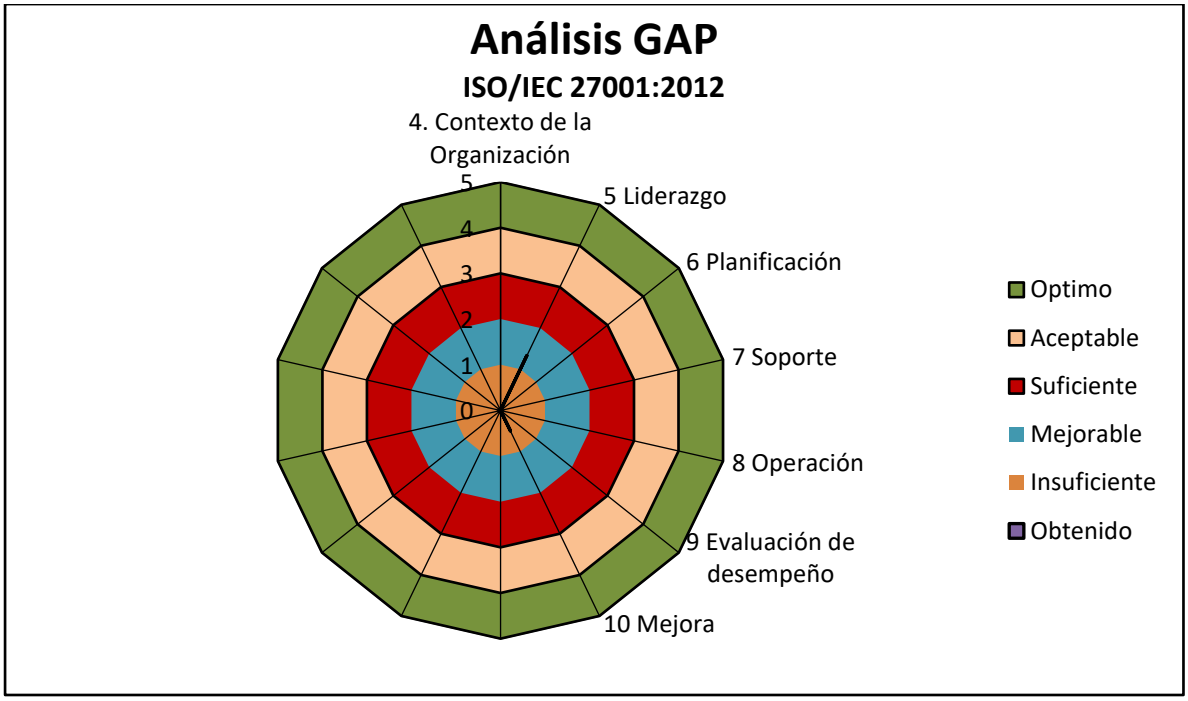


**Imagen 2 Análisis GAP, cumplimiento ISO/IEC 27001:2013**

De igual forma tenemos que en[5] base a los dominios, objetivos de control y controles de la norma ISO/IEC 27002:2013, el estado actual de la institución es:

| CONTROL | | Evaluación | Valor | Total |
|---|---|---|---|---|
| **5. POLÍTICAS DE SEGURIDAD.** | | | | 0 |
| 5.1 Directrices de la Dirección en seguridad de la información. | | | | 0 |
| | 5.1.1 Conjunto de políticas para la seguridad de la información. | No existente | 0 | |
| | 5.1.2 Revisión de las políticas para la seguridad de la información. | No existente | 0 | |
| **6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN** | | | | 0 |
| 6.1 Organización interna. | | | | 0 |
| | 6.1.1 Asignación de responsabilidades para la seguridad de la información. | No existente | 0 | |
| | 6.1.2 Segregación de tareas. | No existente | 0 | |
| | 6.1.3 Contacto con las autoridades. | No existente | 0 | |

[5] Tomada de: http://cv.uoc.edu/webapps/xwiki/wiki/matm1709/view/Main/Análisis+diferencial#Attachments, el 2 de marzo de 2018 a la 1.12 a.m.

| | | | | | |
|---|---|---|---|---|---|
| | | 6.1.4 Contacto con grupos de interés especial. | No existente | 0 | |
| | | 6.1.5 Seguridad de la información en la gestión de proyectos. | No existente | 0 | |
| | 6.2 Dispositivos para movilidad y teletrabajo. | | | | 0 |
| | | 6.2.1 Política de uso de dispositivos para movilidad. | No existente | 0 | |
| | | 6.2.2 Teletrabajo. | No existente | 0 | |
| **7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.** | | | | | 1 |
| | 7.1 Antes de la contratación. | | | | 3 |
| | | 7.1.1 Investigación de antecedentes. | Gestionado | 4 | |
| | | 7.1.2 Términos y condiciones de contratación. | Inicial | 1 | |
| | 7.2 Durante la contratación. | | | | 0 |
| | | 7.2.1 Responsabilidades de gestión. | No existente | 0 | |
| | | 7.2.2 Concienciación, educación y capacitación en seguridad de la información | No existente | 0 | |
| | | 7.2.3 Proceso disciplinario. | No existente | 0 | |
| | 7.3 Cese o cambio de puesto de trabajo. | | | | 0 |
| | | 7.3.1 Cese o cambio de puesto de trabajo. | No existente | 0 | |
| **8. GESTIÓN DE ACTIVOS.** | | | | | 0 |
| | 8.1 Responsabilidad sobre los activos. | | | | 1 |
| | | 8.1.1 Inventario de activos. | No existente | 0 | |
| | | 8.1.2 Propiedad de los activos. | Inicial | 1 | |
| | | 8.1.3 Uso aceptable de los activos. | No existente | 0 | |
| | | 8.1.4 Devolución de activos. | Inicial | 1 | |
| | 8.2 Clasificación de la información. | | | | 0 |
| | | 8.2.1 Directrices de clasificación. | No existente | 0 | |
| | | 8.2.2 Etiquetado y manipulado de la información. | No existente | 0 | |
| | | 8.2.3 Manipulación de activos. | No existente | 0 | |
| | 8.3 Manejo de los soportes de almacenamiento. | | | | 0 |
| | | 8.3.1 Gestión de soportes extraíbles. | | 0 | |
| | | 8.3.2 Eliminación de soportes. | | 0 | |

| | | | | |
|---|---|---|---|---|
| | 8.3.3 Soportes físicos en tránsito. | | 0 | |
| **9. CONTROL DE ACCESOS.** | | | | 0 |
| 9.1 Requisitos de negocio para el control de accesos. | | | | 1 |
| | 9.1.1 Política de control de accesos. | Inicial | 1 | |
| | 9.1.2 Control de acceso a las redes y servicios asociados. | Inicial | 1 | |
| 9.2 Gestión de acceso de usuario. | | | | 0 |
| | 9.2.1 Gestión de altas/bajas en el registro de usuarios. | No existente | 0 | |
| | 9.2.2 Gestión de los derechos de acceso asignados a usuarios. | No existente | 0 | |
| | 9.2.3 Gestión de los derechos de acceso con privilegios especiales. | No existente | 0 | |
| | 9.2.4 Gestión de información confidencial de autenticación de usuarios. | No existente | 0 | |
| | 9.2.5 Revisión de los derechos de acceso de los usuarios. | No existente | 0 | |
| | 9.2.6 Retirada o adaptación de los derechos de acceso | No existente | 0 | |
| 9.3 Responsabilidades del usuario. | | | | 0 |
| | 9.3.1 Uso de información confidencial para la autenticación. | No existente | 0 | |
| 9.4 Control de acceso a sistemas y aplicaciones. | | | | 1 |
| | 9.4.1 Restricción del acceso a la información. | Inicial | 1 | |
| | 9.4.2 Procedimientos seguros de inicio de sesión. | Inicial | 1 | |
| | 9.4.3 Gestión de contraseñas de usuario. | Inicial | 1 | |
| | 9.4.4 Uso de herramientas de administración de sistemas. | No existente | 0 | |
| | 9.4.5 Control de acceso al código fuente de los programas. | No existente | 0 | |
| **10. CIFRADO.** | | | | 1 |
| 10.1 Controles criptográficos. | | | | 1 |
| | 10.1.1 Política de uso de los controles criptográficos. | No existente | 0 | |
| | 10.1.2 Gestión de claves. | Inicial | 1 | |
| **11. SEGURIDAD FÍSICA Y AMBIENTAL.** | | | | 1 |
| 11.1 Áreas seguras. | | | | 1 |

| | | | | | |
|---|---|---|---|---|---|
| | | 11.1.1 Perímetro de seguridad física. | Inicial | 1 | |
| | | 11.1.2 Controles físicos de entrada. | Inicial | 1 | |
| | | 11.1.3 Seguridad de oficinas, despachos y recursos. | Repetible | 2 | |
| | | 11.1.4 Protección contra las amenazas externas y ambientales. | Repetible | 2 | |
| | | 11.1.5 El trabajo en áreas seguras. | Inicial | 1 | |
| | | 11.1.6 Áreas de acceso público, carga y descarga. | Inicial | 1 | |
| | 11.2 Seguridad de los equipos. | | | | 1 |
| | | 11.2.1 Emplazamiento y protección de equipos. | Inicial | 1 | |
| | | 11.2.2 Instalaciones de suministro. | Inicial | 1 | |
| | | 11.2.3 Seguridad del cableado. | No existente | 0 | |
| | | 11.2.4 Mantenimiento de los equipos. | Inicial | 1 | |
| | | 11.2.5 Salida de activos fuera de las dependencias de la empresa. | No existente | 0 | |
| | | 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones. | Repetible | 2 | |
| | | 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento. | No existente | 0 | |
| | | 11.2.8 Equipo informático de usuario desatendido. | No existente | 0 | |
| | | 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla. | No existente | 0 | |
| **12. SEGURIDAD EN LA OPERACIONES** | | | | | 1 |
| | 12.1 Responsabilidades y procedimientos de operación. | | | | 0 |
| | | 12.1.1 Documentación de procedimientos de operación. | No existente | 0 | |
| | | 12.1.2 Gestión de cambios. | No existente | 0 | |
| | | 12.1.3 Gestión de capacidades. | No existente | 0 | |
| | | 12.1.4 Separación de entornos de desarrollo, prueba y producción. | Inicial | 1 | |
| | 12.2 Protección contra código malicioso. | | | | 1 |
| | | 12.2.1 Controles contra el código malicioso. | Inicial | 1 | |
| | 12.3 Copias de seguridad. | | | | 2 |

| | | | | |
|---|---|---|---|---|
| | 12.3.1 Copias de seguridad de la información. | Repetible | 2 | |
| 12.4 Registro de actividad y supervisión. | | | | 1 |
| | 12.4.1 Registro y gestión de eventos de actividad. | No existente | 0 | |
| | 12.4.2 Protección de los registros de información. | No existente | 0 | |
| | 12.4.3 Registros de actividad del administrador y operador del sistema. | No existente | 0 | |
| | 12.4.4 Sincronización de relojes. | Definido | 3 | |
| 12.5 Control del software en explotación. | | | | 2 |
| | 12.5.1 Instalación del software en sistemas en producción. | Repetible | 2 | |
| 12.6 Gestión de la vulnerabilidad técnica. | | | | 1 |
| | 12.6.1 Gestión de las vulnerabilidades técnicas. | No existente | 0 | |
| | 12.6.2 Restricciones en la instalación de software. | Repetible | 2 | |
| 12.7 Consideraciones de las auditorías de los sistemas de información. | | | | 0 |
| | 12.7.1 Controles de auditoría de los sistemas de información. | No existente | 0 | |
| **13. SEGURIDAD EN LAS TELECOMUNICACIONES.** | | | | 1 |
| 13.1 Gestión de la seguridad en las redes. | | | | 1 |
| | 13.1.1 Controles de red. | Inicial | 1 | |
| | 13.1.2 Mecanismos de seguridad asociados a servicios en red. | Inicial | 1 | |
| | 13.1.3 Segregación de redes. | Repetible | 2 | |
| 13.2 Intercambio de información con partes externas. | | | | 0 |
| | 13.2.1 Políticas y procedimientos de intercambio de información. | No existente | 0 | |
| | 13.2.2 Acuerdos de intercambio. | No existente | 0 | |
| | 13.2.3 Mensajería electrónica. | No existente | 0 | |
| | 13.2.4 Acuerdos de confidencialidad y secreto. | No existente | 0 | |
| **14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.** | | | | 0 |
| 14.1 Requisitos de seguridad de los sistemas de información. | | | | 1 |
| | 14.1.1 Análisis y especificación de los requisitos de seguridad. | No existente | 0 | |

| | | | | |
|---|---|---|---|---|
| | 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas. | Repetible | 2 | |
| | 14.1.3 Protección de las transacciones por redes telemáticas. | No existente | 0 | |
| 14.2 Seguridad en los procesos de desarrollo y soporte. | | | | 0 |
| | 14.2.1 Política de desarrollo seguro de software. | No existente | 0 | |
| | 14.2.2 Procedimientos de control de cambios en los sistemas. | No existente | 0 | |
| | 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. | No existente | 0 | |
| | 14.2.4 Restricciones a los cambios en los paquetes de software. | No existente | 0 | |
| | 14.2.5 Uso de principios de ingeniería en protección de sistemas. | No existente | 0 | |
| | 14.2.6 Seguridad en entornos de desarrollo. | No existente | 0 | |
| | 14.2.7 Externalización del desarrollo de software. | Inicial | 1 | |
| | 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas. | No existente | 0 | |
| | 14.2.9 Pruebas de aceptación. | No existente | 0 | |
| 14.3 Datos de prueba. | | | | 0 |
| | 14.3.1 Protección de los datos utilizados en pruebas. | No existente | 0 | |
| **15. RELACIONES CON SUMINISTRADORES.** | | | | 0 |
| 15.1 Seguridad de la información en las relaciones con suministradores. | | | | 0 |
| | 15.1.1 Política de seguridad de la información para suministradores. | No existente | 0 | |
| | 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores. | No existente | 0 | |
| | 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones. | No existente | 0 | |
| 15.2 Gestión de la prestación del servicio por suministradores. | | | | 0 |
| | 15.2.1 Supervisión y revisión de los servicios prestados por terceros. | No existente | 0 | |

| | | | | | |
|---|---|---|---|---|---|
| | | 15.2.2 Gestión de cambios en los servicios prestados por terceros. | No existente | 0 | |
| **16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.** | | | | | 0 |
| | 16.1 Gestión de incidentes de seguridad de la información y mejoras. | | | | 0 |
| | | 16.1.1 Responsabilidades y procedimientos. | No existente | 0 | |
| | | 16.1.2 Notificación de los eventos de seguridad de la información. | No existente | 0 | |
| | | 16.1.3 Notificación de puntos débiles de la seguridad. | No existente | 0 | |
| | | 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones. | No existente | 0 | |
| | | 16.1.5 Respuesta a los incidentes de seguridad. | No existente | 0 | |
| | | 16.1.6 Aprendizaje de los incidentes de seguridad de la información. | No existente | 0 | |
| | | 16.1.7 Recopilación de evidencias. | No existente | 0 | |
| **17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.** | | | | | 0 |
| | 17.1 Continuidad de la seguridad de la información. | | | | 0 |
| | | 17.1.1 Planificación de la continuidad de la seguridad de la información. | No existente | 0 | |
| | | 17.1.2 Implantación de la continuidad de la seguridad de la información. | No existente | 0 | |
| | | 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. | No existente | 0 | |
| | 17.2 Redundancias. | | | | 0 |
| | | 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información. | No existente | 0 | |
| **18. CUMPLIMIENTO.** | | | | | 0 |
| | 18.1 Cumplimiento de los requisitos legales y contractuales. | | | | 0 |
| | | 18.1.1 Identificación de la legislación aplicable. | No existente | 0 | |
| | | 18.1.2 Derechos de propiedad intelectual (DPI). | No existente | 0 | |
| | | 18.1.3 Protección de los registros de la organización. | No existente | 0 | |

| | | | | | |
|---|---|---|---|---|---|
| | | 18.1.4 Protección de datos y privacidad de la información personal. | No existente | 0 | |
| | | 18.1.5 Regulación de los controles criptográficos. | No existente | 0 | |
| | 18.2 Revisiones de la seguridad de la información. | | | | 0 |
| | | 18.2.1 Revisión independiente de la seguridad de la información. | No existente | 0 | |
| | | 18.2.2 Cumplimiento de las políticas y normas de seguridad. | No existente | 0 | |
| | | 18.2.3 Comprobación del cumplimiento. | No existente | 0 | |

**Tabla 4 Dominios, objetivos de control y controles ISO/IEC 27002:2013**

Como se puede apreciar, los controles aplicables a la norma ISO/IEC 27002:2013 existentes en la Institución, son mínimos y por ello la importancia de realizar el plan director correspondiente. En consecuencia, podemos observar:

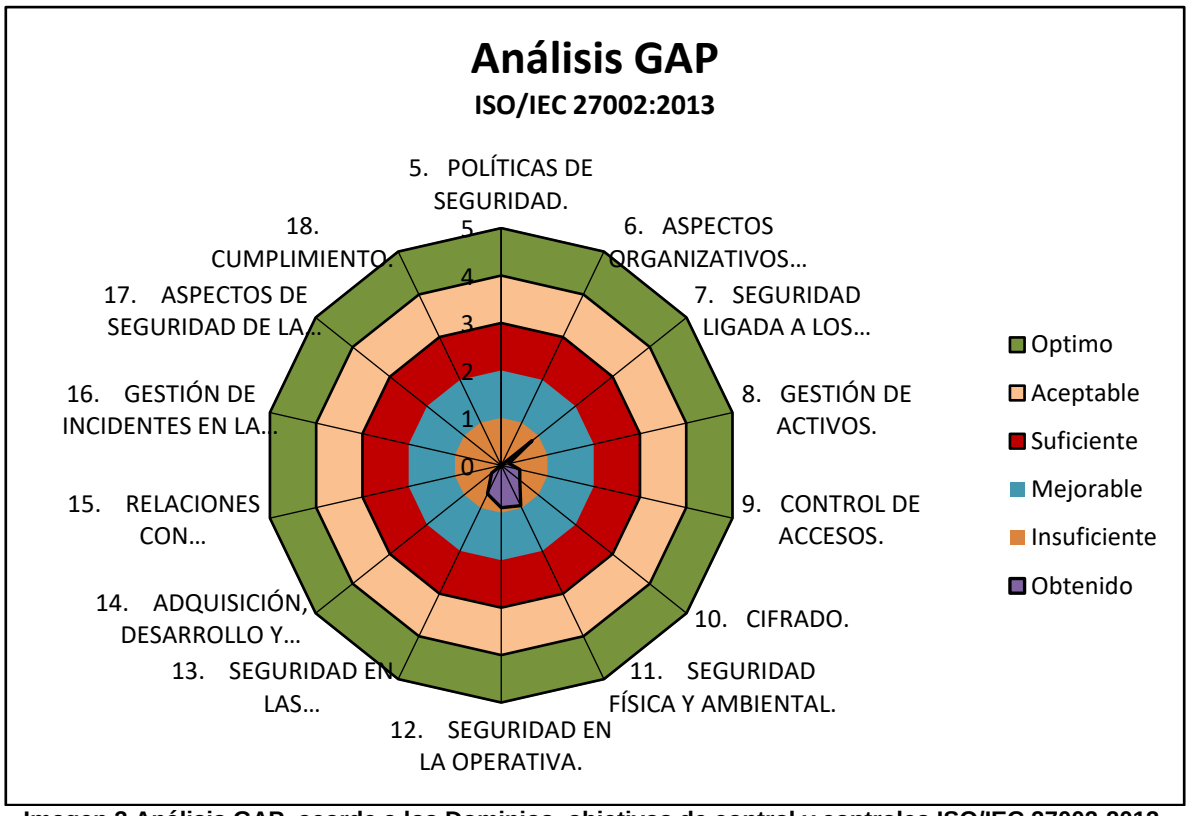


**Imagen 3 Análisis GAP, acorde a los Dominios, objetivos de control y controles ISO/IEC 27002:2013**

## 2. Sistema de Gestión Documental

### 2.1. Esquema Documental

Todo Sistema de Seguridad de la información debe contar con una serie de documentos establecidos en la norma ISO/IEC 27001:2013. En tal sentido, dichos documentos conformarán el plan director de la Institución así:

- Política de Seguridad
- Procedimiento de Auditorías Internas
- Gestión de Indicadores
- Procedimiento Revisión por Dirección
- Gestión de Roles y Responsabilidades
- Metodología de Análisis y Riesgos
- Declaración de Aplicabilidad

En tal sentido, revisaremos el estado de los documentos citados anteriormente y su correspondiente consolidación, acorde al entorno institucional del interior del Colegio.

### 2.2. Política de Seguridad

En el colegio no se encuentra definida la Política de Seguridad, por tal motivo, se adelantan las acciones necesarias para su consolidación. Para lo anterior, nos fijaremos en la norma ISO/IEC 27001:2013 y en lo lineamientos planteados por el Ministerio de Tecnologías de la Información y las Comunicaciones del Gobierno Nacional Colombiano, denominado MINTIC, según Decreto 1078 de 2015[6], para la elaboración de la Política General de Seguridad de la información del Colegio, la cual se describe en el ANEXO 1. POLÍTICA GENERAL DE SEGURIDAD DEL COLEGIO.

### 2.3. Procedimientos de Auditorías Internas

Aunque la cultura de las auditorías internas hace parte de la Institución, las mismas no se tienen estimadas en relación con el SGSI ya que no está implementado aún. Sin embargo, basados en los procesos adelantados para revisar el sistema de gestión de calidad, se optará por plan de auditorías internas, planeadas y periódicas para verificar si el SGSI implementado con posterioridad, cumple con los requisitos establecidos en la norma ISO/IEC 27001:2013. De esta manera, el cumplimiento estará clasificado de la siguiente manera:

- No conformidad Mayor: Representa la ausencia de cualquiera de los controles establecidos en la ISO17002. Por ejemplo, la ausencia del análisis de riesgos,

[6] Consultado en: http://www.mintic.gov.co/portal/604/articles-9528_documento.pdf, el 15 de marzo de 2018, a las 9.15 p.m.

ausencia de un plan de continuidad del negocio, entre otros.

- No conformidad menor: Se establece cuando no se tiene un punto de un determinado control del estándar.

- Observación: Si bien no constituye una no conformidad en ninguna de sus dos instancias presupone un tratamiento adecuado que permita superar en una próxima revisión el punto del detalle. Así las cosas, por ejemplo, la existencia de un control sin una adecuada comunicación o fijación representa un plan específico de cara a una próxima revisión, a expensas de constituirse en una no conformidad en caso de omisión.

- Oportunidades de mejora: Representa un tratamiento opcional que, de ninguna manera, a falta de implementarse se constituirá en una no conformidad. En tal sentido, se puede acoger como una recomendación o buena practica en pro del mejoramiento continuo, que la Entidad decide si opta o no.

De esta manera, se propone en el ANEXO 2. PROCEDIMIENTO DE AUDITORÍAS INTERNAS.

### 2.4. Gestión de Indicadores

Los indicadores son un conjunto de valores que se obtienen a través de la comparación de puntos de referencia. En tal sentido, el MINTIC, ha desarrollado una guía de indicadores que permite su uso para establecerla en el Sistema de Gestión de Seguridad de la Información de una Entidad pública o privada. Dicho lo anterior, nos basamos en los indicadores propuestos por El Ministerio de las Tecnologías de la Información y las Telecomunicaciones para el desarrollo de nuestro proyecto[7].

En consecuencia, los indicadores a evaluar son:

- A.7.2.2 Concienciación, educación y capacitación en seguridad de la información
- A.8.1.3 Uso aceptable de los activos
- A.11.1.2 Controles físicos de entrada
- A.12.6.1 Gestión de las vulnerabilidades técnicas
- A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

Los cuales se pueden revisar en el ANEXO 3. INDICADORES DE GESTIÓN.

[7] Consultado en: http://www.mintic.gov.co/gestionti/615/articles-5482_G9_Indicadores_Gestion_Seguridad.pdf, el 16 de marzo de 2018, a las 8.35 p.m.

## 2.5. Procedimiento Revisión por Dirección

La Norma ISO/IEC 27001:2013 en su numeral 9.3 Revisión por la Dirección, establece[8]:

- La alta dirección debe efectuar revisiones al Sistema de Gestión de Seguridad de la Información a intervalos planificados, con el fin de asegurar que su conveniencia, adecuación y eficacia, perduran en el tiempo.

- Las revisiones deben considerar los siguientes aspectos:

    - Estado de revisiones previas por la dirección y las acciones encaminadas en tal fin.
    - Posibles variaciones en el Colegio que impacten el Sistema de Gestión de Seguridad de la información.
    - Retroalimentación sobre el desempeño de la seguridad de la información.
    - Retroalimentación de los involucrados.
    - Resultados de la valoración de riesgos y el estado del plan de tratamiento de estos.
    - Revisión de las oportunidades de mejora.

- Se conserva la documentación en forma detallada del proceso de revisión.

- Como salidas de la revisión, la dirección da relevancia a las acciones pertinentes a cambios estratégicos y el mejoramiento continuo.

Las revisiones se efectuarán de forma anual, y posterior a la realización del plan de auditorías, con el fin de tener un insumo relevante y facilitador para la revisión por parte de la dirección. Lo anterior podrá modificarse en tanto se efectúen cambios sustanciales en los sistemas de información o procesos relevantes en la institución.

## 2.6. Gestión de Roles y Responsabilidades

La normatividad ISO 27001:2013, establece unos roles y responsabilidades en la organización, que a su vez deben velar por el cumplimiento de una serie de requerimientos, como:

- Se debe asegurar por parte de la dirección, la comunicación y asignación de roles en el interior de la institución.

- Asignar responsabilidades y empoderarlos para asegurar el buen desempeño del SGSI respecto a la normatividad.

- Asignar responsabilidades y empoderarlo para tener un interlocutor que informe

[8] Consultado en: https://www.pmg-ssi.com/norma-27001/9-3-revision-por-la-direccion/, el 16 de marzo de 2018, a las 9.45 p.m.

el grado de desempeño del Sistema de Gestión de Seguridad de la Información.

### 2.6.1. Roles

Se define la siguiente estructura que velará por el seguimiento del SGSI:


**Imagen 4 Conformación SGSI en la Institución**

## 2.7. Metodología de Análisis y Riesgos

Para el Plan Director del Colegio, se tomará como base la metodología MAGERIT, fue desarrollada por el Consejo Superior de Administración electrónica, como una metodología de análisis y gestión de riesgos de la información. Contiene dos pilares fundamentales, uno, se enfoca en estudiar los riesgos que soportan los sistemas de información y el entorno asociado, y el segundo, realizar recomendaciones de las medidas necesarias a adoptarse para conocer, prevenir, reducir o controlar los riesgos establecidos.

El análisis de riesgos se efectúa a través de un examen metódico para determinar de esta manera el riesgo, siguiendo los siguientes pasos:

**a)** **Activos:** En este paso se busca determinar los activos relevantes para la organización, su valor e interrelación, estableciendo de tal forma el costo que puede tener en caso de verse comprometida.

b) **Amenazas:** Establecer a que amenazas están expuestas los activos previamente valorados.

c) **Salvaguardas:** Determinar cuáles salvaguardas hay asociadas a los activos y la eficiencia real de su implantación frente al riesgo asociado.

d) **Impacto residual:** Determinar el impacto en términos de compromiso directo sobre el activo, en caso de verse materializada una amenaza.

e) **Riesgo residual:** Estimar el riesgo, en términos de impacto ponderado con respecto a la probabilidad real de la amenaza.

## 2.8. Declaración de Aplicabilidad

Como lo hemos evidenciado en el análisis diferencial, la Institución carece de la mayoría de los controles. Sin embargo, se pretende fijar una declaración de aplicabilidad que permita seguirse en un futuro, cuando los controles necesarios se adopten.

En tal sentido el anexo 4, recopila la declaración de aplicabilidad del Sistema de Gestión de Seguridad de la Información del Colegio, enmarcada en torno a los controles establecidos en la norma ISO/IEC 27002:2013. En tal sentido, de los 114 controles, se observan exclusiones en nueve (9) de ellos, los cuales se listan a continuación:

- El control 6.2.2 Teletrabajo, se excluye, ya que la institución no tiene ningún tipo de vinculación mediante la modalidad del teletrabajo y no se tiene prevista su implementación en un mediano plazo.

- Los controles 11.2.6 y 11.2.7, no se tienen en cuenta ya que las políticas de la institución, contempla, el uso de equipos y de dispositivos de almacenamiento sin restricción alguna, y se basan en los compromisos de confidencialidad firmados con el colaborador. Adicionalmente no se tiene como medida implementar sistemas de gestión de dispositivos móviles en el mediano plazo.

- Los controles, 12.4.1, 12.4.2, y 12.4.3, se excluyen, ya que no se cuenta con los recursos o soluciones para el monitorio óptimo de los registros o eventos de actividades.

- El control 14.2.1 se excluye, ya que dentro de la institución no se tiene un área encargada de desarrollo de software, el cual es adquirido a través de terceros.

- El control 14.2.6 se excluye, ya que en al no desarrollar software en la institución, su aseguramiento también es inexistente.

- El control 17.2.1, no se tiene en cuenta ya que la inversión para redundancias no se tiene contemplada en un mediano plazo.

## 3. Análisis de Riesgos

Este análisis, constituye la identificación de cada uno de los riesgos, su magnitud y las áreas relacionadas que requieren medidas de protección específicas. Este análisis nos permitirá obtener la información necesaria que permitirá identificar los peligros a los que la Institución está expuesta y de ninguna manera constituye medidas de seguridad, es decir, nos suministra información y no controles como tal.

De esta forma y como se describió con anterioridad, este análisis se efectuará mediante el uso de la metodología MAGERIT, que tiene como objetivos directos[9]:

- Concientizar a los responsables de las organizaciones de la existencia de riesgos y la necesidad de la toma de medidas al respecto.

- Proporcionar un método sistemático para analizar los riesgos inmersos en el uso de las tecnologías de la información y las comunicaciones.

- Facilitar el descubrimiento y la planificación en el tratamiento eficaz para mantener los riesgos dentro de controles indirectos.

- Prepara a las organizaciones para procesos de evaluación, auditoria, certificaciones o acreditaciones según corresponda.

El análisis de riesgos es desarrollado mediante una serie de tareas establecidas en el Método de Análisis de Riesgos MAR, las cuales se describen a continuación[10]:

| MAR |
|---|
| **MAR.1 Caracterización de los activos**<br>**MAR. 11** Identificación de los activos<br>**MAR. 12** Dependencias entre activos<br>**MAR. 13** Valoración de activos |
| **MAR.2 Caracterización de las amenazas**<br>**MAR. 21** Identificación de las amenazas<br>**MAR. 22** Valoración de las amenazas |
| **MAR.3 Caracterización de las salvaguardas**<br>**MAR. 31** Identificación de las salvaguardas pertinentes<br>**MAR. 32** Valoración de las salvaguardas |
| **MAR.4 Estimación del estado de riesgo**<br>**MAR. 41** Estimación del impacto<br>**MAR. 42 Estimación del riesgo** |

**Tabla 5 Método de Análisis de Riesgos MAR**

[9] Consultado en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WsuooojwbIU, el 17 de marzo de 2018, a las 8.50 p.m.
[10] Consultado en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html, el 17 de marzo de 2018 a las 9.30 p.m.

## 3.1. Caracterización de los activos

La tarea de inicio de la metodología es la caracterización de los activos y, en consecuencia, nos centraremos en los activos de la Institución, los cuales representan la importancia de la información que por ellos circula y los servicios que prestan en la operación diaria del colegio. No obstante, la caracterización constituye un insumo esencial en la metodología de análisis y gestión de riesgos que deberá ser revisado periódicamente por la alta probabilidad de aparición de nuevos activos o en su defecto por la supresión de algunos por obsolescencia tecnológica entre otros aspectos.

### 3.1.1. Identificación de los activos

Basado en lo dispuesto en el Libro II, Catálogo de Elementos de la versión 3.0 de la Metodología de Análisis y Gestión de Riesgos de los sistemas de Información MAGERIT, se pueden tipificar setenta y tres (73) activos en la Institución, como se muestra a continuación:

| **Nombre del Documento** | **Activos de Información** | |
|---|---|---|
| **Nivel de confidencialidad** | **Confidencial, para uso y conocimiento del personal involucrado en el proceso del Sistema de Gestión de la Seguridad de la Información** | |
| **Fecha de Creación** | **abril de 2018** | |
| **Aprobado** | **Comité de Seguridad de la Información** | |
| **Inventario de Activos** | | |
| **[I] Información** | | |
| [I Esencial] Datos esenciales | | |
| | [I Notas] Notas de estudiantes | |
| | [I Estudiantes] Registros académicos de estudiantes | |
| | [I Padres de familia] Registros de padres de familia | |
| | [I Mallas Curriculares] Mallas curriculares por áreas | |
| | [I Aspirantes] Registros de candidatos de ingreso | |
| | [I Exalumnas] Registro de exalumnas | |
| [I Carácter Personal] Datos de carácter personal | | |
| | [I estudiantes] Datos personales de estudiantes | |
| | [I Padres de familia] Datos personales de padres de familia | |
| | [I Colaboradores] Datos personales de colaboradores | |
| | [I Profesores] Datos personales de profesores | |
| | [I Exalumnas] Datos personales de exalumnas | |

| | | |
|---|---|---|
| **[S] Servicios** | | |
| [SI] Servicios Internos | | |
| | [SI Internet] Servicio de acceso a internet | |
| | [SI Aula virtual] Servicio web de aulas virtuales | |
| | [SI Correo] Servicio de correo institucional | |
| | [SI Mesa de ayuda] Servicio de help desk | |
| | [SI Mandarin] Sistema web de la biblioteca | |
| | [SI Reservas] Servicio de reservas de espacios | |
| | [SI Sistema de Notas] Servicio de sistema de notas | |
| [SE] Servicios Externos | | |
| | [SE Portal WEB] Portal WEB Institucional | |
| | Nota: El servicio de internet es prestado a través de un enlace dedicado de 240Mbps. | |
| **[D] Datos / Información** | | |
| | [D respaldo] Copias de seguridad y bakups | |
| | [D de config.] Archivos de configuración | |
| | [D de Bit] Archivos de bitácoras y contraseñas | |
| **[SW] Aplicaciones (Software)** | | |
| | [SW SO] Sistemas operativos | |
| | [SW BD] Sistemas manejadores de bases de datos | |
| | [SW Ant.] Software Antivirus | |
| | [SW Ofi] Herramientas ofimáticas | |
| | [SW moodle] Sistema de aulas virtuales | |
| | [SW nav] Navegadores web | |
| | [SW diseñ] Software de diseño y desarrollo | |
| | [SW nomina] Sistema de nómina antares | |
| | [SW contab] Software de contabilidad SIESA | |
| | [SW glpi] Software de mesa de ayuda | |
| | [SW notas] Software de sistema de notas | |
| | [SW plagio] Software anti-plagio | |
| | [SW bibliot] Software biblioteca | |
| | [SW horarios] Software de gestión de horarios | |
| **[HW] Equipos informáticos (Hardware)** | | **Cantidad** |
| | [HW pc] Equipos de escritorio | 326 |
| | [HW portatil] Equipos portátiles | 89 |
| | [HW multif] Impresoras multifuncionales alto rendimiento | 6 |
| | [HW Serv] Servidores | 5 |
| | [HW ap] Access points | 61 |
| | [HW switch] Switches | 13 |

| | | |
|---|---|---|
| | [HW videob] Viedo beams | 66 |
| | [HW pbx] Planta telefónica PBX | 1 |
| | [HW Ipad] Equipos Ipad | 60 |
| | [HW fotocop] Equipo de fotocopiado | 1 |
| | [HW tv] Televisores smart | 10 |
| | [HW modem] Modem portátil de conexión a internet (backup) | 1 |
| **[COM] Redes de Comunicación** | | |
| | [COM LAN] Red local | |
| | [COM wifi] Red wifi | |
| | [COM Internte] Servicio de internet. (Canal dedicado) | |
| | [COM telefonía] Red telefónica | |
| **[MEDIA] Dispositivos de almacenamiento de información** | | |
| | [MEDIA DD] Discos duros externos | 10 |
| | [MEDIA usb] Memorias USB | 1 |
| | [MEDIA electronic] Servidor de backup local | 1 |
| **[AUX] Equipamiento Auxiliar** | | |
| | [AUX ups] Sistemas de información ininterrumpida | 1 |
| | [AUX cableado] Cableado estructurado de la institución | |
| | [AUX rack] Racks de comunicaciones de la Institución | 5 |
| | [AUX gabinte] Gabinetes de comunicación de la Institución | 7 |
| | [AUX fibra] Fibra óptica | 3 |
| **[L] Instalaciones** | | |
| | [L administrativa] Oficinas administrativa | |
| | [L escuelas] Oficinas de escuelas (Preescolar-primaria-media-alta) | |
| **[P] Personal** | | |
| | [P ui] Usuarios internos | |
| | [P ue] Usuarios externos | |
| | [P soperte] Personal soporte | 3 |
| | [P adm] Personal administrador de red | 1 |
| | [P com] Personal comunicaciones | 3 |
| | [P sec] Encargado de la seguridad | 1 |
| | P dba] Administrador de bases de datos | 1 |
| | [P rector] Rectora de la institución | 1 |
| | [P Proc] Procuradora de la Institución | 1 |
| | [P Calidad] directora de calidad | 1 |
| | [P proveedores] Proveedores de la institución | 8 |

**Tabla 6 Inventario de Activos Institucional**

### 3.1.2. Dependencia entre activos

Representa la medida en que un activo de orden superior se ve afectado por la materialización de una amenaza en un activo de orden inferior, es tal sentido tenemos las siguientes dependencias entre los activos de la Institución:

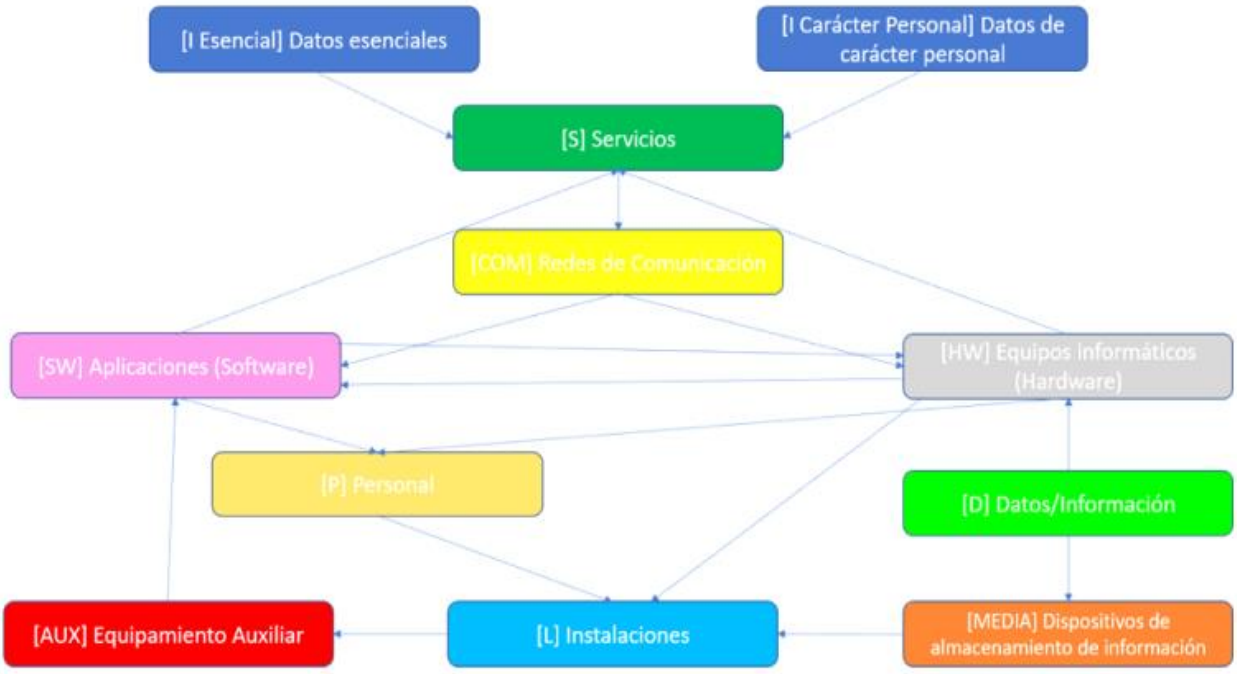


**Imagen 5 Dependencia entre Activos**

### 3.1.3. Valoración de los activos

Para la valoración de los activos, se toman en cuenta las dimensiones descritas por MAGERIT en el Libro II, para valorar las consecuencias de la materialización de una amenaza determinada. En tal sentido, las dimensiones son[11]:

- [D] Disponibilidad
- [I] Integridad de los datos
- [C] Confidencialidad de la información
- [A] Autenticidad

[11] Consultada en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Ws5LY4jwbIU, el 18 de marzo de 2018, a las 10.40 p.m.

- [T] Trazabilidad

#### 3.1.3.1. Disponibilidad

Representa la propiedad de los activos en la que las entidades o procesos autorizados acceden a los mismos en el momento que se requiera. La disponibilidad, afecta a la totalidad de los activos.

#### 3.1.3.2. Integridad de los datos

Es la característica de los activos que consiste en que la información no ha sido alterada de manera fraudulenta o no autorizada. La valoración de este tipo de activos es directamente proporcional al grado de afectación a la organización por la alteración voluntaria o intencionada de los datos.

#### 3.1.3.3. Confidencialidad de la información

Propiedad en la que se asegura que la información no se pone a disposición o se revela a individuos o procesos no autorizados para tal fin. De esta forma, los datos cobran especial valor en cuento su confidencialidad al ser revelada causa grandes daños o perjuicios a la Institución.

#### 3.1.3.4. Autenticidad

Representa la propiedad en la que una entidad es quien asegura ser o se asegura la fuente de la que provienen los datos como tal.

#### 3.1.3.5. Trazabilidad

Representa garantizar que las acciones de una entidad pueden ser atribuidas única y exclusivamente a la entidad en mención.

Teniendo en cuenta lo anterior, se fija una escala de valoración numérica para su cuantificación tal y como se muestra en la siguiente tabla[12]:

| valor | | criterio |
|---|---|---|
| 10 | extremo | Daño extremadamente grave |
| 9 | muy alto | Daño muy grave |
| 6-8 | alto | Daño grave |
| 3-5 | medio | Daño importante |
| 1-2 | bajo | Daño menor |
| 0 | despreciable | Irrelevante para la organización |

**Tabla 7 Escala de valoración numérica para los activos**

[12] Consultado en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Ws6oly_SH-Y, el 19 de marzo de 2018 a las 9.35 p.m.

Así las cosas, basándonos en la escala descrita anteriormente para realizar la cuantificación de los activos de la Institución, tenemos:

| **Valoración de Activos** | | | | | | |
|---|---|---|---|---|---|---|
| **[I] Información** | Valor | D | I | C | A | T |
| [I Notas] Notas de estudiantes, 28944 registros de notas de estudiantes | Muy Alto | 10 | 10 | 7 | 8 | 9 |
| [I Estudiantes] Registros académicos de 800 estudiantes | Alto | 9 | 8 | 7 | 7 | 7 |
| [I Padres de familia] Registros de padres de familia 1809 | Alto | 6 | 8 | 9 | 8 | 7 |
| [I Mallas Curriculares] 122 Mallas curriculares por áreas | Alto | 9 | 8 | 2 | 7 | 6 |
| [I Aspirantes] Tabla de registros de candidatos de ingreso | Alto | 9 | 7 | 7 | 6 | 6 |
| [I Exalumnas] 5100 registros de exalumnas | Alto | 5 | 6 | 7 | 6 | 4 |
| [I estudiantes] Datos personales de 800 estudiantes | Alto | 4 | 6 | 7 | 7 | 7 |
| [I Padres de familia] Datos personales de 1206 padres de familia | Alto | 7 | 7 | 8 | 6 | 3 |
| [I Colaboradores] Datos personales de 200 colaboradores | Alto | 5 | 5 | 7 | 6 | 6 |
| [I Profesores] Datos personales de 100 profesores | Alto | 5 | 5 | 7 | 6 | 6 |
| [I Exalumnas] Datos personales de 5100 exalumnas | Medio | 3 | 5 | 7 | 6 | 6 |
| **[S] Servicios** | | **D** | **I** | **C** | **A** | **T** |
| [SI Internet] Servicio de acceso a internet, canal dedicado 240 Mbps | Alto | 10 | 8 | 7 | 7 | 7 |
| [SI Aula virtual] Servicio web de aulas virtuales para 800 estudiantes y 100 profesores | Alto | 8 | 7 | 5 | 5 | 5 |
| [SI Correo] Servicio de correo institucional, para 800 estudiantes, 200 colaboradores y 100 profesores. | Alto | 9 | 8 | 9 | 8 | 6 |
| [SI Mesa de ayuda] Servicio de help desk para 1100 usuarios | Medio | 7 | 6 | 1 | 1 | 1 |
| [SI Mandarin] Sistema web de la biblioteca mandarín | Medio | 6 | 6 | 6 | 5 | 4 |
| [SI Reservas] Servicio de reservas de espacios | Medio | 4 | 4 | 4 | 2 | 1 |
| [SI Sistema de Notas] Servicio de sistema de notas, software dedicado | Alto | 9 | 9 | 9 | 8 | 6 |
| [SE Portal WEB] Portal WEB Institucional | Alto | 9 | 10 | 3 | 9 | 5 |
| **[D] Datos / Información** | | **D** | **I** | **C** | **A** | **T** |
| [D respaldo] Copias de seguridad y backups. Respaldo de información académica. | Alto | 9 | 9 | 7 | 6 | 6 |

| | | | | | | |
|---|---|---|---|---|---|---|
| [D de config.] Archivos de configuración, servidores, equipos de enrutamiento y demás equipos de TI | Muy Alto | 10 | 10 | 8 | 8 | 7 |
| [D de Bit] Archivos de bitácoras y contraseñas | Extremo | 10 | 10 | 10 | 9 | 9 |
| **[SW] Aplicaciones (Software)** | | **D** | **I** | **C** | **A** | **T** |
| [SW SO] Sistemas operativos | Alto | 8 | 9 | 8 | 9 | 7 |
| [SW BD] Sistemas manejadores de bases de datos | Alto | 8 | 8 | 8 | 8 | 7 |
| [SW Ant.] Software Antivirus | Alto | 7 | 6 | 4 | 7 | 6 |
| [SW Ofi] Herramientas ofimáticas | Alto | 8 | 8 | 6 | 7 | 6 |
| [SW moodle] Sistema de aulas virtuales | Alto | 7 | 7 | 6 | 6 | 6 |
| [SW nav] Navegadores web | Medio | 5 | 5 | 5 | 5 | 4 |
| [SW diseñ] Software de diseño y desarrollo | Medio | 3 | 7 | 3 | 6 | 6 |
| [SW nomina] Sistema de nómina antares | Muy Alto | 9 | 9 | 9 | 9 | 7 |
| [SW contab] Software de contabilidad SIESA | Muy Alto | 9 | 9 | 10 | 9 | 10 |
| [SW glpi] Software de mesa de ayuda | Bajo | 3 | 3 | 2 | 2 | 1 |
| [SW notas] Software de sistema de notas | Muy Alto | 8 | 9 | 10 | 9 | 8 |
| [SW plagio] Software anti-plagio | Medio | 2 | 2 | 2 | 5 | 3 |
| [SW bibliot] Software biblioteca | Bajo | 2 | 2 | 2 | 1 | 1 |
| [SW horarios] Software de gestión de horarios | Bajo | 1 | 1 | 1 | 1 | 1 |
| **[HW] Equipos informáticos (Hardware)** | | **D** | **I** | **C** | **A** | **T** |
| [HW pc] 326 equipos de escritorio | Alto | 7 | 6 | 7 | 6 | 5 |
| [HW portatil] 89 equipos portátiles | Alto | 5 | 5 | 7 | 6 | 7 |
| [HW multif] 6 Impresoras multifuncionales alto rendimiento, para cada escuela y centro de copiado. | Alto | 6 | 6 | 7 | 5 | 4 |
| [HW Serv] 5 Servidores | Alto | 9 | 9 | 9 | 8 | 7 |
| [HW ap] 61 Access points, para una cobertura del 99% del área de la institución | Alto | 7 | 6 | 5 | 6 | 4 |
| [HW switch] 13 Switches | Alto | 9 | 9 | 8 | 7 | 5 |
| [HW videob] 66 Viedo beams, dispuestos en aulas y salas de reuniones | Bajo | 8 | 2 | 1 | 1 | 0 |
| [HW pbx] 1 Planta telefónica PBX | Alto | 9 | 9 | 9 | 8 | 6 |
| [HW Ipad] 60 Equipos Ipad, de consulta continua | Alto | 6 | 6 | 5 | 5 | 8 |
| [HW fotocop] 1 Equipo de fotocopiado de alto rendimiento en el centro de copiado institucional | Alto | 8 | 6 | 6 | 5 | 3 |
| [HW tv] 10 Televisores smart | Medio | 6 | 4 | 1 | 2 | 1 |
| [HW modem] 1 modem portátil de conexión a internet (backup) | Medio | 6 | 5 | 3 | 2 | 2 |
| **[COM] Redes de Comunicación** | | **D** | **I** | **C** | **A** | **T** |
| [COM LAN] Red local | Muy Alto | 9 | 9 | 9 | 9 | 7 |
| [COM wifi] Red wifi | Alto | 8 | 8 | 6 | 5 | 4 |

| | | | | | | |
|---|---|---|---|---|---|---|
| [COM Internet] Servicio de internet. (Canal dedicado) | Alto | 9 | 9 | 8 | 7 | 7 |
| [COM telefonía] Red telefónica | Alto | 7 | 8 | 8 | 7 | 7 |
| **[MEDIA] Dispositivos de almacenamiento de información** | | **D** | **I** | **C** | **A** | **T** |
| [MEDIA DD] 10 Discos duros externos | Alto | 6 | 7 | 8 | 6 | 8 |
| [MEDIA usb] 1 Memorias USB | Alto | 5 | 6 | 7 | 5 | 7 |
| [MEDIA electronic] 1 Servidor de backup local | Alto | 9 | 9 | 9 | 7 | 6 |
| **[AUX] Equipamiento Auxiliar** | | **D** | **I** | **C** | **A** | **T** |
| [AUX ups] 1 Sistemas de información ininterrumpida | Medio | 8 | 5 | 2 | 2 | 1 |
| [AUX cableado] Cableado estructurado de la institución | Alto | 9 | 9 | 6 | 6 | 7 |
| [AUX rack] 5 Racks de comunicaciones de la Institución | Alto | 9 | 7 | 7 | 5 | 3 |
| [AUX gabinete] 7Gabinetes de comunicación de la Institución | Alto | 9 | 7 | 7 | 5 | 3 |
| [AUX fibra] 3 Fibras óptica | Medio | 8 | 6 | 6 | 4 | 2 |
| **[L] Instalaciones** | | **D** | **I** | **C** | **A** | **T** |
| [L administrativa] Oficinas administrativa | Alto | 10 | 8 | 8 | 7 | 4 |
| [L escuelas] Oficinas de escuelas (Preescolar-primaria-media-alta) | Alto | 10 | 7 | 8 | 7 | 3 |
| **[P] Personal** | | **D** | **I** | **C** | **A** | **T** |
| [P ui] Usuarios internos | Alto | 5 | | 8 | | |
| [P ue] Usuarios externos | Alto | 4 | | 7 | | |
| [P soporte] Personal soporte, 3 tecnólogos | Alto | 4 | | 8 | | |
| [P adm] Personal administrador de red, 1 ingeniero. | Alto | 8 | | 8 | | |
| [P com] Personal comunicaciones, 3 profesionales. | Alto | 7 | | 8 | | |
| [P sec] Encargado de la seguridad, 1 ingeniero. | Muy Alto | 8 | | 9 | | |
| P dba] Administrador de bases de datos 1 ingeniero. | Muy Alto | 8 | | 9 | | |
| [P rector] Rectora de la institución | Muy Alto | 8 | | 10 | | |
| [P proc] Procuradora de la Institución | Muy Alto | 8 | | 10 | | |
| [P Calidad] directora de calidad | Alto | 7 | | 8 | | |
| [P proveedores] Proveedores de la institución, 8 proveedores para el área de TI | Alto | 7 | | 8 | | |

**Tabla 8 Valoración de Activos**

## 3.2. Caracterización de las amenazas

La metodología MAGERIT, establece una serie de categorías de amenazas que pueden afectar a los activos de información. Estas categorías son:

- [N] Desastres Naturales
- [I] De origen Industrial
- [E] Errores y fallos no intencionados

- [A] Ataques intencionados

### 3.2.1. Identificación de las amenazas

Acorde con las dimensiones de amenazas descritas anteriormente, se efectúa la identificación de las amenazas para la Institución, según como se muestra en el Anexo 5. Identificación de amenazas.

### 3.2.2. Valoración de las amenazas

Una vez identificadas las amenazas sobre un activo, se debe considerar el grado de afectación y la probabilidad de que éstas amenazas se materialicen. En tal sentido, es común pensar en la degradación total o parcial de un activo y su caracterización se puede establecer como una fracción del valor del activo. De esta manera y basados en la tabla Probabilidad de ocurrencia del libro I, del Método MAGERIT, tenemos:

| Probabilidad | Valor | Descripción | Periodicidad |
|---|---|---|---|
| MA | 100 | Muy frecuente | A diario |
| A | 10 | Frecuente | Mensualmente |
| M | 1 | Normal | Una vez al año |
| B | 1/10 | Poco frecuente | Cada varios años |
| MB | 1/100 | Muy poco frecuente | siglos |

**Tabla 9 Probabilidad de ocurrencia de amenazas**

De igual forma, se debe establecer la fracción en términos porcentuales en la que un determinado activo es degrado una vez se materializa una amenaza, para lo cual seguimos lo establecido en el Método MAGERIT:

| Impacto | Descripción | Valor |
|---|---|---|
| MA | Muy alto | 100% |
| A | Alto | 75% |
| M | Medio | 50% |
| B | Bajo | 20% |
| MB | Muy bajo | 5% |

**Tabla 10 Valoración de los impactos**

Con la información descrita en las dos tablas anteriores, podemos realizar la valoración de las amenazas, como se muestra en el Anexo 6 Valoración de las amenazas.

## 3.3. Estimación del impacto potencial

El impacto denota el daño causado sobre un activo en caso de concretarse una amenaza determinada. Para hallar el valor del impacto potencial, tendremos en cuenta el producto de cada dimensión hallado para la valoración de activos y el valor de amenazas. No obstante, como para la valoración de las amenazas se tuvo en cuenta cada activo inmerso para cada escenario amenaza, es necesario promediar dichos valores para obtener el valor promedio de cada activo como, por ejemplo, para el activo denominado [SI Sistema de Notas], tenemos:

| 1 | Cod. | Amenaza | Activos | Frecuencia | D | I | C | A | T |
|---|---|---|---|---|---|---|---|---|---|
| 254 | [E.1] | Errores de los usuarios | [SI Sistema de Notas] | 0,1 | 75% | 75% | 75% | | |
| 282 | [E.2] | Errores del administrador | [SI Sistema de Notas] | 0,1 | 20% | 20% | 20% | | |
| 320 | [E.9] | Errores de [re-]encaminamiento | [SI Sistema de Notas] | 0,1 | | | 20% | | |
| 346 | [E.10] | Errores de secuencia | [SI Sistema de Notas] | 0,1 | | 75% | | | |
| 375 | [E.15] | Alteración accidental de la información | [SI Sistema de Notas] | 0,1 | | 75% | | | |
| 407 | [E.18] | Destrucción de información | [SI Sistema de Notas] | 0,1 | 100% | | | | |
| 439 | [E.19] | Fugas de información | [SI Sistema de Notas] | 0,1 | | | 20% | | |
| 525 | [E.24] | Caida del sistema por agotamiento de recursos | [SI Sistema de Notas] | 0,1 | 100% | | | | |
| 574 | [A.5] | Suplantación de la identidad del usuario | [SI Sistema de Notas] | 0,1 | | | 75% | 75% | 50% |
| 603 | [A.6] | Abuso de privilegios de acceso | [SI Sistema de Notas] | 0,1 | 75% | 75% | 50% | | |
| 641 | [A.7] | Uso no previsto | [SI Sistema de Notas] | 0,1 | 5% | 5% | 5% | | |
| 703 | [A.9] | Errores de [re-]encaminamiento | [SI Sistema de Notas] | 0,1 | | | 75% | | |
| 729 | [A.10] | Alteración de secuencia | [SI Sistema de Notas] | 0,1 | | 75% | | | |
| 758 | [A.11] | Acceso no autorizado | [SI Sistema de Notas] | 0,1 | | 75% | 75% | | |
| 810 | [A.13] | Repudio | [SI Sistema de Notas] | 0,1 | | 50% | | | 100% |
| 825 | [A.15] | Modificación deliberada de la información | [SI Sistema de Notas] | 0,1 | | 100% | | | |
| 859 | [A.18] | Destrucción de información | [SI Sistema de Notas] | 0,1 | 100% | | | | |
| 889 | [A.19] | Divulgación de información | [SI Sistema de Notas] | 0,1 | | | 100% | | |
| 954 | [A.24] | Denegación de servicio | [SI Sistema de Notas] | 0,1 | 100% | | | | |
| 1046 | | | | | | | | | |
| 1047 | | | | Total | 575% | 625% | 515% | 75% | 150% |
| 1048 | | | | Promedio | 72% | 63% | 52% | 75% | 75% |

**Imagen 6 Valoración promedio de amenaza para cada activo**

Para estimar cualitativamente la valoración del impacto potencial, tomamos como referencia la siguiente valoración:

| valor | Identificación |
|---|---|
| 40 | muy alto |
| 20-30 | alto |
| 10-20 | medio |
| 0-10 | bajo |

**Tabla 11 Escala de Valoración numérica estimación de impacto Potencial**

En consecuencia, tenemos el siguiente impacto potencial por cada uno de los activos fijados:

| Valoración del Impacto | | Valor Activo | | | | | Valor Amenaza | | | | | Impacto Pot. | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| [I] Información | Valor | D | I | C | A | T | D | I | C | A | T | D | I | C | A | T |
| [I Notas] | 27 | 10 | 10 | 7 | 8 | 9 | 75% | 48% | 57% | 75% | 50% | 8 | 5 | 4 | 6 | 5 |
| [I Estudiantes] | 25 | 9 | 8 | 7 | 7 | 7 | 74% | 61% | 66% | 75% | 50% | 7 | 5 | 5 | 5 | 4 |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| [I Padres de familia] | 25 | 6 | 8 | 9 | 8 | 7 | 65% | 48% | 85% | 75% | 50% | 4 | 4 | 8 | 6 | 4 |
| [I Mallas Curriculares] | 19 | 9 | 8 | 2 | 7 | 6 | 65% | 48% | 57% | 75% | 50% | 6 | 4 | 1 | 5 | 3 |
| [I Aspirantes] T | 21 | 9 | 7 | 7 | 6 | 6 | 65% | 48% | 57% | 75% | 50% | 6 | 3 | 4 | 5 | 3 |
| [I Exalumnas] | 16 | 5 | 6 | 7 | 6 | 4 | 48% | 48% | 66% | 75% | 50% | 2 | 3 | 5 | 5 | 2 |
| [I Colaboradores] | 17 | 5 | 5 | 7 | 6 | 6 | 65% | 48% | 57% | 75% | 50% | 3 | 2 | 4 | 5 | 3 |
| [I Profesores] | 7 | 5 | 5 | 7 | 6 | 6 | 22% | 24% | 19% | 38% | 25% | 1 | 1 | 1 | 2 | 2 |
| **[S] Servicios** | **Valor** | **D** | **I** | **C** | **A** | **T** | **D** | **I** | **C** | **A** | **T** | **D** | **I** | **C** | **A** | **T** |
| [SI Internet] | 27 | 10 | 8 | 7 | 7 | 7 | 78% | 67% | 55% | 75% | 75% | 8 | 5 | 4 | 5 | 5 |
| [SI Aula virtual] | 21 | 8 | 7 | 5 | 5 | 5 | 78% | 67% | 55% | 75% | 75% | 6 | 5 | 3 | 4 | 4 |
| [SI Correo] | 28 | 9 | 8 | 9 | 8 | 6 | 78% | 67% | 55% | 75% | 75% | 7 | 5 | 5 | 6 | 5 |
| [SI Mesa de ayuda] | 11 | 7 | 6 | 1 | 1 | 1 | 78% | 67% | 55% | 75% | 75% | 5 | 4 | 1 | 1 | 1 |
| [SI Mandarin] | 19 | 6 | 6 | 6 | 5 | 4 | 78% | 67% | 55% | 75% | 75% | 5 | 4 | 3 | 4 | 3 |
| [SI Reservas] | 10 | 4 | 4 | 4 | 2 | 1 | 78% | 67% | 55% | 75% | 75% | 3 | 3 | 2 | 2 | 1 |
| [SI Sistema de Notas] | 27 | 9 | 9 | 9 | 8 | 6 | 72% | 63% | 52% | 75% | 75% | 6 | 6 | 5 | 6 | 5 |
| [SE Portal WEB] | 27 | 9 | 10 | 3 | 9 | 5 | 89% | 67% | 55% | 75% | 75% | 8 | 7 | 2 | 7 | 4 |
| **[D] Datos / Información** | **Valor** | **D** | **I** | **C** | **A** | **T** | **D** | **I** | **C** | **A** | **T** | **D** | **I** | **C** | **A** | **T** |
| [D respaldo] | 27 | 9 | 9 | 7 | 6 | 6 | 85% | 79% | 67% | 75% | 50% | 8 | 7 | 5 | 5 | 3 |
| [D de config.] | 10 | 10 | 10 | 8 | 8 | 7 | 17% | 11% | 10% | 38% | 50% | 2 | 1 | 1 | 3 | 4 |
| [D de Bit] | 34 | 10 | 10 | 10 | 9 | 9 | 85% | 79% | 67% | 75% | 50% | 9 | 8 | 7 | 7 | 5 |
| **[SW] Aplicaciones (Software)** | **Valor** | **D** | **I** | **C** | **A** | **T** | **D** | **I** | **C** | **A** | **T** | **D** | **I** | **C** | **A** | **T** |
| [SW SO] | 26 | 8 | 9 | 8 | 9 | 7 | 71% | 66% | 52% | 75% | 50% | 6 | 6 | 4 | 7 | 4 |
| [SW BD] | 25 | 8 | 8 | 8 | 8 | 7 | 71% | 66% | 52% | 75% | 50% | 6 | 5 | 4 | 6 | 4 |
| [SW Ant.] | 19 | 7 | 6 | 4 | 7 | 6 | 71% | 66% | 52% | 75% | 50% | 5 | 4 | 2 | 5 | 3 |
| [SW Ofi] | 22 | 8 | 8 | 6 | 7 | 6 | 71% | 66% | 52% | 75% | 50% | 6 | 5 | 3 | 5 | 3 |
| [SW moodle] | 20 | 7 | 7 | 6 | 6 | 6 | 71% | 66% | 52% | 75% | 50% | 5 | 5 | 3 | 5 | 3 |
| [SW nav] | 15 | 5 | 5 | 5 | 5 | 4 | 71% | 66% | 52% | 75% | 50% | 4 | 3 | 3 | 4 | 2 |
| [SW  diseñ] | 16 | 3 | 7 | 3 | 6 | 6 | 71% | 66% | 52% | 75% | 50% | 2 | 5 | 2 | 5 | 3 |
| [SW nomina] | 27 | 9 | 9 | 9 | 9 | 7 | 71% | 66% | 52% | 75% | 50% | 6 | 6 | 5 | 7 | 4 |
| [SW contab] | 29 | 9 | 9 | 10 | 9 | 10 | 71% | 66% | 52% | 75% | 50% | 6 | 6 | 5 | 7 | 5 |
| [SW glpi] | 7 | 3 | 3 | 2 | 2 | 1 | 68% | 69% | 52% | 75% | 50% | 2 | 2 | 1 | 2 | 1 |
| [SW notas] | 28 | 8 | 9 | 10 | 9 | 8 | 71% | 66% | 52% | 75% | 50% | 6 | 6 | 5 | 7 | 4 |
| [SW plagio] | 9 | 2 | 2 | 2 | 5 | 3 | 68% | 69% | 52% | 75% | 50% | 1 | 1 | 1 | 4 | 2 |
| [SW bibliot] | 5 | 2 | 2 | 2 | 1 | 1 | 68% | 69% | 52% | 75% | 50% | 1 | 1 | 1 | 1 | 1 |
| [SW horarios] | 3 | 1 | 1 | 1 | 1 | 1 | 68% | 69% | 52% | 75% | 50% | 1 | 1 | 1 | 1 | 1 |
| **[HW] Equipos informáticos (Hardware)** | **Valor** | **D** | **I** | **C** | **A** | **T** | **D** | **I** | **C** | **A** | **T** | **D** | **I** | **C** | **A** | **T** |
| [HW pc] | 14 | 7 | 6 | 7 | 6 | 5 | 83% | 57% | 66% | 0 | 0 | 6 | 3 | 5 | 0 | 0 |
| [HW portatil] | 12 | 5 | 5 | 7 | 6 | 7 | 83% | 57% | 66% | 0 | 0 | 4 | 3 | 5 | 0 | 0 |
| [HW multif] | 12 | 6 | 6 | 7 | 5 | 4 | 83% | 57% | 54% | 0 | 0 | 5 | 3 | 4 | 0 | 0 |
| [HW Serv] | 18 | 9 | 9 | 9 | 8 | 7 | 84% | 57% | 54% | 0 | 0 | 8 | 5 | 5 | 0 | 0 |
| [HW ap] | 12 | 7 | 6 | 5 | 6 | 4 | 75% | 57% | 62% | 0 | 0 | 5 | 3 | 3 | 0 | 0 |
| [HW switch] | 17 | 9 | 9 | 8 | 7 | 5 | 84% | 57% | 54% | 0 | 0 | 8 | 5 | 4 | 0 | 0 |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| [HW videob] | 8 | 8 | 2 | 1 | 1 | 0 | 77% | 57% | 54% | 0 | 0 | 6 | 1 | 1 | 0 | 0 |
| [HW pbx] | 18 | 9 | 9 | 9 | 8 | 6 | 84% | 57% | 62% | 0 | 0 | 8 | 5 | 6 | 0 | 0 |
| [HW Ipad] | 11 | 6 | 6 | 5 | 5 | 8 | 83% | 57% | 62% | 0 | 0 | 5 | 3 | 3 | 0 | 0 |
| [HW fotocop] | 14 | 8 | 6 | 6 | 5 | 3 | 83% | 57% | 62% | 0 | 0 | 7 | 3 | 4 | 0 | 0 |
| [HW tv] | 8 | 6 | 4 | 1 | 2 | 1 | 83% | 52% | 52% | 0 | 0 | 5 | 2 | 1 | 0 | 0 |
| [HW modem] | 10 | 6 | 5 | 3 | 2 | 2 | 83% | 57% | 62% | 0 | 0 | 5 | 3 | 2 | 0 | 0 |
| **[COM] Redes de Comunicación** | **Valor** | **D** | **I** | **C** | **A** | **T** | **D** | **I** | **C** | **A** | **T** | **D** | **I** | **C** | **A** | **T** |
| [COM LAN] | 29 | 9 | 9 | 9 | 9 | 7 | 83% | 69% | 62% | 75% | 50% | 7 | 6 | 6 | 7 | 4 |
| [COM wifi] | 22 | 8 | 8 | 6 | 5 | 4 | 83% | 69% | 62% | 75% | 50% | 7 | 6 | 4 | 4 | 2 |
| [COM Internte] | 27 | 9 | 9 | 8 | 7 | 7 | 74% | 69% | 62% | 75% | 50% | 7 | 6 | 5 | 5 | 4 |
| [COM telefonía] | 25 | 7 | 8 | 8 | 7 | 7 | 83% | 69% | 62% | 75% | 50% | 6 | 6 | 5 | 5 | 4 |
| **[MEDIA] Dispositivos de almacenamiento de información** | **Valor** | **D** | **I** | **C** | **A** | **T** | **D** | **I** | **C** | **A** | **T** | **D** | **I** | **C** | **A** | **T** |
| [MEDIA DD] | 13 | 6 | 7 | 8 | 6 | 8 | 84% | 51% | 53% | 0 | 0 | 5 | 4 | 4 | 0 | 0 |
| [MEDIA usb] | 11 | 5 | 6 | 7 | 5 | 7 | 84% | 51% | 53% | 0 | 0 | 4 | 3 | 4 | 0 | 0 |
| [MEDIA electronic] | 19 | 9 | 9 | 9 | 7 | 6 | 81% | 69% | 67% | 0 | 0 | 7 | 6 | 6 | 0 | 0 |
| **[AUX] Equipamiento Auxiliar** | **Valor** | **D** | **I** | **C** | **A** | **T** | **D** | **I** | **C** | **A** | **T** | **D** | **I** | **C** | **A** | **T** |
| [AUX ups] | 8 | 8 | 5 | 2 | 2 | 1 | 0,8 | 0,1 | 0,6 | 0 | 0 | 6 | 0 | 1 | 0 | 0 |
| [AUX cableado] | 11 | 9 | 9 | 6 | 6 | 7 | 0,8 | 0,1 | 0,6 | 0 | 0 | 7 | 1 | 3 | 0 | 0 |
| [AUX rack] | 11 | 9 | 7 | 7 | 5 | 3 | 0,8 | 0,1 | 0,6 | 0 | 0 | 7 | 1 | 4 | 0 | 0 |
| [AUX gabinte] | 11 | 9 | 7 | 7 | 5 | 3 | 0,8 | 0,1 | 0,6 | 0 | 0 | 7 | 1 | 4 | 0 | 0 |
| [AUX fibra] | 10 | 8 | 6 | 6 | 4 | 2 | 0,8 | 0,1 | 0,6 | 0 | 0 | 6 | 1 | 3 | 0 | 0 |
| **[L] Instalaciones** | **Valor** | **D** | **I** | **C** | **A** | **T** | **D** | **I** | **C** | **A** | **T** | **D** | **I** | **C** | **A** | **T** |
| [L administrativa] | 17 | 10 | 8 | 8 | 7 | 4 | 77% | 48% | 74% | 0 | 0 | 8 | 4 | 6 | 0 | 0 |
| [L escuelas] | 18 | 10 | 7 | 8 | 7 | 3 | 87% | 48% | 74% | 0 | 0 | 9 | 3 | 6 | 0 | 0 |
| **[P] Personal** | **Valor** | **D** | **I** | **C** | **A** | **T** | **D** | **I** | **C** | **A** | **T** | **D** | **I** | **C** | **A** | **T** |
| [P ui] | 6 | 5 | | 8 | | | 38% | 75% | 48% | 0 | 0 | 2 | 0 | 4 | 0 | 0 |
| [P ue] | 5 | 4 | | 7 | | | 48% | 75% | 48% | 0 | 0 | 2 | 0 | 3 | 0 | 0 |
| [P soperte] | 6 | 4 | | 8 | | | 58% | 75% | 48% | 0 | 0 | 2 | 0 | 4 | 0 | 0 |
| [P adm] | 7 | 8 | | 8 | | | 38% | 75% | 48% | 0 | 0 | 3 | 0 | 4 | 0 | 0 |
| [P com] | 8 | 7 | | 8 | | | 58% | 75% | 48% | 0 | 0 | 4 | 0 | 4 | 0 | 0 |
| [P sec] | 9 | 8 | | 9 | | | 58% | 75% | 48% | 0 | 0 | 5 | 0 | 4 | 0 | 0 |
| P dba] | 4 | 8 | | 9 | | | 29% | 75% | 24% | 0 | 0 | 2 | 0 | 2 | 0 | 0 |
| [P rector] | 9 | 8 | | 10 | | | 58% | 75% | 48% | 0 | 0 | 5 | 0 | 5 | 0 | 0 |
| [P Proc] | 8 | 8 | | 10 | | | 38% | 75% | 48% | 0 | 0 | 3 | 0 | 5 | 0 | 0 |
| [P Calidad] | 6 | 7 | | 8 | | | 38% | 75% | 48% | 0 | 0 | 3 | 0 | 4 | 0 | 0 |
| [P proveedores] | 7 | 7 | | 8 | | | 48% | 75% | 48% | 0 | 0 | 3 | 0 | 4 | 0 | 0 |

**Tabla 12 Impacto Potencial**

## 3.4. Riesgo aceptable y Riesgo Residual

Evaluado el impacto de materialización de una amenaza sobre un activo puntual, nos resta estimar el riesgo que la Institución asume y aquellos en los cuales se debe fijar medidas para su tratamiento y control. En tal sentido, el riesgo se calcula como el producto de la frecuencia por el impacto potencial, donde los valores < 10 serán tomados como riesgo bajo, los valores entre 10 y 50 estarán en un nivel medio, y los valores >50, serán riesgos importantes, como se muestra a continuación:

| Valor | Nivel de Riesgo |
|---|---|
| >50 | Riesgo Importante |
| 10-50 | Riesgo Moderado |
| <10 | Riesgo Bajo |

**Tabla 13 Escala de Valoración de niveles de riesgos**

Dicho lo anterior tenemos:

| Valoración del Impacto | | Impact. Pot. | | | | | Frecuencia | Riesgo | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **[I] Información** | | **D** | **I** | **C** | **A** | **T** | | **D** | **I** | **C** | **A** | **T** |
| | [I Notas] | 8 | 5 | 4 | 6 | 5 | 10,0 | 75 | 48 | 40 | 60 | 45 |
| | [I Estudiantes] | 7 | 5 | 5 | 5 | 4 | 10,0 | 67 | 49 | 46 | 53 | 35 |
| | [I Padres de familia] | 4 | 4 | 8 | 6 | 4 | 10,0 | 39 | 38 | 77 | 60 | 35 |
| | [I Mallas Curriculares] | 6 | 4 | 1 | 5 | 3 | 1,0 | 6 | 4 | 1 | 5 | 3 |
| | [I Aspirantes] T | 6 | 3 | 4 | 5 | 3 | 10,0 | 59 | 33 | 40 | 45 | 30 |
| | [I Exalumnas] | 2 | 3 | 5 | 5 | 2 | 10,0 | 24 | 29 | 46 | 45 | 20 |
| | [I Colaboradores] | 3 | 2 | 4 | 5 | 3 | 10,0 | 33 | 24 | 40 | 45 | 30 |
| | [I Profesores] | 1 | 1 | 1 | 2 | 2 | 10,0 | 11 | 12 | 13 | 23 | 15 |
| **[S] Servicios** | | **D** | **I** | **C** | **A** | **T** | **Frecuencia** | **D** | **I** | **C** | **A** | **T** |
| | [SI Internet] | 8 | 5 | 4 | 5 | 5 | 0,1 | 1 | 1 | 0 | 1 | 1 |
| | [SI Aula virtual] | 6 | 5 | 3 | 4 | 4 | 1,0 | 6 | 5 | 3 | 4 | 4 |
| | [SI Correo] | 7 | 5 | 5 | 6 | 5 | 0,1 | 1 | 1 | 0 | 1 | 0 |
| | [SI Mesa de ayuda] | 5 | 4 | 1 | 1 | 1 | 0,1 | 1 | 0 | 0 | 0 | 0 |
| | [SI Mandarin] | 5 | 4 | 3 | 4 | 3 | 0,1 | 0 | 0 | 0 | 0 | 0 |
| | [SI Reservas] | 3 | 3 | 2 | 2 | 1 | 0,1 | 0 | 0 | 0 | 0 | 0 |
| | [SI Sistema de Notas] | 6 | 6 | 5 | 6 | 5 | 0,1 | 1 | 1 | 0 | 1 | 0 |
| | [SE Portal WEB] | 8 | 7 | 2 | 7 | 4 | 1,0 | 8 | 7 | 2 | 7 | 4 |
| **[D] Datos / Información** | | **D** | **I** | **C** | **A** | **T** | **Frecuencia** | **D** | **I** | **C** | **A** | **T** |
| | [D respaldo] | 8 | 7 | 5 | 5 | 3 | 10,0 | 77 | 71 | 47 | 45 | 30 |
| | [D de config.] | 2 | 1 | 1 | 3 | 4 | 10,0 | 17 | 11 | 8 | 30 | 35 |
| | [D de Bit] | 9 | 8 | 7 | 7 | 5 | 10,0 | 85 | 79 | 67 | 68 | 45 |
| **[SW] Aplicaciones (Software)** | | **D** | **I** | **C** | **A** | **T** | **Frecuencia** | **D** | **I** | **C** | **A** | **T** |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | [SW SO] | 6 | 6 | 4 | 7 | 4 | 10,0 | 57 | 59 | 42 | 68 | 35 |
| | [SW BD] | 6 | 5 | 4 | 6 | 4 | 10,0 | 57 | 53 | 42 | 60 | 35 |
| | [SW Ant.] | 5 | 4 | 2 | 5 | 3 | 10,0 | 50 | 40 | 21 | 53 | 30 |
| | [SW Ofi] | 6 | 5 | 3 | 5 | 3 | 10,0 | 57 | 53 | 31 | 53 | 30 |
| | [SW moodle] | 5 | 5 | 3 | 5 | 3 | 10,0 | 50 | 46 | 31 | 45 | 30 |
| | [SW nav] | 4 | 3 | 3 | 4 | 2 | 10,0 | 35 | 33 | 26 | 38 | 20 |
| | [SW diseñ] | 2 | 5 | 2 | 5 | 3 | 10,0 | 21 | 46 | 16 | 45 | 30 |
| | [SW nomina] | 6 | 6 | 5 | 7 | 4 | 10,0 | 64 | 59 | 47 | 68 | 35 |
| | [SW contab] | 6 | 6 | 5 | 7 | 5 | 10,0 | 64 | 59 | 52 | 68 | 50 |
| | [SW glpi] | 2 | 2 | 1 | 2 | 1 | 10,0 | 20 | 21 | 10 | 15 | 5 |
| | [SW notas] | 6 | 6 | 5 | 7 | 4 | 10,0 | 57 | 59 | 52 | 68 | 40 |
| | [SW plagio] | 1 | 1 | 1 | 4 | 2 | 1,0 | 1 | 1 | 1 | 4 | 2 |
| | [SW bibliot] | 1 | 1 | 1 | 1 | 1 | 1,0 | 1 | 1 | 1 | 1 | 1 |
| | [SW horarios] | 1 | 1 | 1 | 1 | 1 | 1,0 | 1 | 1 | 1 | 1 | 1 |
| **[HW] Equipos informáticos (Hardware)** | | **D** | **I** | **C** | **A** | **T** | **Frecuencia** | **D** | **I** | **C** | **A** | **T** |
| | [HW pc] | 6 | 3 | 5 | 0 | 0 | 0,1 | 1 | 0 | 0 | 0 | 0 |
| | [HW portatil] | 4 | 3 | 5 | 0 | 0 | 0,1 | 0 | 0 | 0 | 0 | 0 |
| | [HW multif] | 5 | 3 | 4 | 0 | 0 | 0,1 | 0 | 0 | 0 | 0 | 0 |
| | [HW Serv] | 8 | 5 | 5 | 0 | 0 | 0,1 | 1 | 1 | 0 | 0 | 0 |
| | [HW ap] | 5 | 3 | 3 | 0 | 0 | 0,1 | 1 | 0 | 0 | 0 | 0 |
| | [HW switch] | 8 | 5 | 4 | 0 | 0 | 0,1 | 1 | 1 | 0 | 0 | 0 |
| | [HW videob] | 6 | 1 | 1 | 0 | 0 | 0,1 | 1 | 0 | 0 | 0 | 0 |
| | [HW pbx] | 8 | 5 | 6 | 0 | 0 | 0,1 | 1 | 1 | 1 | 0 | 0 |
| | [HW Ipad] | 5 | 3 | 3 | 0 | 0 | 0,1 | 0 | 0 | 0 | 0 | 0 |
| | [HW fotocop] | 7 | 3 | 4 | 0 | 0 | 0,1 | 1 | 0 | 0 | 0 | 0 |
| | [HW tv] | 5 | 2 | 1 | 0 | 0 | 0,1 | 0 | 0 | 0 | 0 | 0 |
| | [HW modem] | 5 | 3 | 2 | 0 | 0 | 0,1 | 0 | 0 | 0 | 0 | 0 |
| **[COM] Redes de Comunicación** | | **D** | **I** | **C** | **A** | **T** | **Frecuencia** | **D** | **I** | **C** | **A** | **T** |
| | [COM LAN] | 7 | 6 | 6 | 7 | 4 | 1,0 | 7 | 6 | 6 | 7 | 4 |
| | [COM wifi] | 7 | 6 | 4 | 4 | 2 | 1,0 | 7 | 6 | 4 | 4 | 2 |
| | [COM Internte] | 7 | 6 | 5 | 5 | 4 | 1,0 | 7 | 6 | 5 | 5 | 4 |
| | [COM telefonía] | 6 | 6 | 5 | 5 | 4 | 1,0 | 6 | 6 | 5 | 5 | 4 |
| **[MEDIA] Dispositivos de almacenamiento de información** | | **D** | **I** | **C** | **A** | **T** | **Frecuencia** | **D** | **I** | **C** | **A** | **T** |
| | [MEDIA DD] | 5 | 4 | 4 | 0 | 0 | 1,0 | 5 | 4 | 4 | 0 | 0 |
| | [MEDIA usb] | 4 | 3 | 4 | 0 | 0 | 1,0 | 4 | 3 | 4 | 0 | 0 |
| | [MEDIA electronic] | 7 | 6 | 6 | 0 | 0 | 1,0 | 7 | 6 | 6 | 0 | 0 |

| [AUX] Equipamiento Auxiliar | | D | I | C | A | T | Frecuencia | D | I | C | A | T |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | [AUX ups] | 6 | 0 | 1 | 0 | 0 | 1,0 | 6 | 0 | 1 | 0 | 0 |
| | [AUX cableado] | 7 | 1 | 3 | 0 | 0 | 1,0 | 7 | 1 | 3 | 0 | 0 |
| | [AUX rack] | 7 | 1 | 4 | 0 | 0 | 1,0 | 7 | 1 | 4 | 0 | 0 |
| | [AUX gabinte] | 7 | 1 | 4 | 0 | 0 | 1,0 | 7 | 1 | 4 | 0 | 0 |
| | [AUX fibra] | 6 | 1 | 3 | 0 | 0 | 1,0 | 6 | 1 | 3 | 0 | 0 |
| **[L] Instalaciones** | | **D** | **I** | **C** | **A** | **T** | **Frecuencia** | **D** | **I** | **C** | **A** | **T** |
| | [L administrativa] | 8 | 4 | 6 | 0 | 0 | 1,0 | 8 | 4 | 6 | 0 | 0 |
| | [L escuelas] | 9 | 3 | 6 | 0 | 0 | 1,0 | 9 | 3 | 6 | 0 | 0 |
| **[P] Personal** | | **D** | **I** | **C** | **A** | **T** | **Frecuencia** | **D** | **I** | **C** | **A** | **T** |
| | [P ui] | 2 | 0 | 4 | 0 | 0 | 0,01 | 0 | 0 | 0 | 0 | 0 |
| | [P ue] | 2 | 0 | 3 | 0 | 0 | 0,01 | 0 | 0 | 0 | 0 | 0 |
| | [P soperte] | 2 | 0 | 4 | 0 | 0 | 0,10 | 0 | 0 | 0 | 0 | 0 |
| | [P adm] | 3 | 0 | 4 | 0 | 0 | 0,10 | 0 | 0 | 0 | 0 | 0 |
| | [P com] | 4 | 0 | 4 | 0 | 0 | 0,10 | 0 | 0 | 0 | 0 | 0 |
| | [P sec] | 5 | 0 | 4 | 0 | 0 | 0,10 | 0 | 0 | 0 | 0 | 0 |
| | P dba] | 2 | 0 | 2 | 0 | 0 | 0,10 | 0 | 0 | 0 | 0 | 0 |
| | [P rector] | 5 | 0 | 5 | 0 | 0 | 0,10 | 0 | 0 | 0 | 0 | 0 |
| | [P Proc] | 3 | 0 | 5 | 0 | 0 | 0,10 | 0 | 0 | 0 | 0 | 0 |
| | [P Calidad] | 3 | 0 | 4 | 0 | 0 | 0,01 | 0 | 0 | 0 | 0 | 0 |
| | [P proveedores] | 3 | 0 | 4 | 0 | 0 | 0,01 | 0 | 0 | 0 | 0 | 0 |

**Tabla 14 Valoración de riesgos de activos**

El Colegio, a través de su comité de seguridad de la información, acogió que las valoraciones mayores a 50, recibirán la evaluación correspondiente a fin de encaminar acciones para la mitigación del riesgo en un plazo corto. Por su parte, una valoración menor, se considera aceptable. En tal sentido, los controles a implementar pretenderán ubicar como mínimo la valoración del riesgo en niveles de aceptación.

Así las cosas, para las valoraciones de riesgos comprendidas entre 10 y 50, se evaluarán a fin de poder encaminar esfuerzos a través de su integración con planes de acción de mitigación de riesgos y controles específicos en un plazo medio.

Sin embargo, las valoraciones menores a 10, se estimarán de tal manera que se efectúen mediciones periódicas a fin de concertar que sus niveles permanecen bajo este rango y de tal manera no presuponen acciones a corto ni mediano plazo.

No obstante, después de la implementación de controles a que haya lugar, el riesgo se reduce, pero no se elimina completamente. Dicho riesgo es denominado riesgo residual, aquel que continúa existiendo una vez se aplican los controles de seguridad estimados.

## 4. Propuestas de Proyectos

Identificados los niveles de riesgos asociados a cada uno de los activos de la Institución, se procede a plantear una serie de proyectos que permitan la mitigación de los niveles de riesgos hasta niveles de aceptación. Esta consideración se toma ya que el Colegio está en una fase inicial en cuanto al aseguramiento de la información.

Así las cosas, se planean una serie de proyectos que permitan ubicar el nivel del riesgo de los activos en un nivel de "Riesgo moderado", es decir, riesgos cuya valoración tengan un valor inferior a 50. De esta manera nos centraremos en aquellos activos en los que actualmente su riesgo supera el valor de 50.

### 4.1. Proyectos Planteados

Con los siguientes proyectos avanzamos hacia el cumplimiento ISO y por ende iniciamos el camino de la mitigación de riesgos y la mejora continua al interior de la Institución. Así las cosas, tenemos:

| PROYECTO | | DOMINIO | RIESGOS POR MITIGAR |
|---|---|---|---|
| 1 | Selección, adquisición, parametrización y puesta en funcionamiento de una solución de Firewall perimetral de nueva generación. | 9.1.2, 9.4.1, 9.4.4, 12.2.1, 12.5.1, 13.1, 14.1.2, 14.1.3, | [A.5], [A.6], [A.7], [A.8], [A.11], [A.12], [A.14], [A.15], [A.19], [A.24], [A.25] |
| 2 | Selección, adquisición, parametrización y puesta en funcionamiento de una solución de IDS/IPS. | 12.2.1, 13.1.1, 16.1.2 | [A.5], [A.6], [A.7], [A.8], [A.11], [A.12], [A.14], [A.24] |
| 3 | Adquisición, parametrización y puesta en funcionamiento de una solución de administración, almacenamiento y reporte de Logs. | 12.7.1, 16.1, 18.1.3 | [E.2], [A.5], [A,6], [A.7], [A.12], [A.13], [A.14], [A.15], [A.24] |
| 4 | Campaña de Sensibilización en seguridad de la Información, enfocados hacia la población Administrativa, técnica y estudiantil. | 7.2, 9.2, 11.2.8, 11.2.9, 15.1.1, 16.1.2, 16.1.3, 16.1.6, 18.1.1, 18.1.4, 18.2.2 | [E.1], [E.8], [E.19], [A.15], [A.19], [A.30] |
| 5 | Consolidación e implementación de Política de Seguridad Institucional | 5.1, 6.1, 9.1.1, 9.2, 9.3 | [A.11], [A.23], [E.1], [E.2], [E.15] |
| 6 | Consolidación y reubicación del centro de datos. | 11.1.2, 11.1.4, 11.1.5, 17.2.1, | [E.2], [E.23], [I*], [I.1], [I.2], [I.6], [I.7] |
| 7 | Consolidación y reubicación de los centros de cableados. | 11.1.2, 11.1.4, 17.2.1, | [I*], [I.1], [I.2], [I.6], [I.7] |

| | | | |
|---|---|---|---|
| 8 | Implementación de un sistema para copias de respaldo. | 12.3 | [A.23], [A.24], [A.25], [E.1], [E.2], [E.15], [E.18], [E.21] |
| 9 | Clasificación de la información y reporte de bases de datos. | 8.2.1, 8.2.2, 18.1.3, 18.1.4, 18.1.5 | [A.6], [A.11], [A.25] |
| 10 | Disposición del sistema de mesa de ayuda para el reporte de incidentes de seguridad de la información. | 16.1.2, 16.1.3, 16.1.4, 16.1.5, 16.1.6 | |
| 11 | Implementación de plan de auditoria al SGSI. | 18.2.2, 18.2.3 | |

**Tabla 15 Proyectos Planteados**

Para el desarrollo de los proyectos planteados, se estiman los siguientes detalles para su desarrollo:

### 4.1.1. Selección, adquisición, parametrización y puesta en funcionamiento de una solución de Firewall perimetral de nueva generación.

- **Objetivo:** Realizar el proceso de selección que permita adquirir, parametrizar y poner en funcionamiento una solución de firewall perimetral de nueva generación.

- **Alcance:** Deberá cubrir la totalidad de la Institución.

- **Responsables:** Director de Tecnología

- **Departamentos Involucrados:** Rectoría y Procuraduría**.**

- **Etapas del proyecto:**

  - ✓ Estudio de mercados
  - ✓ Proceso de selección
  - ✓ Diseño de implementación
  - ✓ Etapa de identificación de tráfico
  - ✓ Configuración de políticas
  - ✓ Pruebas
  - ✓ Puesta en funcionamiento

- **Recursos**

  - **Recursos Tecnológicos**

    - Hardware de propósito especifico de solución seleccionada.
    - Software de solución seleccionada. Tanto el hardware como el software deberán ser del mismo fabricante.
    - Licenciamiento a un año del fabricante con los módulos adquiridos

- Todos los elementos necesarios para la correcta instalación de la solución.

- **Recursos de personal**

  - Ingeniero certificado por el fabricante para la instalación, configuración y puesta en funcionamiento de la solución adquirida.
  - El contratista deberá garantizar la entrega de la solución acorde a las etapas del proyecto y suministrar transferencia de conocimiento de la solución adquirida y capacitación en la gestión y administración de esta a mínimo dos ingenieros de la Institución.
  - Posterior a la entrega por parte del contratista, se destinará un ingeniero para la administración de la solución perteneciente al departamento de Tecnología por cuanto no es necesaria la contratación de personal externo.

- **Costo Aproximado:** $180.000.000

- **Plazo:** El plazo para este proyecto es considerado como un tiempo medio, teniendo en cuenta que los proyectos se ejecutan acorde a la valoración presupuestal que se realiza para cada año académico. En tal sentido, su disposición está estimada en un lapso de 12 meses.

### 4.1.2. Selección, adquisición, parametrización y puesta en funcionamiento de una solución de IDS/IPS.

- **Objetivo:** Realizar el proceso de selección que permita adquirir, parametrizar y poner en funcionamiento una solución de detección y prevención de intrusos IDS/IPS.

- **Alcance:** Deberá cubrir la totalidad de la Institución.

- **Responsables:** Director de Tecnología

- **Departamentos Involucrados:** Rectoría y Procuraduría**.**

- **Etapas del proyecto:**

  - ✓ Estudio de mercados
  - ✓ Proceso de selección
  - ✓ Diseño de implementación
  - ✓ Etapa de identificación de tráfico
  - ✓ Configuración de políticas
  - ✓ Pruebas
  - ✓ Puesta en funcionamiento

- **Recursos**

    - **Recursos Tecnológicos**

        - Hardware de la solución seleccionada.
        - Software de solución seleccionada. Tanto el hardware como el software deberán ser del mismo fabricante.
        - Licenciamiento a un año del fabricante con los módulos adquiridos
        - Todos los elementos necesarios para la correcta instalación de la solución.

    - **Recursos de personal**

        - Ingeniero certificado por el fabricante para la instalación, configuración y puesta en funcionamiento de la solución adquirida.
        - El contratista deberá garantizar la entrega de la solución acorde a las etapas del proyecto y suministrar transferencia de conocimiento de la solución adquirida y capacitación en la gestión y administración de esta a mínimo dos ingenieros de la Institución.
        - Posterior a la entrega por parte del contratista, se destinará un ingeniero para la administración de la solución perteneciente al departamento de Tecnología por cuanto no es necesaria la contratación de personal externo.

- **Costo Aproximado:** $90.000.000

- **Plazo:** El plazo para este proyecto es considerado como un tiempo medio, teniendo en cuenta que los proyectos se ejecutan acorde a la valoración presupuestal que se realiza para cada año académico. En tal sentido, su disposición está estimada en un lapso de 10 meses.

### 4.1.3. Adquisición, parametrización y puesta en funcionamiento de una solución de administración, almacenamiento y reporte de Logs.

- **Objetivo:** Realizar el proceso de selección que permita adquirir, parametrizar y poner en funcionamiento una solución de almacenamiento y reporte de Los.

- **Alcance:** Deberá integrar, almacenar y parametrizar los reportes generados por la solución de Firewall perimetral y la solución de IDS/IPS.

- **Responsables:** Director de Tecnología

- **Departamentos Involucrados:** Rectoría y Procuraduría**.**

- **Etapas del proyecto:**

    - ✓ Estudio de mercados

- ✓ Proceso de selección
- ✓ Diseño de implementación
- ✓ Etapa de identificación de tráficos
- ✓ Configuración de políticas
- ✓ Pruebas
- ✓ Puesta en funcionamiento

- **Recursos**

  - **Recursos Tecnológicos**

    - Hardware de la solución seleccionada.
    - Software de solución seleccionada. Tanto el hardware como el software deberán ser del mismo fabricante.
    - Licenciamiento a un año del fabricante con los módulos adquiridos
    - Todos los elementos necesarios para la correcta instalación de la solución.

  - **Recursos de personal**

    - Ingeniero certificado por el fabricante para la instalación, configuración y puesta en funcionamiento de la solución adquirida.
    - El contratista deberá garantizar la entrega de la solución acorde a las etapas del proyecto y suministrar transferencia de conocimiento de la solución adquirida y capacitación en la gestión y administración de esta a mínimo dos ingenieros de la Institución.
    - Posterior a la entrega por parte del contratista, se destinará un ingeniero para la administración de la solución perteneciente al departamento de Tecnología por cuanto no es necesaria la contratación de personal externo.

- **Costo Aproximado:** $40.000.000

- **Plazo:** El plazo para este proyecto es considerado como un tiempo corto, teniendo en cuenta que los proyectos se ejecutan acorde a la valoración presupuestal que se realiza para cada año académico. En tal sentido, su disposición está estimada en un lapso de 4 meses.

### 4.1.4. Campaña de Sensibilización en seguridad de la Información, enfocados hacia la población Administrativa, técnica y estudiantil.

- **Objetivo:** Realizar campaña de sensibilización en seguridad de la información a toda la comunidad educativa.

- **Alcance:** El programa de sensibilización deberá cubrir toda la comunidad educativa, es decir: áreas administrativas, profesores y estudiantes.

- **Responsables:** Director de Tecnología

- **Departamentos Involucrados:** Rectoría, Procuraduría y Direcciones de escuelas**.**

- **Etapas del proyecto:**

    - ✓ Elaboración de plan de capacitación
    - ✓ Selección de conferencistas
    - ✓ Cronograma de actividades
    - ✓ Ejecución del plan de capacitación
    - ✓ Evaluación de las actividades de capacitación a través de encuestas y propuesta de mejora.

- **Recursos**

    - **Recursos Tecnológicos**

        - Computadores de colaboradores
        - Salas de TI
        - Sistema de carteleras digitales
        - Correo electrónico Institucional

    - **Recursos de personal**

        - Tres conferencistas seleccionados para la ejecución del plan de capacitación.

- **Costo Aproximado:** $8.500.000

- **Plazo:** El plazo para este proyecto es considerado como un tiempo corto, teniendo en cuenta que los proyectos se ejecutan acorde a la valoración presupuestal que se realiza para cada año académico. En tal sentido, su disposición está estimada en un lapso de 6 meses.

### 4.1.5. Consolidación e implementación de Política de Seguridad Institucional

- **Objetivo:** Crear la norma rectora que permita apalancar el cumplimiento del Sistema de Seguridad de la Información de la Institución.

- **Alcance:** Fijar el compendio de normas, directrices y buenas prácticas de seguridad teniendo en cuenta, la necesidad de su cumplimiento en la totalidad de los departamentos.

- **Responsables:** Director de Tecnología

- **Departamentos Involucrados:** Rectoría y Procuraduría.

- **Etapas del proyecto:**

    - ✓ Revisión de normatividad
    - ✓ Consolidación de procesos
    - ✓ Redacción de políticas
    - ✓ Socialización
    - ✓ Revisión por parte de la dirección
    - ✓ Puesta en conocimiento de la Institución

- **Recursos**

    - **Recursos Tecnológicos**

        - Computadores de colaboradores
        - Salas de conferencias
        - Sistema de carteleras digitales
        - Correo electrónico Institucional

    - **Recursos de personal**

        - Ingeniero director del departamento de TI, de la Institución.
        - Ingeniero coordinador de proyectos, de la Institución.

- **Costo Aproximado:** $5.000.000

- **Plazo:** El plazo para este proyecto es considerado como un tiempo corto, teniendo en cuenta que los proyectos se ejecutan acorde a la valoración presupuestal que se realiza para cada año académico. En tal sentido, su disposición está estimada en un lapso de 4 meses.

### 4.1.6. Consolidación y reubicación del centro de datos.

- **Objetivo:** Construir el centro de datos Institucional.

- **Alcance:** Se deberá consolidad el centro de datos, acorde con las recomendaciones en cuanto a ubicación y tecnología para tal fin.

- **Responsables:** Director de Tecnología

- **Departamentos Involucrados:** Rectoría, Procuraduría y consejo superior.

- **Etapas del proyecto:**

    - ✓ Consultoría para el diseño y ubicación
    - ✓ Proceso de selección
    - ✓ Estudio de ofertas
    - ✓ Disposición y construcción

- ✓ Traslado de elementos
- ✓ Puesta en operación

- **Recursos**

  - **Recursos Tecnológicos**

    - Reemplazo de equipos según consultoría.
    - Equipos de TI existentes en el centro de datos actual.

  - **Recursos de personal**

    - Ingeniero líder de proyecto de la consultoría.
    - Equipo de trabajo contratista,
    - Posterior a la entrega por parte del contratista, es decir posterior a la etapa de puesta en operación, se destinará un Ingeniero como administrador del centro de datos institucional. El Ingeniero actualmente esta adscrito a la Institución y no se requiere contratación de nuevo personal para tal fin.

- **Costo Aproximado:** $600.000.000

- **Plazo:** El plazo para este proyecto es considerado a largo plazo, teniendo en cuenta que los proyectos se ejecutan acorde a la valoración presupuestal que se realiza para cada año académico. En tal sentido, su disposición está estimada para ejecutarse en su totalidad en los próximos 5 años.

### 4.1.7. Consolidación y reubicación de los centros de cableados.

- **Objetivo:** consolidar los cuartos de cableados en sitios acordes para tal fin.

- **Alcance:** Se deberá consolidar los cuartos de cableado en máximo 5 cuartos de cableado con la disposición necesaria para tal fin.

- **Responsables:** Director de Tecnología

- **Departamentos Involucrados:** Rectoría, Procuraduría y consejo superior.

- **Etapas del proyecto:**

  - ✓ Auditoria para el diseño y ubicación
  - ✓ Proceso de selección
  - ✓ Estudio de ofertas
  - ✓ Disposición y construcción
  - ✓ Traslado de elementos
  - ✓ Puesta en operación

- **Recursos**

    - **Recursos Tecnológicos**

        - Reemplazo de equipos según consultoría.
        - Equipos de TI existentes en el centro de datos actual.

    - **Recursos de personal**

        - Ingeniero líder de proyecto de la consultoría.
        - Equipo de trabajo contratista,
        - Posterior a la entrega por parte del contratista, se destinará un Tecnólogo para el seguimiento constante de los nuevos centros de cableado. El tecnólogo propuesto actualmente está adscrito a la Institución y no se requiere contratación de nuevo personal para tal fin

- **Costo Aproximado:** $200.000.000

- **Plazo:** El plazo para este proyecto es considerado a largo plazo, teniendo en cuenta que los proyectos se ejecutan acorde a la valoración presupuestal que se realiza para cada año académico. En tal sentido, su disposición está estimada para ejecutarse en su totalidad en los próximos 3 años.

### 4.1.8. Implementación de un sistema para copias de respaldo.

- **Objetivo:** Implementar un sistema para realizar copias de respaldo y recuperación.

- **Alcance:** Sistema de almacenamiento en la nube para el respaldo de información, configuraciones y recuperación en caso de ser necesario.

- **Responsables:** Director de Tecnología

- **Departamentos Involucrados:** Procuraduría.

- **Etapas del proyecto:**

    - ✓ Estudio de mercados
    - ✓ Proceso de selección
    - ✓ Puesta en funcionamiento

- **Recursos**

    - **Recursos Tecnológicos**

        - Solución de almacenamiento en la nube.
        - Canal de internet.
        - Servidor para generar las copias de seguridad.

- **Recursos de personal**

    - Se destinará un ingeniero para la administración de la solución perteneciente al departamento de Tecnología por cuanto no es necesaria la contratación de personal externo.

- **Costo Aproximado:** $800.000 canon mensual.

- **Plazo:** El plazo para este proyecto es considerado en un corto plazo, teniendo en cuenta que los proyectos se ejecutan acorde a la valoración presupuestal que se realiza para cada año académico. En tal sentido, su disposición está estimada para ejecutarse en su totalidad en los próximos 3 meses.

### 4.1.9. Clasificación de la información y reporte de bases de datos.

- **Objetivo:** Realizar la clasificación de la información y proceder con el respectivo registro de bases de datos ante la SIC.

- **Alcance:** Clasificar la totalidad de la información y estimar las bases de datos contenedoras en la Institución.

- **Responsables:** Director de Tecnología

- **Departamentos Involucrados:** Procuraduría.

- **Etapas del proyecto:**

    - ✓ Clasificación de la Información
    - ✓ Inscripción de las bases de datos
    - ✓ Actualizaciones periódicas

- **Recursos**

    - **Recursos Tecnológicos**

        - Computadores de los colaboradores.
        - Servidores donde se encuentran alojadas bases de datos.

    - **Recursos de personal**

        - Se destinarán dos ingenieros para la liderar el proceso de clasificación de la información y el correspondiente reporte a la SIC.
        - Abogado asesor para la actividad descrita anteriormente.
        - Los tres profesionales se encuentran adscritos a la Institución y en consecuencia no se requiere contratación de personal adicional.

- **Costo Aproximado:** $2.000.000. Se estima el costo como el porcentaje mensual de los dos colaboradores dispuestos para tal fin.

- **Plazo:** El plazo para este proyecto es considerado en un corto plazo, teniendo en cuenta que los proyectos se ejecutan acorde a la valoración presupuestal que se realiza para cada año académico. En tal sentido, su disposición está estimada para ejecutarse en su totalidad en los próximos 4 meses.

### 4.1.10. Disposición del sistema de mesa de ayuda para el reporte de incidentes de seguridad de la información.

- **Objetivo:** Disponer del sistema de mesa de ayuda para el reporte de incidentes de seguridad de la información.

- **Alcance:** Adquirir solución especializada para mesa de ayuda y parametrizarla acorde a las necesidades de la institución.

- **Responsables:** Director de Tecnología

- **Departamentos Involucrados:** Procuraduría.

- **Etapas del proyecto:**

  - ✓ Estudio de mercados
  - ✓ Proceso de selección
  - ✓ Parametrización de la solución
  - ✓ Pruebas
  - ✓ Puesta en funcionamiento

- **Recursos**

  - **Recursos Tecnológicos**

    - Software de mesa de ayuda y creación de tickes
    - Servidor para implementar la solución
    - Computadores para gestión de requerimientos.

  - **Recursos de personal**

    - Se destinarán dos técnicos para atender los requerimientos dispuestos en la solución de mesa de ayuda. Los dos colaboradores actualmente desempeñan este rol, con controles a través de software libre sin parametrización acorde a la institución.

- **Costo Aproximado:** $10.000.000.

- **Plazo:** El plazo para este proyecto es considerado en un corto plazo, teniendo en cuenta que los proyectos se ejecutan acorde a la valoración presupuestal que se

realiza para cada año académico. En tal sentido, su disposición está estimada para ejecutarse en su totalidad en los próximos 6 meses.

### 4.1.11. Implementación de plan de auditoria al SGSI.

- **Objetivo:** Realizar el seguimiento posterior al SGSI acorde con la norma ISO 270001:2013

- **Alcance:** Se abarcan todos los departamentos contemplados en el SGSI.

- **Responsables:** Director de Tecnología

- **Departamentos Involucrados:** Procuraduría, Dirección de calidad y Rectoría.

- **Etapas del proyecto:**

  - ✓ Designación de auditores
  - ✓ Formación de auditores
  - ✓ Planeación del programa de auditorias
  - ✓ Realización de auditorias
  - ✓ Revisión de resultados.

- **Recursos**

  - **Recursos Tecnológicos**

    - Computadores de colaboradores
    - Almacenamiento de auditorías en solución dispuesta para tal fin.

  - **Recursos de personal**

    - Instructor o centro de estudios para la formación del personal auditor.
    - Se destinarán dos profesionales para liderar el plan de auditoria del SGSI, el director de tecnología y la directora de Calidad.

- **Costo Aproximado:** $9.000.000.

- **Plazo:** El plazo para este proyecto es considerado en un mediano plazo, teniendo en cuenta que los proyectos se ejecutan acorde a la valoración presupuestal que se realiza para cada año académico. En tal sentido, su disposición está estimada para ejecutarse en su totalidad en los próximos 18 meses.

La ejecución, costo y tiempo de ejecución de los proyectos planteados anteriormente se pueden resumir de la siguiente manera:

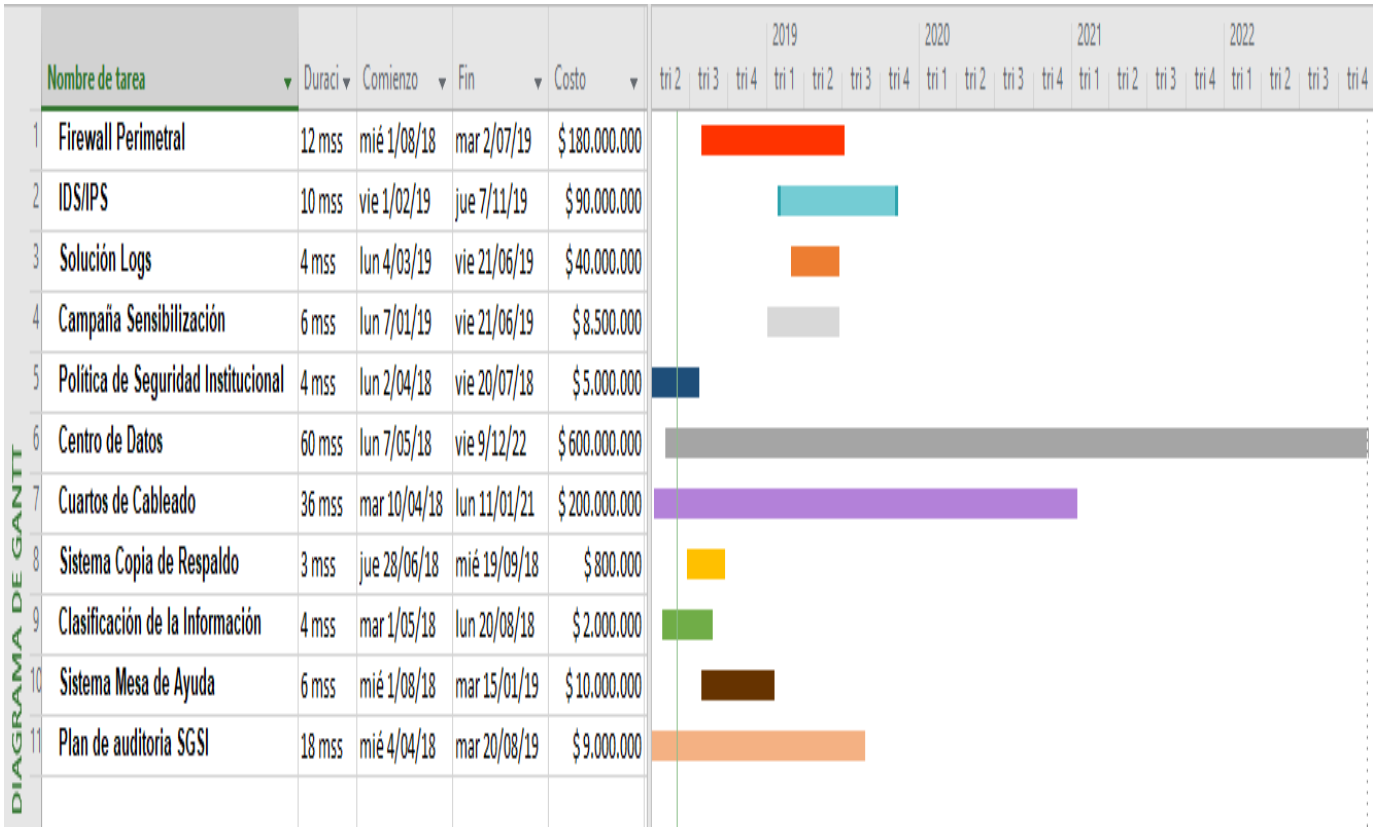


**Imagen 7 Planificación de Proyectos**

## 5. Auditoria de Cumplimiento

Como se ha mencionado anteriormente, la Institución está en una fase inicial para la adopción de un Sistema de Gestión de Seguridad de la Información, por lo que supondremos la puesta en marcha de los proyectos planteados para la evaluación de la madurez de los controles concebidos en la norma ISO/IEC 27002:2013, mediante Auditoria de Cumplimiento.

### 5.1. Metodología

Para el desarrollo de la Auditoria de Cumplimiento, usaremos el Modelo de Madurez de la Capacidad (CMM Capability Maturity Model), desarrollado por el Software Engineer Insitute, el cual comprende un análisis de los 114 controles concebidos en la norma ISO/IEC 27002:2013 para alcanzar los diferentes objetivos de control. Así las cosas, nos basaremos en la siguiente escala de valoración:

| EFECTIVIDAD | CMM | SIGNIFICADO | DESCRIPCIÓN |
|---|---|---|---|
| **0%** | **L0** | Inexistente | Carencia completa de cualquier proceso reconocible.<br>No se ha reconocido siquiera que existe un problema a resolver. |
| **10%** | **L1** | Inicial / Ad-hoc | Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal.<br>Los procedimientos son inexistentes o localizados en áreas concretas.<br>No existen plantillas definidas a nivel corporativo. |
| **50%** | **L2** | Reproducible,<br>pero intuitivo | Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea.<br>Se normalizan las buenas prácticas en base a la experiencia y al método.<br>No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo.<br>Se depende del grado de conocimiento de cada individuo. |
| **90%** | **L3** | Proceso definido | La organización entera participa en el proceso.<br>Los procesos están implantados, documentados y comunicados mediante entrenamiento. |
| **95%** | **L4** | Gestionado y medible | Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos.<br>Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia. |

| | | | |
|---|---|---|---|
| **100%** | **L5** | Optimizado | Los procesos están bajo constante mejora.<br>En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos. |

**Tabla 16 Criterios para la Evaluación del Modelo de Madurez**

## 5.2. Evaluación de la Madurez

Teniendo en cuenta los criterios descritos en la Tabla 16 Criterios para la Evaluación del Modelo de Madurez, procedemos a revisar los controles de la norma ISO/IEC 27002:2013, tal y como se describe en el Anexo 7 Nivel de Cumplimiento. De manera tal que nos enfocamos para la evaluación de la madurez de la seguridad, en los controles de la norma, es decir en los siguientes dominios:

| Dominios |
|---|
| 5. POLÍTICAS DE SEGURIDAD. |
| 6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN |
| 7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS. |
| 8. GESTIÓN DE ACTIVOS. |
| 9. CONTROL DE ACCESOS. |
| 10. CIFRADO. |
| 11. SEGURIDAD FÍSICA Y AMBIENTAL. |
| 12. SEGURIDAD EN LA OPERACIONES |
| 13. SEGURIDAD EN LAS TELECOMUNICACIONES. |
| 14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN. |
| 15. RELACIONES CON SUMINISTRADORES |
| 16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN. |
| 17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO. |
| 18. CUMPLIMIENTO. |

**Tabla 17 Dominios de control ISO/IEC 27002:2013**

## 5.3. Presentación de Resultados

Teniendo en cuenta las consideraciones de los numerales previos, podemos resumir el número de controles implementados y la clasificación de estos en los niveles de madurez descritos en la metodología, como se observa a continuación:

| Nivel de Madurez | Controles por Nivel |
|---|---|
| L0 | 2 |
| L1 | 7 |
| L2 | 11 |
| L3 | 27 |
| L4 | 60 |
| L5 | 2 |
| N.A | 5 |
| Total | 114 |

**Tabla 18 Nivel de Madurez por control**

De esta manera, podemos establecer el nivel de madurez porcentual para los 114 controles, así:

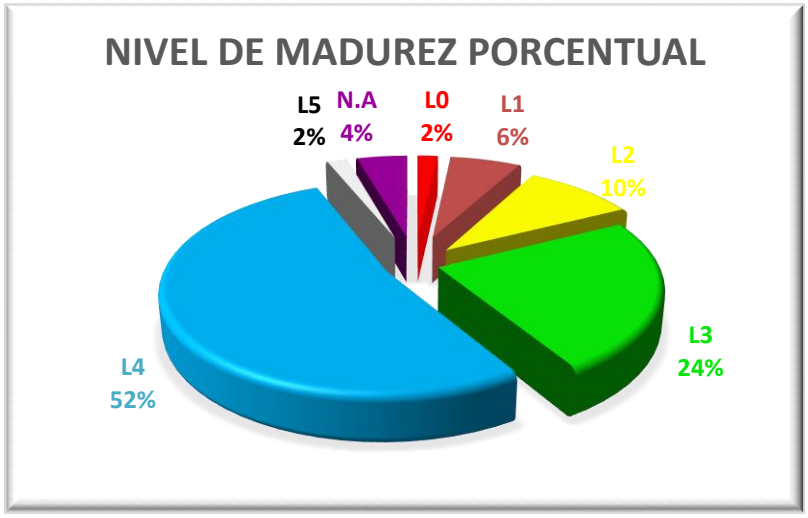


**Imagen 8 Nivel de Madurez Porcentual**

Una apreciación un poco más en detalle la podemos observar en el siguiente diagrama de radar, donde se evidencia el nivel cumplimiento para cada uno de los dominios de la norma. De esta manera tenemos:


**Imagen 9 Nivel de Cumplimiento por Capítulo ISO**

Para la Institución, el nivel de cumplimiento objetivo es el denominado “Proceso Definido”, que acumula un porcentaje de 90%, y seguir con las medidas necesarias de mejora continua para optar a un cumplimiento “Optimizado” o del 100%. En consecuencia, haremos la comparación del nivel de cumplimiento posterior a los proyectos y el nivel objetivo inicial en el Colegio:

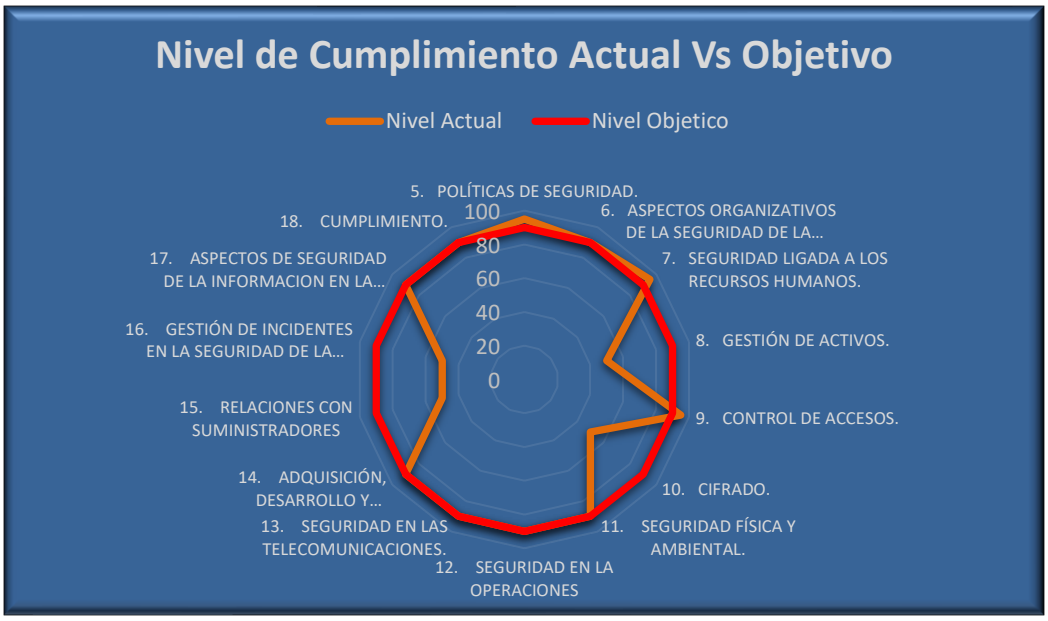


**Imagen 10 Nivel de Cumplimiento Actual Vs Objetivo**

Así las cosas, podemos revisar el aumento en el nivel de cumplimiento posterior a la implantación de los proyectos, frente al estado inicial establecido en el análisis diferencial efectuado en los comienzos del proyecto. No obstante, tenemos:

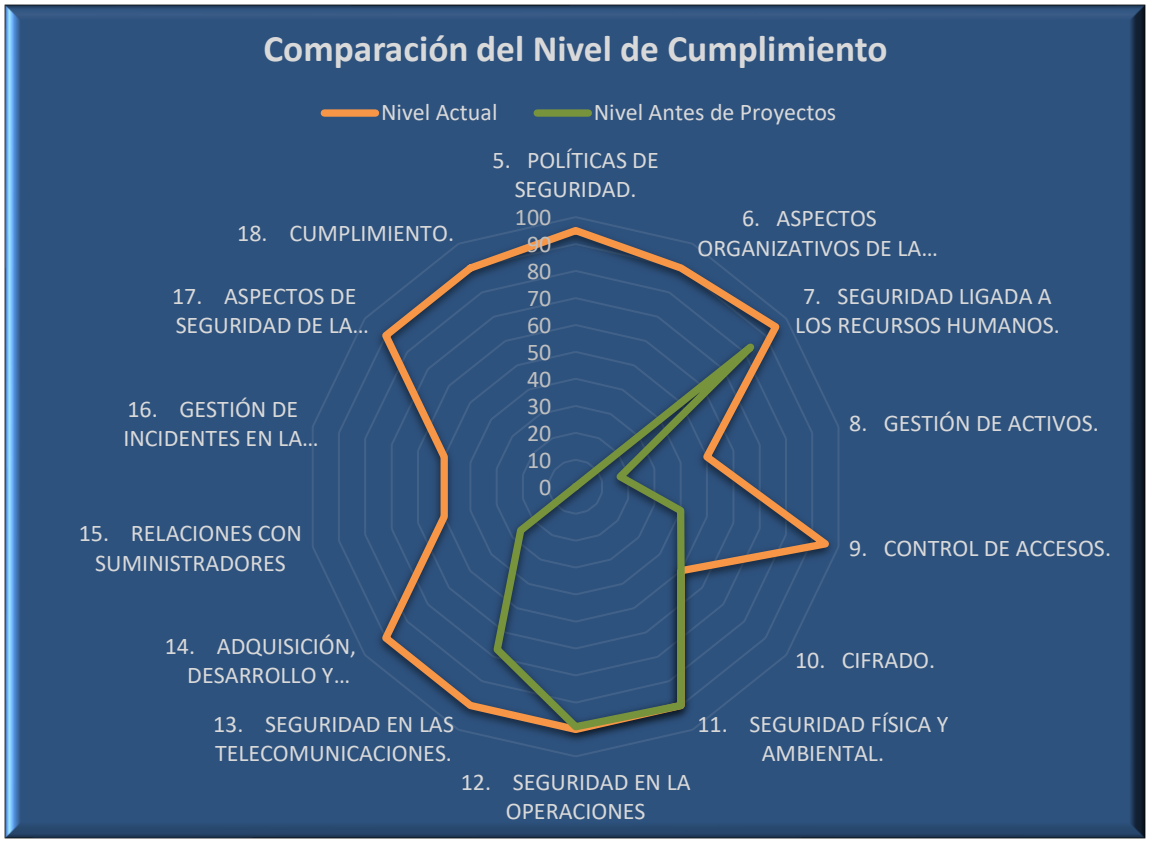


**Imagen 11 Nivel de Cumplimiento Actual Vs Inicial**

De los 114 controles, se encuentra en la evaluación de la madurez, que 13 de ellos requieren atención debido a la criticidad de estas, entre las que se encuentra, 9 no conformidades mayores y 4 no conformidades menores.

| Dominios | NC Menor | NC Mayor |
|---|---|---|
| 5. POLÍTICAS DE SEGURIDAD. | | |
| 6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN | | |
| 7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS. | | |
| 8. GESTIÓN DE ACTIVOS. | 2 | 3 |
| 9. CONTROL DE ACCESOS. | | |
| 10. CIFRADO. | | |
| 11. SEGURIDAD FÍSICA Y AMBIENTAL. | | |
| 12. SEGURIDAD EN LA OPERACIONES | 2 | |
| 13. SEGURIDAD EN LAS TELECOMUNICACIONES. | | |

| | | |
|---|---|---|
| 14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN. | | |
| 15. RELACIONES CON SUMINISTRADORES | | 1 |
| 16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN. | 3 | |
| 17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO. | 1 | |
| 18. CUMPLIMIENTO. | 1 | |

**Tabla 19 Resumen de No Conformidades**

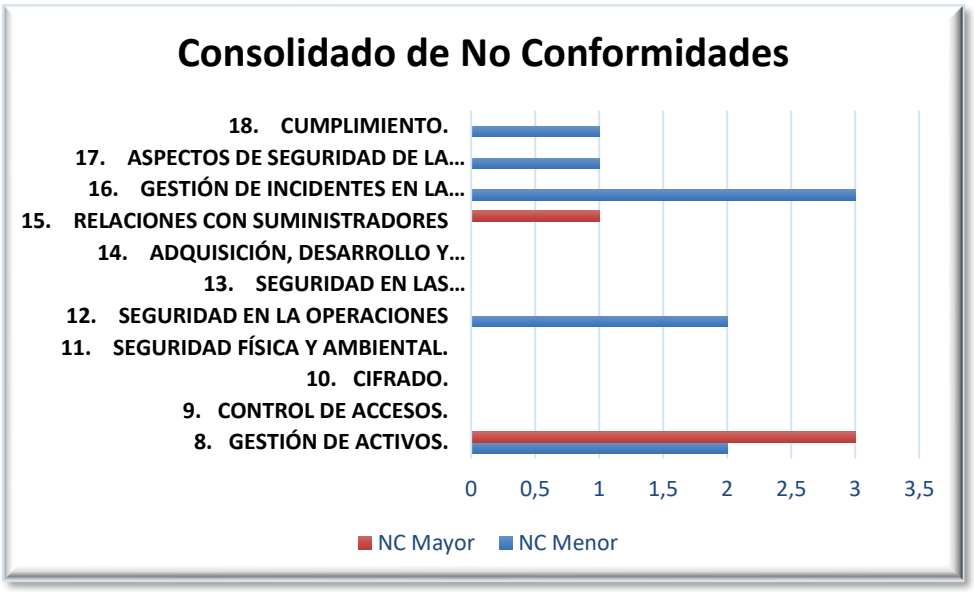


**Imagen 12 Consolidado de No Conformidades**

Los detalles de las no conformidades se encuentran estipulados en el Anexo 8 Informe de Auditoria.

## 6. Resultados Finales

Este apartado concentra la realización de una serie de documentos que permiten apalancar el proyecto y presentar los resultados de las diferentes actividades que se realizaron a lo largo de este documento. Así las cosas, se tiene:

### 6.1. Resumen Ejecutivo

El resumen ejecutivo comprende un resumen del proyecto realizado de forma clara y concreta que se pueda socializar ante la alta dirección. Dicho documento se encuentra descrito en el documento complementario denominado “Resumen Ejecutivo”.

### 6.2. Presentación de Riesgos

Presentación efectuada debido al análisis de Riesgos efectuado, destacando principalmente los activos más significativos, riesgos identificados y los proyectos estimados para la mitigación de los riesgos hasta niveles de aceptación. Esta presentación se encuentra en el documento complementario denominado “Presentación de Riesgos”.

### 6.3. Presentación del Proyecto

Presentación elaborada en razón a la realización del proyecto, donde se encuentran las fases de este, desarrollo de cada una y las conclusiones obtenidas como resultado. Esta presentación se documenta en archivo complementario denominado “Presentación Global del Proyecto”.

### 6.4. Video de Presentación del Proyecto

El vídeo se elabora a modo explicativo y de sustentación del apartado denominado Presentación del Proyecto. En tal sentido, configura el relato del desarrollo del proyecto, su realización y principales aportes o conclusiones. Este vídeo se encuentra en el documento complementario denominado “Video de Presentación del Proyecto”.

## 7. Conclusiones

- Al inicio del proyecto se pudo establecer que el nivel de cumplimiento respecto a la normatividad ISO era mínimo y por ello la importancia de adelantar el plan director correspondiente.

- Para la creación del Sistema de Seguridad de la Información, se debe consolidar un esquema documental acorde a las necesidades institucionales, basados en la norma ISO/IEC 27002:2013.

- El análisis de riesgos permitió establecer y cuantificar los riesgos asociados a cada uno de los activos pertenecientes a la Institución.

- La estimación de once proyectos permite a la Institución un avance hacia el cumplimiento ISO y por ende la mitigación de riesgos asociados a los activos que impacta cada proyecto.

- El plan director marca la pauta y la guía inequívoca para la consecución e implementación del Sistema de Seguridad de la Información en la Institución, que

en todo caso se debe a la continua revisión y compromiso que permita la mejora continua en la totalidad de los procesos ejecutados al interior del Colegio.

- Se puede evidenciar que, a través del desarrollo de plan director, el nivel de cumplimiento de la seguridad de la información en la Institución y la concientización de su importancia va tomando fuerza en la Comunidad. De tal forma y aun cuando no se tiene cubierta la totalidad de los controles en el nivel objetivo por la Institución, el desarrollo de los proyectos planteados ha asegurado un amplio cumplimiento y un avance significativo en la madurez de la seguridad de la información.

## ANEXO 1 POLÍTICA GENERAL DE SEGURIDAD DEL COLEGIO.

Para el Colegio la información es un activo de suma importancia para la toma de decisiones en sus actividades diarias, razón por la cual se adelantan gestiones concernientes a la protección de sus aspectos más relevantes como estrategia fundamental para la administración de riesgos y la integración de la cultura de la seguridad al interior de la Institución y en su relación con terceros.

Así las cosas, el Sistema de Gestión de Seguridad de la Información es el instrumento que permite al Colegio la identificación y mitigación de los riesgos asociados a la información. En consecuencia, conlleva a la cultura de la seguridad de la información, al cumplimiento de las regulaciones legales y se fijan bases para una posterior certificación ISO/IEC 27001:2013, objetivo de la alta dirección. Esta Política General se basa en la guía proporcionada por el MINTIC[13] como estrategia para fijar un modelo que permita implementar las políticas del modelo de Gestión de Seguridad de la Información.

La alta dirección del Colegio, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con colaboradores, estudiantes y terceros, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Institución.

Para el Colegio, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica al Colegio según lo definido en el alcance, sus colaboradores, estudiantes y terceros, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, estudiantes y terceros del Colegio.
- Garantizar la continuidad del negocio frente a incidentes.

[13] Consultado en: http://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf, el 15 de marzo de 2018, a las 11.10 p.m.

- El Colegio ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

Finalmente es de gran ayuda incluir la descripción general de otras políticas relevantes para el cumplimiento de los Objetivos planteados dentro del proyecto del SGSI ya que éstas son el apoyo sobre el cual se desarrolla; éstas deben ser descritas de forma sencilla, puntual y muy efectiva.

Dentro de las temáticas que se tocan en este punto se encuentran por ejemplo la gestión de activos, seguridad física y ambiental, control de accesos, etc. Para abordar este punto es necesario remitirse a la “Guía de políticas específicas de seguridad y privacidad de la información” y mencionar aquellas que la Entidad haya establecido como necesarias y primordiales. De esta forma se presenta el siguiente ejemplo:

A continuación, se establecen 12 principios de seguridad que soportan el SGSI del Colegio:

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los colaboradores, estudiantes y terceros.

- El Colegio protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

- El Colegio protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- El Colegio protegerá su información de las amenazas originadas por parte del personal.

- El Colegio protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

- El Colegio controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- El Colegio implementará control de acceso a la información, sistemas y recursos de red.

- El Colegio garantizará que la seguridad sea parte integral del ciclo de vida de los

sistemas de información.

- El Colegio garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- El Colegio garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

- El Colegio garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

# ANEXO 2. PROCEDIMIENTO DE AUDITORÍAS INTERNAS.

## 1. Alcance

El procedimiento de auditorías internas se aplicará a todas las dependencias involucradas en los procesos estimados en el alcance del SGSI.

## 2. Equipo Auditor

Este equipo auditor estará conformado por una serie de colaboradores que cumplan con ciertas exigencias o requisitos, las cuales se estipulan enseguida:

### 2.1. Formación

Estará conformado por colaboradores que cumplan con el siguiente grado de formación:

- Título Universitario en Ingeniería de Sistemas, Telecomunicaciones, Electrónica o afines.
- Curso o formación en auditorías internas ISO/IEC 27001. Para lo cual, se fijará un plan de capacitación.

### 2.2. Atributos personales

El equipo auditor deberá contar, además con una serie de atributos personales, como:

- Independencia
- Imparcial
- Íntegro
- Versátil
- Buenas relaciones interpersonales
- Diplomático
- Capacidad de trabajo en equipo
- Perseverante
- Capacidad de Gestión

### 2.3. Estructura del Equipo Auditor

El equipo auditor debe contar con los siguientes roles en su estructura o composición:

- Auditor jefe: Es la persona con más experiencia del equipo, adicionalmente debe tener conocimiento amplío de todos los sistemas y que se auditan.
- Auditores: Dos auditores con la formación descrita para tal fin.
- Expertos: Tres expertos que conozcan los sistemas y procesos auditados, que

permiten realizar informes especializados al auditor en jefe, que no conozca en detalle algún proceso o sistema.

## 3. Plan de Auditoria

Alcanzada la certificación ISO/IEC 27001:2013, el Colegio deberá realizar una serie de auditorías internas que permitan revisar en el tiempo, la mejora continua y posteriores recertificaciones según evolución de la norma. En tal sentido, se efectuará como mínimo una auditoria anual completa, para la revisión de forma dedicada a los controles previstos en la ISO/IEC 27002:2013, en consecuencia:

| Control | Fecha de Realización (mes) | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| **5. Políticas de seguridad** | | X | | | | | | | | | | |
| **6. Aspectos organizativos de la seguridad de la información** | | X | | | | | | | | | | |
| **7. Seguridad ligada a los recursos humanos** | | X | | | | | | | | | | |
| **8. Gestión de activos** | | | | X | | | | | | | | |
| **9. Control de accesos** | | | | X | | | | | | | | |
| **10. Cifrado** | | | | X | | | | | | | | |
| **11. Seguridad física y ambiental** | | | | | | X | | | | | | |
| **12. Seguridad en las operaciones** | | | | | | X | | | | | | |
| **13. Seguridad en las telecomunicaciones** | | | | | | X | | | | | | |
| **14. Adquisición, desarrollo y mantenimiento de los sistemas de información** | | | | | | | | X | | | | |
| **15. Relaciones con suministradores** | | | | | | | | X | | | | |
| **16. Gestión de incidentes en la seguridad de la información** | | | | | | | | X | | | | |
| **17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio** | | | | | | | | | | | X | |
| **18. Cumplimiento** | | | | | | | | | | | X | |

## 4. Modelo de Auditoria

Con el fin de registrar las actividades previstas en las auditorías internas en la Institución, se elabora el siguiente modelo de informe:

| Informe de Auditoria Interna | | Logo Institucional |
|---|---|---|
| Versión del Documento: | | |

| | | | | |
|---|---|---|---|---|
| Código de Auditoria | | | | |
| Información General: | | | | |
| Fecha: | Día: | Mes: | | Año: |
| Localización: | | | | |
| Equipo Auditor: | | | | |
| Alcance: | | | | |
| Exclusiones Justificadas: | | | | |
| Objetivos de la Auditoria: | | | | |
| Actividades Desarrolladas: | | | | |
| Oportunidades de Mejora: | | | | |
| No conformidades | En el proceso de auditoria se han encontrado (#) no conformidades menores: | | | |
| | No. | Control: | Descripción: | Responsable: |
| | | | | |

| | | | | |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | En el proceso de auditoria se han encontrado (#) no conformidades mayores: | | | |
| | No. | Control: | Descripción: | Responsable: |
| | | | | |
| | | | | |
| | | | | |
| Observaciones: | | | | |
| Conclusiones: | | | | |

# ANEXO 3. INDICADORES DE GESTIÓN

| **INDICADOR – CONCIENCIACIÓN, EDUCACIÓN Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN** | | |
|---|---|---|
| **INDICADOR** | **A.7.2.2** | |
| Indicador que permite cuantificar la aplicación de los temas impartidos en seguridad de la información y apropiados por los usuarios. Se realizará la medición a través de auditorías externas especializadas o por parte de los encargados de impartir dichos programas de sensibilización. | | |
| **OBJETIVO:** Medir la efectividad de un programa de capacitación y sensibilización en seguridad de la información para disminuir los incidentes en la materia. | | |
| **DESCRIPCIÓN DE VARIABLES** | **FORMULA** | **FUENTE DE INFORMACIÓN** |
| **VCS72:** Número de asistentes al programa de capacitación | (VCS72/VCS73)*100 | Grupo capacitador, oficial de seguridad, auditorías internas, listados de asistencia. |
| **VCS73:** Número total de personas habilitadas para asistir al programa de capacitación. | | Total, funcionarios de la compañía |
| **METAS** | | |
| **MÍNIMA** 60-70% | **SATISFACTORIA** 70-80% | **SOBRESALIENTE** 100% |
| **OBSERVACIONES** | | |
| A fin de obtener los datos necesarios para la medición, el responsable o responsables, deben idear las actividades periódicas necesarias para establecer el grado de apropiación de los temas impartidos. | | |

| **INDICADOR – USO ACEPTABLE DE LOS ACTIVOS** | | |
|---|---|---|
| **INDICADOR** | A**.8.1.3** | |
| Indicador para establecer y gestionar el cubrimiento realizado en activos críticos de información de la compañía y los controles correspondientes aplicados sobre cada uno de ellos. | | |
| **OBJETIVO:** Realizar un seguimiento a los activos críticos existentes y los nuevos incorporados en la compañía, así como a los controles implementados para el aseguramiento de la información. | | |
| **DESCRIPCIÓN DE VARIABLES** | **FORMULA** | **FUENTE DE INFORMACIÓN** |
| **VAC81:** Número de activos clasificados | (VAC81/VAC82)*100 | Inventario de activos de información y matriz de riesgos |
| **VAC82**: Número total de activos identificados. | | Inventario de activos de información y activos recientes. |

| **METAS** | | |
|---|---|---|
| **MÍNIMA** 75-85% | **SATISFACTORIA** 85-95% | **SOBRESALIENTE** 100% |
| **OBSERVACIONES** | | |
| Se deberá realizar la clasificación del activo, tratamiento, evaluación del riesgo asociado y la correspondiente estimación de controles para mitigar el impacto del riesgo, previo a la incorporación del nuevo activo. | | |

| **INDICADOR – CONTROLES FÍSICOS DE ENTRADA** | | |
|---|---|---|
| **INDICADOR** | **A.11.1.2** | |
| Indicador para establecer nivel y robustez de acceso físico de entrada al Colegio. | | |
| **OBJETIVO:** Identificar el grado de apropiación de lineamientos y estándares para el control de acceso a la compañía. | | |
| **DESCRIPCIÓN DE VARIABLES** | **FORMULA** | **FUENTE DE INFORMACIÓN** |
| **VCE111:** Número de accesos solicitados y autorizados. | (VCE111/VCE112)*100 | Solicitudes de acceso a áreas seguras |
| **VCE112:** Número total de accesos | | Registro de ingresos áreas seguras |
| **METAS** | | |
| **MÍNIMA** 75-85% | **SATISFACTORIA** 85-95% | **SOBRESALIENTE** 100% |
| **OBSERVACIONES** | | |
| Optar medidas que garanticen el acceso a zonas seguras, únicamente de personal autorizado. | | |

| **INDICADOR – GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS** | | |
|---|---|---|
| **INDICADOR** | **A.12.6.1** | |
| Indicador para estimar y gestionar las vulnerabilidades técnicas asociadas a los sistemas de información del Colegio y las medidas adoptadas para su mitigación o remediación. | | |
| **OBJETIVO:** Efectuar pruebas de vulnerabilidades periódicas y establecer planes de acción para su correcta remediación o mitigación. | | |
| **DESCRIPCIÓN DE VARIABLES** | **FORMULA** | **FUENTE DE INFORMACIÓN** |
| **VVT126:** Número de pruebas de vulnerabilidad por sistema de información. | (VVT126/VVT127)*100 | Oficial de seguridad, inventario de sistemas de información, administradores de los sistemas de información. |
| **VVT127:** Número total de vulnerabilidades encontradas. | | Auditorías internas y externas. |
| **METAS** | | |
| **MÍNIMA** 70-80% | **SATISFACTORIA** 80-90% | **SOBRESALIENTE** 100% |
| **OBSERVACIONES** | | |

| |
|---|
| Se deberá realizar la remediación a las vulnerabilidades encontradas, optando por medidas de contingencia o remediación que permitan su solución en un plazo establecido. |

| **INDICADOR – VERIFICACIÓN, REVISIÓN Y EVALUACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN** | | |
|---|---|---|
| **INDICADOR** | **A.17.1.3** | |
| Áreas del Colegio con planes de continuidad del negocio que han sido probados y documentados a través de listas de chequeo. | | |
| **OBJETIVO:** Identificar el porcentaje de áreas que han apropiado medidas de continuidad del negocio en un periodo de doce meses. | | |
| **DESCRIPCIÓN DE VARIABLES** | **FORMULA** | **FUENTE DE INFORMACIÓN** |
| **VCS171:** Número de planes documentados. | (VCS171/VCS172)*100 | Oficial de seguridad y colaboradores. |
| **VCS172:** Número de planes totales. | | Oficial de seguridad y colaboradores. |
| **METAS** | | |
| **MÍNIMA** 70-80% | **SATISFACTORIA** 80-90% | **SOBRESALIENTE** 100% |
| **OBSERVACIONES** | | |
| El indicador permite establecer el estado de los controles a nivel de continuidad del negocio y por consiguiente fijar estrategias que permitan la cobertura total de los mismos. | | |

## ANEXO 4. DECLARACIÓN DE APLICABILIDAD

Para la fijación del origen del control tenemos:

- AR: Análisis de riesgos
- L: Cumplimiento legal
- RC: Requerimiento contractual
- NI: Normatividad interna
- BP: Buenas prácticas

| DECLARACIÓN DE APLICABILIDAD | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| VERSIÓN 1.0 | | | | | | | | | | |
| ABRIL DE 2018 | | | | | | | | | | |
| CONTROL | | Justificación para exclusión | Aplica | Control | Evidencia de Implementación | Origen del control | | | | |
| | | | | | | AR | L | RC | NI | BP |
| **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. | | SI | Se elaborará la política de seguridad, acorde con las necesidades de la institución y los parámetros fijados en el plan director. | | X | | | | X |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 5.1.2 Revisión de las políticas para la seguridad de la información. | | SI | El comité de seguridad y la alta dirección deben acordar reuniones periódicas para la revisión de la política institucional de seguridad. | | X | | | | X |
| **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. | | SI | Se deberán fijar los roles y responsabilidades para el aseguramiento de la información. | | X | | | | X |
| | | 6.1.2 Segregación de tareas. | | SI | Se deberán segmentar las tareas dependiendo de los roles fijados., | | X | | | | X |
| | | 6.1.3 Contacto con las autoridades. | | SI | Se debe implementar canales de comunicación con las autoridades | | | X | | | X |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Nacionales. | | | | | | | |
| | | 6.1.4 Contacto con grupos de interés especial. | | SI | Se debe mantener comunicación constante con entidades especializadas en el tema de la seguridad. Para lo anterior, se establecen, SLAS con los proveedores especializados de la institución. | | | | X | | X |
| | | 6.1.5 Seguridad de la información en la gestión de proyectos. | | SI | Se deben implementar acuerdos de confidencialidad en la gestión de proyectos. | | | X | X | | X |
| | 6.2 Dispositivos para movilidad y teletrabajo. | | | | | | | | | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 6.2.1 Política de uso de dispositivos para movilidad. | | SI | Se debe adoptar una política para el manejo y gestión de dispositivos móviles, que permitan el aseguramiento de la información | | X | | | X | X |
| | | 6.2.2 Teletrabajo. | La institución no tiene ningún tipo de vinculación mediante la modalidad del teletrabajo y no se tiene prevista su implementación en un mediano plazo. | NO | | | | | | | | |
| **7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.** | | | | | | | | | | | | |
| | 7.1 Antes de la contratación. | | | | | | | | | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 7.1.1 Investigación de antecedentes. | | SI | Se tiene un servicio tercerizado encargado de realizar un estudio de seguridad, tanto en el ámbito profesional como en la vida personal. | Servicio de seguridad tercerizado y reportes. | | X | X | X | |
| | | 7.1.2 Términos y condiciones de contratación. | | SI | Se tiene establecidos contratos dependiendo el tipo de colaborador a vincular | Grupo de Gestión Humana, contratos de colaboradores. | | X | X | X | |
| | 7.2 Durante la contratación. | | | | | | | | | | | |
| | | 7.2.1 Responsabilidades de gestión. | | SI | Se debe establecer responsabilidades claras para la gestión. Por lo que este control se implementará acorde a lo determinado en el plan director. | | | | | | | X |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 7.2.2 Concienciación, educación y capacitación en seguridad de la información | | SI | Se deberá fijar campañas de sensibilización y concientización a todos los colaboradores y estudiantes. En tal sentido se deberá fijar un cronograma claro al respecto. | | X | | | | X |
| | | 7.2.3 Proceso disciplinario. | | SI | El contrato firmado por los colaboradores tiene especificadas una serie de cláusulas con sus respectivos correctivos en caso de su incumplimiento. | Contrato laboral. Grupo de Gestión Humana. | | X | X | X | |
| | 7.3 Cese o cambio de puesto de trabajo. | | | | | | | | | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 7.3.1 Cese o cambio de puesto de trabajo. | | SI | Se tiene el proceso denominado, Retiro de Colaboradores, que fija las actividades una vez un colaborador se retira de la institución. | Proceso Retiro de Colaboradores | | | | X | X |
| **8. GESTIÓN DE ACTIVOS.** | | | | | | | | | | | | |
| | 8.1 Responsabilidad sobre los activos. | | | | | | | | | | | |
| | | 8.1.1 Inventario de activos. | | SI | Se debe efectuar el inventario de activos. | | X | | | | X | |
| | | 8.1.2 Propiedad de los activos. | | SI | Se debe efectuar la clasificación de los propietarios de los activos. | | X | | | | X | |
| | | 8.1.3 Uso aceptable de los activos. | | SI | Se debe fijar el uso aceptable de los activos. | | X | | | | X | |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 8.1.4 Devolución de activos. | | SI | Se tiene establecidos los procedimientos para la devolución de equipos a colaboradores cuando se retiren de la Institución. | Acta de Devolución de Equipos. | X | | | X | X |
| 8.2 Clasificación de la información. | | | | | | | | | | | |
| | 8.2.1 Directrices de clasificación. | | SI | Se debe efectuar la clasificación de la información acorde con la ley 1581 de 2012. | | | X | | | | |
| | 8.2.2 Etiquetado y manipulado de la información. | | SI | Se debe realizar la correcta estimación y fijación de parámetros para el uso de la información. | | | | | | | X |
| | 8.2.3 Manipulación de activos. | | SI | Se debe realizar las cláusulas de usos de activos. | | | | | | | X |
| 8.3 Manejo de los soportes de almacenamiento. | | | | | | | | | | | |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 8.3.1 Gestión de soportes extraíbles. | | SI | Se debe realizar el control para la Gestión de soportes extraíbles. | | | | | | X |
| | | 8.3.2 Eliminación de soportes. | | SI | Se deberá fijar el control para la eliminación de soportes. | | | | | | X |
| | | 8.3.3 Soportes físicos en tránsito. | | SI | Se deberá fijar controles para los soportes físicos y en tránsito. | | | | | | X |
| **9. CONTROL DE ACCESOS.** | | | | | | | | | | | |
| | 9.1 Requisitos de negocio para el control de accesos. | | | | | | | | | | |
| | | 9.1.1 Política de control de accesos. | | SI | Se tienen controles de acceso tanto físicos como accesos lógicos. | Procedimiento de Gestión de contraseñas. | | | | X | X |
| | | 9.1.2 Control de acceso a las redes y servicios asociados. | | SI | Se tienen controles de acceso tanto físicos como accesos lógicos. | Procedimiento de Gestión de contraseñas. | | | | | X |
| | 9.2 Gestión de acceso de usuario. | | | | | | | | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 9.2.1 Gestión de altas/bajas en el registro de usuarios. | | SI | Se tiene el procedimiento para la creación o eliminación de registros de usuarios. | Procedimiento para la creación de colaborador nuevo | | | | | | X |
| | | 9.2.2 Gestión de los derechos de acceso asignados a usuarios. | | SI | Se deberá fijar control que informe derechos y responsabilidades de perfil a usuario. | | | | | | | X |
| | | 9.2.3 Gestión de los derechos de acceso con privilegios especiales. | | SI | Se deberá implementar el control para la Gestión de los derechos de acceso a usuarios privilegiados, acorde con la política para tal fin. | | | | | | | X |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 9.2.4 Gestión de información confidencial de autenticación de usuarios. | | SI | Se debe implementar el control de auditoria de gestión de información confidencial para la autenticación de usuarios. | | | | | | X |
| | | 9.2.5 Revisión de los derechos de acceso de los usuarios. | | SI | Se deberá realizar el perfilamiento de los usuarios y los accesos concedidos. | | | | | | X |
| | | 9.2.6 Retirada o adaptación de los derechos de acceso | | SI | Se debe fijar el control para el upgrade o retiro de derechos de acceso. | | | | | | X |
| | 9.3 Responsabilidades del usuario. | | | | | | | | | | |
| | | 9.3.1 Uso de información confidencial para la autenticación. | | SI | Se deberá fijar el control y la política para la gestión de contraseñas | | | | X | X | X |
| | 9.4 Control de acceso a sistemas y aplicaciones. | | | | | | | | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 9.4.1 Restricción del acceso a la información. | | SI | Se tiene establecidos controles de acceso a la información mediante directorio activo. | Procedimiento perfilamiento de usuarios | | | | | | X |
| | | 9.4.2 Procedimientos seguros de inicio de sesión. | | SI | Se tiene establecidos controles de acceso a la información mediante directorio activo. | Procedimiento perfilamiento de usuarios | | | | | | X |
| | | 9.4.3 Gestión de contraseñas de usuario. | | SI | Se tiene establecidos controles de acceso a la información mediante directorio activo. | Procedimiento perfilamiento de usuarios | | | | | | X |
| | | 9.4.4 Uso de herramientas de administración de sistemas. | | SI | Se deberá implementar la adquisición de herramientas para el control | | | | | | | X |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 9.4.5 Control de acceso al código fuente de los programas. | | SI | No se concede el acceso a códigos fuentes de programas ya que este servicio es tercerizado y se establecen controles en los SLAS del contrato. | Contratos de Desarrollo de Software. | | | X | | X |
| **10. CIFRADO.** | | | | | | | | | | | | |
| | 10.1 Controles criptográficos. | | | | | | | | | | | |
| | | 10.1.1 Política de uso de los controles criptográficos. | | SI | Se deberá implementar controles criptográficos para la protección de la información. | | | | | | | X |
| | | 10.1.2 Gestión de claves. | | SI | Se deberá establecer una gestión de las claves que respalde el uso de las técnicas criptográficas en la Institución. | | | | | | | X |
| **11. SEGURIDAD FÍSICA Y AMBIENTAL.** | | | | | | | | | | | | |
| | 11.1 Áreas seguras. | | | | | | | | | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 11.1.1 Perímetro de seguridad física. | | SI | Se debe revisar periódicamente el contrato de seguridad y revisar incidentes que permitan un aseguramiento evolutivo y constante. | | | | X | X | X |
| | | 11.1.2 Controles físicos de entrada. | | SI | Se debe revisar el control físico a áreas sensibles como cuartos de cableado, y re disponer su ubicación. | | | | X | X | X |
| | | 11.1.3 Seguridad de oficinas, despachos y recursos. | | SI | Se debe implementar control de seguridad de acceso hacía el área de oficinas. | | | | X | X | X |
| | | 11.1.4 Protección contra las amenazas externas y ambientales. | | SI | Se deben implementar controles de amenazas externas como extinción de | | X | | | | X |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | incendios. | | | | | | |
| | | 11.1.5 El trabajo en áreas seguras. | | SI | Se debe implementar controles para áreas seguras. | | X | | | | X |
| | | 11.1.6 Áreas de acceso público, carga y descarga. | | SI | Se debe implementar controles en las zonas de acceso público y las zonas de carga y descarga. | | | | | | X |
| | 11.2 Seguridad de los equipos. | | | | | | | | | | |
| | | 11.2.1 Emplazamiento y protección de equipos. | | SI | Se deberá fijar controles para la protección y emplazamiento de equipos | | | | | | X |
| | | 11.2.2 Instalaciones de suministro. | | SI | Se deberá fijar control para las instalaciones de suministro | | | | | | X |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 11.2.3 Seguridad del cableado. | | SI | Se debe implementar control para la seguridad del cableado. | | X | | | | X |
| | | 11.2.4 Mantenimiento de los equipos. | | SI | Se deben ampliar los programas de mantenimientos de equipos, a fin de contemplar la totalidad de ellos. En tal sentido se deben fijar controles con cronogramas estipulados. | | | | | | X |
| | | 11.2.5 Salida de activos fuera de las dependencias de la empresa. | | SI | Se debe implementar control para activos que se usan fuera de la institución. | | | | | | X |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones. | Las políticas de la institución, contempla, el uso de equipos y de dispositivos de almacenamiento sin restricción alguna, y se basan en los compromisos de confidencialidad firmados con el colaborador. Adicionalmente no se tiene como medida implementar sistemas de gestión de dispositivos móviles en el mediano plazo. | NO | | | | | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento. | Las políticas de la institución, contempla, el uso de equipos y de dispositivos de almacenamiento sin restricción alguna, y se basan en los compromisos de confidencialidad firmados con el colaborador. Adicionalmente no se tiene como medida implementar sistemas de gestión de dispositivos móviles en el mediano plazo. | NO | | | | | | | |
| | | 11.2.8 Equipo informático de usuario desatendido. | | SI | Se debe fijar control para equipos desatendidos. | | | | | | | X |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla. | | SI | Se debe fijar políticas de concientización en los usuarios para el bloqueo de equipos cuando no están en uso. | | | | | | X |
| **12. SEGURIDAD EN LA OPERACIONES** | | | | | | | | | | | |
| 12.1 Responsabilidades y procedimientos de operación. | | | | | | | | | | | |
| | | 12.1.1 Documentación de procedimientos de operación. | | SI | Se deberán complementar los procedimientos de operación y realizar su registro formal. | | | | | | X |
| | | 12.1.2 Gestión de cambios. | | SI | Se debe implementar el procedimiento para el control y gestión de cambios. | | | | | | X |
| | | 12.1.3 Gestión de capacidades. | | SI | Se deberá fijar el control para la gestión de capacidades. | | | | | | X |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 12.1.4 Separación de entornos de desarrollo, prueba y producción. | | SI | Aunque no se tiene establecida un área de desarrollo en la institución, se deberá fijar un entorno de prueba para entre otros, realizar actualización en los servidores. | | | | | | X |
| 12.2 Protección contra código malicioso. | | | | | | | | | | | |
| | 12.2.1 Controles contra el código malicioso. | | | SI | Se debe implementar controles para el código malicioso. | | X | | | | X |
| 12.3 Copias de seguridad. | | | | | | | | | | | |
| | 12.3.1 Copias de seguridad de la información. | | | SI | Se tienen establecidos procedimientos de copias de seguridad. | Procedimiento copias de seguridad y backup | X | | | | X |
| 12.4 Registro de actividad y supervisión. | | | | | | | | | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 12.4.1 Registro y gestión de eventos de actividad. | No se cuenta con los recursos o soluciones para el monitorio óptimo de los registros o eventos de actividades. | NO | | | | | | | | |
| | | 12.4.2 Protección de los registros de información. | No se cuenta con los recursos o soluciones para el monitorio óptimo de los registros o eventos de actividades. | NO | | | | | | | | |
| | | 12.4.3 Registros de actividad del administrador y operador del sistema. | No se cuenta con los recursos o soluciones para el monitorio óptimo de los registros o eventos de actividades. | NO | | | | | | | | |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 12.4.4 Sincronización de relojes. | | SI | Se debe hacer el control formal de la sincronización de relojes. En la actualidad se realiza, pero no se tiene documentado el procedimiento | | | | | | X |
| 12.5 Control del software en explotación. | | | | | | | | | | | |
| | | 12.5.1 Instalación del software en sistemas en producción. | | SI | Se debe fijar el control para la instalación de software en servidores de producción. | | | | | | X |
| 12.6 Gestión de la vulnerabilidad técnica. | | | | | | | | | | | |
| | | 12.6.1 Gestión de las vulnerabilidades técnicas. | | SI | Se debe realizar el control que permita gestionar las vulnerabilidades de tipo técnicas que se encuentren. | | X | | | | X |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 12.6.2 Restricciones en la instalación de software. | | SI | Se debe implementar controles para la instalación de software. | | X | | | | X |
| 12.7 Consideraciones de las auditorías de los sistemas de información. | | | | | | | | | | |
| | 12.7.1 Controles de auditoría de los sistemas de información. | | SI | Se debe implementar una solución de auditoria para los sistemas de información | | X | | | | X |
| **13. SEGURIDAD EN LAS TELECOMUNICACIONES.** | | | | | | | | | | |
| 13.1 Gestión de la seguridad en las redes. | | | | | | | | | | |
| | 13.1.1 Controles de red. | | SI | Se deben implementar controles de red | | X | | | | X |
| | 13.1.2 Mecanismos de seguridad asociados a servicios en red. | | SI | Se deben implementar soluciones para la seguridad de la red | | X | | | | X |
| | 13.1.3 Segregación de redes. | | SI | Se debe realizar segmentación de redes. | | X | | | | X |
| 13.2 Intercambio de información con partes externas. | | | | | | | | | | |
| | 13.2.1 Políticas y procedimientos de intercambio de información. | | SI | Se debe fijar políticas para el intercambio de información interna | | | | X | | X |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | y con terceros | | | | | | |
| | | 13.2.2 Acuerdos de intercambio. | | SI | Se debe implementar acuerdos de intercambio de información entre áreas y con terceros. | | | | X | X | X |
| | | 13.2.3 Mensajería electrónica. | | SI | Se debe implementar controles de mensajería electrónica y acuerdos de uso | | | | | | X |
| | | 13.2.4 Acuerdos de confidencialidad y secreto. | | SI | Se tiene implementado el acuerdo de confidencialidad | Acuerdo de confidencialidad. Gestión Humana | | X | X | X | X |
| **14. ADQUISICIÓN, 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. | | SI | Se debe realizar análisis de vulnerabilidad a los sistemas de información a fin de fijar medidas y controles sobre ellos | | | | | | | X |
| | | 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas. | | SI | Se debe implementar soluciones de seguridad que permita controlar de manera óptima el acceso a servicios de información desde el exterior. | | X | | | | | X |
| | | 14.1.3 Protección de las transacciones por redes telemáticas. | | SI | Se debe fijar control para la protección de transacciones en las redes | | | | | | | X |
| | 14.2 Seguridad en los procesos de desarrollo y soporte. | | | | | | | | | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 14.2.1 Política de desarrollo seguro de software. | Dentro de la institución no se tiene un área encargada de desarrollo de software, el cual es adquirido a través de terceros. | NO | | | | | | | | |
| | | 14.2.2 Procedimientos de control de cambios en los sistemas. | | SI | Se debe fijar control para la gestión de cambios | | | | | | | X |
| | | 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. | | SI | Se debe fijar una lista de chequeo de cada aplicación posterior a cambios realizados. | | | | | | | X |
| | | 14.2.4 Restricciones a los cambios en los paquetes de software. | | SI | Se debe fijar control para el control de cambios en los paquetes de software | | | | | | | X |
| | | 14.2.5 Uso de principios de ingeniería en protección de sistemas. | | SI | Se debe implementar medidas de aseguramiento para la protecció | | | | | | | X |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | n de sistemas | | | | | | | |
| | | 14.2.6 Seguridad en entornos de desarrollo. | Al no desarrollar software en la institución, su aseguramiento también es inexistente. | NO | | | | | | | | |
| | | 14.2.7 Externalización del desarrollo de software. | | SI | Se debe fijar SLAS claros para el desarrollo de software a través de terceros contratistas | | | | | X | | X |
| | | 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas. | | SI | Se debe realizar control para pruebas durante el desarrollo. | | | | | | | X |
| | | 14.2.9 Pruebas de aceptación. | | SI | Se debe realizar control para el recibo a satisfacción. | | | | | X | | X |
| | 14.3 Datos de prueba. | | | | | | | | | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 14.3.1 Protección de los datos utilizados en pruebas. | | SI | Realizar controles para la protección de datos y acuerdos de confidencialidad en pruebas | | | | X | | X | |
| **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. | | SI | Se tiene implementado el acuerdo de confidencialidad con contratistas | Acuerdo de confidencialidad Externos. Gestión Humana | | | X | X | X | |
| | | 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores. | | SI | Se debe fijar control para el tratamiento del riesgo en los contratos | | | | | X | | |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones. | | SI | Se debe implementar control para garantizar la cadena de suministro en tecnologías de la información y comunicaciones mediante SLAS claros establecidos y pólizas de respaldo | | | | X | | X |
| 15.2 Gestión de la prestación del servicio por suministradores. | | | | | | | | | | | |
| | | 15.2.1 Supervisión y revisión de los servicios prestados por terceros. | | SI | Se debe implementar controles para la supervisión de contratos | | | | X | | X |
| | | 15.2.2 Gestión de cambios en los servicios prestados por terceros. | | SI | Se debe implementar control de cambios en los servicios contratados, mediante SLAS contractuales | | | | X | | X |
| **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. | | SI | Se debe realizar la asignación de responsabilidades y la consolidación de los procedimientos para la atención de incidentes. | | | | | | | X |
| | | 16.1.2 Notificación de los eventos de seguridad de la información. | | SI | Se debe fijar el control para notificar y tomar las medidas respectivas | | | | | | | X |
| | | 16.1.3 Notificación de puntos débiles de la seguridad. | | SI | Se debe realizar controles para el establecimiento de puntos débiles de seguridad | | X | | | | | X |
| | | 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones. | | SI | Se debe fijar control para la valoración de un evento y la toma de medidas. | | | | | | | X |
| | | 16.1.5 Respuesta a los incidentes de seguridad. | | SI | Se deberá fijar procedimiento para la atención de | | | | | | | X |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | incidentes | | | | | | | |
| | | 16.1.6 Aprendizaje de los incidentes de seguridad de la información. | | SI | Se deberá tener un control y repositorio de datos para la toma de decisiones futuras | | | | | | | X |
| | | 16.1.7 Recopilación de evidencias. | | SI | Se deberá fijar procedimiento para el levantamiento de información y evidencias durante y después de un incidente. | | | | | | | X |
| **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. | | SI | Se debe efectuar el plan de continuidad del negocio. | | X | | | | | X |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 17.1.2 Implantación de la continuidad de la seguridad de la información. | | SI | Se debe implementar los planes para la continuidad de la seguridad de la información en todo momento. | | X | | | | X |
| | | 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. | | SI | Se debe fijar cronograma para pruebas y evaluaciones del plan de continuidad. | | X | | | | X |
| | 17.2 Redundancias. | | | | | | | | | | |
| | | 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información. | La inversión para redundancias no se tiene contemplada en un mediano plazo. | NO | | | | | | | |
| **18. CUMPLIMIENTO.** | | | | | | | | | | | |
| | 18.1 Cumplimiento de los requisitos legales y contractuales. | | | | | | | | | | |
| | | 18.1.1 Identificación de la legislación aplicable. | | SI | Se tiene implementado control en el contrato laboral. | Contrato laboraral. Grupo de Gestión Humana. | | X | | | X |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 18.1.2 Derechos de propiedad intelectual (DPI). | | SI | Se tiene establecido el control de propiedad intelectual en el contrato laboral | Contrato laboraral. Grupo de Gestión Humana. | | X | X | X | |
| | | 18.1.3 Protección de los registros de la organización. | | SI | Se tiene implementado el acuerdo de confidencialidad y uso de la información con colaboradores. | Acuerdo de confidencialidad. Gestión Humana | | X | X | X | |
| | | 18.1.4 Protección de datos y privacidad de la información personal. | | SI | Se debe clasificar la información y realizar el registro de las bases de datos ante la SIC. | | | X | | | |
| | | 18.1.5 Regulación de los controles criptográficos. | | SI | Se deben implementar controles de regulación criptográfica | | | | | | X |
| | 18.2 Revisiones de la seguridad de la información. | | | | | | | | | | | |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 18.2.1 Revisión independiente de la seguridad de la información. | | SI | Se debe realizar un estudio de seguridad de la información a través de una auditoria externa | | | | | | X |
| | | 18.2.2 Cumplimiento de las políticas y normas de seguridad. | | SI | Se debe implementar auditorías internas de cumplimiento | | | | | | X |
| | | 18.2.3 Comprobación del cumplimiento. | | SI | Se debe revisar y contrastar los controles a través de las diferentes auditorias. | | | | | | X |

# ANEXO 5. IDENTIFICACIÓN DE AMENAZAS

| Identificación de amenazas | | | |
|---|---|---|---|
| **[N] Desastres Naturales** | | | |
| **Cod.** | **Activos** | **Amenaza** | **Dimensión** |
| [N1] | [HW pc] | Fuego | [D] |
| | [HW portatil] | | |
| | [HW multif] | | |
| | [HW Serv] | | |
| | [HW ap] | | |
| | [HW switch] | | |
| | [HW videob] | | |
| | [HW pbx] | | |
| | [HW Ipad] | | |
| | [HW fotocop] | | |
| | [HW tv] | | |
| | [HW modem] | | |
| | [MEDIA DD] | | |
| | [MEDIA usb] | | |
| | [MEDIA electronic] | | |
| | [AUX ups] | | |
| | [AUX cableado] | | |
| | [AUX rack] | | |
| | [AUX gabinte] | | |
| | [AUX fibra] | | |
| | [L administrativa] | | |
| | [L escuelas] | | |
| [N2] | [HW pc] | Daños por agua | [D] |
| | [HW portatil] | | |
| | [HW multif] | | |
| | [HW Serv] | | |
| | [HW ap] | | |
| | [HW switch] | | |
| | [HW videob] | | |
| | [HW pbx] | | |
| | [HW Ipad] | | |
| | [HW fotocop] | | |
| | [HW tv] | | |

| | | | |
|---|---|---|---|
| | [HW modem] | | |
| | [MEDIA DD] | | |
| | [MEDIA usb] | | |
| | [MEDIA electronic] | | |
| | [AUX ups] | | |
| | [AUX cableado] | | |
| | [AUX rack] | | |
| | [AUX gabinte] | | |
| | [AUX fibra] | | |
| | [L administrativa] | | |
| | [L escuelas] | | |
| [N.*] | [HW pc] | Desastres Naturales | [D] |
| | [HW portatil] | | |
| | [HW multif] | | |
| | [HW Serv] | | |
| | [HW ap] | | |
| | [HW switch] | | |
| | [HW videob] | | |
| | [HW pbx] | | |
| | [HW Ipad] | | |
| | [HW fotocop] | | |
| | [HW tv] | | |
| | [HW modem] | | |
| | [MEDIA DD] | | |
| | [MEDIA usb] | | |
| | [MEDIA electronic] | | |
| | [AUX ups] | | |
| | [AUX cableado] | | |
| | [AUX rack] | | |
| | [AUX gabinte] | | |
| | [AUX fibra] | | |
| | [L administrativa] | | |
| | [L escuelas] | | |
| **[I] De origen industrial** | | | |
| **Cod.** | **Activos** | **Amenaza** | **Dimensión** |
| [I1] | [HW pc] | Fuego | [D] |
| | [HW portatil] | | |
| | [HW multif] | | |
| | [HW Serv] | | |
| | [HW ap] | | |
| | [HW switch] | | |

| | | | |
|---|---|---|---|
| | [HW videob] | | |
| | [HW pbx] | | |
| | [HW Ipad] | | |
| | [HW fotocop] | | |
| | [HW tv] | | |
| | [HW modem] | | |
| | [MEDIA DD] | | |
| | [MEDIA usb] | | |
| | [MEDIA electronic] | | |
| | [AUX ups] | | |
| | [AUX cableado] | | |
| | [AUX rack] | | |
| | [AUX gabinte] | | |
| | [AUX fibra] | | |
| | [L administrativa] | | |
| | [L escuelas] | | |
| [I2] | [HW pc] | Daños por agua | [D] |
| | [HW portatil] | | |
| | [HW multif] | | |
| | [HW Serv] | | |
| | [HW ap] | | |
| | [HW switch] | | |
| | [HW videob] | | |
| | [HW pbx] | | |
| | [HW Ipad] | | |
| | [HW fotocop] | | |
| | [HW tv] | | |
| | [HW modem] | | |
| | [MEDIA DD] | | |
| | [MEDIA usb] | | |
| | [MEDIA electronic] | | |
| | [AUX ups] | | |
| | [AUX cableado] | | |
| | [AUX rack] | | |
| | [AUX gabinte] | | |
| | [AUX fibra] | | |
| | [L administrativa] | | |
| | [L escuelas] | | |
| [I.*] | [HW pc] | Desastres Naturales | [D] |
| | [HW portatil] | | |
| | [HW multif] | | |

| | | | |
|---|---|---|---|
| | [HW Serv] | | |
| | [HW ap] | | |
| | [HW switch] | | |
| | [HW videob] | | |
| | [HW pbx] | | |
| | [HW Ipad] | | |
| | [HW fotocop] | | |
| | [HW tv] | | |
| | [HW modem] | | |
| | [MEDIA DD] | | |
| | [MEDIA usb] | | |
| | [MEDIA electronic] | | |
| | [AUX ups] | | |
| | [AUX cableado] | | |
| | [AUX rack] | | |
| | [AUX gabinte] | | |
| | [AUX fibra] | | |
| | [L administrativa] | | |
| | [L escuelas] | | |
| [I.3] | [HW pc] | Contaminación mecánica | [D] |
| | [HW portatil] | | |
| | [HW multif] | | |
| | [HW Serv] | | |
| | [HW ap] | | |
| | [HW switch] | | |
| | [HW videob] | | |
| | [HW pbx] | | |
| | [HW Ipad] | | |
| | [HW fotocop] | | |
| | [HW tv] | | |
| | [HW modem] | | |
| | [MEDIA DD] | | |
| | [MEDIA usb] | | |
| | [MEDIA electronic] | | |
| | [AUX ups] | | |
| | [AUX cableado] | | |
| | [AUX rack] | | |
| | [AUX gabinte] | | |
| | [AUX fibra] | | |
| [I.4] | [HW Serv] | Contaminación electromagnética | [D] |
| | [HW ap] | | |

| | | | |
|---|---|---|---|
| | [HW switch] | | |
| | [HW pbx] | | |
| | [MEDIA DD] | | |
| | [MEDIA usb] | | |
| | [MEDIA electronic] | | |
| | [AUX cableado] | | |
| | [AUX fibra] | | |
| [I.5] | [SW SO] | Averia de origen físico o lógico | [D] |
| | [SW BD] | | |
| | [SW Ant.] | | |
| | [SW Ofi] | | |
| | [SW moodle] | | |
| | [SW nav] | | |
| | [SW diseñ] | | |
| | [SW nomina] | | |
| | [SW contab] | | |
| | [SW glpi] | | |
| | [SW notas] | | |
| | [SW plagio] | | |
| | [SW bibliot] | | |
| | [SW horarios] | | |
| | [HW pc] | | |
| | [HW portatil] | | |
| | [HW multif] | | |
| | [HW Serv] | | |
| | [HW ap] | | |
| | [HW switch] | | |
| | [HW videob] | | |
| | [HW pbx] | | |
| | [HW Ipad] | | |
| | [HW fotocop] | | |
| | [HW tv] | | |
| | [HW modem] | | |
| | [MEDIA DD] | | |
| | [MEDIA usb] | | |
| | [MEDIA electronic] | | |
| | [AUX ups] | | |
| | [AUX cableado] | | |
| | [AUX rack] | | |
| | [AUX gabinte] | | |
| | [AUX fibra] | | |

| | | | |
|---|---|---|---|
| [I.6] | [HW pc] | Corte de suministro eléctrico | [D] |
| | [HW portatil] | | |
| | [HW multif] | | |
| | [HW Serv] | | |
| | [HW ap] | | |
| | [HW switch] | | |
| | [HW videob] | | |
| | [HW pbx] | | |
| | [HW Ipad] | | |
| | [HW fotocop] | | |
| | [HW tv] | | |
| | [HW modem] | | |
| | [MEDIA electronic] | | |
| | [AUX ups] | | |
| | [AUX cableado] | | |
| | [AUX rack] | | |
| | [AUX gabinte] | | |
| | [AUX fibra] | | |
| [I.7] | [HW pc] | Condiciones inadecuadas de temperatura o humedad | [D] |
| | [HW portatil] | | |
| | [HW multif] | | |
| | [HW Serv] | | |
| | [HW ap] | | |
| | [HW switch] | | |
| | [HW videob] | | |
| | [HW pbx] | | |
| | [HW Ipad] | | |
| | [HW fotocop] | | |
| | [HW tv] | | |
| | [HW modem] | | |
| | [MEDIA electronic] | | |
| | [AUX ups] | | |
| | [AUX cableado] | | |
| | [AUX rack] | | |
| | [AUX gabinte] | | |
| | [AUX fibra] | | |
| [I.8] | [COM LAN] | Fallo de servicios de comunicaciones | [D] |
| | [COM wifi] | | |
| | [COM Internte] | | |
| | [COM telefonía] | | |

| | | | |
|---|---|---|---|
| [I.9] | [AUX ups] | Interrupción de otros servicios y suministros esenciales | [D] |
| [I. 10] | [MEDIA DD] | Degradación de los soportes de almacenamiento de la información | |
| | [MEDIA usb] | | |
| | [MEDIA electronic] | | |
| **[E] Errores y fallos no intencionados** | | | |
| **Cod.** | **Activos** | **Amenaza** | **Dimensión** |
| [E.1] | [D respaldo] | Errores de los usuarios | [I]<br>[C]<br>[D] |
| | [D de config.] | | |
| | [D de Bit] | | |
| | [SI Internet] | | |
| | [SI Aula virtual] | | |
| | [SI Correo] | | |
| | [SI Mesa de ayuda] | | |
| | [SI Mandarin] | | |
| | [SI Reservas] | | |
| | [SI Sistema de Notas] | | |
| | [SE Portal WEB] | | |
| | [SW SO] | | |
| | [SW BD] | | |
| | [SW Ant.] | | |
| | [SW Ofi] | | |
| | [SW moodle] | | |
| | [SW nav] | | |
| | [SW diseñ] | | |
| | [SW nomina] | | |
| | [SW contab] | | |
| | [SW glpi] | | |
| | [SW notas] | | |
| | [SW plagio] | | |
| | [SW bibliot] | | |
| | [SW horarios] | | |
| | [MEDIA DD] | | |
| | [MEDIA usb] | | |
| | [MEDIA electronic] | | |
| | [I Notas] | | |
| | [I Estudiantes] | | |
| | [I Padres de familia] | | |

| | | | |
|---|---|---|---|
| | [I Mallas Curriculares] | | |
| | [I Aspirantes] | | |
| | [I Exalumnas] | | |
| | [I estudiantes] | | |
| | [I Padres de familia] | | |
| | [I Colaboradores] | | |
| | [I Profesores] | | |
| | [I Exalumnas] | | |
| [E.2] | [D respaldo] | Errores del administrador | [I]<br>[C]<br>[D] |
| | [D de config.] | | |
| | [D de Bit] | | |
| | [SI Internet] | | |
| | [SI Aula virtual] | | |
| | [SI Correo] | | |
| | [SI Mesa de ayuda] | | |
| | [SI Mandarin] | | |
| | [SI Reservas] | | |
| | [SI Sistema de Notas] | | |
| | [SE Portal WEB] | | |
| | [SW SO] | | |
| | [SW BD] | | |
| | [SW Ant.] | | |
| | [SW Ofi] | | |
| | [SW moodle] | | |
| | [SW nav] | | |
| | [SW diseñ] | | |
| | [SW nomina] | | |
| | [SW contab] | | |
| | [SW glpi] | | |
| | [SW notas] | | |
| | [SW plagio] | | |
| | [SW bibliot] | | |
| | [SW horarios] | | |
| | [MEDIA electronic] | | |
| | [I Notas] | | |
| | [I Estudiantes] | | |
| | [I Padres de familia] | | |
| | [I Mallas Curriculares] | | |
| | [I Aspirantes] | | |

| | | | |
|---|---|---|---|
| | [I Exalumnas] | | |
| | [I estudiantes] | | |
| | [I Padres de familia] | | |
| | [I Colaboradores] | | |
| | [I Profesores] | | |
| | [I Exalumnas] | | |
| [E.4] | [D de config.] | Errores de configuración | [I] |
| [E.8] | [SW SO] | Difusión de software dañino | [D]<br>[I]<br>[C] |
| | [SW BD] | | |
| | [SW Ant.] | | |
| | [SW Ofi] | | |
| | [SW moodle] | | |
| | [SW nav] | | |
| | [SW diseñ] | | |
| | [SW nomina] | | |
| | [SW contab] | | |
| | [SW glpi] | | |
| | [SW notas] | | |
| | [SW plagio] | | |
| | [SW bibliot] | | |
| | [SW horarios] | | |
| [E.9] | [SI Internet] | Errores de [re-]encaminamiento | [C] |
| | [SI Aula virtual] | | |
| | [SI Correo] | | |
| | [SI Mesa de ayuda] | | |
| | [SI Mandarin] | | |
| | [SI Reservas] | | |
| | [SI Sistema de Notas] | | |
| | [SE Portal WEB] | | |
| | [SW SO] | | |
| | [SW BD] | | |
| | [SW Ant.] | | |
| | [SW Ofi] | | |
| | [SW moodle] | | |
| | [SW nav] | | |
| | [SW diseñ] | | |
| | [SW nomina] | | |
| | [SW contab] | | |
| | [SW glpi] | | |

| | | | |
|---|---|---|---|
| | [SW notas] | | |
| | [SW plagio] | | |
| | [SW bibliot] | | |
| | [SW horarios] | | |
| | [COM LAN] | | |
| | [COM wifi] | | |
| | [COM Internte] | | |
| | [COM telefonía] | | |
| [E.10] | [SI Internet] | Errores de secuencia | [I] |
| | [SI Aula virtual] | | |
| | [SI Correo] | | |
| | [SI Mesa de ayuda] | | |
| | [SI Mandarin] | | |
| | [SI Reservas] | | |
| | [SI Sistema de Notas] | | |
| | [SE Portal WEB] | | |
| | [SW SO] | | |
| | [SW BD] | | |
| | [SW Ant.] | | |
| | [SW Ofi] | | |
| | [SW moodle] | | |
| | [SW nav] | | |
| | [SW diseñ] | | |
| | [SW nomina] | | |
| | [SW contab] | | |
| | [SW glpi] | | |
| | [SW notas] | | |
| | [SW plagio] | | |
| | [SW bibliot] | | |
| | [SW horarios] | | |
| | [COM LAN] | | |
| | [COM wifi] | | |
| | [COM Internte] | | |
| | [COM telefonía] | | |
| [E.15] | [D respaldo] | Alteración accidental de la información | [I] |
| | [D de config.] | | |
| | [D de Bit] | | |
| | [SI Internet] | | |
| | [SI Aula virtual] | | |
| | [SI Correo] | | |

| | | | |
|---|---|---|---|
| | [SI Mesa de ayuda] | | |
| | [SI Mandarin] | | |
| | [SI Reservas] | | |
| | [SI Sistema de Notas] | | |
| | [SE Portal WEB] | | |
| | [SW SO] | | |
| | [SW BD] | | |
| | [SW Ant.] | | |
| | [SW Ofi] | | |
| | [SW moodle] | | |
| | [SW nav] | | |
| | [SW diseñ] | | |
| | [SW nomina] | | |
| | [SW contab] | | |
| | [SW glpi] | | |
| | [SW notas] | | |
| | [SW plagio] | | |
| | [SW bibliot] | | |
| | [SW horarios] | | |
| | [COM LAN] | | |
| | [COM wifi] | | |
| | [COM Internet] | | |
| | [COM telefonía] | | |
| | [MEDIA DD] | | |
| | [MEDIA usb] | | |
| | [MEDIA electronic] | | |
| | [I Notas] | | |
| | [I Estudiantes] | | |
| | [I Padres de familia] | | |
| | [I Mallas Curriculares] | | |
| | [I Aspirantes] | | |
| | [I Exalumnas] | | |
| | [I estudiantes] | | |
| | [I Padres de familia] | | |
| | [I Colaboradores] | | |
| | [I Profesores] | | |
| | [I Exalumnas] | | |
| [E.18] | [D respaldo] | Destrucción de información | [D] |
| | [D de config.] | | |

| | | | |
|---|---|---|---|
| | [D de Bit] | | |
| | [SI Internet] | | |
| | [SI Aula virtual] | | |
| | [SI Correo] | | |
| | [SI Mesa de ayuda] | | |
| | [SI Mandarin] | | |
| | [SI Reservas] | | |
| | [SI Sistema de Notas] | | |
| | [SE Portal WEB] | | |
| | [SW SO] | | |
| | [SW BD] | | |
| | [SW Ant.] | | |
| | [SW Ofi] | | |
| | [SW moodle] | | |
| | [SW nav] | | |
| | [SW diseñ] | | |
| | [SW nomina] | | |
| | [SW contab] | | |
| | [SW glpi] | | |
| | [SW notas] | | |
| | [SW plagio] | | |
| | [SW bibliot] | | |
| | [SW horarios] | | |
| | [COM LAN] | | |
| | [COM wifi] | | |
| | [COM Internte] | | |
| | [COM telefonía] | | |
| | [MEDIA DD] | | |
| | [MEDIA usb] | | |
| | [MEDIA electronic] | | |
| | [I Notas] | | |
| | [I Estudiantes] | | |
| | [I Padres de familia] | | |
| | [I Mallas Curriculares] | | |
| | [I Aspirantes] | | |
| | [I Exalumnas] | | |
| | [I estudiantes] | | |
| | [I Padres de familia] | | |
| | [I Colaboradores] | | |

| | | | |
|---|---|---|---|
| | [I Profesores] | | |
| | [I Exalumnas] | | |
| [E.19] | [D respaldo] | Fugas de información | [C] |
| | [D de config.] | | |
| | [D de Bit] | | |
| | [SI Internet] | | |
| | [SI Aula virtual] | | |
| | [SI Correo] | | |
| | [SI Mesa de ayuda] | | |
| | [SI Mandarin] | | |
| | [SI Reservas] | | |
| | [SI Sistema de Notas] | | |
| | [SE Portal WEB] | | |
| | [SW SO] | | |
| | [SW BD] | | |
| | [SW Ant.] | | |
| | [SW Ofi] | | |
| | [SW moodle] | | |
| | [SW nav] | | |
| | [SW diseñ] | | |
| | [SW nomina] | | |
| | [SW contab] | | |
| | [SW glpi] | | |
| | [SW notas] | | |
| | [SW plagio] | | |
| | [SW bibliot] | | |
| | [SW horarios] | | |
| | [COM LAN] | | |
| | [COM wifi] | | |
| | [COM Internte] | | |
| | [COM telefonía] | | |
| | [MEDIA DD] | | |
| | [MEDIA usb] | | |
| | [MEDIA electronic] | | |
| | [P ui] | | |
| | [P ue] | | |
| | [P soperte] | | |
| | [P adm] | | |
| | [P com] | | |
| | [P sec] | | |

| | | | |
|---|---|---|---|
| | [P dba] | | |
| | [P rector] | | |
| | [P Proc] | | |
| | [P Calidad] | | |
| | [P proveedores] | | |
| | [I Notas] | | |
| | [I Estudiantes] | | |
| | [I Padres de familia] | | |
| | [I Mallas Curriculares] | | |
| | [I Aspirantes] | | |
| | [I Exalumnas] | | |
| | [I estudiantes] | | |
| | [I Padres de familia] | | |
| | [I Colaboradores] | | |
| | [I Profesores] | | |
| | [I Exalumnas] | | |
| [E.20] | [SW SO] | Vulnerabilidad de los programas | [I]<br>[D]<br>[C] |
| | [SW BD] | | |
| | [SW Ant.] | | |
| | [SW Ofi] | | |
| | [SW moodle] | | |
| | [SW nav] | | |
| | [SW diseñ] | | |
| | [SW nomina] | | |
| | [SW contab] | | |
| | [SW glpi] | | |
| | [SW notas] | | |
| | [SW plagio] | | |
| | [SW bibliot] | | |
| | [SW horarios] | | |
| [E.21] | [SW SO] | Errores de mantenimiento/actualizado de programas | [I]<br>[D] |
| | [SW BD] | | |
| | [SW Ant.] | | |
| | [SW Ofi] | | |
| | [SW moodle] | | |
| | [SW nav] | | |
| | [SW diseñ] | | |
| | [SW nomina] | | |
| | [SW contab] | | |
| | [SW glpi] | | |

| | | | |
|---|---|---|---|
| | [SW notas] | | |
| | [SW plagio] | | |
| | [SW bibliot] | | |
| | [SW horarios] | | |
| [E.23] | [HW pc] | Errores de mantenimiento/actualización de equipos | [D] |
| | [HW portatil] | | |
| | [HW multif] | | |
| | [HW Serv] | | |
| | [HW ap] | | |
| | [HW switch] | | |
| | [HW videob] | | |
| | [HW pbx] | | |
| | [HW Ipad] | | |
| | [HW fotocop] | | |
| | [HW tv] | | |
| | [HW modem] | | |
| | [MEDIA electronic] | | |
| | [AUX ups] | | |
| | [AUX cableado] | | |
| | [AUX rack] | | |
| | [AUX gabinte] | | |
| | [AUX fibra] | | |
| [E.24] | [SI Internet] | Caida del sistema por agotamiento de recursos | [D] |
| | [SI Aula virtual] | | |
| | [SI Correo] | | |
| | [SI Mesa de ayuda] | | |
| | [SI Mandarin] | | |
| | [SI Reservas] | | |
| | [SI Sistema de Notas] | | |
| | [SE Portal WEB] | | |
| | [HW pc] | | |
| | [HW portatil] | | |
| | [HW multif] | | |
| | [HW Serv] | | |
| | [HW ap] | | |
| | [HW switch] | | |
| | [HW videob] | | |
| | [HW pbx] | | |
| | [HW Ipad] | | |
| | [HW fotocop] | | |

| | | | |
|---|---|---|---|
| | [HW tv] | | |
| | [HW modem] | | |
| | [COM LAN] | | |
| | [COM wifi] | | |
| | [COM Internte] | | |
| | [COM telefonía] | | |
| [E.25] | [HW pc] | Pérdida de equipos | [D]<br>[C] |
| | [HW portatil] | | |
| | [HW multif] | | |
| | [HW Serv] | | |
| | [HW ap] | | |
| | [HW switch] | | |
| | [HW videob] | | |
| | [HW pbx] | | |
| | [HW Ipad] | | |
| | [HW fotocop] | | |
| | [HW tv] | | |
| | [HW modem] | | |
| | [MEDIA DD] | | |
| | [MEDIA usb] | | |
| | [MEDIA electronic] | | |
| | [AUX ups] | | |
| | [AUX cableado] | | |
| | [AUX rack] | | |
| | [AUX gabinte] | | |
| | [AUX fibra] | | |
| **[A] Ataques intencionados** | | | |
| **Cod.** | **Activos** | **Amenaza** | **Dimensión** |
| [A.5] | [D respaldo] | Suplantación de la identidad del usuario | [C]<br>[A]<br>[I] |
| | [D de config.] | | |
| | [D de Bit] | | |
| | [SI Internet] | | |
| | [SI Aula virtual] | | |
| | [SI Correo] | | |
| | [SI Mesa de ayuda] | | |
| | [SI Mandarin] | | |
| | [SI Reservas] | | |
| | [SI Sistema de Notas] | | |
| | [SE Portal WEB] | | |

| | | | |
|---|---|---|---|
| | [SW SO] | | |
| | [SW BD] | | |
| | [SW Ant.] | | |
| | [SW Ofi] | | |
| | [SW moodle] | | |
| | [SW nav] | | |
| | [SW diseñ] | | |
| | [SW nomina] | | |
| | [SW contab] | | |
| | [SW glpi] | | |
| | [SW notas] | | |
| | [SW plagio] | | |
| | [SW bibliot] | | |
| | [SW horarios] | | |
| | [COM LAN] | | |
| | [COM wifi] | | |
| | [COM Internte] | | |
| | [COM telefonía] | | |
| | [I Notas] | | |
| | [I Estudiantes] | | |
| | [I Padres de familia] | | |
| | [I Mallas Curriculares] | | |
| | [I Aspirantes] | | |
| | [I Exalumnas] | | |
| | [I estudiantes] | | |
| | [I Padres de familia] | | |
| | [I Colaboradores] | | |
| | [I Profesores] | | |
| | [I Exalumnas] | | |
| [A.6] | [D respaldo] | Abuso de privilegios de acceso | [C]<br>[I]<br>[D] |
| | [D de config.] | | |
| | [D de Bit] | | |
| | [SI Internet] | | |
| | [SI Aula virtual] | | |
| | [SI Correo] | | |
| | [SI Mesa de ayuda] | | |
| | [SI Mandarin] | | |
| | [SI Reservas] | | |

| | | | |
|---|---|---|---|
| | [SI Sistema de Notas] | | |
| | [SE Portal WEB] | | |
| | [SW SO] | | |
| | [SW BD] | | |
| | [SW Ant.] | | |
| | [SW Ofi] | | |
| | [SW moodle] | | |
| | [SW nav] | | |
| | [SW diseñ] | | |
| | [SW nomina] | | |
| | [SW contab] | | |
| | [SW glpi] | | |
| | [SW notas] | | |
| | [SW plagio] | | |
| | [SW bibliot] | | |
| | [SW horarios] | | |
| | [HW pc] | | |
| | [HW portatil] | | |
| | [HW multif] | | |
| | [HW Serv] | | |
| | [HW ap] | | |
| | [HW switch] | | |
| | [HW videob] | | |
| | [HW pbx] | | |
| | [HW Ipad] | | |
| | [HW fotocop] | | |
| | [HW tv] | | |
| | [HW modem] | | |
| | [COM LAN] | | |
| | [COM wifi] | | |
| | [COM Internte] | | |
| | [COM telefonía] | | |
| [A.7] | [SI Internet] | Uso no previsto | [D]<br>[C]<br>[I] |
| | [SI Aula virtual] | | |
| | [SI Correo] | | |
| | [SI Mesa de ayuda] | | |
| | [SI Mandarin] | | |
| | [SI Reservas] | | |
| | [SI Sistema de Notas] | | |

| | | | |
|---|---|---|---|
| | [SE Portal WEB] | | |
| | [SW SO] | | |
| | [SW BD] | | |
| | [SW Ant.] | | |
| | [SW Ofi] | | |
| | [SW moodle] | | |
| | [SW nav] | | |
| | [SW diseñ] | | |
| | [SW nomina] | | |
| | [SW contab] | | |
| | [SW glpi] | | |
| | [SW notas] | | |
| | [SW plagio] | | |
| | [SW bibliot] | | |
| | [SW horarios] | | |
| | [HW pc] | | |
| | [HW portatil] | | |
| | [HW multif] | | |
| | [HW Serv] | | |
| | [HW ap] | | |
| | [HW switch] | | |
| | [HW videob] | | |
| | [HW pbx] | | |
| | [HW Ipad] | | |
| | [HW fotocop] | | |
| | [HW tv] | | |
| | [HW modem] | | |
| | [COM LAN] | | |
| | [COM wifi] | | |
| | [COM Internte] | | |
| | [COM telefonía] | | |
| | [MEDIA DD] | | |
| | [MEDIA usb] | | |
| | [MEDIA electronic] | | |
| | [AUX ups] | | |
| | [AUX cableado] | | |
| | [AUX rack] | | |
| | [AUX gabinte] | | |
| | [AUX fibra] | | |
| | [L administrativa] | | |
| | [L escuelas] | | |

| | | | |
|---|---|---|---|
| [A.8] | [SW SO] | Difusión de software dañino | [D]<br>[I]<br>[C] |
| | [SW BD] | | |
| | [SW Ant.] | | |
| | [SW Ofi] | | |
| | [SW moodle] | | |
| | [SW nav] | | |
| | [SW diseñ] | | |
| | [SW nomina] | | |
| | [SW contab] | | |
| | [SW glpi] | | |
| | [SW notas] | | |
| | [SW plagio] | | |
| | [SW bibliot] | | |
| | [SW horarios] | | |
| [A.9] | [SI Internet] | Errores de [re-<br>]encaminamiento | [C] |
| | [SI Aula virtual] | | |
| | [SI Correo] | | |
| | [SI Mesa de ayuda] | | |
| | [SI Mandarin] | | |
| | [SI Reservas] | | |
| | [SI Sistema de Notas] | | |
| | [SE Portal WEB] | | |
| | [SW SO] | | |
| | [SW BD] | | |
| | [SW Ant.] | | |
| | [SW Ofi] | | |
| | [SW moodle] | | |
| | [SW nav] | | |
| | [SW diseñ] | | |
| | [SW nomina] | | |
| | [SW contab] | | |
| | [SW glpi] | | |
| | [SW notas] | | |
| | [SW plagio] | | |
| | [SW bibliot] | | |
| | [SW horarios] | | |
| | [COM LAN] | | |
| | [COM wifi] | | |
| | [COM Internte] | | |
| | [COM telefonía] | | |

| | | | |
|---|---|---|---|
| [A.10] | [SI Internet] | Alteración de secuencia | [I] |
| | [SI Aula virtual] | | |
| | [SI Correo] | | |
| | [SI Mesa de ayuda] | | |
| | [SI Mandarin] | | |
| | [SI Reservas] | | |
| | [SI Sistema de Notas] | | |
| | [SE Portal WEB] | | |
| | [SW SO] | | |
| | [SW BD] | | |
| | [SW Ant.] | | |
| | [SW Ofi] | | |
| | [SW moodle] | | |
| | [SW nav] | | |
| | [SW diseñ] | | |
| | [SW nomina] | | |
| | [SW contab] | | |
| | [SW glpi] | | |
| | [SW notas] | | |
| | [SW plagio] | | |
| | [SW bibliot] | | |
| | [SW horarios] | | |
| | [COM LAN] | | |
| | [COM wifi] | | |
| | [COM Internte] | | |
| | [COM telefonía] | | |
| [A.11] | [D respaldo] | Acceso no autorizado | [C]<br>[I] |
| | [D de config.] | | |
| | [D de Bit] | | |
| | [SI Internet] | | |
| | [SI Aula virtual] | | |
| | [SI Correo] | | |
| | [SI Mesa de ayuda] | | |
| | [SI Mandarin] | | |
| | [SI Reservas] | | |
| | [SI Sistema de Notas] | | |
| | [SE Portal WEB] | | |
| | [SW SO] | | |
| | [SW BD] | | |

| | | | |
|---|---|---|---|
| | [SW Ant.] | | |
| | [SW Ofi] | | |
| | [SW moodle] | | |
| | [SW nav] | | |
| | [SW diseñ] | | |
| | [SW nomina] | | |
| | [SW contab] | | |
| | [SW glpi] | | |
| | [SW notas] | | |
| | [SW plagio] | | |
| | [SW bibliot] | | |
| | [SW horarios] | | |
| | [HW pc] | | |
| | [HW portatil] | | |
| | [HW multif] | | |
| | [HW Serv] | | |
| | [HW ap] | | |
| | [HW switch] | | |
| | [HW videob] | | |
| | [HW pbx] | | |
| | [HW Ipad] | | |
| | [HW fotocop] | | |
| | [HW tv] | | |
| | [HW modem] | | |
| | [COM LAN] | | |
| | [COM wifi] | | |
| | [COM Internte] | | |
| | [COM telefonía] | | |
| | [MEDIA DD] | | |
| | [MEDIA usb] | | |
| | [MEDIA electronic] | | |
| | [AUX ups] | | |
| | [AUX cableado] | | |
| | [AUX rack] | | |
| | [AUX gabinte] | | |
| | [AUX fibra] | | |
| | [L administrativa] | | |
| | [L escuelas] | | |
| [A.12] | [COM LAN] | Análisis de tráfico | [C] |
| | [COM wifi] | | |
| | [COM Internte] | | |

| | | | |
|---|---|---|---|
| | [COM telefonía] | | |
| [A.13] | [SI Internet] | Repudio | [I]<br>[T] |
| | [SI Aula virtual] | | |
| | [SI Correo] | | |
| | [SI Mesa de ayuda] | | |
| | [SI Mandarin] | | |
| | [SI Reservas] | | |
| | [SI Sistema de Notas] | | |
| | [SE Portal WEB] | | |
| [A.14] | [COM LAN] | Interceptación de información | [C] |
| | [COM wifi] | | |
| | [COM Internte] | | |
| | [COM telefonía] | | |
| [A.15] | [D respaldo] | Modificación deliberada de la información | [I] |
| | [D de config.] | | |
| | [D de Bit] | | |
| | [SI Internet] | | |
| | [SI Aula virtual] | | |
| | [SI Correo] | | |
| | [SI Mesa de ayuda] | | |
| | [SI Mandarin] | | |
| | [SI Reservas] | | |
| | [SI Sistema de Notas] | | |
| | [SE Portal WEB] | | |
| | [SW SO] | | |
| | [SW BD] | | |
| | [SW Ant.] | | |
| | [SW Ofi] | | |
| | [SW moodle] | | |
| | [SW nav] | | |
| | [SW diseñ] | | |
| | [SW nomina] | | |
| | [SW contab] | | |
| | [SW glpi] | | |
| | [SW notas] | | |
| | [SW plagio] | | |
| | [SW bibliot] | | |
| | [SW horarios] | | |
| | [COM LAN] | | |

| | | | |
|---|---|---|---|
| | [COM wifi] | | |
| | [COM Internte] | | |
| | [COM telefonía] | | |
| | [MEDIA DD] | | |
| | [MEDIA usb] | | |
| | [MEDIA electronic] | | |
| | [L administrativa] | | |
| | [L escuelas] | | |
| [A.18] | [D respaldo] | Destrucción de información | [D] |
| | [D de config.] | | |
| | [D de Bit] | | |
| | [SI Internet] | | |
| | [SI Aula virtual] | | |
| | [SI Correo] | | |
| | [SI Mesa de ayuda] | | |
| | [SI Mandarin] | | |
| | [SI Reservas] | | |
| | [SI Sistema de Notas] | | |
| | [SE Portal WEB] | | |
| | [SW SO] | | |
| | [SW BD] | | |
| | [SW Ant.] | | |
| | [SW Ofi] | | |
| | [SW moodle] | | |
| | [SW nav] | | |
| | [SW diseñ] | | |
| | [SW nomina] | | |
| | [SW contab] | | |
| | [SW glpi] | | |
| | [SW notas] | | |
| | [SW plagio] | | |
| | [SW bibliot] | | |
| | [SW horarios] | | |
| | [MEDIA DD] | | |
| | [MEDIA usb] | | |
| | [MEDIA electronic] | | |
| | [L administrativa] | | |
| | [L escuelas] | | |
| [A.19] | [D respaldo] | Divulgación de información | [C] |
| | [D de config.] | | |

| | | | |
|---|---|---|---|
| | [D de Bit] | | |
| | [SI Internet] | | |
| | [SI Aula virtual] | | |
| | [SI Correo] | | |
| | [SI Mesa de ayuda] | | |
| | [SI Mandarin] | | |
| | [SI Reservas] | | |
| | [SI Sistema de Notas] | | |
| | [SE Portal WEB] | | |
| | [SW SO] | | |
| | [SW BD] | | |
| | [SW Ant.] | | |
| | [SW Ofi] | | |
| | [SW moodle] | | |
| | [SW nav] | | |
| | [SW diseñ] | | |
| | [SW nomina] | | |
| | [SW contab] | | |
| | [SW glpi] | | |
| | [SW notas] | | |
| | [SW plagio] | | |
| | [SW bibliot] | | |
| | [SW horarios] | | |
| | [COM LAN] | | |
| | [COM wifi] | | |
| | [COM Internte] | | |
| | [COM telefonía] | | |
| | [MEDIA DD] | | |
| | [MEDIA usb] | | |
| | [MEDIA electronic] | | |
| | [L administrativa] | | |
| | [L escuelas] | | |
| [A.22] | [SW SO] | Manipulación de programas | [C]<br>[I]<br>[D] |
| | [SW BD] | | |
| | [SW Ant.] | | |
| | [SW Ofi] | | |
| | [SW moodle] | | |
| | [SW nav] | | |
| | [SW diseñ] | | |
| | [SW nomina] | | |

| | | | |
|---|---|---|---|
| | [SW contab] | | |
| | [SW glpi] | | |
| | [SW notas] | | |
| | [SW plagio] | | |
| | [SW bibliot] | | |
| | [SW horarios] | | |
| [A.23] | [HW pc] | Manipulación de los equipos | [C]<br>[D] |
| | [HW portatil] | | |
| | [HW multif] | | |
| | [HW Serv] | | |
| | [HW ap] | | |
| | [HW switch] | | |
| | [HW videob] | | |
| | [HW pbx] | | |
| | [HW Ipad] | | |
| | [HW fotocop] | | |
| | [HW tv] | | |
| | [HW modem] | | |
| | [MEDIA DD] | | |
| | [MEDIA usb] | | |
| | [MEDIA electronic] | | |
| | [AUX ups] | | |
| | [AUX cableado] | | |
| | [AUX rack] | | |
| | [AUX gabinte] | | |
| | [AUX fibra] | | |
| [A.24] | [SI Internet] | Denegación de servicio | [D] |
| | [SI Aula virtual] | | |
| | [SI Correo] | | |
| | [SI Mesa de ayuda] | | |
| | [SI Mandarin] | | |
| | [SI Reservas] | | |
| | [SI Sistema de Notas] | | |
| | [HW pc] | | |
| | [HW portatil] | | |
| | [HW multif] | | |
| | [HW Serv] | | |
| | [HW ap] | | |
| | [HW switch] | | |
| | [HW videob] | | |

| | | | |
|---|---|---|---|
| | [HW pbx] | | |
| | [HW Ipad] | | |
| | [HW fotocop] | | |
| | [HW tv] | | |
| | [HW modem] | | |
| | [COM LAN] | | |
| | [COM wifi] | | |
| | [COM Internte] | | |
| | [COM telefonía] | | |
| [A.25] | [HW pc] | Robo | [D]<br>[C] |
| | [HW portatil] | | |
| | [HW multif] | | |
| | [HW Serv] | | |
| | [HW ap] | | |
| | [HW switch] | | |
| | [HW videob] | | |
| | [HW pbx] | | |
| | [HW Ipad] | | |
| | [HW fotocop] | | |
| | [HW tv] | | |
| | [HW modem] | | |
| | [MEDIA DD] | | |
| | [MEDIA usb] | | |
| | [MEDIA electronic] | | |
| | [AUX ups] | | |
| | [AUX cableado] | | |
| | [AUX rack] | | |
| | [AUX gabinte] | | |
| | [AUX fibra] | | |
| [A.26] | [HW pc] | Ataque destructivo | [D] |
| | [HW portatil] | | |
| | [HW multif] | | |
| | [HW Serv] | | |
| | [HW ap] | | |
| | [HW switch] | | |
| | [HW videob] | | |
| | [HW pbx] | | |
| | [HW Ipad] | | |
| | [HW fotocop] | | |
| | [HW tv] | | |
| | [HW modem] | | |

| | | | |
|---|---|---|---|
| | [MEDIA DD] | | |
| | [MEDIA usb] | | |
| | [MEDIA electronic] | | |
| | [AUX ups] | | |
| | [AUX cableado] | | |
| | [AUX rack] | | |
| | [AUX gabinte] | | |
| | [AUX fibra] | | |
| | [L administrativa] | | |
| | [L escuelas] | | |
| [A.27] | [L administrativa] | Ocupación enemiga | [D]<br>[C] |
| | [L escuelas] | | |
| [A.28] | [P ui] | Indisponibilidad del personal | [D] |
| | [P soperte] | | |
| | [P adm] | | |
| | [P com] | | |
| | [P sec] | | |
| | [P dba] | | |
| | [P rector] | | |
| | [P Proc] | | |
| | [P Calidad] | | |
| [A.29] | [P ui] | Extrosión | [D] |
| | [P ue] | | |
| | [P soperte] | | |
| | [P adm] | | |
| | [P com] | | |
| | [P sec] | | |
| | [P dba] | | |
| | [P rector] | | |
| | [P Proc] | | |
| | [P Calidad] | | |
| | [P proveedores] | | |
| [A.30] | [P ui] | Ingeniería social | [C]<br>[I]<br>[D] |
| | [P ue] | | |
| | [P soperte] | | |
| | [P adm] | | |
| | [P com] | | |
| | [P sec] | | |
| | [P dba] | | |
| | [P rector] | | |
| | [P Proc] | | |

| | | | |
|---|---|---|---|
| | [P Calidad]<br>[P proveedores] | | |

# ANEXO 6. VALORACIÓN DE LAS AMENAZAS

| Valoración de las amenazas | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **[N] Desastres Naturales** | | | | | | | | |
| **Cod.** | **Amenaza** | **Activos** | **Frecuencia** | **D** | **I** | **C** | **A** | **T** |
| [N1] | Fuego | [HW pc] | 0,01 | 100% | | | | |
| | | [HW portatil] | 0,01 | 100% | | | | |
| | | [HW multif] | 0,01 | 100% | | | | |
| | | [HW Serv] | 0,01 | 100% | | | | |
| | | [HW ap] | 0,01 | 100% | | | | |
| | | [HW switch] | 0,01 | 100% | | | | |
| | | [HW videob] | 0,01 | 100% | | | | |
| | | [HW pbx] | 0,01 | 100% | | | | |
| | | [HW Ipad] | 0,01 | 100% | | | | |
| | | [HW fotocop] | 0,01 | 100% | | | | |
| | | [HW tv] | 0,01 | 100% | | | | |
| | | [HW modem] | 0,01 | 100% | | | | |
| | | [MEDIA DD] | 0,01 | 100% | | | | |
| | | [MEDIA usb] | 0,01 | 100% | | | | |
| | | [MEDIA electronic] | 0,01 | 100% | | | | |
| | | [AUX ups] | 0,01 | 100% | | | | |
| | | [AUX cableado] | 0,01 | 100% | | | | |
| | | [AUX rack] | 0,01 | 100% | | | | |
| | | [AUX gabinte] | 0,01 | 100% | | | | |
| | | [AUX fibra] | 0,01 | 100% | | | | |
| | | [L administrativa] | 0,01 | 100% | | | | |
| | | [L escuelas] | 0,01 | 100% | | | | |
| [N2] | Daños por agua | [HW pc] | 0,01 | 100% | | | | |
| | | [HW portatil] | 0,01 | 100% | | | | |
| | | [HW multif] | 0,01 | 100% | | | | |
| | | [HW Serv] | 0,01 | 100% | | | | |
| | | [HW ap] | 0,01 | 100% | | | | |
| | | [HW switch] | 0,01 | 100% | | | | |
| | | [HW videob] | 0,01 | 100% | | | | |
| | | [HW pbx] | 0,01 | 100% | | | | |
| | | [HW Ipad] | 0,01 | 100% | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | [HW fotocop] | 0,01 | 100% | | | | |
| | | [HW tv] | 0,01 | 100% | | | | |
| | | [HW modem] | 0,01 | 100% | | | | |
| | | [MEDIA DD] | 0,01 | 100% | | | | |
| | | [MEDIA usb] | 0,01 | 100% | | | | |
| | | [MEDIA electronic] | 0,01 | 100% | | | | |
| | | [AUX ups] | 0,01 | 100% | | | | |
| | | [AUX cableado] | 0,01 | 100% | | | | |
| | | [AUX rack] | 0,01 | 100% | | | | |
| | | [AUX gabinte] | 0,01 | 100% | | | | |
| | | [AUX fibra] | 0,01 | 100% | | | | |
| | | [L administrativa] | 0,01 | 75% | | | | |
| | | [L escuelas] | 0,01 | 75% | | | | |
| [N.*] | Desastres Naturales | [HW pc] | 0,01 | 100% | | | | |
| | | [HW portatil] | 0,01 | 100% | | | | |
| | | [HW multif] | 0,01 | 100% | | | | |
| | | [HW Serv] | 0,01 | 100% | | | | |
| | | [HW ap] | 0,01 | 100% | | | | |
| | | [HW switch] | 0,01 | 100% | | | | |
| | | [HW videob] | 0,01 | 100% | | | | |
| | | [HW pbx] | 0,01 | 100% | | | | |
| | | [HW Ipad] | 0,01 | 100% | | | | |
| | | [HW fotocop] | 0,01 | 100% | | | | |
| | | [HW tv] | 0,01 | 100% | | | | |
| | | [HW modem] | 0,01 | 100% | | | | |
| | | [MEDIA DD] | 0,01 | 100% | | | | |
| | | [MEDIA usb] | 0,01 | 100% | | | | |
| | | [MEDIA electronic] | 0,01 | 100% | | | | |
| | | [AUX ups] | 0,01 | 100% | | | | |
| | | [AUX cableado] | 0,01 | 100% | | | | |
| | | [AUX rack] | 0,01 | 100% | | | | |
| | | [AUX gabinte] | 0,01 | 100% | | | | |
| | | [AUX fibra] | 0,01 | 100% | | | | |
| | | [L administrativa] | 0,01 | 100% | | | | |
| | | [L escuelas] | 0,01 | 100% | | | | |
| **[I] De origen industrial** | | | | | | | | |
| **Cod.** | **Amenaza** | **Activos** | | **D** | **I** | **C** | **A** | **T** |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [I1] | Fuego | [HW pc] | 0,01 | 100% | | | | |
| | | [HW portatil] | 0,01 | 100% | | | | |
| | | [HW multif] | 0,01 | 100% | | | | |
| | | [HW Serv] | 0,01 | 100% | | | | |
| | | [HW ap] | 0,01 | 100% | | | | |
| | | [HW switch] | 0,01 | 100% | | | | |
| | | [HW videob] | 0,01 | 100% | | | | |
| | | [HW pbx] | 0,01 | 100% | | | | |
| | | [HW Ipad] | 0,01 | 100% | | | | |
| | | [HW fotocop] | 0,01 | 100% | | | | |
| | | [HW tv] | 0,01 | 100% | | | | |
| | | [HW modem] | 0,01 | 100% | | | | |
| | | [MEDIA DD] | 0,01 | 100% | | | | |
| | | [MEDIA usb] | 0,01 | 100% | | | | |
| | | [MEDIA electronic] | 0,01 | 100% | | | | |
| | | [AUX ups] | 0,01 | 100% | | | | |
| | | [AUX cableado] | 0,01 | 100% | | | | |
| | | [AUX rack] | 0,01 | 100% | | | | |
| | | [AUX gabinte] | 0,01 | 100% | | | | |
| | | [AUX fibra] | 0,01 | 100% | | | | |
| | | [L administrativa] | 0,01 | 100% | | | | |
| | | [L escuelas] | 0,01 | 100% | | | | |
| [I2] | Daños por agua | [HW pc] | 0,01 | 100% | | | | |
| | | [HW portatil] | 0,01 | 100% | | | | |
| | | [HW multif] | 0,01 | 100% | | | | |
| | | [HW Serv] | 0,01 | 100% | | | | |
| | | [HW ap] | 0,01 | 100% | | | | |
| | | [HW switch] | 0,01 | 100% | | | | |
| | | [HW videob] | 0,01 | 100% | | | | |
| | | [HW pbx] | 0,01 | 100% | | | | |
| | | [HW Ipad] | 0,01 | 100% | | | | |
| | | [HW fotocop] | 0,01 | 100% | | | | |
| | | [HW tv] | 0,01 | 100% | | | | |
| | | [HW modem] | 0,01 | 100% | | | | |
| | | [MEDIA DD] | 0,01 | 100% | | | | |
| | | [MEDIA usb] | 0,01 | 100% | | | | |
| | | [MEDIA electronic] | 0,01 | 100% | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | [AUX ups] | 0,01 | 100% | | | | |
| | | [AUX cableado] | 0,01 | 100% | | | | |
| | | [AUX rack] | 0,01 | 100% | | | | |
| | | [AUX gabinte] | 0,01 | 100% | | | | |
| | | [AUX fibra] | 0,01 | 100% | | | | |
| | | [L administrativa] | 0,01 | 75% | | | | |
| | | [L escuelas] | 0,01 | 75% | | | | |
| [I.*] | Desastres Naturales | [HW pc] | 0,01 | 100% | | | | |
| | | [HW portatil] | 0,01 | 100% | | | | |
| | | [HW multif] | 0,01 | 100% | | | | |
| | | [HW Serv] | 0,01 | 100% | | | | |
| | | [HW ap] | 0,01 | 100% | | | | |
| | | [HW switch] | 0,01 | 100% | | | | |
| | | [HW videob] | 0,01 | 100% | | | | |
| | | [HW pbx] | 0,01 | 100% | | | | |
| | | [HW Ipad] | 0,01 | 100% | | | | |
| | | [HW fotocop] | 0,01 | 100% | | | | |
| | | [HW tv] | 0,01 | 100% | | | | |
| | | [HW modem] | 0,01 | 100% | | | | |
| | | [MEDIA DD] | 0,01 | 100% | | | | |
| | | [MEDIA usb] | 0,01 | 100% | | | | |
| | | [MEDIA electronic] | 0,01 | 100% | | | | |
| | | [AUX ups] | 0,01 | 100% | | | | |
| | | [AUX cableado] | 0,01 | 100% | | | | |
| | | [AUX rack] | 0,01 | 100% | | | | |
| | | [AUX gabinte] | 0,01 | 100% | | | | |
| | | [AUX fibra] | 0,01 | 100% | | | | |
| | | [L administrativa] | 0,01 | 100% | | | | |
| | | [L escuelas] | 0,01 | 100% | | | | |
| [I.3] | Contaminación mecánica | [HW pc] | 0,1 | 20% | | | | |
| | | [HW portatil] | 0,1 | 5% | | | | |
| | | [HW multif] | 0,1 | 5% | | | | |
| | | [HW Serv] | 0,1 | 5% | | | | |
| | | [HW ap] | 0,1 | 5% | | | | |
| | | [HW switch] | 0,1 | 5% | | | | |
| | | [HW videob] | 0,1 | 5% | | | | |
| | | [HW pbx] | 0,1 | 5% | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | [HW Ipad] | 0,1 | 5% | | | | |
| | | [HW fotocop] | 0,1 | 5% | | | | |
| | | [HW tv] | 0,1 | 5% | | | | |
| | | [HW modem] | 0,1 | 5% | | | | |
| | | [MEDIA DD] | 0,1 | 5% | | | | |
| | | [MEDIA usb] | 0,1 | 5% | | | | |
| | | [MEDIA electronic] | 0,1 | 5% | | | | |
| | | [AUX ups] | 0,1 | 5% | | | | |
| | | [AUX cableado] | 0,1 | 5% | | | | |
| | | [AUX rack] | 0,1 | 5% | | | | |
| | | [AUX gabinte] | 0,1 | 5% | | | | |
| | | [AUX fibra] | 0,1 | 5% | | | | |
| [I.4] | Contaminación electromagnética | [HW Serv] | 0,01 | 20% | | | | |
| | | [HW ap] | 0,01 | 20% | | | | |
| | | [HW switch] | 0,01 | 20% | | | | |
| | | [HW pbx] | 0,01 | 20% | | | | |
| | | [MEDIA DD] | 0,01 | 20% | | | | |
| | | [MEDIA usb] | 0,01 | 20% | | | | |
| | | [MEDIA electronic] | 0,01 | 20% | | | | |
| | | [AUX cableado] | 0,01 | 20% | | | | |
| | | [AUX fibra] | 0,01 | 20% | | | | |
| [I.5] | Averia de origen físico o lógico | [SW SO] | 1 | 100% | | | | |
| | | [SW BD] | 1 | 100% | | | | |
| | | [SW Ant.] | 1 | 100% | | | | |
| | | [SW Ofi] | 1 | 100% | | | | |
| | | [SW moodle] | 1 | 100% | | | | |
| | | [SW nav] | 1 | 100% | | | | |
| | | [SW diseñ] | 1 | 100% | | | | |
| | | [SW nomina] | 1 | 100% | | | | |
| | | [SW contab] | 1 | 100% | | | | |
| | | [SW glpi] | 1 | 100% | | | | |
| | | [SW notas] | 1 | 100% | | | | |
| | | [SW plagio] | 1 | 100% | | | | |
| | | [SW bibliot] | 1 | 100% | | | | |
| | | [SW horarios] | 1 | 100% | | | | |
| | | [HW pc] | 1 | 100% | | | | |
| | | [HW portatil] | 1 | 100% | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | [HW multif] | 1 | 100% | | | | |
| | | [HW Serv] | 1 | 100% | | | | |
| | | [HW ap] | 1 | 100% | | | | |
| | | [HW switch] | 1 | 100% | | | | |
| | | [HW videob] | 1 | 100% | | | | |
| | | [HW pbx] | 1 | 100% | | | | |
| | | [HW Ipad] | 1 | 100% | | | | |
| | | [HW fotocop] | 1 | 100% | | | | |
| | | [HW tv] | 1 | 100% | | | | |
| | | [HW modem] | 1 | 100% | | | | |
| | | [MEDIA DD] | 1 | 100% | | | | |
| | | [MEDIA usb] | 1 | 100% | | | | |
| | | [MEDIA electronic] | 1 | 100% | | | | |
| | | [AUX ups] | 1 | 100% | | | | |
| | | [AUX cableado] | 1 | 100% | | | | |
| | | [AUX rack] | 0,1 | 100% | | | | |
| | | [AUX gabinte] | 0,1 | 100% | | | | |
| | | [AUX fibra] | 0,1 | 100% | | | | |
| [I.6] | Corte de suministro eléctrico | [HW pc] | 10 | 100% | | | | |
| | | [HW portatil] | 10 | 100% | | | | |
| | | [HW multif] | 10 | 100% | | | | |
| | | [HW Serv] | 10 | 100% | | | | |
| | | [HW ap] | 10 | 100% | | | | |
| | | [HW switch] | 10 | 100% | | | | |
| | | [HW videob] | 10 | 100% | | | | |
| | | [HW pbx] | 10 | 100% | | | | |
| | | [HW Ipad] | 10 | 100% | | | | |
| | | [HW fotocop] | 10 | 100% | | | | |
| | | [HW tv] | 10 | 100% | | | | |
| | | [HW modem] | 10 | 100% | | | | |
| | | [MEDIA electronic] | 10 | 100% | | | | |
| | | [AUX ups] | 10 | 100% | | | | |
| | | [AUX cableado] | 10 | 100% | | | | |
| | | [AUX rack] | 10 | 100% | | | | |
| | | [AUX gabinte] | 10 | 100% | | | | |
| | | [AUX fibra] | 10 | 100% | | | | |
| [I.7] | | [HW pc] | 0,01 | 20% | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Condiciones inadecuadas de temperatura o humedad | [HW portatil] | 0,01 | 20% | | | | |
| | | [HW multif] | 0,01 | 20% | | | | |
| | | [HW Serv] | 0,01 | 20% | | | | |
| | | [HW ap] | 0,01 | 20% | | | | |
| | | [HW switch] | 0,01 | 20% | | | | |
| | | [HW videob] | 0,01 | 20% | | | | |
| | | [HW pbx] | 0,01 | 20% | | | | |
| | | [HW Ipad] | 0,01 | 20% | | | | |
| | | [HW fotocop] | 0,01 | 20% | | | | |
| | | [HW tv] | 0,01 | 20% | | | | |
| | | [HW modem] | 0,01 | 20% | | | | |
| | | [MEDIA electronic] | 0,01 | 20% | | | | |
| | | [AUX ups] | 0,01 | 20% | | | | |
| | | [AUX cableado] | 0,01 | 5% | | | | |
| | | [AUX rack] | 0,01 | 5% | | | | |
| | | [AUX gabinte] | 0,01 | 5% | | | | |
| | | [AUX fibra] | 0,01 | 5% | | | | |
| [I.8] | Fallo de servicios de comunicaciones | [COM LAN] | 0,1 | 100% | | | | |
| | | [COM wifi] | 0,1 | 100% | | | | |
| | | [COM Internte] | 0,1 | 100% | | | | |
| | | [COM telefonía] | 0,1 | 100% | | | | |
| [I.9] | Interrupción de otros servicios y suministros esenciales | [AUX ups] | 0,1 | 50% | | | | |
| [I. 10] | Degradación de los soportes de almacenamiento de la información | [MEDIA DD] | 0,1 | 100% | | | | |
| | | [MEDIA usb] | 0,1 | 100% | | | | |
| | | [MEDIA electronic] | 0,1 | 100% | | | | |
| **[E] Errores y fallos no intencionados** | | | | | | | | |
| **Cod.** | **Amenaza** | **Activos** | | **D** | **I** | **C** | **A** | **T** |
| [E.1] | Errores de los usuarios | [D respaldo] | 0,1 | 75% | 75% | 75% | | |
| | | [D de config.] | 0,1 | 75% | 75% | 75% | | |
| | | [D de Bit] | 0,1 | 75% | 75% | 75% | | |
| | | [SI Internet] | 0,1 | 75% | 75% | 75% | | |
| | | [SI Aula virtual] | 0,1 | 75% | 75% | 75% | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | [SI Correo] | 0,1 | 75% | 75% | 75% | | |
| | | [SI Mesa de ayuda] | 0,1 | 75% | 75% | 75% | | |
| | | [SI Mandarin] | 0,1 | 75% | 75% | 75% | | |
| | | [SI Reservas] | 0,1 | 75% | 75% | 75% | | |
| | | [SI Sistema de Notas] | 0,1 | 75% | 75% | 75% | | |
| | | [SE Portal WEB] | 0,1 | 75% | 75% | 75% | | |
| | | [SW SO] | 0,1 | 75% | 75% | 75% | | |
| | | [SW BD] | 0,1 | 75% | 75% | 75% | | |
| | | [SW Ant.] | 0,1 | 75% | 75% | 75% | | |
| | | [SW Ofi] | 0,1 | 75% | 75% | 75% | | |
| | | [SW moodle] | 0,1 | 75% | 75% | 75% | | |
| | | [SW nav] | 0,1 | 75% | 75% | 75% | | |
| | | [SW diseñ] | 0,1 | 75% | 75% | 75% | | |
| | | [SW nomina] | 0,1 | 75% | 75% | 75% | | |
| | | [SW contab] | 0,1 | 75% | 75% | 75% | | |
| | | [SW glpi] | 0,1 | 75% | 75% | 75% | | |
| | | [SW notas] | 0,1 | 75% | 75% | 75% | | |
| | | [SW plagio] | 0,1 | 75% | 75% | 75% | | |
| | | [SW bibliot] | 0,1 | 75% | 75% | 75% | | |
| | | [SW horarios] | 0,1 | 75% | 75% | 75% | | |
| | | [MEDIA DD] | 0,1 | 75% | 75% | 75% | | |
| | | [MEDIA usb] | 0,1 | 75% | 75% | 75% | | |
| | | [MEDIA electronic] | 0,1 | 75% | 75% | 75% | | |
| | | [I Notas] | 0,1 | 75% | 75% | 75% | | |
| | | [I Estudiantes] | 0,1 | 75% | 75% | 75% | | |
| | | [I Padres de familia] | 0,1 | 75% | 75% | 75% | | |
| | | [I Mallas Curriculares] | 0,1 | 75% | 75% | 75% | | |
| | | [I Aspirantes] | 0,1 | 75% | 75% | 75% | | |
| | | [I Exalumnas] | 0,1 | 75% | 75% | 75% | | |
| | | [I estudiantes] | 0,1 | 75% | 75% | 75% | | |
| | | [I Padres de familia] | 0,1 | 75% | 75% | 75% | | |
| | | [I Colaboradores] | 0,1 | 75% | 75% | 75% | | |
| | | [I Profesores] | 0,1 | 75% | 75% | 75% | | |
| | | [I Exalumnas] | 0,1 | 75% | 75% | 75% | | |
| [E.2] | Errores del administrador | [D respaldo] | 0,1 | 75% | 50% | 50% | | |
| | | [D de config.] | 0,1 | 75% | 75% | 75% | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | [D de Bit] | 0,1 | 75% | 75% | 75% | | |
| | | [SI Internet] | 0,1 | 50% | 50% | 50% | | |
| | | [SI Aula virtual] | 0,1 | 75% | 75% | 75% | | |
| | | [SI Correo] | 0,1 | 20% | 20% | 20% | | |
| | | [SI Mesa de ayuda] | 0,1 | 20% | 20% | 20% | | |
| | | [SI Mandarin] | 0,1 | 20% | 20% | 20% | | |
| | | [SI Reservas] | 0,1 | 20% | 20% | 20% | | |
| | | [SI Sistema de Notas] | 0,1 | 20% | 20% | 20% | | |
| | | [SE Portal WEB] | 0,1 | 20% | 20% | 20% | | |
| | | [SW SO] | 0,1 | 20% | 20% | 20% | | |
| | | [SW BD] | 0,1 | 20% | 20% | 20% | | |
| | | [SW Ant.] | 0,1 | 20% | 20% | 20% | | |
| | | [SW Ofi] | 0,1 | 20% | 20% | 20% | | |
| | | [SW moodle] | 0,1 | 20% | 20% | 20% | | |
| | | [SW nav] | 0,1 | 20% | 20% | 20% | | |
| | | [SW diseñ] | 0,1 | 20% | 20% | 20% | | |
| | | [SW nomina] | 0,1 | 20% | 20% | 20% | | |
| | | [SW contab] | 0,1 | 20% | 20% | 20% | | |
| | | [SW glpi] | 0,1 | 20% | 20% | 20% | | |
| | | [SW notas] | 0,1 | 20% | 20% | 20% | | |
| | | [SW plagio] | 0,1 | 5% | 5% | 5% | | |
| | | [SW bibliot] | 0,1 | 20% | 20% | 20% | | |
| | | [SW horarios] | 0,1 | 20% | 20% | 20% | | |
| | | [MEDIA electronic] | 0,1 | 75% | 75% | 75% | | |
| | | [I Notas] | 0,1 | 50% | 50% | 50% | | |
| | | [I Estudiantes] | 0,1 | 75% | 75% | 75% | | |
| | | [I Padres de familia] | 0,1 | 20% | 20% | 20% | | |
| | | [I Mallas Curriculares] | 0,1 | 20% | 20% | 20% | | |
| | | [I Aspirantes] | 0,1 | 20% | 20% | 20% | | |
| | | [I Exalumnas] | 0,1 | 20% | 20% | 20% | | |
| | | [I estudiantes] | 0,1 | 20% | 20% | 20% | | |
| | | [I Padres de familia] | 0,1 | 20% | 20% | 20% | | |
| | | [I Colaboradores] | 0,1 | 20% | 20% | 20% | | |
| | | [I Profesores] | 0,1 | 20% | 20% | 20% | | |
| | | [I Exalumnas] | 0,1 | 20% | 20% | 20% | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [E.4] | Errores de configuración | [D de config.] | 0,1 | | 50% | | | |
| [E.8] | Difusión de software dañino | [SW SO] | 0,1 | 75% | 75% | 20% | | |
| | | [SW BD] | 0,1 | 75% | 75% | 20% | | |
| | | [SW Ant.] | 0,1 | 75% | 75% | 20% | | |
| | | [SW Ofi] | 0,1 | 75% | 75% | 20% | | |
| | | [SW moodle] | 0,1 | 50% | 50% | 20% | | |
| | | [SW nav] | 0,1 | 75% | 75% | 20% | | |
| | | [SW diseñ] | 0,1 | 75% | 75% | 20% | | |
| | | [SW nomina] | 0,1 | 75% | 75% | 20% | | |
| | | [SW contab] | 0,1 | 75% | 75% | 20% | | |
| | | [SW glpi] | 0,1 | 75% | 75% | 20% | | |
| | | [SW notas] | 0,1 | 75% | 75% | 20% | | |
| | | [SW plagio] | 0,1 | 50% | 50% | 20% | | |
| | | [SW bibliot] | 0,1 | 75% | 75% | 20% | | |
| | | [SW horarios] | 0,1 | 75% | 75% | 20% | | |
| [E.9] | Errores de [re-]encaminamiento | [SI Internet] | 0,1 | | | 20% | | |
| | | [SI Aula virtual] | 0,1 | | | 20% | | |
| | | [SI Correo] | 0,1 | | | 20% | | |
| | | [SI Mesa de ayuda] | 0,1 | | | 20% | | |
| | | [SI Mandarin] | 0,1 | | | 20% | | |
| | | [SI Reservas] | 0,1 | | | 20% | | |
| | | [SI Sistema de Notas] | 0,1 | | | 20% | | |
| | | [SE Portal WEB] | 0,1 | | | 20% | | |
| | | [SW SO] | 0,1 | | | 20% | | |
| | | [SW BD] | 0,1 | | | 20% | | |
| | | [SW Ant.] | 0,1 | | | 20% | | |
| | | [SW Ofi] | 0,1 | | | 20% | | |
| | | [SW moodle] | 0,1 | | | 20% | | |
| | | [SW nav] | 0,1 | | | 20% | | |
| | | [SW diseñ] | 0,1 | | | 20% | | |
| | | [SW nomina] | 0,1 | | | 20% | | |
| | | [SW contab] | 0,1 | | | 20% | | |
| | | [SW glpi] | 0,1 | | | 20% | | |
| | | [SW notas] | 0,1 | | | 20% | | |
| | | [SW plagio] | 0,1 | | | 20% | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | [SW bibliot] | 0,1 | | | 20% | | |
| | | [SW horarios] | 0,1 | | | 20% | | |
| | | [COM LAN] | 0,1 | | | 20% | | |
| | | [COM wifi] | 0,1 | | | 20% | | |
| | | [COM Internte] | 0,1 | | | 20% | | |
| | | [COM telefonía] | 0,1 | | | 20% | | |
| [E.10] | Errores de secuencia | [SI Internet] | 0,1 | | 75% | | | |
| | | [SI Aula virtual] | 0,1 | | 75% | | | |
| | | [SI Correo] | 0,1 | | 75% | | | |
| | | [SI Mesa de ayuda] | 0,1 | | 75% | | | |
| | | [SI Mandarin] | 0,1 | | 75% | | | |
| | | [SI Reservas] | 0,1 | | 75% | | | |
| | | [SI Sistema de Notas] | 0,1 | | 75% | | | |
| | | [SE Portal WEB] | 0,1 | | 75% | | | |
| | | [SW SO] | 0,1 | | 75% | | | |
| | | [SW BD] | 0,1 | | 75% | | | |
| | | [SW Ant.] | 0,1 | | 75% | | | |
| | | [SW Ofi] | 0,1 | | 75% | | | |
| | | [SW moodle] | 0,1 | | 75% | | | |
| | | [SW nav] | 0,1 | | 75% | | | |
| | | [SW diseñ] | 0,1 | | 75% | | | |
| | | [SW nomina] | 0,1 | | 75% | | | |
| | | [SW contab] | 0,1 | | 75% | | | |
| | | [SW glpi] | 0,1 | | 75% | | | |
| | | [SW notas] | 0,1 | | 75% | | | |
| | | [SW plagio] | 0,1 | | 75% | | | |
| | | [SW bibliot] | 0,1 | | 75% | | | |
| | | [SW horarios] | 0,1 | | 75% | | | |
| | | [COM LAN] | 0,1 | | 75% | | | |
| | | [COM wifi] | 0,1 | | 75% | | | |
| | | [COM Internte] | 0,1 | | 75% | | | |
| | | [COM telefonía] | 0,1 | | 75% | | | |
| [E.15] | Alteración accidental de la información | [D respaldo] | 0,1 | | 75% | | | |
| | | [D de config.] | 0,1 | | 75% | | | |
| | | [D de Bit] | 0,1 | | 75% | | | |
| | | [SI Internet] | 0,1 | | 75% | | | |
| | | [SI Aula virtual] | 0,1 | | 75% | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | [SI Correo] | 0,1 | | 75% | | | |
| | | [SI Mesa de ayuda] | 0,1 | | 75% | | | |
| | | [SI Mandarin] | 0,1 | | 75% | | | |
| | | [SI Reservas] | 0,1 | | 75% | | | |
| | | [SI Sistema de Notas] | 0,1 | | 75% | | | |
| | | [SE Portal WEB] | 0,1 | | 75% | | | |
| | | [SW SO] | 0,1 | | 75% | | | |
| | | [SW BD] | 0,1 | | 75% | | | |
| | | [SW Ant.] | 0,1 | | 75% | | | |
| | | [SW Ofi] | 0,1 | | 75% | | | |
| | | [SW moodle] | 0,1 | | 75% | | | |
| | | [SW nav] | 0,1 | | 75% | | | |
| | | [SW diseñ] | 0,1 | | 75% | | | |
| | | [SW nomina] | 0,1 | | 75% | | | |
| | | [SW contab] | 0,1 | | 75% | | | |
| | | [SW glpi] | 0,1 | | 75% | | | |
| | | [SW notas] | 0,1 | | 75% | | | |
| | | [SW plagio] | 0,1 | | 75% | | | |
| | | [SW bibliot] | 0,1 | | 75% | | | |
| | | [SW horarios] | 0,1 | | 75% | | | |
| | | [COM LAN] | 0,1 | | 75% | | | |
| | | [COM wifi] | 0,1 | | 75% | | | |
| | | [COM Internte] | 0,1 | | 75% | | | |
| | | [COM telefonía] | 0,1 | | 75% | | | |
| | | [MEDIA DD] | 0,1 | | 75% | | | |
| | | [MEDIA usb] | 0,1 | | 75% | | | |
| | | [MEDIA electronic] | 0,1 | | 75% | | | |
| | | [SW notas] | 0,1 | | 75% | | | |
| | | [SW plagio] | 0,1 | | 75% | | | |
| | | [SW bibliot] | 0,1 | | 75% | | | |
| | | [SW horarios] | 0,1 | | 75% | | | |
| | | [COM LAN] | 0,1 | | 75% | | | |
| | | [COM wifi] | 0,1 | | 75% | | | |
| | | [COM Internte] | 0,1 | | 75% | | | |
| | | [COM telefonía] | 0,1 | | 75% | | | |
| | | [MEDIA DD] | 0,1 | | 75% | | | |
| | | [MEDIA usb] | 0,1 | | 75% | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | [MEDIA electronic] | 0,1 | | 75% | | | |
| [E.18] | Destrucción de información | [D respaldo] | 0,1 | 100% | | | | |
| | | [D de config.] | 0,1 | 100% | | | | |
| | | [D de Bit] | 0,1 | 100% | | | | |
| | | [SI Internet] | 0,1 | 100% | | | | |
| | | [SI Aula virtual] | 0,1 | 100% | | | | |
| | | [SI Correo] | 0,1 | 100% | | | | |
| | | [SI Mesa de ayuda] | 0,1 | 100% | | | | |
| | | [SI Mandarin] | 0,1 | 100% | | | | |
| | | [SI Reservas] | 0,1 | 100% | | | | |
| | | [SI Sistema de Notas] | 0,1 | 100% | | | | |
| | | [SE Portal WEB] | 0,1 | 100% | | | | |
| | | [SW SO] | 0,1 | 100% | | | | |
| | | [SW BD] | 0,1 | 100% | | | | |
| | | [SW Ant.] | 0,1 | 100% | | | | |
| | | [SW Ofi] | 0,1 | 100% | | | | |
| | | [SW moodle] | 0,1 | 100% | | | | |
| | | [SW nav] | 0,1 | 100% | | | | |
| | | [SW diseñ] | 0,1 | 100% | | | | |
| | | [SW nomina] | 0,1 | 100% | | | | |
| | | [SW contab] | 0,1 | 100% | | | | |
| | | [SW glpi] | 0,1 | 100% | | | | |
| | | [SW notas] | 0,1 | 100% | | | | |
| | | [SW plagio] | 0,1 | 100% | | | | |
| | | [SW bibliot] | 0,1 | 100% | | | | |
| | | [SW horarios] | 0,1 | 100% | | | | |
| | | [COM LAN] | 0,1 | 100% | | | | |
| | | [COM wifi] | 0,1 | 100% | | | | |
| | | [COM Internte] | 0,1 | 100% | | | | |
| | | [COM telefonía] | 0,1 | 100% | | | | |
| | | [MEDIA DD] | 0,1 | 100% | | | | |
| | | [MEDIA usb] | 0,1 | 100% | | | | |
| | | [MEDIA electronic] | 0,1 | 100% | | | | |
| | | [I Notas] | 0,1 | 100% | | | | |
| | | [I Estudiantes] | 0,1 | 100% | | | | |
| | | [I Padres de familia] | 0,1 | 100% | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | [I Mallas Curriculares] | 0,1 | 100% | | | | |
| | | [I Aspirantes] | 0,1 | 100% | | | | |
| | | [I Exalumnas] | 0,1 | 100% | | | | |
| | | [I estudiantes] | 0,1 | 100% | | | | |
| | | [I Padres de familia] | 0,1 | 100% | | | | |
| | | [I Colaboradores] | 0,1 | 100% | | | | |
| | | [I Profesores] | 0,1 | 100% | | | | |
| | | [I Exalumnas] | 0,1 | 100% | | | | |
| [E.19] | Fugas de información | [D respaldo] | 0,1 | | | 20% | | |
| | | [D de config.] | 0,1 | | | 20% | | |
| | | [D de Bit] | 0,1 | | | 20% | | |
| | | [SI Internet] | 0,1 | | | 20% | | |
| | | [SI Aula virtual] | 0,1 | | | 20% | | |
| | | [SI Correo] | 0,1 | | | 20% | | |
| | | [SI Mesa de ayuda] | 0,1 | | | 20% | | |
| | | [SI Mandarin] | 0,1 | | | 20% | | |
| | | [SI Reservas] | 0,1 | | | 20% | | |
| | | [SI Sistema de Notas] | 0,1 | | | 20% | | |
| | | [SE Portal WEB] | 0,1 | | | 20% | | |
| | | [SW SO] | 0,1 | | | 20% | | |
| | | [SW BD] | 0,1 | | | 20% | | |
| | | [SW Ant.] | 0,1 | | | 20% | | |
| | | [SW Ofi] | 0,1 | | | 20% | | |
| | | [SW moodle] | 0,1 | | | 20% | | |
| | | [SW nav] | 0,1 | | | 20% | | |
| | | [SW diseñ] | 0,1 | | | 20% | | |
| | | [SW nomina] | 0,1 | | | 50% | | |
| | | [SW contab] | 0,1 | | | 20% | | |
| | | [SW glpi] | 0,1 | | | 20% | | |
| | | [SW notas] | 0,1 | | | 50% | | |
| | | [SW plagio] | 0,1 | | | 20% | | |
| | | [SW bibliot] | 0,1 | | | 20% | | |
| | | [SW horarios] | 0,1 | | | 20% | | |
| | | [COM LAN] | 0,1 | | | 20% | | |
| | | [COM wifi] | 0,1 | | | 20% | | |
| | | [COM Internte] | 0,1 | | | 20% | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | [COM telefonía] | 0,1 | | | 20% | | |
| | | [MEDIA DD] | 0,1 | | | 20% | | |
| | | [MEDIA usb] | 0,1 | | | 20% | | |
| | | [MEDIA electronic] | 0,1 | | | 20% | | |
| | | [P ui] | 0,1 | | | 20% | | |
| | | [P ue] | 0,1 | | | 20% | | |
| | | [P soperte] | 0,1 | | | 20% | | |
| | | [P adm] | 0,1 | | | 20% | | |
| | | [P com] | 0,1 | | | 20% | | |
| | | [P sec] | 0,1 | | | 20% | | |
| | | [P dba] | 0,1 | | | 20% | | |
| | | [P rector] | 0,1 | | | 20% | | |
| | | [P Proc] | 0,1 | | | 20% | | |
| | | [P Calidad] | 0,1 | | | 20% | | |
| | | [P proveedores] | 0,1 | | | 20% | | |
| [E.20] | Vulnerabilidad de los programas | [SW SO] | 0,1 | 50% | 50% | 20% | | |
| | | [SW BD] | 0,1 | 50% | 50% | 20% | | |
| | | [SW Ant.] | 0,1 | 50% | 50% | 20% | | |
| | | [SW Ofi] | 0,1 | 50% | 50% | 20% | | |
| | | [SW moodle] | 0,1 | 50% | 50% | 20% | | |
| | | [SW nav] | 0,1 | 50% | 50% | 20% | | |
| | | [SW diseñ] | 0,1 | 50% | 50% | 20% | | |
| | | [SW nomina] | 0,1 | 50% | 50% | 20% | | |
| | | [SW contab] | 0,1 | 50% | 50% | 20% | | |
| | | [SW glpi] | 0,1 | 50% | 50% | 20% | | |
| | | [SW notas] | 0,1 | 50% | 50% | 20% | | |
| | | [SW plagio] | 0,1 | 50% | 50% | 20% | | |
| | | [SW bibliot] | 0,1 | 50% | 50% | 20% | | |
| | | [SW horarios] | 0,1 | 50% | 50% | 20% | | |
| [E.21] | Errores de mantenimiento/actualizado de programas | [SW SO] | 0,1 | 75% | 50% | | | |
| | | [SW BD] | 0,1 | 75% | 50% | | | |
| | | [SW Ant.] | 0,1 | 75% | 50% | | | |
| | | [SW Ofi] | 0,1 | 75% | 50% | | | |
| | | [SW moodle] | 0,1 | 75% | 50% | | | |
| | | [SW nav] | 0,1 | 75% | 50% | | | |
| | | [SW diseñ] | 0,1 | 75% | 50% | | | |
| | | [SW nomina] | 0,1 | 75% | 50% | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | [SW contab] | 0,1 | 75% | 50% | | | |
| | | [SW glpi] | 0,1 | 75% | 50% | | | |
| | | [SW notas] | 0,1 | 75% | 50% | | | |
| | | [SW plagio] | 0,1 | 75% | 50% | | | |
| | | [SW bibliot] | 0,1 | 75% | 50% | | | |
| | | [SW horarios] | 0,1 | 75% | 50% | | | |
| [E.23] | Errores de mantenimiento/actualización de equipos | [HW pc] | 0,1 | 75% | | | | |
| | | [HW portatil] | 0,1 | 75% | | | | |
| | | [HW multif] | 0,1 | 75% | | | | |
| | | [HW Serv] | 0,1 | 75% | | | | |
| | | [HW ap] | 0,1 | 75% | | | | |
| | | [HW switch] | 0,1 | 75% | | | | |
| | | [HW videob] | 0,1 | 75% | | | | |
| | | [HW pbx] | 0,1 | 75% | | | | |
| | | [HW Ipad] | 0,1 | 75% | | | | |
| | | [HW fotocop] | 0,1 | 75% | | | | |
| | | [HW tv] | 0,1 | 75% | | | | |
| | | [HW modem] | 0,1 | 75% | | | | |
| | | [MEDIA electronic] | 0,1 | 75% | | | | |
| | | [AUX ups] | 0,1 | 75% | | | | |
| | | [AUX cableado] | 0,1 | 75% | | | | |
| | | [AUX rack] | 0,1 | 75% | | | | |
| | | [AUX gabinte] | 0,1 | 75% | | | | |
| | | [AUX fibra] | 0,1 | 75% | | | | |
| [E.24] | Caida del sistema por agotamiento de recursos | [SI Internet] | 0,1 | 100% | | | | |
| | | [SI Aula virtual] | 0,1 | 100% | | | | |
| | | [SI Correo] | 0,1 | 100% | | | | |
| | | [SI Mesa de ayuda] | 0,1 | 100% | | | | |
| | | [SI Mandarin] | 0,1 | 100% | | | | |
| | | [SI Reservas] | 0,1 | 100% | | | | |
| | | [SI Sistema de Notas] | 0,1 | 100% | | | | |
| | | [SE Portal WEB] | 0,1 | 100% | | | | |
| | | [HW pc] | 0,1 | 75% | | | | |
| | | [HW portatil] | 0,1 | 75% | | | | |
| | | [HW multif] | 0,1 | 75% | | | | |
| | | [HW Serv] | 0,1 | 75% | | | | |
| | | [HW ap] | 0,1 | 75% | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | [HW switch] | 0,1 | 75% | | | | |
| | | [HW videob] | 0,1 | 75% | | | | |
| | | [HW pbx] | 0,1 | 75% | | | | |
| | | [HW Ipad] | 0,1 | 75% | | | | |
| | | [HW fotocop] | 0,1 | 75% | | | | |
| | | [HW tv] | 0,1 | 75% | | | | |
| | | [HW modem] | 0,1 | 75% | | | | |
| | | [COM LAN] | 0,1 | 100% | | | | |
| | | [COM wifi] | 0,1 | 100% | | | | |
| | | [COM Internte] | 0,1 | 100% | | | | |
| | | [COM telefonía] | 0,1 | 100% | | | | |
| [E.25] | Pérdida de equipos | [HW pc] | 0,1 | 100% | | 75% | | |
| | | [HW portatil] | 0,1 | 100% | | 75% | | |
| | | [HW multif] | 0,1 | 100% | | 75% | | |
| | | [HW Serv] | 0,1 | 100% | | 75% | | |
| | | [HW ap] | 0,1 | 100% | | 75% | | |
| | | [HW switch] | 0,1 | 100% | | 75% | | |
| | | [HW videob] | 0,1 | 100% | | 75% | | |
| | | [HW pbx] | 0,1 | 100% | | 75% | | |
| | | [HW Ipad] | 0,1 | 100% | | 75% | | |
| | | [HW fotocop] | 0,1 | 100% | | 75% | | |
| | | [HW tv] | 0,1 | 100% | | 75% | | |
| | | [HW modem] | 0,1 | 100% | | 75% | | |
| | | [MEDIA DD] | 0,1 | 100% | | 75% | | |
| | | [MEDIA usb] | 0,1 | 100% | | 75% | | |
| | | [MEDIA electronic] | 0,1 | 100% | | 75% | | |
| | | [AUX ups] | 0,1 | 100% | | 75% | | |
| | | [AUX cableado] | 0,1 | 100% | | 75% | | |
| | | [AUX rack] | 0,1 | 100% | | 75% | | |
| | | [AUX gabinte] | 0,1 | 100% | | 75% | | |
| | | [AUX fibra] | 0,1 | 100% | | 75% | | |
| **[A] Ataques intencionados** | | | | | | | | |
| **Cod.** | **Amenaza** | **Activos** | | **D** | **I** | **C** | **A** | **T** |
| [A.5] | Suplantación de la identidad del usuario | [D respaldo] | 0,1 | | | 75% | 75% | 50% |
| | | [D de config.] | 0,1 | | | 75% | 75% | 50% |
| | | [D de Bit] | 0,1 | | | 75% | 75% | 50% |
| | | [SI Internet] | 0,1 | | | 75% | 75% | 50% |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | [SI Aula virtual] | 0,1 | | | 75% | 75% | 50% |
| | | [SI Correo] | 0,1 | | | 75% | 75% | 50% |
| | | [SI Mesa de ayuda] | 0,1 | | | 75% | 75% | 50% |
| | | [SI Mandarin] | 0,1 | | | 75% | 75% | 50% |
| | | [SI Reservas] | 0,1 | | | 75% | 75% | 50% |
| | | [SI Sistema de Notas] | 0,1 | | | 75% | 75% | 50% |
| | | [SE Portal WEB] | 0,1 | | | 75% | 75% | 50% |
| | | [SW SO] | 0,1 | | | 75% | 75% | 50% |
| | | [SW BD] | 0,1 | | | 75% | 75% | 50% |
| | | [SW Ant.] | 0,1 | | | 75% | 75% | 50% |
| | | [SW Ofi] | 0,1 | | | 75% | 75% | 50% |
| | | [SW moodle] | 0,1 | | | 75% | 75% | 50% |
| | | [SW nav] | 0,1 | | | 75% | 75% | 50% |
| | | [SW diseñ] | 0,1 | | | 75% | 75% | 50% |
| | | [SW nomina] | 0,1 | | | 75% | 75% | 50% |
| | | [SW contab] | 0,1 | | | 75% | 75% | 50% |
| | | [SW glpi] | 0,1 | | | 75% | 75% | 50% |
| | | [SW notas] | 0,1 | | | 75% | 75% | 50% |
| | | [SW plagio] | 0,1 | | | 75% | 75% | 50% |
| | | [SW bibliot] | 0,1 | | | 75% | 75% | 50% |
| | | [SW horarios] | 0,1 | | | 75% | 75% | 50% |
| | | [COM LAN] | 0,1 | | | 75% | 75% | 50% |
| | | [COM wifi] | 0,1 | | | 75% | 75% | 50% |
| | | [COM Internte] | 0,1 | | | 75% | 75% | 50% |
| | | [COM telefonía] | 0,1 | | | 75% | 75% | 50% |
| | | [I Notas] | 0,1 | | | 75% | 75% | 50% |
| | | [I Estudiantes] | 0,1 | | | 75% | 75% | 50% |
| | | [I Padres de familia] | 0,1 | | | 75% | 75% | 50% |
| | | [I Mallas Curriculares] | 0,1 | | | 75% | 75% | 50% |
| | | [I Aspirantes] | 0,1 | | | 75% | 75% | 50% |
| | | [I Exalumnas] | 0,1 | | | 75% | 75% | 50% |
| | | [I estudiantes] | 0,1 | | | 75% | 75% | 50% |
| | | [I Padres de familia] | 0,1 | | | 75% | 75% | 50% |
| | | [I Colaboradores] | 0,1 | | | 75% | 75% | 50% |
| | | [I Profesores] | 0,1 | | | 75% | 75% | 50% |
| | | [I Exalumnas] | 0,1 | | | 75% | 75% | 50% |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [A.6] | Abuso de privilegios de acceso | [D respaldo] | 0,1 | 75% | 75% | 50% | | |
| | | [D de config.] | 0,1 | 75% | 75% | 50% | | |
| | | [D de Bit] | 0,1 | 75% | 75% | 50% | | |
| | | [SI Internet] | 0,1 | 75% | 75% | 50% | | |
| | | [SI Aula virtual] | 0,1 | 75% | 75% | 50% | | |
| | | [SI Correo] | 0,1 | 75% | 75% | 50% | | |
| | | [SI Mesa de ayuda] | 0,1 | 75% | 75% | 50% | | |
| | | [SI Mandarin] | 0,1 | 75% | 75% | 50% | | |
| | | [SI Reservas] | 0,1 | 75% | 75% | 50% | | |
| | | [SI Sistema de Notas] | 0,1 | 75% | 75% | 50% | | |
| | | [SE Portal WEB] | 0,1 | 75% | 75% | 50% | | |
| | | [SW SO] | 0,1 | 75% | 75% | 50% | | |
| | | [SW BD] | 0,1 | 75% | 75% | 50% | | |
| | | [SW Ant.] | 0,1 | 75% | 75% | 50% | | |
| | | [SW Ofi] | 0,1 | 75% | 75% | 50% | | |
| | | [SW moodle] | 0,1 | 75% | 75% | 50% | | |
| | | [SW nav] | 0,1 | 75% | 75% | 50% | | |
| | | [SW diseñ] | 0,1 | 75% | 75% | 50% | | |
| | | [SW nomina] | 0,1 | 75% | 75% | 50% | | |
| | | [SW contab] | 0,1 | 75% | 75% | 50% | | |
| | | [SW glpi] | 0,1 | 75% | 75% | 50% | | |
| | | [SW notas] | 0,1 | 75% | 75% | 50% | | |
| | | [SW plagio] | 0,1 | 75% | 75% | 50% | | |
| | | [SW bibliot] | 0,1 | 75% | 75% | 50% | | |
| | | [SW horarios] | 0,1 | 75% | 75% | 50% | | |
| | | [HW pc] | 0,1 | 75% | 75% | 50% | | |
| | | [HW portatil] | 0,1 | 75% | 75% | 50% | | |
| | | [HW multif] | 0,1 | 75% | 75% | 50% | | |
| | | [HW Serv] | 0,1 | 75% | 75% | 50% | | |
| | | [HW ap] | 0,1 | 75% | 75% | 50% | | |
| | | [HW switch] | 0,1 | 75% | 75% | 50% | | |
| | | [HW videob] | 0,1 | 75% | 75% | 50% | | |
| | | [HW pbx] | 0,1 | 75% | 75% | 50% | | |
| | | [HW Ipad] | 0,1 | 75% | 75% | 50% | | |
| | | [HW fotocop] | 0,1 | 75% | 75% | 50% | | |
| | | [HW tv] | 0,1 | 75% | 75% | 50% | | |
| | | [HW modem] | 0,1 | 75% | 75% | 50% | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | [COM LAN] | 0,1 | 75% | 75% | 50% | | |
| | | [COM wifi] | 0,1 | 75% | 75% | 50% | | |
| | | [COM Internte] | 0,1 | 75% | 75% | 50% | | |
| | | [COM telefonía] | 0,1 | 75% | 75% | 50% | | |
| [A.7] | Uso no previsto | [SI Internet] | 0,1 | 20% | 20% | 10% | | |
| | | [SI Aula virtual] | 0,1 | 5% | 5% | 5% | | |
| | | [SI Correo] | 0,1 | 5% | 5% | 5% | | |
| | | [SI Mesa de ayuda] | 0,1 | 5% | 5% | 5% | | |
| | | [SI Mandarin] | 0,1 | 5% | 5% | 5% | | |
| | | [SI Reservas] | 0,1 | 5% | 5% | 5% | | |
| | | [SI Sistema de Notas] | 0,1 | 5% | 5% | 5% | | |
| | | [SE Portal WEB] | 0,1 | 5% | 5% | 5% | | |
| | | [SW SO] | 0,1 | 5% | 5% | 5% | | |
| | | [SW BD] | 0,1 | 5% | 5% | 5% | | |
| | | [SW Ant.] | 0,1 | 5% | 5% | 5% | | |
| | | [SW Ofi] | 0,1 | 5% | 5% | 5% | | |
| | | [SW moodle] | 0,1 | 5% | 5% | 5% | | |
| | | [SW nav] | 0,1 | 5% | 5% | 5% | | |
| | | [SW diseñ] | 0,1 | 5% | 5% | 5% | | |
| | | [SW nomina] | 0,1 | 5% | 5% | 5% | | |
| | | [SW contab] | 0,1 | 5% | 5% | 5% | | |
| | | [SW glpi] | 0,1 | 5% | 5% | 5% | | |
| | | [SW notas] | 0,1 | 5% | 5% | 5% | | |
| | | [SW plagio] | 0,1 | 5% | 5% | 5% | | |
| | | [SW bibliot] | 0,1 | 5% | 5% | 5% | | |
| | | [SW horarios] | 0,1 | 5% | 5% | 5% | | |
| | | [HW pc] | 0,1 | 20% | 20% | 20% | | |
| | | [HW portatil] | 0,1 | 20% | 20% | 20% | | |
| | | [HW multif] | 0,1 | 20% | 20% | 20% | | |
| | | [HW Serv] | 0,1 | 20% | 20% | 20% | | |
| | | [HW ap] | 0,1 | 20% | 20% | 20% | | |
| | | [HW switch] | 0,1 | 20% | 20% | 20% | | |
| | | [HW videob] | 0,1 | 20% | 20% | 20% | | |
| | | [HW pbx] | 0,1 | 20% | 20% | 20% | | |
| | | [HW Ipad] | 0,1 | 20% | 20% | 20% | | |
| | | [HW fotocop] | 0,1 | 20% | 20% | 20% | | |
| | | [HW tv] | 0,1 | 20% | 5% | 5% | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | [HW modem] | 0,1 | 20% | 20% | 20% | | |
| | | [COM LAN] | 0,1 | 20% | 5% | 5% | | |
| | | [COM wifi] | 0,1 | 20% | 5% | 5% | | |
| | | [COM Internte] | 0,1 | 20% | 5% | 5% | | |
| | | [COM telefonía] | 0,1 | 20% | 5% | 5% | | |
| | | [MEDIA DD] | 0,1 | 20% | 5% | 5% | | |
| | | [MEDIA usb] | 0,1 | 20% | 5% | 5% | | |
| | | [MEDIA electronic] | 0,1 | 20% | 5% | 5% | | |
| | | [AUX ups] | 0,1 | 20% | 20% | 20% | | |
| | | [AUX cableado] | 0,1 | 20% | 20% | 20% | | |
| | | [AUX rack] | 0,1 | 20% | 20% | 20% | | |
| | | [AUX gabinte] | 0,1 | 20% | 20% | 20% | | |
| | | [AUX fibra] | 0,1 | 20% | 20% | 20% | | |
| | | [L administrativa] | 0,1 | 20% | 20% | 20% | | |
| | | [L escuelas] | 0,1 | 20% | 20% | 20% | | |
| [A.8] | Difusión de software dañino | [SW SO] | 0,1 | 75% | 75% | 75% | | |
| | | [SW BD] | 0,1 | 75% | 75% | 75% | | |
| | | [SW Ant.] | 0,1 | 75% | 75% | 75% | | |
| | | [SW Ofi] | 0,1 | 75% | 75% | 75% | | |
| | | [SW moodle] | 0,1 | 75% | 75% | 75% | | |
| | | [SW nav] | 0,1 | 75% | 75% | 75% | | |
| | | [SW diseñ] | 0,1 | 75% | 75% | 75% | | |
| | | [SW nomina] | 0,1 | 75% | 75% | 75% | | |
| | | [SW contab] | 0,1 | 75% | 75% | 75% | | |
| | | [SW glpi] | 0,1 | 75% | 75% | 75% | | |
| | | [SW notas] | 0,1 | 75% | 75% | 75% | | |
| | | [SW plagio] | 0,1 | 75% | 75% | 75% | | |
| | | [SW bibliot] | 0,1 | 75% | 75% | 75% | | |
| | | [SW horarios] | 0,1 | 75% | 75% | 75% | | |
| [A.9] | Errores de [re-]encaminamiento | [SI Internet] | 0,1 | | | 75% | | |
| | | [SI Aula virtual] | 0,1 | | | 75% | | |
| | | [SI Correo] | 0,1 | | | 75% | | |
| | | [SI Mesa de ayuda] | 0,1 | | | 75% | | |
| | | [SI Mandarin] | 0,1 | | | 75% | | |
| | | [SI Reservas] | 0,1 | | | 75% | | |
| | | [SI Sistema de Notas] | 0,1 | | | 75% | | |
| | | [SE Portal WEB] | 0,1 | | | 75% | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | [SW SO] | 0,1 | | | 75% | | |
| | | [SW BD] | 0,1 | | | 75% | | |
| | | [SW Ant.] | 0,1 | | | 75% | | |
| | | [SW Ofi] | 0,1 | | | 75% | | |
| | | [SW moodle] | 0,1 | | | 75% | | |
| | | [SW nav] | 0,1 | | | 75% | | |
| | | [SW diseñ] | 0,1 | | | 75% | | |
| | | [SW nomina] | 0,1 | | | 75% | | |
| | | [SW contab] | 0,1 | | | 75% | | |
| | | [SW glpi] | 0,1 | | | 75% | | |
| | | [SW notas] | 0,1 | | | 75% | | |
| | | [SW plagio] | 0,1 | | | 75% | | |
| | | [SW bibliot] | 0,1 | | | 75% | | |
| | | [SW horarios] | 0,1 | | | 75% | | |
| | | [COM LAN] | 0,1 | | | 75% | | |
| | | [COM wifi] | 0,1 | | | 75% | | |
| | | [COM Internte] | 0,1 | | | 75% | | |
| | | [COM telefonía] | 0,1 | | | 75% | | |
| [A.10] | Alteración de secuencia | [SI Internet] | 0,1 | | 75% | | | |
| | | [SI Aula virtual] | 0,1 | | 75% | | | |
| | | [SI Correo] | 0,1 | | 75% | | | |
| | | [SI Mesa de ayuda] | 0,1 | | 75% | | | |
| | | [SI Mandarin] | 0,1 | | 75% | | | |
| | | [SI Reservas] | 0,1 | | 75% | | | |
| | | [SI Sistema de Notas] | 0,1 | | 75% | | | |
| | | [SE Portal WEB] | 0,1 | | 75% | | | |
| | | [SW SO] | 0,1 | | 75% | | | |
| | | [SW BD] | 0,1 | | 75% | | | |
| | | [SW Ant.] | 0,1 | | 75% | | | |
| | | [SW Ofi] | 0,1 | | 75% | | | |
| | | [SW moodle] | 0,1 | | 75% | | | |
| | | [SW nav] | 0,1 | | 75% | | | |
| | | [SW diseñ] | 0,1 | | 75% | | | |
| | | [SW nomina] | 0,1 | | 75% | | | |
| | | [SW contab] | 0,1 | | 75% | | | |
| | | [SW glpi] | 0,1 | | 75% | | | |
| | | [SW notas] | 0,1 | | 75% | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | [SW plagio] | 0,1 | | 75% | | | |
| | | [SW bibliot] | 0,1 | | 75% | | | |
| | | [SW horarios] | 0,1 | | 75% | | | |
| | | [COM LAN] | 0,1 | | 75% | | | |
| | | [COM wifi] | 0,1 | | 75% | | | |
| | | [COM Internte] | 0,1 | | 75% | | | |
| | | [COM telefonía] | 0,1 | | 75% | | | |
| [A.11] | Acceso no autorizado | [D respaldo] | 0,1 | | 75% | 75% | | |
| | | [D de config.] | 0,1 | | 75% | 75% | | |
| | | [D de Bit] | 0,1 | | 75% | 75% | | |
| | | [SI Internet] | 0,1 | | 75% | 75% | | |
| | | [SI Aula virtual] | 0,1 | | 75% | 75% | | |
| | | [SI Correo] | 0,1 | | 75% | 75% | | |
| | | [SI Mesa de ayuda] | 0,1 | | 75% | 75% | | |
| | | [SI Mandarin] | 0,1 | | 75% | 75% | | |
| | | [SI Reservas] | 0,1 | | 75% | 75% | | |
| | | [SI Sistema de Notas] | 0,1 | | 75% | 75% | | |
| | | [SE Portal WEB] | 0,1 | | 75% | 75% | | |
| | | [SW SO] | 0,1 | | 75% | 75% | | |
| | | [SW BD] | 0,1 | | 75% | 75% | | |
| | | [SW Ant.] | 0,1 | | 75% | 75% | | |
| | | [SW Ofi] | 0,1 | | 75% | 75% | | |
| | | [SW moodle] | 0,1 | | 75% | 75% | | |
| | | [SW nav] | 0,1 | | 75% | 75% | | |
| | | [SW diseñ] | 0,1 | | 75% | 75% | | |
| | | [SW nomina] | 0,1 | | 75% | 75% | | |
| | | [SW contab] | 0,1 | | 75% | 75% | | |
| | | [SW glpi] | 0,1 | | 75% | 75% | | |
| | | [SW notas] | 0,1 | | 75% | 75% | | |
| | | [SW plagio] | 0,1 | | 75% | 75% | | |
| | | [SW bibliot] | 0,1 | | 75% | 75% | | |
| | | [SW horarios] | 0,1 | | 75% | 75% | | |
| | | [HW pc] | 0,1 | | 75% | 100% | | |
| | | [HW portatil] | 0,1 | | 75% | 100% | | |
| | | [HW multif] | 0,1 | | 75% | 75% | | |
| | | [HW Serv] | 0,1 | | 75% | 75% | | |
| | | [HW ap] | 0,1 | | 75% | 75% | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | [HW switch] | 0,1 | | 75% | 75% | | |
| | | [HW videob] | 0,1 | | 75% | 75% | | |
| | | [HW pbx] | 0,1 | | 75% | 75% | | |
| | | [HW Ipad] | 0,1 | | 75% | 75% | | |
| | | [HW fotocop] | 0,1 | | 75% | 75% | | |
| | | [HW tv] | 0,1 | | 75% | 75% | | |
| | | [HW modem] | 0,1 | | 75% | 75% | | |
| | | [COM LAN] | 0,1 | | 75% | 75% | | |
| | | [COM wifi] | 0,1 | | 75% | 75% | | |
| | | [COM Internte] | 0,1 | | 75% | 75% | | |
| | | [COM telefonía] | 0,1 | | 75% | 75% | | |
| | | [MEDIA DD] | 0,1 | | 75% | 100% | | |
| | | [MEDIA usb] | 0,1 | | 75% | 100% | | |
| | | [MEDIA electronic] | 0,1 | | 75% | 100% | | |
| | | [AUX ups] | 0,1 | | 75% | 75% | | |
| | | [AUX cableado] | 0,1 | | 75% | 75% | | |
| | | [AUX rack] | 0,1 | | 75% | 75% | | |
| | | [AUX gabinte] | 0,1 | | 75% | 75% | | |
| | | [AUX fibra] | 0,1 | | 75% | 75% | | |
| | | [L administrativa] | 0,1 | | 75% | 75% | | |
| | | [L escuelas] | 0,1 | | 75% | 75% | | |
| [A.12] | Análisis de tráfico | [COM LAN] | 0,1 | | | 100% | | |
| | | [COM wifi] | 0,1 | | | 100% | | |
| | | [COM Internte] | 0,1 | | | 100% | | |
| | | [COM telefonía] | 0,1 | | | 100% | | |
| [A.13] | Repudio | [SI Internet] | 0,1 | | 50% | | | 100% |
| | | [SI Aula virtual] | 0,1 | | 50% | | | 100% |
| | | [SI Correo] | 0,1 | | 50% | | | 100% |
| | | [SI Mesa de ayuda] | 0,1 | | 50% | | | 100% |
| | | [SI Mandarin] | 0,1 | | 50% | | | 100% |
| | | [SI Reservas] | 0,1 | | 50% | | | 100% |
| | | [SI Sistema de Notas] | 0,1 | | 50% | | | 100% |
| | | [SE Portal WEB] | 0,1 | | 50% | | | 100% |
| [A.14] | Interceptación de información | [COM LAN] | 0,1 | | | 100% | | |
| | | [COM wifi] | 0,1 | | | 100% | | |
| | | [COM Internte] | 0,1 | | | 100% | | |
| | | [COM telefonía] | 0,1 | | | 100% | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [A.15] | Modificación deliberada de la información | [D respaldo] | 0,1 | | 100% | | | |
| | | [D de config.] | 0,1 | | 100% | | | |
| | | [D de Bit] | 0,1 | | 100% | | | |
| | | [SI Internet] | 0,1 | | 100% | | | |
| | | [SI Aula virtual] | 0,1 | | 100% | | | |
| | | [SI Correo] | 0,1 | | 100% | | | |
| | | [SI Mesa de ayuda] | 0,1 | | 100% | | | |
| | | [SI Mandarin] | 0,1 | | 100% | | | |
| | | [SI Reservas] | 0,1 | | 100% | | | |
| | | [SI Sistema de Notas] | 0,1 | | 100% | | | |
| | | [SE Portal WEB] | 0,1 | | 100% | | | |
| | | [SW SO] | 0,1 | | 100% | | | |
| | | [SW BD] | 0,1 | | 100% | | | |
| | | [SW Ant.] | 0,1 | | 100% | | | |
| | | [SW Ofi] | 0,1 | | 100% | | | |
| | | [SW moodle] | 0,1 | | 100% | | | |
| | | [SW nav] | 0,1 | | 100% | | | |
| | | [SW diseñ] | 0,1 | | 100% | | | |
| | | [SW nomina] | 0,1 | | 100% | | | |
| | | [SW contab] | 0,1 | | 100% | | | |
| | | [SW glpi] | 0,1 | | 100% | | | |
| | | [SW notas] | 0,1 | | 100% | | | |
| | | [SW plagio] | 0,1 | | 100% | | | |
| | | [SW bibliot] | 0,1 | | 100% | | | |
| | | [SW horarios] | 0,1 | | 100% | | | |
| | | [COM LAN] | 0,1 | | 100% | | | |
| | | [COM wifi] | 0,1 | | 100% | | | |
| | | [COM Internte] | 0,1 | | 100% | | | |
| | | [COM telefonía] | 0,1 | | 100% | | | |
| | | [MEDIA DD] | 0,1 | | 100% | | | |
| | | [MEDIA usb] | 0,1 | | 100% | | | |
| | | [MEDIA electronic] | 0,1 | | 100% | | | |
| | | [L administrativa] | 0,1 | | 50% | | | |
| | | [L escuelas] | 0,1 | | 50% | | | |
| [A.18] | Destrucción de información | [D respaldo] | 0,1 | 100% | | | | |
| | | [D de config.] | 0,1 | 100% | | | | |
| | | [D de Bit] | 0,1 | 100% | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | [SI Internet] | 0,1 | 100% | | | | |
| | | [SI Aula virtual] | 0,1 | 100% | | | | |
| | | [SI Correo] | 0,1 | 100% | | | | |
| | | [SI Mesa de ayuda] | 0,1 | 100% | | | | |
| | | [SI Mandarin] | 0,1 | 100% | | | | |
| | | [SI Reservas] | 0,1 | 100% | | | | |
| | | [SI Sistema de Notas] | 0,1 | 100% | | | | |
| | | [SE Portal WEB] | 0,1 | 100% | | | | |
| | | [SW SO] | 0,1 | 100% | | | | |
| | | [SW BD] | 0,1 | 100% | | | | |
| | | [SW Ant.] | 0,1 | 100% | | | | |
| | | [SW Ofi] | 0,1 | 100% | | | | |
| | | [SW moodle] | 0,1 | 100% | | | | |
| | | [SW nav] | 0,1 | 100% | | | | |
| | | [SW diseñ] | 0,1 | 100% | | | | |
| | | [SW nomina] | 0,1 | 100% | | | | |
| | | [SW contab] | 0,1 | 100% | | | | |
| | | [SW glpi] | 0,1 | 100% | | | | |
| | | [SW notas] | 0,1 | 100% | | | | |
| | | [SW plagio] | 0,1 | 100% | | | | |
| | | [SW bibliot] | 0,1 | 100% | | | | |
| | | [SW horarios] | 0,1 | 100% | | | | |
| | | [MEDIA DD] | 0,1 | 100% | | | | |
| | | [MEDIA usb] | 0,1 | 100% | | | | |
| | | [MEDIA electronic] | 0,1 | 100% | | | | |
| | | [L administrativa] | 0,1 | 100% | | | | |
| | | [L escuelas] | 0,1 | 100% | | | | |
| [A.19] | Divulgación de información | [D respaldo] | 0,1 | | | 100% | | |
| | | [D de config.] | 0,1 | | | 100% | | |
| | | [D de Bit] | 0,1 | | | 100% | | |
| | | [SI Internet] | 0,1 | | | 100% | | |
| | | [SI Aula virtual] | 0,1 | | | 100% | | |
| | | [SI Correo] | 0,1 | | | 100% | | |
| | | [SI Mesa de ayuda] | 0,1 | | | 100% | | |
| | | [SI Mandarin] | 0,1 | | | 100% | | |
| | | [SI Reservas] | 0,1 | | | 100% | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | [SI Sistema de Notas] | 0,1 | | | 100% | | |
| | | [SE Portal WEB] | 0,1 | | | 100% | | |
| | | [SW SO] | 0,1 | | | 100% | | |
| | | [SW BD] | 0,1 | | | 100% | | |
| | | [SW Ant.] | 0,1 | | | 100% | | |
| | | [SW Ofi] | 0,1 | | | 100% | | |
| | | [SW moodle] | 0,1 | | | 100% | | |
| | | [SW nav] | 0,1 | | | 100% | | |
| | | [SW diseñ] | 0,1 | | | 100% | | |
| | | [SW nomina] | 0,1 | | | 100% | | |
| | | [SW contab] | 0,1 | | | 100% | | |
| | | [SW glpi] | 0,1 | | | 100% | | |
| | | [SW notas] | 0,1 | | | 100% | | |
| | | [SW plagio] | 0,1 | | | 100% | | |
| | | [SW bibliot] | 0,1 | | | 100% | | |
| | | [SW horarios] | 0,1 | | | 100% | | |
| | | [COM LAN] | 0,1 | | | 100% | | |
| | | [COM wifi] | 0,1 | | | 100% | | |
| | | [COM Internte] | 0,1 | | | 100% | | |
| | | [COM telefonía] | 0,1 | | | 100% | | |
| | | [MEDIA DD] | 0,1 | | | 100% | | |
| | | [MEDIA usb] | 0,1 | | | 100% | | |
| | | [MEDIA electronic] | 0,1 | | | 100% | | |
| | | [L administrativa] | 0,1 | | | 100% | | |
| | | [L escuelas] | 0,1 | | | 100% | | |
| [A.22] | Manipulación de programas | [SW SO] | 0,1 | 100% | 100% | 100% | | |
| | | [SW BD] | 0,1 | 100% | 100% | 100% | | |
| | | [SW Ant.] | 0,1 | 100% | 100% | 100% | | |
| | | [SW Ofi] | 0,1 | 100% | 100% | 100% | | |
| | | [SW moodle] | 0,1 | 100% | 100% | 100% | | |
| | | [SW nav] | 0,1 | 100% | 100% | 100% | | |
| | | [SW diseñ] | 0,1 | 100% | 100% | 100% | | |
| | | [SW nomina] | 0,1 | 100% | 100% | 100% | | |
| | | [SW contab] | 0,1 | 100% | 100% | 100% | | |
| | | [SW glpi] | 0,1 | 100% | 100% | 100% | | |
| | | [SW notas] | 0,1 | 100% | 100% | 100% | | |
| | | [SW plagio] | 0,1 | 100% | 100% | 100% | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | [SW bibliot] | 0,1 | 100% | 100% | 100% | | |
| | | [SW horarios] | 0,1 | 100% | 100% | 100% | | |
| [A.23] | Manipulación de los equipos | [HW pc] | 0,1 | 100% | | 100% | | |
| | | [HW portatil] | 0,1 | 100% | | 100% | | |
| | | [HW multif] | 0,1 | 100% | | 100% | | |
| | | [HW Serv] | 0,1 | 100% | | 100% | | |
| | | [HW ap] | 0,1 | 100% | | 100% | | |
| | | [HW switch] | 0,1 | 100% | | 100% | | |
| | | [HW videob] | 0,1 | 100% | | 100% | | |
| | | [HW pbx] | 0,1 | 100% | | 100% | | |
| | | [HW Ipad] | 0,1 | 100% | | 100% | | |
| | | [HW fotocop] | 0,1 | 100% | | 100% | | |
| | | [HW tv] | 0,1 | 100% | | 100% | | |
| | | [HW modem] | 0,1 | 100% | | 100% | | |
| | | [MEDIA DD] | 0,1 | 100% | | 100% | | |
| | | [MEDIA usb] | 0,1 | 100% | | 100% | | |
| | | [MEDIA electronic] | 0,1 | 100% | | 100% | | |
| | | [AUX ups] | 0,1 | 100% | | 100% | | |
| | | [AUX cableado] | 0,1 | 100% | | 100% | | |
| | | [AUX rack] | 0,1 | 100% | | 100% | | |
| | | [AUX gabinte] | 0,1 | 100% | | 100% | | |
| | | [AUX fibra] | 0,1 | 100% | | 100% | | |
| [A.24] | Denegación de servicio | [SI Internet] | 0,1 | 100% | | | | |
| | | [SI Aula virtual] | 0,1 | 100% | | | | |
| | | [SI Correo] | 0,1 | 100% | | | | |
| | | [SI Mesa de ayuda] | 0,1 | 100% | | | | |
| | | [SI Mandarin] | 0,1 | 100% | | | | |
| | | [SI Reservas] | 0,1 | 100% | | | | |
| | | [SI Sistema de Notas] | 0,1 | 100% | | | | |
| | | [HW pc] | 0,1 | 100% | | | | |
| | | [HW portatil] | 0,1 | 100% | | | | |
| | | [HW multif] | 0,1 | 100% | | | | |
| | | [HW Serv] | 0,1 | 100% | | | | |
| | | [HW ap] | 0,1 | 100% | | | | |
| | | [HW switch] | 0,1 | 100% | | | | |
| | | [HW videob] | 0,1 | 100% | | | | |
| | | [HW pbx] | 0,1 | 100% | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | [HW Ipad] | 0,1 | 100% | | | | |
| | | [HW fotocop] | 0,1 | 100% | | | | |
| | | [HW tv] | 0,1 | 100% | | | | |
| | | [HW modem] | 0,1 | 100% | | | | |
| | | [COM LAN] | 0,1 | 100% | | | | |
| | | [COM wifi] | 0,1 | 100% | | | | |
| | | [COM Internte] | 0,1 | 100% | | | | |
| | | [COM telefonía] | 0,1 | 100% | | | | |
| [A.25] | Robo | [HW pc] | 0,1 | 100% | | 50% | | |
| | | [HW portatil] | 0,1 | 100% | | 50% | | |
| | | [HW multif] | 0,1 | 100% | | 5% | | |
| | | [HW Serv] | 0,1 | 100% | | 50% | | |
| | | [HW ap] | 0,1 | 100% | | 50% | | |
| | | [HW switch] | 0,1 | 100% | | 50% | | |
| | | [HW videob] | 0,1 | 100% | | 5% | | |
| | | [HW pbx] | 0,1 | 100% | | 50% | | |
| | | [HW Ipad] | 0,1 | 100% | | 50% | | |
| | | [HW fotocop] | 0,1 | 100% | | 50% | | |
| | | [HW tv] | 0,1 | 100% | | 5% | | |
| | | [HW modem] | 0,1 | 100% | | 50% | | |
| | | [MEDIA DD] | 0,1 | 100% | | 50% | | |
| | | [MEDIA usb] | 0,1 | 100% | | 50% | | |
| | | [MEDIA electronic] | 0,1 | 100% | | 50% | | |
| | | [AUX ups] | 0,1 | 100% | | 5% | | |
| | | [AUX cableado] | 0,1 | 100% | | 5% | | |
| | | [AUX rack] | 0,1 | 100% | | 5% | | |
| | | [AUX gabinte] | 0,1 | 100% | | 5% | | |
| | | [AUX fibra] | 0,1 | 100% | | 5% | | |
| [A.26] | Ataque destructivo | [HW pc] | 0,01 | 100% | | | | |
| | | [HW portatil] | 0,01 | 100% | | | | |
| | | [HW multif] | 0,01 | 100% | | | | |
| | | [HW Serv] | 0,01 | 100% | | | | |
| | | [HW ap] | 0,01 | 100% | | | | |
| | | [HW switch] | 0,01 | 100% | | | | |
| | | [HW videob] | 0,01 | 100% | | | | |
| | | [HW pbx] | 0,01 | 100% | | | | |
| | | [HW Ipad] | 0,01 | 100% | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | [HW fotocop] | 0,01 | 100% | | | | |
| | | [HW tv] | 0,01 | 100% | | | | |
| | | [HW modem] | 0,01 | 100% | | | | |
| | | [MEDIA DD] | 0,01 | 100% | | | | |
| | | [MEDIA usb] | 0,01 | 100% | | | | |
| | | [MEDIA electronic] | 0,01 | 100% | | | | |
| | | [AUX ups] | 0,01 | 100% | | | | |
| | | [AUX cableado] | 0,01 | 100% | | | | |
| | | [AUX rack] | 0,01 | 100% | | | | |
| | | [AUX gabinte] | 0,01 | 100% | | | | |
| | | [AUX fibra] | 0,01 | 100% | | | | |
| | | [L administrativa] | 0,01 | 100% | | | | |
| | | [L escuelas] | 0,01 | 100% | | | | |
| [A.27] | Ocupación enemiga | [L administrativa] | 0,01 | 100% | | 100% | | |
| | | [L escuelas] | 0,01 | 100% | | 100% | | |
| [A.28] | Indisponibilidad del personal | [P ui] | 0,1 | 20% | | | | |
| | | [P soperte] | 0,1 | 20% | | | | |
| | | [P adm] | 0,1 | 20% | | | | |
| | | [P com] | 0,1 | 20% | | | | |
| | | [P sec] | 0,1 | 20% | | | | |
| | | [P dba] | 0,1 | 20% | | | | |
| | | [P rector] | 0,1 | 20% | | | | |
| | | [P Proc] | 0,1 | 20% | | | | |
| | | [P Calidad] | 0,1 | 20% | | | | |
| [A.29] | Extrosión | [P ui] | 0,01 | 20% | | | | |
| | | [P ue] | 0,01 | 20% | | | | |
| | | [P soperte] | 0,01 | 20% | | | | |
| | | [P adm] | 0,01 | 20% | | | | |
| | | [P com] | 0,01 | 20% | | | | |
| | | [P sec] | 0,01 | 20% | | | | |
| | | [P dba] | 0,01 | 20% | | | | |
| | | [P rector] | 0,01 | 20% | | | | |
| | | [P Proc] | 0,01 | 20% | | | | |
| | | [P Calidad] | 0,01 | 20% | | | | |
| | | [P proveedores] | 0,01 | 20% | | | | |
| [A.30] | Ingeniería social | [P ui] | 0,1 | 75% | 75% | 75% | | |
| | | [P ue] | 0,1 | 75% | 75% | 75% | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | [P soperte] | 0,1 | 75% | 75% | 75% | | |
| | | [P adm] | 0,1 | 75% | 75% | 75% | | |
| | | [P com] | 0,1 | 75% | 75% | 75% | | |
| | | [P sec] | 0,1 | 75% | 75% | 75% | | |
| | | [P dba] | 0,1 | 75% | 75% | 75% | | |
| | | [P rector] | 0,1 | 75% | 75% | 75% | | |
| | | [P Proc] | 0,1 | 75% | 75% | 75% | | |
| | | [P Calidad] | 0,1 | 75% | 75% | 75% | | |
| | | [P proveedores] | 0,1 | 75% | 75% | 75% | | |

# ANEXO 7. NIVEL DE CUMPLIMIENTO

| NIVEL DE CUMPLIMIENTO | | | | | | |
|---|---|---|---|---|---|---|
| ISO 27002:2013 | | | | | | |
| **CONTROL** | **Objetivo del Control** | **Cumple** | **CMM** | **No Conformidad Menor** | **No Conformidad Mayor** | **Observación** |
| **5. POLÍTICAS DE SEGURIDAD.** | | | L4 | | | |
| 5.1 Directrices de la Dirección en seguridad de la información. | Compendio de lineamientos para gestionar y propender la seguridad de la información en la Institución | | L4 | | | |
| 5.1.1 Conjunto de políticas para la seguridad de la información. | El documento se debe crear contando con la participación de la alta dirección, el departamento de TI y Calidad. Posterior aprobación y socialización en la Institución y con colaboradores. | SI | L4 | | | Se cuenta con documento de políticas de seguridad de la información, aprobado y apoyado por la alta dirección. El documento es de amplio conocimiento por la comunidad y dispuesto en el portal WEB para fácil consulta. |
| 5.1.2 Revisión de las políticas para la seguridad de la información. | Se debe garantizar cronograma de revisión periódica de las políticas para la seguridad de la información. Revisiones extraordinarias cuando se surtan cambios sustanciales. | SI | L4 | | | Se cuenta con un cronograma de revisión para mejora continua de las políticas de Seguridad de la Información Institucional. Se lleva un control detallado de los cambios efectuados. |
| **6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN** | | | L3 | | | |
| 6.1 Organización interna. | Estructura Organizacional para velar por el cumplimiento y gestión de la Seguridad de la Información en la Institución | | L3 | | | |
| 6.1.1 Asignación de responsabilidades para la seguridad de la información. | Se debe fijar la estructura organizacional con las responsabilidades en relación con el aseguramiento continuo de la información. | SI | L4 | | | El documento de políticas fija los roles y responsabilidades acorde con cada proceso. Así mismo se encuentran segregadas las responsabilidades en términos contractuales. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 6.1.2 Segregación de tareas. | Se define responsabilidades puntuales acorde al rol de cada colaborador en los procesos que tienen a su cargo y aquellos en los que participan de manera indirecta. | SI | L4 | | | Las segregaciones de tareas se tienen tipificadas en términos contractuales, acorde con los lineamientos planteados en la Política Institucional. |
| | 6.1.3 Contacto con las autoridades. | Se deben fijar canales de comunicaciones con las autoridades nacionales y pares institucionales a fin de poder gestionar posibles soluciones ante determinadas situaciones. | SI | L2 | | | Se tiene contacto con las autoridades y pares. Sin embargo, no se cuenta con procedimiento claro para escalamiento en caso de determinadas situaciones. |
| | 6.1.4 Contacto con grupos de interés especial. | Es importante contar con cercanía a grupos con experiencia en la materia, teniendo en cuenta retroalimentación e información rápida y verás en caso de ocurrencia de algún suceso relevante. | SI | L4 | | | A partir de los proyectos implementados, se cuenta con soporte local y canal directo con los fabricantes de las soluciones que permiten fortalecer el vínculo con grupos especializados. Todos los niveles de servicio se tienen documentados de manera clara en los contratos. |
| | 6.1.5 Seguridad de la información en la gestión de proyectos. | Se debe fijar lineamientos claros que motiven el aseguramiento de la información en la ejecución y gestión de proyectos en la Institución. | SI | L4 | | | Contractualmente se tienen definidos los acuerdos de confidencialidad y se fijan pólizas que cubren alguna degradación en el aseguramiento de la información por malos tratamientos. |
| 6.2 Dispositivos para movilidad y teletrabajo. | | | | L3 | | | |
| | 6.2.1 Política de uso de dispositivos para movilidad. | Se deben fijar políticas claras para el uso de dispositivos móviles. Así mismo, se deben especificar las responsabilidades de los usuarios en torno al traslado y uso de estos. | SI | L3 | | | Se tiene política para el uso de dispositivos móviles. Sin embargo, no se cuenta con las herramientas para gestionar dichos dispositivos en |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | caso de pérdida o hurto. |
| 6.2.2 Teletrabajo. | N. A | | | | | N. A |
| **7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.** | | | L4 | | | |
| 7.1 Antes de la contratación. | | | L5 | | | |
| 7.1.1 Investigación de antecedentes. | Se tiene definida una política en el proceso de contratación. El servicio es tercerizado y se encargan de realizar un estudio de seguridad, tanto en el ámbito profesional como en la vida personal. | SI | L5 | | | Política del departamento de recursos humanos establecida, con seguimiento y ejecución a través de un tercero. |
| 7.1.2 Términos y condiciones de contratación. | Se tiene definido un proceso contractual claramente establecido y aplicable a los cargos determinados en la Institución. | SI | L5 | | | Grupo de Gestión Humana, contratos de colaboradores, revisión periódica en el marco legal por un tercero. |
| 7.2 Durante la contratación. | | | L4 | | | |
| 7.2.1 Responsabilidades de gestión. | Se establece la política para determinar responsabilidades claras para la gestión. | SI | L4 | | | Se tiene definidas las responsabilidades de gestión de cada colaborador, a través de las cláusulas contractuales de vinculación. |
| 7.2.2 Concienciación, educación y capacitación en seguridad de la información | Se efectúan campañas de sensibilización periódicas donde se abarca el cubrimiento de la totalidad de la Institución y terceros. | SI | L4 | | | Se tiene establecidas campañas de sensibilización periódicas y se realiza seguimiento posterior para la mejora continua. |
| 7.2.3 Proceso disciplinario. | El contrato debe contener clausulas claras y concretas, que se aplican en caso de adelantarse algún proceso disciplinario. | SI | L3 | | | Los Contratos laborarles, cuentan con una serie de cláusulas con las respectivas sanciones en caso de su no cumplimiento. El Grupo de Gestión Humana debe realizar seguimiento a las |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | cláusulas en cada periodo académico. |
| 7.3 Cese o cambio de puesto de trabajo. | | | L4 | | | |
| 7.3.1 Cese o cambio de puesto de trabajo. | Establecer el procedimiento para colaboradores que dejan el puesto o cambian a otro en la Institución. | SI | L4 | | | El documento Retiro de colaboradores, fija las actividades necesarias una vez el colaborador deja la Institución. |
| **8. GESTIÓN DE ACTIVOS.** | | | L2 | | | |
| 8.1 Responsabilidad sobre los activos. | | | L2 | | | |
| 8.1.1 Inventario de activos. | Se debe contar con un inventario claro de activos. Donde se indique el responsable del activo y la ubicación de este. | NO | L2 | Se cuenta con una aplicación de software libre, para el registro del inventario de activos. Sin Embargo, se debe fijar un proceso claro para dar de baja los activos que presentan daños y realizar un seguimiento continuo al inventario existente. | | |
| 8.1.2 Propiedad de los activos. | Es necesario contar con la clasificación de los propietarios de los activos y su ubicación. | NO | L2 | En la aplicación para el inventario de activos, se encuentra consignado el colaborador que tiene bajo su responsabilidad dicho activo. Sin embargo, se debe fijar proceso para traslado y seguimiento de los propietarios y activos. | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 8.1.3 Uso aceptable de los activos. | Se debe contar con una política clara de uso aceptable de los activos. | NO | L0 | | No se cuenta con documentación alguna que fije políticas claras del uso de activos. Por lo tanto, se debe generar dicha documentación, publicarla y socializarla con la comunidad. | |
| | 8.1.4 Devolución de activos. | Se debe contar con procedimiento para la devolución de activos por parte de colaboradores. | SI | L4 | | | Se cuenta con documento acta de devolución de equipos, en el cual se detallan las condiciones establecidas para su devolución o el cobro de ser el caso. |
| 8.2 Clasificación de la información. | | | | L2 | | | |
| | 8.2.1 Directrices de clasificación. | Se debe contar con una correcta clasificación de la información acorde con la Ley 1581 de 2012 y su correspondiente registro ante la SIC. | SI | L3 | | | Se cuenta con el documento de registro de las bases de datos ante la SIC. La clasificación de la información se tiene consolidada. Se debe garantizar un cronograma de revisión periódica y un proceso de revisión extemporánea en casos puntuales. |
| | 8.2.2 Etiquetado y manipulado de la información. | La clasificación de la información debe tener un etiquetado que permita su reconocimiento y correcta manipulación. | SI | L3 | | | Se tienen establecida una política de tratamiento de información. Esta publicada y ampliamente socializada con la comunidad. Se debe fijar seguimiento de la política y actualización de ser el caso. |
| | 8.2.3 Manipulación de activos. | Se debe fijar política para el tratamiento y manipulación de los activos. | NO | L1 | | No se cuenta con documentación para el uso apropiado de los activos. Se efectúa gracias a la voluntad de los colaboradores. | |
| 8.3 Manejo de los soportes de almacenamiento. | | | | L2 | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 8.3.1 Gestión de soportes extraíbles. | Establecer documento para gestionar de manera correcta todos los dispositivos de almacenamiento extraíbles, asegura un buen tratamiento de la información y minimiza el riesgo de fuga de información. | SI | L4 | | | Se tiene un procedimiento claro sobre el uso y gestión de soportes extraíbles, correctamente documentado y con seguimiento constante. |
| 8.3.2 Eliminación de soportes. | La correcta eliminación de soportes permite minimizar los riesgos de fuga de información. | SI | L4 | | | Se tiene documento y seguimiento de los soportes eliminado. |
| 8.3.3 Soportes físicos en tránsito. | Contar con seguimiento a soportes en tránsito, asegura un correcto uso de estos. | NO | L1 | | No se cuenta procedimiento alguno, se llevan registros de manera informal en el préstamo de información hacia otras dependencias. | |
| **9. CONTROL DE ACCESOS.** | | | L4 | | | |
| 9.1 Requisitos de negocio para el control de accesos. | | | L4 | | | |
| 9.1.1 Política de control de accesos. | Se debe implementar controles de acceso tanto físicos como lógicos que permitan el reforzamiento del acceso a la información. | SI | L4 | | | Se tiene establecidos y documentados procedimientos para el acceso a las instalaciones físicas y procedimientos para el acceso lógico a la información. |
| 9.1.2 Control de acceso a las redes y servicios asociados. | Es necesario contar con controles de acceso a las redes y servicios asociados a las mismas. | SI | L4 | | | Se tiene establecidos y documentados procedimientos para el acceso a las instalaciones físicas y procedimientos para el acceso lógico a la información. |
| 9.2 Gestión de acceso de usuario. | | | L4 | | | |
| 9.2.1 Gestión de altas/bajas en el registro de usuarios. | Se debe garantizar la correcta gestión de altas/bajas en el registro de los usuarios. | SI | L4 | | | Se tiene procedimiento establecido para la creación o eliminación de registro de usuarios. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 9.2.2 Gestión de los derechos de acceso asignados a usuarios. | Se deberá fijar control que informe derechos y responsabilidades de perfil a usuario. | SI | L4 | | | Se tiene establecidos perfiles de acceso de usuario acorde con rajos asociados a los cargos de los colaboradores. Se debe realizar cronogramas de seguimiento de los derechos de acceso. |
| | 9.2.3 Gestión de los derechos de acceso con privilegios especiales. | Se debe fijar política para la gestión de los derechos de acceso con privilegios especiales. | SI | L4 | | | Se tiene establecida la gestión de accesos privilegiados. Se tienen registros y trazabilidad de los accesos generados con dichas cuentas. |
| | 9.2.4 Gestión de información confidencial de autenticación de usuarios. | Se debe contar con el control de auditoria de gestión de información confidencial para la autenticación de usuarios. | SI | L4 | | | Se tiene documentación y controles para la autenticación de usuarios. El dispositivo de autenticación genera reportes trazables en repositorios seguros. Se debe revisar periódicamente los reportes garantizando la confidencialidad de la actividad. |
| | 9.2.5 Revisión de los derechos de acceso de los usuarios. | Se debe realizar el perfilamiento de los usuarios y los accesos concedidos. | SI | L3 | | | Se tiene documentados los derechos de acceso de usuarios y los perfiles asociados a los mismos. Es necesario establecer cronograma de revisión periódica. |
| | 9.2.6 Retirada o adaptación de los derechos de acceso | Se debe fijar el control para el agrade o retiro de derechos de acceso. | SI | L4 | | | Se tiene establecido procedimiento de retiro o adaptación de derechos de acceso a los usuarios. Se efectúa revisión mensual de los colaboradores. |
| 9.3 Responsabilidades del usuario. | | | | L4 | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 9.3.1 Uso de información confidencial para la autenticación. | Es necesario fijar el control y la política para la gestión de contraseñas | SI | L4 | | | Se tiene establecida una política clara para la gestión de contraseñas. Se realiza revisión periódica |
| 9.4 Control de acceso a sistemas y aplicaciones. | | | L4 | | | |
| 9.4.1 Restricción del acceso a la información. | Es necesario establecer controles de acceso a la información. | SI | L4 | | | Se tienen establecidos controles de acceso a la información a través de usuario y contraseñas de directorio activo. El sistema obliga el cambio de credenciales cada 30 días. |
| 9.4.2 Procedimientos seguros de inicio de sesión. | Se debe contar con procedimiento de inicio de sesión. | SI | L4 | | | Se tienen establecidos controles de acceso a la información a través de usuario y contraseñas de directorio activo. El sistema obliga el cambio de credenciales cada 30 días. |
| 9.4.3 Gestión de contraseñas de usuario. | Se debe contar con procedimientos claramente establecidos para la gestión de contraseña de usuarios. | SI | L4 | | | Se tienen establecidos controles de acceso a la información a través de usuario y contraseñas de directorio activo. El sistema obliga el cambio de credenciales cada 30 días. |
| 9.4.4 Uso de herramientas de administración de sistemas. | Se debe establecer la adquisición, parametrización y uso de herramientas de administración de sistemas. | SI | L3 | | | Se cuentan con herramientas de administración de sistemas. Se debe realizar capacitación a personal de respaldo. |
| 9.4.5 Control de acceso al código fuente de los programas. | Se debe restringir el acceso a códigos fuentes de programas, entre otras, porque este servicio es tercerizado y se deben establecer controles en los SLAS del contrato. | SI | L4 | | | Se tiene documentados en detalle los Contratos de Desarrollo de Software. |
| **10. CIFRADO.** | | | L2 | | | |
| 10.1 Controles criptográficos. | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 10.1.1 Política de uso de los controles criptográficos. | Se debe establecer controles criptográficos para la protección de la información. | SI | L0 | | | No se cuenta con política de uso de controles criptográficos ni con herramientas para generar la gestión de estas. |
| | 10.1.2 Gestión de claves. | Se debe contar con procedimientos claros para la gestión de claves. | SI | L3 | | | Se tiene establecido y documentado procedimiento para la gestión de claves. Se debe fijar cronogramas de seguimiento. |
| **11. SEGURIDAD FÍSICA Y AMBIENTAL.** | | | | L3 | | | |
| 11.1 Áreas seguras. | | | | L4 | | | |
| | 11.1.1 Perímetro de seguridad física. | Se deben establecer perímetros de acceso restringidos y de transito libre. | SI | L4 | | | Se cuenta con contrato de seguridad vigente que efectúa análisis para el aseguramiento físico de la institución. Se realiza seguimiento mensual y extraordinario en caso de falla alguna. |
| | 11.1.2 Controles físicos de entrada. | Se deben establecer controles físicos de entrada, acorde con la criticidad de las diferentes zonas de la Institución. | SI | L4 | | | Se cuenta con diferentes controles de acceso, que en todo caso mínimo refleja un doble factor de controles para el acceso a zonas de transito libre. |
| | 11.1.3 Seguridad de oficinas, despachos y recursos. | Se debe establecer controles y protocoles de acceso a las zonas administrativas. | SI | L4 | | | Se tienen controles de acceso a zonas de acceso restringido, como lo son las zonas de administración. |
| | 11.1.4 Protección contra las amenazas externas y ambientales. | Se debe garantizar con controles de amenazas externas y ambientales, como aires acondicionados y controles de contención y extinción de incendios. | SI | L3 | | | Se cuenta con centro de datos equipado con sistema de contención y extinción de incendios. Es necesario ampliar el control de incendios a áreas de administración. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 11.1.5 El trabajo en áreas seguras. | Se debe garantizar el aislamiento para el trabajo en áreas seguras. | SI | L4 | | | Se cuenta con delimitación y restricción a zonas especiales. Entre ellas las consideradas áreas seguras en la Institución |
| | 11.1.6 Áreas de acceso público, carga y descarga. | Se debe implementar controles en las zonas de acceso público y las zonas de carga y descarga. | SI | L4 | | | Se tiene demarcadas las zonas de acceso libre y las zonas de carga y descarga. |
| 11.2 Seguridad de los equipos. | | | | L3 | | | |
| | 11.2.1 Emplazamiento y protección de equipos. | Se deberá fijar controles para la protección y emplazamiento de equipos | SI | L4 | | | Se tiene establecido y documentado el procedimiento para emplazamiento y traslado de equipos. |
| | 11.2.2 Instalaciones de suministro. | Se deberá fijar control para las instalaciones de suministro, principalmente la disposición de una planta generadora en caso de cortes de energía de larga duración. | SI | L3 | | | Se tienen equipos UPS para el suministro de energía en caso de falla. Si embargo la autonomía es de 25 minutos, por cuanto cortes superiores a ese lapso generaría interrupción en los servicios. |
| | 11.2.3 Seguridad del cableado. | Se debe garantizar la seguridad física de los cuartos de cableado. | SI | L4 | | | Se tienen controles establecidos para el acceso a los cuartos de cableado. |
| | 11.2.4 Mantenimiento de los equipos. | Se deben establecer programas de mantenimientos de equipos, a fin de contemplar la totalidad de ellos. En tal sentido se deben fijar controles con cronogramas estipulados. | SI | L4 | | | Se tiene establecidos cronograma de mantenimientos acorde a las necesidades de la institución. |
| | 11.2.5 Salida de activos fuera de las dependencias de la empresa. | Se debe implementar control para activos que se usan fuera de la institución. | SI | L4 | | | Se tienen establecidos procedimientos para el uso de activos fuera de la institución. Está documentado y aceptado por las partes. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones. | No se tienen en cuenta ya que las políticas de la institución, contempla, el uso de equipos y de dispositivos de almacenamiento sin restricción alguna, y se basan en los compromisos de confidencialidad firmados con el colaborador. | NO | | | | N. A |
| | 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento. | No se tienen en cuenta ya que las políticas de la institución, contempla, el uso de equipos y de dispositivos de almacenamiento sin restricción alguna, y se basan en los compromisos de confidencialidad firmados con el colaborador. | NO | | | | N. A |
| | 11.2.8 Equipo informático de usuario desatendido. | Se deben fijar campañas de sensibilización a fin de que los usuarios no dejen de manera descuidada los equipos con sesión iniciada. | SI | L4 | | | La campaña de sensibilización ha fijado como punto a tratar la responsabilidad de los usuarios frente a los equipos cuando no se encuentran en las estaciones de trabajo. |
| | 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla. | Se debe fijar campañas periódicas de concientización en los usuarios para el bloqueo de equipos cuando no están en uso. | SI | L4 | | | La campaña de sensibilización ha fijado como punto a tratar la responsabilidad de los usuarios frente a los equipos cuando no se encuentran en las estaciones de trabajo. |
| **12. SEGURIDAD EN LA OPERACIONES** | | | | L2 | | | |
| 12.1 Responsabilidades y procedimientos de operación. | | | | L2 | | | |
| | 12.1.1 Documentación de procedimientos de operación. | Se deben fijar procedimientos de operación y realizar su registro formal. | SI | L4 | | | Se tiene documentado los procedimientos de operación y se realiza seguimiento periódico. |
| | 12.1.2 Gestión de cambios. | Se debe establecer el procedimiento para el control y gestión de cambios. | SI | L4 | | | Se tiene documentado el procedimiento para la gestión de cambios. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 12.1.3 Gestión de capacidades. | Se debe fijar estrategias anuales para la gestión de capacidades. De tal manera que se tenga como mínimo una escalabilidad del 10% en cada anualidad. | NO | L1 | No se tiene registro documentado. La gestión de capacidades está a juicio de la dirección de TI. | | |
| 12.1.4 Separación de entornos de desarrollo, prueba y producción. | Se debe garantizar e implementar zonas seguras de desarrollo para posterior paso a producción. | SI | L3 | | | Se tienen establecidos acuerdos con terceros desarrolladores, ya que la Institución no cuenta con área dedicada al desarrollo. La documentación obedece a acuerdos contractuales. |
| 12.2 Protección contra código malicioso. | | | L4 | | | |
| 12.2.1 Controles contra el código malicioso. | Se deben fijar estrategias y herramientas para controlar código malicioso. | SI | L4 | | | Se cuenta con herramientas de aseguramiento para la prevención de propagación de código malicioso. Se realiza actualizaciones periódicas a las soluciones y se generan las bitácoras de actividades correspondientes. |
| 12.3 Copias de seguridad. | | | L4 | | | |
| 12.3.1 Copias de seguridad de la información. | Se deben establecer procesos de copias de seguridad. | SI | L4 | | | Procedimiento copias de seguridad y Backus es el documento que contiene la información del proceso efectuado para las copas de respaldo. |
| 12.4 Registro de actividad y supervisión. | | | L3 | | | |
| 12.4.1 Registro y gestión de eventos de actividad. | Se debe registrar y gestionar los eventos de las diferentes actividades | SI | L4 | | | Se cuenta con una solución para el almacenamiento y gestión de logs. Se tiene acceso a repositorios de dichas actividades. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 12.4.2 Protección de los registros de información. | Se deben proteger los registros de información | SI | L4 | | | Se cuenta con una solución para el almacenamiento y gestión de logs. Se tiene acceso a repositorios de dichas actividades. |
| 12.4.3 Registros de actividad del administrador y operador del sistema. | Se deben conservar los registros de actividad del administrado de los diferentes sistemas. | SI | L4 | | | Se cuenta con una solución para el almacenamiento y gestión de logs. Se tiene acceso a repositorios de dichas actividades. |
| 12.4.4 Sincronización de relojes. | Se debe hacer el control formal de la sincronización de relojes. En la actualidad se realiza, pero no se tiene documentado el procedimiento | SI | L2 | | | Se realiza la gestión, pero no se cuenta con procedimientos estándares que garanticen la actividad. |
| 12.5 Control del software en explotación. | | | L4 | | | |
| 12.5.1 Instalación del software en sistemas en producción. | Se debe fijar el control para la instalación de software en servidores de producción. | SI | L4 | | | Se tiene establecidos y documentados los procedimientos para desplegar software en sistemas de producción. |
| 12.6 Gestión de la vulnerabilidad técnica. | | | L3 | | | |
| 12.6.1 Gestión de las vulnerabilidades técnicas. | Se debe realizar el control que permita gestionar las vulnerabilidades de tipo técnicas que se encuentren. | SI | L2 | | | Se realiza gracias a la gestión del personal de TI de manera proactiva. Falta establecer procedimientos claros y unificar con los que se cuentan actualmente. |
| 12.6.2 Restricciones en la instalación de software. | Se debe garantizar que no se puede instalar software de manera indiscriminada. Se debe generar controles y aprobaciones para tal fin. | SI | L4 | | | Se tiene política documentada y socializada para la instalación de software en la institución. |
| 12.7 Consideraciones de las auditorías de los sistemas de información. | | | L1 | | | |
| 12.7.1 Controles de auditoría de los sistemas de información. | Se debe fijar controles de auditoria para los sistemas de información. | NO | L1 | Se realizan procesos de manera selectiva y personal. No se cuenta con procedimientos para tal fin. | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **13. SEGURIDAD EN LAS TELECOMUNICACIONES.** | | | | | | |
| 13.1 Gestión de la seguridad en las redes. | | | L3 | | | |
| 13.1.1 Controles de red. | Se deberían administrar y gestionar las redes para salvaguardar la información en las diferentes aplicaciones y sistemas. | SI | L3 | | | Se tienen controles y documentación de estas a fin de aislar las diferentes redes y poder poner salva guardas a cada segmento. |
| 13.1.2 Mecanismos de seguridad asociados a servicios en red. | Se deben implementar soluciones y acuerdos de niveles de servicio para la seguridad de la red | SI | L3 | | | Se tienen definidos algunos acuerdos de servicios para gestionar el aseguramiento a servicios de red internos. |
| 13.1.3 Segregación de redes. | Se debe realizar segmentación de redes. | SI | L4 | | | Se tiene documentado los segmentos de red acorde a los usuarios y aplicaciones que se manejan en cada una de ellas. Se debe realizar pruebas y seguimientos periódicos. |
| 13.2 Intercambio de información con partes externas. | | | L3 | | | |
| 13.2.1 Políticas y procedimientos de intercambio de información. | Se debe fijar políticas para el intercambio de información interna y con terceros | SI | L3 | | | Se tienen establecidos protocolos para el intercambio de información con tercero. Si embargo de manera interna no se evidencia el seguimiento estricto del procedimiento. |
| 13.2.2 Acuerdos de intercambio. | Se debe garantizar acuerdos para la transferencia segura de información con terceros. | SI | L3 | | | Se tienen establecidos protocolos para el intercambio de información con tercero |
| 13.2.3 Mensajería electrónica. | Se debe implementar controles de mensajería electrónica y acuerdos de uso | SI | L3 | | | Se cuentan con campañas de concientización del uso de mensajería electrónica para fines Corporativos. Se debe revisar el procedimiento de comunicación institucional. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 13.2.4 Acuerdos de confidencialidad y secreto. | Se deben implementar acuerdos de confidencialidad | SI | L4 | | | Se cuenta con el documento Acuerdo de confidencialidad. Gestión Humana realiza seguimiento contractual al procedimiento |
| **14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.** | | | L3 | | | |
| 14.1 Requisitos de seguridad de los sistemas de información. | | | L3 | | | |
| 14.1.1 Análisis y especificación de los requisitos de seguridad. | Se debe realizar análisis de vulnerabilidad a los sistemas de información a fin de fijar medidas y controles sobre ellos | SI | L3 | | | Se corren análisis de seguridad con terceros cada periodo académico según recomendación del comité de seguridad. Se deja la documentación del caso. |
| 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas. | Se debe implementar soluciones de seguridad que permita controlar de manera óptima el acceso a servicios de información desde el exterior. | SI | L3 | | | Se cuenta con soluciones de seguridad que aseguran el sitio y las comunicaciones o transacciones efectuadas desde el exterior. |
| 14.1.3 Protección de las transacciones por redes telemáticas. | Se debe fijar control para la protección de transacciones en las redes | SI | L3 | | | Se cuenta con soluciones de seguridad que aseguran el sitio y las comunicaciones o transacciones efectuadas desde el exterior. |
| 14.2 Seguridad en los procesos de desarrollo y soporte. | | | L3 | | | |
| 14.2.1 Política de desarrollo seguro de software. | Dentro de la institución no se tiene un área encargada de desarrollo de software, el cual es adquirido a través de terceros | NO | | | | N. A |
| 14.2.2 Procedimientos de control de cambios en los sistemas. | Se debe fijar control para la gestión de cambios | SI | L3 | | | Se tiene documentado el procedimiento para implementar cambios en los sistemas. |
| 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. | Se debe fijar una lista de chequeo de cada aplicación posterior a cambios realizados. | SI | L3 | | | Se tiene procedimiento con lista de chequeo para probar que los cambios no |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | afectaron las funcionalidades. |
| | 14.2.4 Restricciones a los cambios en los paquetes de software. | Se debe garantizar que no se efectúan modificaciones a los paquetes de software entregados por terceros. | SI | L2 | | | No se realizan cambios sustanciales a los paquetes de software entregados por terceros. Falta programa de revisión de software para garantizar su integridad. |
| | 14.2.5 Uso de principios de ingeniería en protección de sistemas. | Se debe implementar medidas de aseguramiento para la protección de sistemas | SI | L2 | | | Se aseguran medidas para la protección de los sistemas siempre que se hagan labores de implementación en los sistemas de información. Se debe socializar el documento. |
| | 14.2.6 Seguridad en entornos de desarrollo. | Al no desarrollar software en la institución, el aseguramiento de entrones de desarrollo es inexistente | NO | | | | N. A |
| | 14.2.7 Externalización del desarrollo de software. | Se debe fijar SLAS claros para el desarrollo de software a través de terceros contratistas | SI | L4 | | | Se tienen obligaciones contractuales y se fijan cronogramas para el seguimiento del desarrollo. |
| | 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas. | Se debe realizar control para pruebas durante el desarrollo. | SI | L4 | | | Se realizan pruebas de seguridad durante la fase del desarrollo. Se pide certificación de código seguro de terceros no relacionados con el contratista elegido para el desarrollo. |
| | 14.2.9 Pruebas de aceptación. | Se debe realizar control para el recibo a satisfacción. | SI | L4 | | | Se tiene previsto listas de chequeo y documentos de aceptación de los desarrollos efectuados. |
| 14.3 Datos de prueba. | | | | L3 | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 14.3.1 Protección de los datos utilizados en pruebas. | Realizar controles para la protección de datos y acuerdos de confidencialidad en pruebas | SI | L3 | | | Los datos usados en las pruebas se salvaguardan de manera óptima a través de acuerdos específicos en el documento contrato. |
| **15. RELACIONES CON SUMINISTRADORES** | | | | L2 | | | |
| 15.1 Seguridad de la información en las relaciones con suministradores. | | | | L4 | | | |
| | 15.1.1 Política de seguridad de la información para suministradores. | Se debe implementar política de seguridad de la información, debido a las concesiones otorgadas en vínculos contractuales a terceros. | SI | L4 | | | Se tiene documentado el Acuerdo de confidencialidad Externos. Gestión Humana realiza seguimiento de las obligaciones y la suscripción de pólizas de respaldo en caso de incumplimiento |
| | 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores. | Se debe fijar control para el tratamiento del riesgo en los contratos | SI | L4 | | | Se tienen estimados una serie de riesgos asociados a los procesos de contratación. En tal sentido se ajustan las pólizas de cumplimiento requeridas. |
| | 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones. | Se debe implementar control para garantizar la cadena de suministro en tecnologías de la información y comunicaciones mediante SLAS claros establecidos y pólizas de respaldo | SI | L4 | | | En los contratos se especifican los riesgos de seguridad asociados y se fijan pólizas de cumplimiento. |
| 15.2 Gestión de la prestación del servicio por suministradores. | | | | L2 | | | |
| | 15.2.1 Supervisión y revisión de los servicios prestados por terceros. | Se debe implementar controles para la supervisión de contratos | SI | L4 | | | Se tienen estimadas fases en las diferentes contrataciones y documentos asociados que se irán suscribiendo conforme avanza la ejecución del contrato. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 15.2.2 Gestión de cambios en los servicios prestados por terceros. | Se debe implementar control de cambios en los servicios contratados, mediante SLAS contractuales | SI | L1 | | Se debe administrar la provisión de los servicios prestados por terceros y en consecuencia los cambios efectuados en tal sentido. En consecuencia, es necesario fijar un procedimiento detallado que permita la mejora continua. | |
| **16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.** | | | | L2 | | | |
| 16.1 Gestión de incidentes de seguridad de la información y mejoras. | | | | | | | |
| | 16.1.1 Responsabilidades y procedimientos. | Se debe realizar la asignación de responsabilidades y la consolidación de los procedimientos para la atención de incidentes. | NO | L1 | Se cuenta con un responsable para la atención de incidentes de seguridad. Sin embargo, no se cuenta con procedimiento detallado para tal fin | | |
| | 16.1.2 Notificación de los eventos de seguridad de la información. | Se debe fijar el control para notificar y tomar las medidas respectivas | SI | L3 | | | Se cuenta con canales establecidos para la comunicación de incidentes de seguridad. |
| | 16.1.3 Notificación de puntos débiles de la seguridad. | Se debe realizar controles para el establecimiento de puntos débiles de seguridad | SI | L3 | | | Se debe comprometer a los colaboradores y terceros para comunicar cualquier punto débil de seguridad de la información en los procesos que hacen parte. |
| | 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones. | Se debe fijar control para la valoración de un evento y la toma de medidas. | SI | L2 | | | A través de la comunicación del evento, se evalúa y decide el tratamiento del evento. No se tiene documentación década para este tipo de eventos, |

| | | | | | | |
|---|---|---|---|---|---|---|
| 16.1.5 Respuesta a los incidentes de seguridad. | Se deberá fijar procedimiento para la atención de incidentes | NO | L2 | Se realiza el procedimiento de atención, sin embargo, no se cuenta con documentación al respecto. | | |
| 16.1.6 Aprendizaje de los incidentes de seguridad de la información. | Se deberá tener un control y repositorio de datos para la toma de daciones futuras | SI | L3 | | | Se cuenta con bitácoras de servicio que permiten tomar medidas preventivas de cara a afrontar situaciones similares. |
| 16.1.7 Recopilación de evidencias. | Se deberá fijar procedimiento para el levantamiento de información y evidencias durante y después de un incidente. | NO | L2 | Se realiza el procedimiento de atención, sin embargo, no se cuenta con documentación al respecto. | | |
| **17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.** | | | L3 | | | |
| 17.1 Continuidad de la seguridad de la información. | | | | | | |
| 17.1.1 Planificación de la continuidad de la seguridad de la información. | Se debe efectuar el plan de continuidad del negocio. | SI | L3 | | | Se tiene documentado el plan de continuidad del negocio. |
| 17.1.2 Implantación de la continuidad de la seguridad de la información. | Se debe implementar los planes para la continuidad de la seguridad de la información en todo momento. | NO | L2 | Se deben crear los procedimientos y controles para garantizar la continuidad de la seguridad de la información | | |
| 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. | Se debe fijar cronograma para pruebas y evaluaciones del plan de continuidad. | SI | L3 | | | Se efectúa revisión semestral del plan de continuidad del negocio a través de pruebas. |
| 17.2 Redundancias. | | | | | | |
| 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información. | No se tiene en cuenta ya que la inversión para redundancias no se tiene contemplada en un mediano plazo | NO | | | | N. A |
| **18. CUMPLIMIENTO.** | | | L3 | | | |
| 18.1 Cumplimiento de los requisitos legales y contractuales. | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 18.1.1 Identificación de la legislación aplicable. | Se debe revisar las condiciones y obligaciones legales a fin de evitar un posible incumplimiento. | SI | L4 | | | Se tiene reglamentación del Core del negocio y un servicio legal externo que modifica según varié la normatividad vigente. |
| | 18.1.2 Derechos de propiedad intelectual (DPI). | Se tiene establecido el centro de propiedad intelectual en el contrato laboral | SI | L4 | | | Se tienen establecidas causas de derechos de propiedad intelectual en el documento Contrato laborara. El Grupo de Gestión Humana, realiza seguimientos periódicos. |
| | 18.1.3 Protección de los registros de la organización. | Se tiene implementado el acuerdo de confidencialidad y uso de la información con colaboradores. | SI | L4 | | | Acuerdo de confidencialidad y accesos controlados con credenciales propias de usuarios. |
| | 18.1.4 Protección de datos y privacidad de la información personal. | Se debe clasificar la información y realizar el registro de las bases de datos ante la SIC. | SI | L4 | | | Se realiza la respectiva inscripción ante la SIC y se tiene seguimiento periódico. |
| | 18.1.5 Regulación de los controles criptográficos. | Se deben implementar controles de regulación criptográfica | NO | L1 | No se cuenta con política de protección criptográfica. | | |
| 18.2 Revisiones de la seguridad de la información. | | | | | | | |
| | 18.2.1 Revisión independiente de la seguridad de la información. | Se debe realizar un estudio de seguridad de la información a través de una auditoria externa | SI | L3 | | | Se tiene contemplado revisiones externas cada año académico. |
| | 18.2.2 Cumplimiento de las políticas y normas de seguridad. | Se debe implementar auditorías internas de cumplimiento | SI | L4 | | | Se tienen estimadas auditorías internas de cumplimiento que permitan evidenciar el estado de los controles que establece la norma. |
| | 18.2.3 Comprobación del cumplimiento. | Se debe revisar y contrastar los controles a través de las diferentes auditorias. | SI | L4 | | | Se tienen estimadas auditorías internas de cumplimiento que permitan evidenciar el estado de los controles que |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | establece la norma. |

# ANEXO 8 INFORME DE AUDITORÍA

## Resumen Ejecutivo

## Alcance

Auditoría del Sistema de Gestión de Seguridad de la Información conforme al alcance del SGSI Institucional.

## Objetivo

Realizar la evaluación del nivel de madurez de la seguridad de la información, gracias a la revisión de los 114 controles estipulados en la norma ISO/IEC 27002:2013.

## Metodología

La metodología empleada es el Modelo de Madurez de la Capacidad (CMM).

## Principales Conclusiones

Si bien se observa un avance muy significativo en el cumplimiento de los controles, es necesario tomar y planificar una serie de proyectos adicionales que permitan obtener el nivel objetivo de la Institución. En tanto se encontraron nueve (9) No conformidades Menores y cinco (5) No Conformidades Mayores. En consecuencia, se deben concentrar esfuerzo principalmente en los dominios relacionados con: Gestión de Activos, Seguridad en las Operaciones, Relaciones con Suministradores, Gestión de incidentes en la seguridad de la información, Aspectos de Seguridad de da Información en la Gestión de la Continuidad del Negocio y Cumplimiento.

## Recomendaciones

Los proyectos o acciones encaminadas a mejorar el nivel de cumplimiento se deben centrar en las No Conformidades Mayores, que presuponen un mayor impacto Institucional y posteriormente abordar las No Conformidades Menores, garantizando la revisión conjunta de los controles para establecer así una mejora continua. Por lo tanto, se debe establecer un cronograma de trabajo para la ejecución de proyectos y acciones en plazos considerables en relación costo beneficio.

## Hallazgos y Recomendaciones

## No conformidades:

| **Fecha: 7 de mayo de 2018** | **ID: NC 001** |
|---|---|
| **Descripción** | Se cuenta con una aplicación de software libre, para el registro del inventario de activos. Sin embargo, se debe fijar un proceso claro para dar de baja los activos que |

| | |
|---|---|
| | presentan daños y realizar un seguimiento continuo al inventario existente. |
| **Dominio** | **8. GESTIÓN DE ACTIVOS.** |
| **Control** | **8.1.1 Inventario de activos.** |
| **Acción** | Implementar un procedimiento claro que incluya el tratamiento de los activos a dar de baja. Adicionalmente se debe estudiar la posibilidad de cambio de software para dicha gestión. |
| **Detalle** | No Conformidad Menor |
| **Responsable** | Director TI y Procuradora. |

| **Fecha: 7 de mayo de 2018** | **ID: NC 002** |
|---|---|
| **Descripción** | En la aplicación para el inventario de activos, se encuentra consignado el colaborador que tiene bajo su responsabilidad dicho activo. Sin embargo, se debe fijar proceso para |
| **Dominio** | **8. GESTIÓN DE ACTIVOS.** |
| **Control** | **8.1.2 Propiedad de los activos.** |
| **Acción** | Implementar un procedimiento claro que incluya el tratamiento de los activos a dar de baja. Adicionalmente se debe consignar los propietarios de los activos y su ubicación. |
| **Detalle** | No Conformidad Menor |
| **Responsable** | Director TI y Procuradora. |

| **Fecha: 7 de mayo de 2018** | **ID: NC 003** |
|---|---|
| **Descripción** | No se tiene registro documentado. La gestión de capacidades está a juicio de la dirección de TI. |
| **Dominio** | **12. SEGURIDAD EN LA OPERACIONES** |
| **Control** | **12.1.3 Gestión de capacidades.** |
| **Acción** | Se debe fijar estrategias anuales para la gestión de capacidades. De tal manera que se tenga como mínimo una escalabilidad del 10% en cada anualidad. |
| **Detalle** | No Conformidad Menor |
| **Responsable** | Comité de seguridad y Dirección. |

| **Fecha: 7 de mayo de 2018** | **ID: NC 004** |
|---|---|
| **Descripción** | No se tiene registro documentado. La gestión de capacidades está a juicio de la dirección de TI. |
| **Dominio** | **12. SEGURIDAD EN LA OPERACIONES** |
| **Control** | **12.1.3 Gestión de capacidades.** |
| **Acción** | Se debe fijar estrategias anuales para la gestión de capacidades. De tal manera que se tenga como mínimo una escalabilidad del 10% en cada anualidad. |
| **Detalle** | No Conformidad Menor |
| **Responsable** | Comité de seguridad y Dirección. |

| Fecha: 7 de mayo de 2018 | ID: NC 005 |
|---|---|
| **Descripción** | Se cuenta con un responsable para la atención de incidentes de seguridad. Sin embargo, no se cuenta con procedimiento detallado para tal fin. |
| **Dominio** | **16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.** |
| **Control** | **16.1.1 Responsabilidades y procedimientos.** |
| **Acción** | Se debe realizar la asignación de responsabilidades y la consolidación de los procedimientos para la atención de incidentes. |
| **Detalle** | No Conformidad Menor |
| **Responsable** | Área de Gestión Humana y Procuradora. |

| Fecha: 7 de mayo de 2018 | ID: NC 006 |
|---|---|
| **Descripción** | Se realiza el procedimiento de atención, sin embargo, no se cuenta con documentación al respecto. |
| **Dominio** | **16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.** |
| **Control** | **16.1.5 Respuesta a los incidentes de seguridad.** |
| **Acción** | Se debe fijar procedimiento para la atención de incidentes. |
| **Detalle** | No Conformidad Menor |
| **Responsable** | Comité de Seguridad. |

| Fecha: 7 de mayo de 2018 | ID: NC 007 |
|---|---|
| **Descripción** | Se realiza el procedimiento de atención, sin embargo, no se cuenta con documentación al respecto. |
| **Dominio** | **16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.** |
| **Control** | **16.1.7 Recopilación de evidencias.** |
| **Acción** | Se debe fijar procedimiento para la atención de incidentes. |
| **Detalle** | No Conformidad Menor |
| **Responsable** | Comité de Seguridad. |

| Fecha: 7 de mayo de 2018 | ID: NC 008 |
|---|---|
| **Descripción** | Se deben crear los procedimientos y controles para garantizar la continuidad de la seguridad de la información |
| **Dominio** | **17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.** |
| **Control** | **17.1.2 Implantación de la continuidad de la seguridad de la información.** |
| **Acción** | Se debe implementar los planes para la continuidad de la seguridad de la información en todo momento. |

| | |
|---|---|
| | No Conformidad Menor |
| **Responsable** | Comité de Seguridad. |

| **Fecha: 7 de mayo de 2018** | **ID: NC 009** |
|---|---|
| **Descripción** | No se cuenta con política de protección criptográfica. |
| **Dominio** | **18. CUMPLIMIENTO.** |
| **Control** | **18.1.5 Regulación de los controles criptográficos.** |
| **Acción** | Se deben implementar controles de regulación criptográfica. |
| **Detalle** | No Conformidad Menor |
| **Responsable** | Comité de Seguridad y Procuradora. |

| **Fecha: 7 de mayo de 2018** | **ID: NC 010** |
|---|---|
| **Descripción** | No se cuenta con documentación alguna que fije políticas claras del uso de activos. Por lo tanto, se debe generar dicha documentación, publicarla y socializarla con la |
| **Dominio** | **8. GESTIÓN DE ACTIVOS.** |
| **Control** | **8.1.3 Uso aceptable de los activos.** |
| **Acción** | Se debe desarrollar procedimientos claros de uso aceptable de los activos. |
| **Detalle** | No Conformidad Mayor |
| **Responsable** | Director TI. |

| **Fecha: 7 de mayo de 2018** | **ID: NC 011** |
|---|---|
| **Descripción** | No se cuenta con documentación para el uso apropiado de los activos. Se efectúa gracias a la voluntad de los colaboradores. |
| **Dominio** | **8. GESTIÓN DE ACTIVOS.** |
| **Control** | **8.2.3 Manipulación de activos.** |
| **Acción** | Se debe fijar procedimientos para el tratamiento y manipulación de los activos. |
| **Detalle** | No Conformidad Mayor |
| **Responsable** | Director TI. |

| **Fecha: 7 de mayo de 2018** | **ID: NC 012** |
|---|---|
| **Descripción** | No se cuenta procedimiento alguno, se llevan registros de manera informal en el préstamo de información hacia otras dependencias. |
| **Dominio** | **8. GESTIÓN DE ACTIVOS.** |
| **Control** | **8.3.3 Soportes físicos en tránsito.** |
| **Acción** | Contar con seguimiento a soportes en tránsito, asegura un correcto uso de estos. |
| **Detalle** | No Conformidad Mayor |
| **Responsable** | Comité de seguridad |

| Fecha: 7 de mayo de 2018 | ID: NC 013 |
|---|---|
| **Descripción** | Se debe administrar la provisión de los servicios prestados por terceros y en consecuencia los cambios efectuados en tal sentido. En consecuencia, es necesario fijar un procedimiento detallado que permita la mejora continua. |
| **Dominio** | **15. RELACIONES CON SUMINISTRADORES** |
| **Control** | **15.2.2 Gestión de cambios en los servicios prestados por terceros.** |
| **Acción** | Se debe implementar control de cambios en los servicios contratados, mediante SLAS contractuales. |
| **Detalle** | No Conformidad Mayor |
| **Responsable** | Comité de seguridad |

**Conclusión**

Se puede evidenciar que, a través del desarrollo de este proyecto, el nivel de cumplimiento de la seguridad de la información en la Institución y la concientización de su importancia va tomando fuerza en la Comunidad. De tal forma y aun cuando no se tiene cubierta la totalidad de los controles en el nivel objetivo por la Institución, el desarrollo de los proyectos planteados ha asegurado un amplio cumplimiento y un avance significativo en la madurez de la seguridad de la información.