UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

TEMA:

"SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001 PARA EL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN DEL DISTRITO 18D01 DE EDUCACIÓN"

Trabajo de Graducación. Modalidad: Proyecto de Investigación, presentado previo la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos.

SUBLÍNEA DE INVESTIGACIÓN: Seguridad de Unidades Informáticas

AUTOR: Guevara Tucta Ramiro Alejandro

TUTOR: Ing. Franklin Oswaldo Mayorga Mayorga

Ambato – Ecuador

Noviembre, 2017

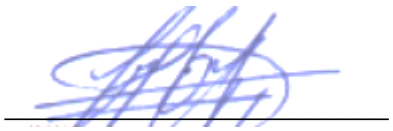
CERTIFICACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Investigación sobre el Tema:

"SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001 PARA EL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN DEL DISTRITO 18D01 DE EDUCACIÓN", del señor Ramiro Alejandro Guevara Tucta, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el Art. 16 del Capítulo II, del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad técnica de Ambato

Ambato, noviembre de 2017

EL TUTOR



Ing. Mg. Franklin O. Mayorga M.

AUTORÍA DEL TRABAJO

El presente trabajo de investigación titulado: SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001 PARA EL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN DEL DISTRITO 18D01 DE EDUCACIÓN, es absolutamente original, auténtico y personal. En tal virtud, el contenido, efectos legales y académicos que se desprendan del mismo son de exclusiva responsabilidad del autor.

Ambato, noviembre de 2017

Ramiro Alejandro Guevara Tucta

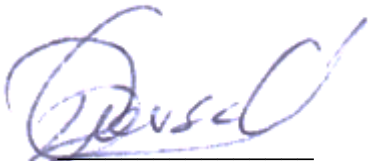
CC: 1804627568

APROBACIÓN DEL TRIBUNAL DE GRADO

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. David Guevara e Ing. Carlos Núñez, revisó y aprobó el Informe Final del trabajo de graduación titulado "SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001 PARA EL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN DEL DISTRITO 18D01 DE EDUCACIÓN", presentado por el señor Guevara Tucta Ramiro Alejandro de acuerdo al Art. 17 del Reglamento de Graduación para obtener el título Terminal de tercer nivel de la Universidad Técnica de Ambato.

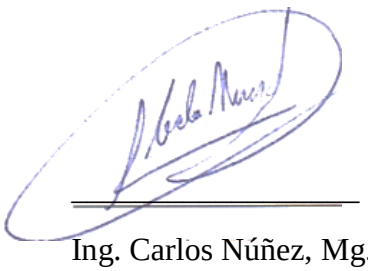
Ing. Pilar Urrutia, Mg.

PRESIDENTE DEL TRIBUNAL



Ing. David Guevara, Mg.

DOCENTE CALIFICADOR



Ing. Carlos Núñez, Mg.

DOCENTE CALIFICADOR

DEDICATORIA

El presente trabajo lo dedico en primer lugar a Dios, quien me brindó sabiduría y tenacidad a lo largo de mi carrera universitaria.

En segundo lugar a mi familia ya que con amor, paciencia y fortaleza guiaron cada momento de mi vida, pero de manera especial a mi madre, pilar fundamental en mi formación tanto personal como académica.

De igual manera a todos mis amigos y compañeros quienes me brindaron su apoyo incondicional en todo momento y con quienes compartimos momentos inolvidables.

Quiero además hacer una mención particular a Verónica, por su apoyo y cariño incondicional en el ámbito personal y académico motivándome siempre a mejorar y cumplir mis objetivos.

Guevara Tucta Ramiro Alejandro

AGRADECIMIENTO

Emito un sincero agradecimiento a la Universidad Técnica de Ambato y en especial a mi querida facultad de Ingeniería en Sistemas, Electrónica e Industrial la cual me brindó la oportunidad de formarme profesionalmente.

De manera especial a mi tutor de tesis el Ing. Franklin Mayorga por su apoyo y asesoramiento durante el desarrollo mi proyecto de investigación.

Guevara Tucta Ramiro Alejandro

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

El proyecto de investigación tiene como objetivo garantizar la seguridad de los procesos organizacionales a través de un modelo estructurado de carácter preventivo (sistema de gestión de seguridad de la información) basado en la norma ISO/IEC 27001. La importancia radica en los dominios de seguridad que lo conforman, entre ellos políticas de seguridad, administración de activos, seguridad de los recursos humanos, sistema de control de accesos, etc. cada uno con sus respectivos controles. Se presentan los resultados de una experiencia aplicando las fases de análisis y evaluación de riesgos a través de herramientas como entrevistas al personal de sistemas y observación directa mediante visitas programadas.

Posteriormente se realiza un análisis de controles basados en la declaración de aplicabilidad donde se justifican aquellos controles aplicables en razón de las necesidades institucionales y a partir de ello se proponen políticas de seguridad coherentes y enmarcadas dentro de los límites de cumplimiento institucional, cuyo objetivo será apoyar y proporcionar la guía para gestionar adecuadamente la seguridad de la información.

ABSTRACT

The project aims to guarantee the safety of organizational processes through a structured model of a preventive nature based on ISO / IEC 2 7001. The importance lies in the security domains that conform it, including security policies, Assets, human resources security, access control system, etc. Each with their respective controls. The results of an experience are presented applying the phases of analysis and risk assessment through tools such as personal interview of systems and direct observation through scheduled visits. Subsequently an analysis of controls based on the declaration of applicability is carried out where these controls are justified in the reason of the institutional needs and from the beginning are proposed coherent security policies and framed within the limits of institutional compliance Provide the guide to manage Security of information..

INTRODUCCIÓN

Considerando la importancia que tiene actualmente la información para cualquier institución u organización y el incremento de incidentes a nivel organizacional con afectación no sólo a los procesos sino a la continuidad operativa del negocio lo cual acarrea problemas a nivel económico e incluso legal se torna indispensable buscar una solución efectiva para combatir o minimizar el impacto de afectación de dichas amenazas y garantizar la seguridad de los procesos y por ende del activo de mayor importancia, la información.

Garantizar un nivel de protección total es prácticamente imposible independientemente de los recursos económicos o financieros que maneje la empresa en cuestión.

Para toda organización o empresa indistintamente de su campo de aplicación la situación es la misma; todas manejan información incluso de carácter "confidencial" por lo que es necesario tomar medidas para precautelar la seguridad de la misma frente a posibles intrusiones producto de las vulnerabilidades existentes en los sistemas de seguridad, garantizando de esta manera la integridad, confidencialidad y disponibilidad de dicha información. La medida más común en la mayoría de organizaciones es la ejecución de medidas correctivas o sobre la marcha, las mismas que significan pérdida de información, activos y como consecuencia de ello desperdicio de recursos.

El presente proyecto promueve la implementación de un sistema de gestión de seguridad de la información basado en el estándar ISO 27001; una solución efectiva no solamente debido a que su aplicabilidad es de carácter preventivo sino también debido a que el mismo está basado en la norma ISO 27001 con lo cual aumentan los campos de aplicabilidad de salvaguardas y su contribución a establecer políticas de seguridad, y gestionar los riesgos asociados.

CAPÍTULO 1

EL PROBLEMA

1.1 Tema:

"Sistema de Gestión de Seguridad de la información basado en la Norma ISO/IEC 27001 para el Departamento de Tecnologías de la Información y Comunicación del Distrito 18D01 de Educación".

1.2 Planteamiento del problema

El uso de tecnologías para el procesamiento de información en las organizaciones como ordenadores potentes además de conexiones a internet de alta velocidad, permite que se conviertan en un blanco fácil para entidades malintencionadas cuyo objetivo es causar daños como: robar o destruir información, provocar caídas del sistema, denegar servicios, entre otros [1].

Ante esto y considerando el alcance que tiene hoy en día la tecnología para vulnerar cualquier sistema sofisticado, resulta imprescindible que la información esté protegida con un nivel de seguridad lo más elevado posible .

Para llevar a cabo dicha necesidad, las empresas u organizaciones se apoyan en el uso de herramientas, metodologías o estándares que apoyan la gestión de la seguridad informática. Estos proporcionan mecanismos de seguridad, indispensables si se desea un manejo adecuado de la información [1].

En nuestro país, la gestión de riesgos y la seguridad informática son áreas fundamentales que poco se han estudiado o dicho de otra manera no se ha indagado demasiado en cuanto a estos ámbitos se refiere, a pesar de ser dos de los principales puntos a tomar en cuenta dentro de cualquier empresa o institución en la cual se maneje un sistema informático.

Con el afán de aprovechar dichas falencias, cada momento, se desarrollan nuevos métodos que afectan la seguridad de la información por lo cual se hace necesario realizar un análisis de dichas amenazas y definir un sistema de gestión de seguridad de la información que ayuden a minimizar los riesgos asociados al

acceso y utilización de determinado sistema de forma no autorizada y en general malintencionada, minimizando así el porcentaje de riesgo.

Los distintos departamentos, distritos y coordinaciones zonales de educación manejan información sumamente importante como por ejemplo la información personal académica de cada uno de los estudiantes de la ciudad. Por tal motivo se hace indispensable que ésta tome en cuenta aspectos trascendentales como son: confidencialidad, integridad y disponibilidad.

Actualmente el distrito 18D01 de Educación no cuenta con ningún estándar implementado, únicamente toma ciertas medidas preventivas las cuales no garantizan la correcta gestión y seguridad de la información, por lo que personas o entidades mal intencionadas podrían tener acceso a datos que se manejan internamente y hacer uso inadecuado de los mismos.

Para el desarrollo del mismo se tomarán como guía las Normas ISO 27000, específicamente la ISO 27001. Estos estándares nos brindan las pautas referentes a la gestión de la seguridad, haciendo énfasis en tres aspectos mencionados anteriormente: confidencialidad, disponibilidad e integridad de la información.

1.3 Delimitación

1.3.1 De contenidos

Línea de Investigación:

- Normas y Estándares

Sublínea de Investigación:

- Seguridad de Unidades Informáticas.

1.3.2 Espacial

La presente investigación se desarrollará en el "Departamento de Tecnologías de la Información y Comunicación del Distrito 18D01 de Educación".

1.3.3 Temporal

La presente investigación se desarrollará en el periodo académico: octubre/2016 – marzo/2017.

1.4 Justificación

La información es un recurso de vital importancia para el Ministerio de Educación, por tal motivo se debe gestionar de manera eficiente la seguridad de la misma, más aun cuando en nuestro entorno han aparecido graves amenazas para los sistemas informáticos con lo cual se corre el riesgo de que dicha información sea robada o usada inapropiadamente.

Es así que la elaboración e implantación de un SGSI basada en la ISO 27001 aportará de manera substancial al adecuado manejo y gestión de la información en el Distrito 18D01 de Educación, el cual no cuenta con una metodología de gestión adecuada de la información.

Al hablar de seguridad de la información existen diversos estándares aplicables pero para el presente proyecto se ha optado por las normas ISO 27001 debido a que las mismas son las más apropiadas para cumplir con el objetivo de crear una estructura de la seguridad de la información para el Distrito de Educación. En futuros proyectos se podría optar por el uso de normas como la 27002 o 27005 con el propósito de implementar controles o realizar una evaluación y tratamiento de riesgos.

Los beneficios más importantes que alcanzará el Distrito de Educación con la implementación del SGSI serán integridad, confidencialidad y disponibilidad de la información. Además la correcta gestión de la misma producirá una serie de ventajas para la institución debido a que una administración adecuada y efectiva se traduce en mayor eficiencia de los procesos que se llevan a cabo en la institución.

Por lo expuesto anteriormente se justifica el desarrollo del presente proyecto, el mismo que de ser aplicado brindará un aporte de suma importancia para el distrito de Educación.

1.5 Objetivos

1.5.1 Objetivo General

- Implementar un Sistema de Gestión de Seguridad de la Información bajo parámetros de las normas ISO/IEC 27001, para el mejoramiento de la seguridad de la información en el Distrito 18D01 de Educación.

1.5.2 Objetivos Específicos

- Evaluar los mecanismos que se llevan a cabo actualmente para el tratamiento de la información y control de vulnerabilidades.

- Desarrollar el Sistema de Gestión de la Seguridad de la Información en base a parámetros de la Norma ISO/IEC 27001 lo cual disminuya la probabilidad y ocurrencia de amenazas.

- Establecer una metodología de gestión y mejora continua del SGSI lo cual garantice un adecuado tratamiento de la información.

CAPÍTULO 2

MARCO TEÓRICO

2.1 Antecedentes Investigativos

- Klever Ibán Tipán Guayta en su proyecto de investigación "Propuesta de Políticas de Seguridad de la Información para la CORPAIRE", creado en la Escuela Politécnica Nacional, lleva a cabo un análisis y evaluación de los riesgos informáticos para posteriormente elaborar políticas de seguridad a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la organización [2].

- Silvia Zurita Manosalvas en su proyecto de investigación "Políticas de seguridad y los riesgos informáticos en industria catedral s.a. de la ciudad de Ambato durante el año 2010" determina el impacto de riesgos en los activos informáticos en la organización y basándose en ello propone políticas de seguridad para salvaguardar dicha información. Además afirma que la falta de una cultura informática en los usuarios se ha convertido en uno de los principales factores para poner en riesgo la información que se maneja [3].

- Juan Honorato Mazzinghi en su artículo "Gestión del riesgo en la seguridad informática: el nuevo escenario del control", saca a la luz aspectos de gran importancia acerca de las políticas de seguridad y manejo del riesgo en los órganos de la administración del estado en Chile, así como aspectos relativos al diseño y puesta en marcha de un sistema de gestión de riesgo en la Seguridad Informática [4].

- Jeime J. Cano en su artículo presentado en la revista de Ingeniería de la Universidad de Los Andes plantea realizar un análisis actual dentro de cada organización, lo cual contribuya a fortalecer sus esquemas de seguridad, no para contar con mayores niveles de seguridad, sino para evidenciar el nivel de dificultad que deben asumir los intrusos para ingresar a los sistemas [5].

- Mauricio Baldeón Garzón y Christian Coronel Guerrero presentan una propuesta formal para implementar políticas y controles de buenas prácticas que recomienda la Norma ISO/IEC 27002 enfocado a dos procesos de la UTIC: Base de Datos y Redes y Comunicaciones. Además mencionan que las mejores prácticas de TI y el uso de políticas y controles son muy importantes dentro de las organizaciones para alcanzar objetivos estratégicos institucionales, además de alcanzar una gestión eficaz de las actividades que realiza el personal de TI [6].

2.2 Fundamentación Teórica

2.2.1 Seguridad de la información

- **Definición**

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma [7].

De esta manera los tres pilares fundamentales de la seguridad de la información son [8]:

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

La seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia. Se entiende como seguridad un estado de cualquier sistema o tipo de información (informático o no) que nos indica que ese sistema o información está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar a su funcionamiento directo o a los resultados que se obtienen [7].

- **Riesgos**

En la gestión de riesgos existe un factor de incertidumbre asociado con la probabilidad de que aparezcan las amenazas. Es decir que la amenaza solo se puede predecir dentro de ciertos límites [9].

Un incidente no deseado presenta tres componentes: amenaza, vulnerabilidad e impacto. Las vulnerabilidades indican la debilidad del activo que puede ser aprovechada por una amenaza.

Estos riesgos se contrarrestan con la implantación de políticas, es decir medidas que se deben llevar a cabo para cumplir con dicho objetivo.

- **Tipos de Seguridad**

  - **Activa**

    Es un conjunto de medidas que se implementan con el fin de minimizar la repercusión debida a un incidente de seguridad y permitir la recuperación del sistema. A estas medidas también se las denomina "de corrección" [10].

  - **Pasiva**

    Son los mecanismos y procedimientos que permiten prevenir y detectar riesgos para la seguridad del sistema de información [10].

    Tanto la seguridad activa como pasiva se aplica tanto a los elementos físicos como lógicos que componen el sistema de información [10].

2.2.2 Normas ISO

- **Definición**

ISO (Organización Internacional para la Normalización) es una red mundial que identifica cuáles normas internacionales son requeridas por el comercio, los

gobiernos y la sociedad; las desarrolla conjuntamente con los sectores que las van a utilizar; las adopta por medio de procedimientos transparentes basados en contribuciones nacionales proveniente de múltiples partes interesadas; y las ofrece para ser utilizadas a nivel mundial [11].

Las normas ISO están basadas en un consenso internacional conseguido de la base más amplia de grupos de partes interesadas. La contribución de expertos proviene de aquellos más cercanos a las necesidades en materia de normas y de los resultados de su implementación [11].

- **Normas ISO 27000**

La serie de normas ISO/IEC 27000 se denomina "Requisitos para la especificación de sistemas de gestión de la seguridad de la información (SGSI)".

Proporciona un marco de estandarización para la seguridad de la información para que sea aplicado en una organización o empresa y comprende un conjunto de normas sobre las siguientes materias [12]:

- Sistema de gestión de la seguridad de la información.
- Valoración de riesgos.
- Controles.

- **ISO 27001**

La norma 27001 abarca un conjunto de normas relacionadas con la seguridad informática. Según esta norma que es la principal de la serie, la seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento [13].

El modelo del sistema de gestión de la seguridad de la información ISO 27001 sigue la estructura PHVA (planear – hacer – verificar - actuar). El proceso inicia con la planificación del alcance del SGSI, determinando las áreas o procesos de las organizaciones en los que se va a aplicar el sistema [13].

Generalmente se eligen las áreas más críticas o vulnerables en materia de gestión de la información. Luego de definido el alcance, se debe formular y divulgar una política de la gestión de la seguridad de la información, que establezca los lineamientos generales que la organización debe tener en cuenta frente a los riesgos de la información, considerando en ello los requisitos legales, contractuales y propios de la empresa [13].

EL eje central de la planificación del SGSI consiste en identificar los riesgos de la información, en relación con las posibles amenazas y los puntos vulnerables de la organización en cuanto a la confiabilidad, seguridad y disponibilidad de la información [13].

A partir de la identificación de estos riesgos, y de su análisis y valoración, se definirán los planes de control o tratamiento de riesgo. Incluye también la documentación y la aplicación de los procedimientos necesarios para aplicar tales controles, así como la formación y la concienciación de los empleados respecto a la seguridad de la información y los controles que se han de aplicar [13].

La verificación incluye la medición del desempeño del SGSI, la evaluación de los riesgos y la eficacia de los controles implementados, la realización de auditorías internas al sistema y la recisión del mismo por parte de la dirección [13].

- **Áreas o Dominios de Seguridad de la ISO/IEC 27001** [14]

1. Políticas de seguridad.
2. Organización de seguridad.
3. Administración de activos.
4. Seguridad de los recursos humanos.
5. Seguridad física y ambiental.
6. Gestión de comunicaciones y operaciones.
7. Sistema de control de accesos.

8. Adquisición, desarrollo y mantenimiento de sistemas de información.
9. Administración de incidentes de seguridad de la información.
10. Plan de continuidad del negocio.
11. Cumplimiento.
12. Gestión de incidentes en la seguridad de la información.
13. Aspectos de seguridad de la información en la gestión de continuidad del negocio.
14. Cumplimiento.

- **Etapas de la seguridad de la información**

Todo sistema de gestión de seguridad se basa en el conocido ciclo de DEMING (PDCA). Es una estrategia de mejora continua de la calidad la cual se basa en cuatro fases: planear, hacer, verificar y actuar. La estructura completa se puede observar en la figura:

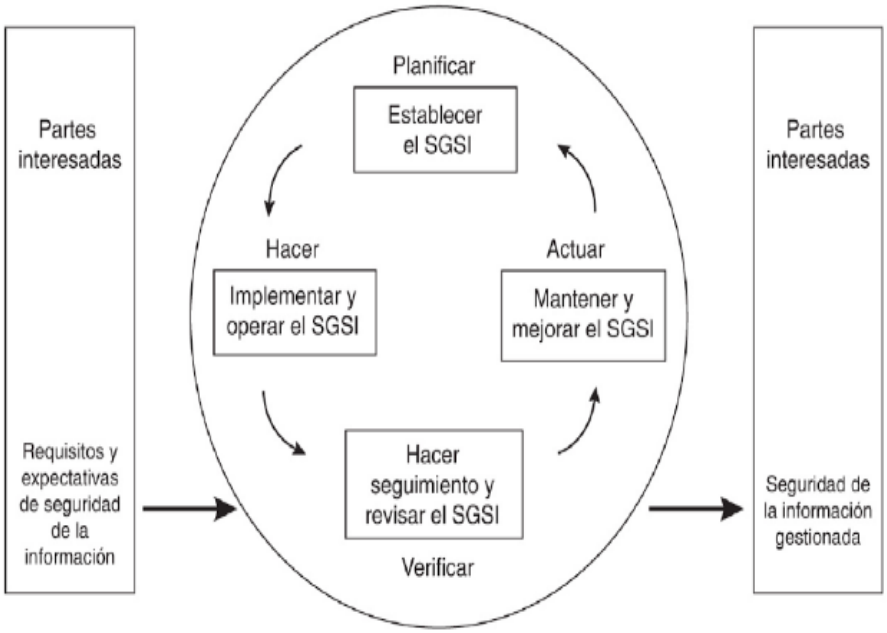


Fig. 1 Modelo del SGSI de la norma ISO 27001[13]

a) **Planificación.-** La dirección toma conciencia de la situación actual real mediante la recolección y análisis de datos.

b) **Hacer.-** Consiste en la implementación de procesos a partir del análisis y planificación previos.

c) **Verificar.-** Consiste en la monitorización y evaluación de los procesos y de los resultados, relacionándolos con los objetivos y especificaciones planteados inicialmente.

d) **Actuar.-** Se realizan las correcciones necesarias y se realiza la estandarización de los cambios con el propósito de garantizar el mejoramiento continuo de los procesos [15].

2.3 Propuesta de solución

Este proyecto plantea la implementación de un SGSI basado en la Norma ISO/IEC 27001, el cual mediante una planificación estructurada, servirá como plan de acción para el mejoramiento de la seguridad, con el fin de alcanzar un alto grado de eficiencia en las actividades de resguardo y protección de la información. Además se busca abrir el camino para la certificación ISO/IEC 27001 del Distrito 18D01 de Educación.

CAPÍTULO 3

METODOLOGÍA

3.1 Modalidad de Investigación

La presente investigación se contextualizará en la modalidad de campo y documental – bibliográfica.

Investigación de Campo, debido que se realiza la investigación en el lugar en el que se presenta el problema es decir el Distrito de Educación, determinando de mejor manera los inconvenientes que se presentan dentro de la misma y documental-bibliográfica, ya que se utilizarán fuentes como libros, artículos y bibliotecas virtuales, los mismos que brindarán un aporte vital tanto para la identificación y análisis de las amenazas informáticas como para la elaboración de un modelo de gestión adecuado que garantice un adecuado tratamiento de la información dentro de la Institución.

3.2 Población y muestra

3.2.1 Población

Para la presente investigación se tomó como población al personal del departamento de tecnologías de la información y comunicación del distrito 18D01 de Ambato.

3.2.2 Muestra

No es necesario realizar un muestreo debido a que la población es reducida y se puede acceder a ella sin restricciones. Por tanto la muestra viene a ser la misma población definida anteriormente [16].

3.3 Recolección de Información

Para la recolección de información se utilizarán fuentes bibliográficas como libros, artículos técnicos, etc. relacionado con la temática propuesta con los cuales se pretende tener una idea general sobre el impacto que tendrá el proyecto planteado.

Se realizará una observación de campo debido a que será necesaria una inspección de la infraestructura de red y la arquitectura de los sistemas informáticos que se manejan con su respectiva documentación.

Además esta investigación se apoya en la realización de una entrevista estructurada mediante cuestionarios de evaluación elaborados en base a estándares de seguridad informática, dirigida al personal del departamento de Tecnologías de Información y Comunicación del Distrito de Educación, con el fin de conocer los procesos que se realizan a diario de manera que no se omita ningún aspecto relevante en la investigación.

3.4 Procesamiento y análisis de datos

El plan para el procesamiento y análisis de la información es el siguiente:

- Revisión crítica de la información recogida.
- Organización de la información.
- Interpretación de los resultados obtenidos los cuales contribuirán a desarrollar la solución para el problema planteado.

3.5 Desarrollo del Proyecto

Para cumplir el desarrollo del proyecto de investigación, se llevaran a cabo de forma secuencial las siguientes actividades:

1. Evaluar los mecanismos que se llevan a cabo actualmente para el tratamiento de la información y control de vulnerabilidades

    - Análisis de la situación actual de la institución.
    - Evaluación de resultados de la encuesta aplicada.

2. Desarrollar el Sistema de Gestión de Seguridad de la Información en base a parámetros de la Norma ISO/IEC 27001 lo cual disminuya la probabilidad y ocurrencia de amenazas.

- Gestión de riesgos.
- Declaración de aplicabilidad.
- Implementación de procedimientos y controles para la gestión de incidentes de seguridad de la información.

3. Establecer una metodología de evaluación y mejoramiento continuo del SGSI lo cual garantice un adecuado tratamiento de la información.

    - Monitorización e implementación de mejoras.

CAPÍTULO 4

DESARROLLO DE LA PROPUESTA

Antes de llevar a cabo la implementación del sistema de gestión de seguridad, es importante aclarar que no necesariamente se asocia el término "sistema" con la implementación o desarrollo de una aplicación informática.

De forma general el término sistema hace relación a un conjunto de normas y procedimientos relacionados entre sí para contribuir a la consecución de un objetivo.

Para llevar a cabo la implementación del Sistema de Gestión de Seguridad se ha adoptado el ciclo de Deming o también llamado de mejora continua (PDCA), cuyas fases de desarrollo se detallan a continuación.

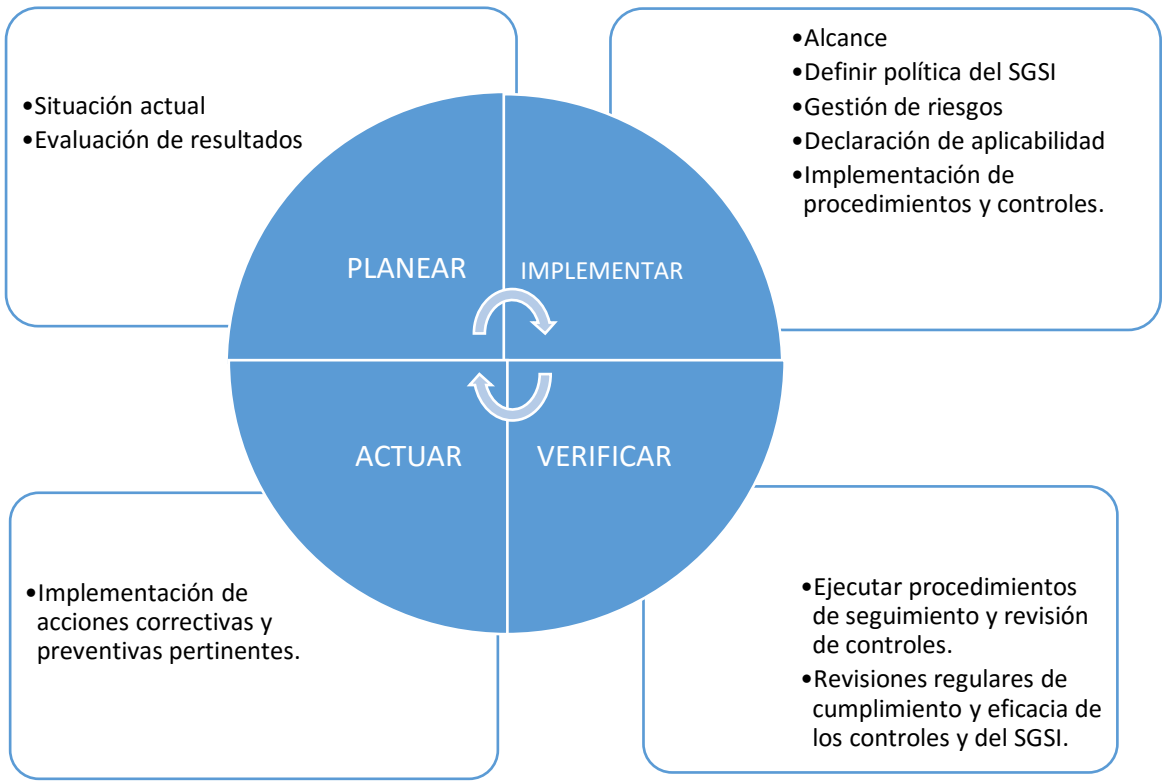


Fig. 2 Metodología de aplicación – ciclo de Deming

Elaborado por: Investigador

4.1. Planeación

4.1.1 Análisis de la situación actual

El punto más importante para el desarrollo del proyecto de investigación es determinar la situación actual del Distrito 18D01 respecto a la gestión de seguridad de la información.

El primer paso es la aplicación de una entrevista al responsable del área de sistemas con el objetivo de recolectar datos y de esta manera conocer la forma en que se maneja la información actualmente por parte del departamento de tecnología.

Luego será importante realizar un análisis de la entrevista para tener un punto de partida y realizar una gestión adecuada, haciendo énfasis en aquellos puntos negativos desde el punto de vista del manejo correcto de la información.

La entrevista en mención se la realizó al Ingeniero Diego Silva, director del departamento de Tecnologías de Información y Comunicación, con lo que se pudo comprobar que el Distrito 18D01 de Educación no sigue un plan o sistema de gestión de seguridad para manejar adecuadamente la información.

TABLA DE PREGUNTAS - RESPUESTAS

Encuestado / **Pregunta**	**Administrador del departamento de sistemas.**
1. ¿Se aplican actualmente políticas de seguridad para gestionar la información? Si ( ) Enúncielas No ( )	Si. Se aplican ciertas políticas como por ejemplo: ▪ Acceso a recursos compartidos con gestión de usuarios. ▪ Limitación de acceso a internet con restricción. ▪ Restricción de acceso a equipos de comunicación. ▪ Restricción de instalación y modificación en el sistema operativo.

2. ¿Están definidas responsabilidades del personal en cuanto al uso adecuado de los recursos?	Las responsabilidades las conoce cada funcionario por socialización. Sin embargo no existe un documento de aval.
3. ¿Existe un control sobre el acceso no autorizado de personal con la finalidad de proteger el equipamiento y sistemas que se manejan en la institución?	Si. Solamente personal autorizado tiene acceso ya sea a equipos o programas. El resto del personal de la institución tiene restricción en cuanto al acceso.
4. ¿Se realiza un mantenimiento periódico de los equipos de institución?	Si, existe un plan de mantenimiento anual de los equipos.
5. ¿Se han realizado simulacros de caídas de los sistemas que manejan?	No, no existe un plan de contingencia para realizar un simulacro.
6. ¿Se realizan tareas de monitoreo a los sistemas de información que manejan?	▪ Los sistemas de información son manejados en planta central. Cada unidad Distrital es un usuario de los sistemas del MINEDUC. ▪ El monitoreo se lo realiza a los equipos de comunicación y servidor de archivos.
7. ¿Se realiza gestión de riesgos en cuanto a la seguridad de la información?	No. Lamentablemente no disponemos de un plan de contingencia ante eventualidades que puedan ocurrir.
8. ¿Qué mecanismos o técnicas de seguridad se aplican a los sistemas de información y comunicación?	▪ Firewall, NAT. ▪ Control de usuarios

9. Dispone de un control sobre el inventario de los activos informáticos existentes en la institución?	Si, existe un inventario donde constan todos los activos físicos y lógicos a nuestro cargo sobre los cuales llevamos un control.

Tabla 1. Desarrollo de preguntas - entrevista

Elaborado por: Investigador

4.1.2. Evaluación de la Entrevista aplicada:

Después de realizar la entrevista al director del departamento de tecnologías se puede concluir lo siguiente:

- Se aplican ciertas políticas para gestionar la información pero éstas son hasta cierto punto básicas como la gestión de usuarios, limitación en cuanto al uso de internet, etc. las cuales no son suficientes para garantizar que la información esté asegurada.

- No existe un documento formal donde consten responsabilidades de los funcionarios respecto a los equipos, es decir no están definidas formalmente. Únicamente se socializa a aquellos funcionarios que tienen cierta responsabilidad de algún recurso lo cual no es aconsejable.

- Un punto positivo es que se lleva un control de acceso de los usuarios hacia el equipamiento de la institución por lo que en cierta medida el mismo se encuentran protegido contra usuarios malintencionados.

- El mantenimiento de equipos se realiza anualmente. Actualmente se encuentra en desarrollo un plan para brindar mantenimiento a los equipos periódicamente con lo cual se espera mejorar el rendimiento de los mismos.

- Actualmente en el Distrito 18D01 de Educación únicamente se realiza el monitoreo de los equipos de comunicación físicos que disponen. Lamentablemente no se pueden monitorear ciertos sistemas que manejan ya que existe cierta restricción por parte de planta central en la ciudad de Quito.

- No existe un plan de contingencia ante caídas de los sistemas que manejan.

Tampoco se realiza una gestión de riesgos ante eventualidades como robos o ataques de la información que manejan por parte de personas malintencionadas.

4.2. Implementación

A continuación se presenta el SGSI, un modelo estructurado de carácter preventivo cuyo objetivo es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por el Distrito de Educación de una forma eficiente y estructurada.

El Sistema de Gestión de Seguridad propuesto consta de las siguientes etapas:

- Alcance
- Definir política del SGSI
- Gestión de riesgos
- Declaración de aplicabilidad
- Implementación de procedimientos y controles

Cabe mencionar que las mismas serán desarrolladas en base a los dominios y controles de la ISO 27001.

4.2.1 Definición del Alcance

Será necesario realizar la definición del alcance en base a las características de la institución, tomando en cuenta aspectos trascendentales como activos, organización, recursos, etc.

Una vez elaborada la definición del alcance, la responsabilidad de la misma correrá a cargo del director del distrito, asesorado por el departamento de tecnología.

El distrito 18D01 de Educación define el alcance del SGSI a los servicios y sistemas que manejan información relacionada con los procesos cotidianos de la institución.

Para facilitar la comprensión de los procesos que contempla el alcance, a continuación se detallan los servicios hacia los que está orientado el mismo:

- Mantenimiento preventivo tanto del equipamiento físico como de los diferentes sistemas que se manejan (hardware & software).- Se realizará una revisión periódica de ciertos aspectos de hardware y software,

orientado a mantener un desempeño fiable tanto de equipos como sistemas manteniendo siempre la integridad de los datos almacenados.

- Gestión de recursos humanos.- El personal deberá estar comprometido con la salvaguarda de la información. Se definirán responsabilidades de gestión así como lineamientos para garantizar la seguridad de recursos e información durante el periodo laboral además de la fase posterior o de terminación o cambio de empleo.

- Gestión de activos.- Uno de los apartados de mayor importancia es sin duda la gestión de los activos propiedad del Distrito de Educación. Se establecerán parámetros como la definición de responsabilidades por los mismos y la regulación del uso adecuado, obviamente luego de realizada la gestión completa de los mismos respecto a riesgos y vulnerabilidades potenciales.

- Control de acceso.- Es necesaria la verificación de identidad de un funcionario para que tenga acceso a un determinado recurso físico o lógico, manteniendo así la confidencialidad e integridad de la información.

- Gestión de operaciones y comunicaciones. Para garantizar la disponibilidad de la información y evitar que la institución se arriesgue a detener sus procesos se definirán herramientas procedimientos para garantizar el correcto funcionamiento y operación de los mismos a través de lineamientos.

Cabe mencionar que la definición del alcance está a cargo de la dirección del distrito de Educación y el departamento de TICS brindará soporte y apoyo en los diversos servicios y procesos mencionados.

4.2.2 Política de seguridad del SGSI

Se define la siguiente política de seguridad para la implementación del Sistema de Gestión de Seguridad de la Información, la cual cubre de manera general la mayoría de necesidades relacionadas a la gestión de seguridad de la información:

"Promover prácticas que aseguren la continuidad de las funciones del distrito 18D01 de Educación mediante un Sistema de Gestión de Seguridad de la Información basado en un control preventivo y enfocado a lograr un nivel adecuado de integridad, confidencialidad y disponibilidad de la información institucional relevante".

Objetivos:

Se han definido objetivos para asegurar el cumplimiento de la política mencionada:

- Establecer controles para para prevenir vulnerabilidades referentes a la seguridad de la información.
- Definir un plan de gestión de control y gestión de riesgos de la información.
- Implementar el sistema de gestión de seguridad de la información.
- Monitorizar el SGSI para garantizar el adecuado tratamiento de la información.

4.2.3 Gestión de Riesgos

Es importante analizar y evaluar el impacto que tienen los riesgos para la institución teniendo en consideración las posibles consecuencias que afecten a los procesos que se llevan a cabo y más aún si en ellos se maneja información de suma importancia.

La finalidad de este proceso es determinar si un determinado riesgo es aceptable o caso contrario buscar y aplicar un tratamiento adecuado para mitigarlo.

Para la realización de este apartado se ha definido una metodología con la cual se dará cumplimiento al análisis y evaluación de riesgos.

Consiste en un método cualitativo donde se detallan todos los activos pertenecientes a la institución y se identifican las amenazas relacionadas con los mismos y su probabilidad de ocurrencia; a partir de ello se detallan vulnerabilidades que podrían causar que dichas amenazas se efectúen o materialicen.

A continuación se presenta un esquema de la metodología a utilizar:

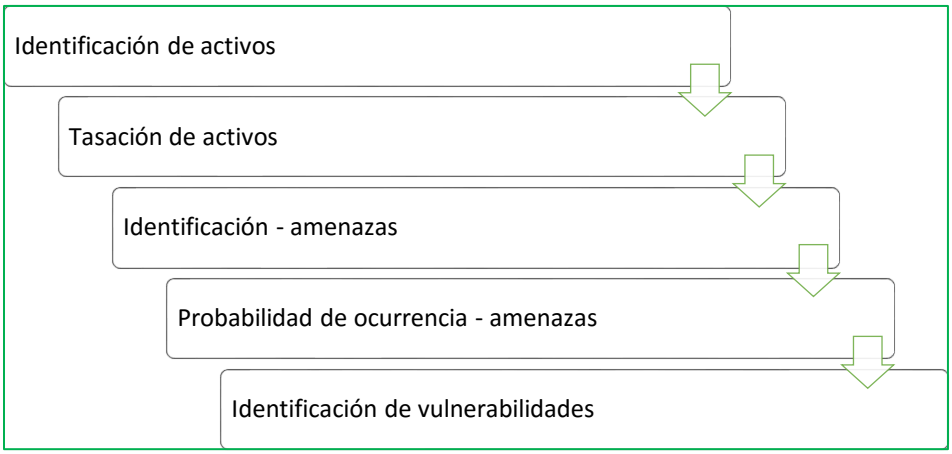


Fig. 3 Metodología para la gestión de riesgos

Elaborado por: Investigador

- Identificación de activos:

  Todos los activos con que cuenta la institución tienen un valor significativo debido a que contiene o manipula información y por tanto es imprescindible brindarle una protección adecuada.

  Luego de identificar todos los activos se procede a tasarlos con el objetivo de gestionar aquellos considerados como "más importantes" o de "mayor relevancia" en cuanto al desarrollo de las actividades del distrito se refiere, basándonos en el nivel de afectación respecto a la confidencialidad, integridad y disponibilidad de la información.

- Una vez identificados los activos considerados de "mayor importancia" se identifican tanto amenazas como vulnerabilidades y a partir de ello se determina el nivel de afectación sobre los activos de la institución.

- Posteriormente se procede a evaluar y determinar la probabilidad real de ocurrencia de dicha amenaza tomando en cuenta las consecuencias o el impacto que tendrán en caso de materializarse lo cual supone un riesgo respecto a la confidencialidad, integridad y disponibilidad de la información.

- Finalmente el valor del riesgo se obtiene del producto entre el valor del activo según la tasación realizada por el valor de la probabilidad de amenaza.

- INVENTARIOS DE ACTIVOS INFORMÁTICOS:

Uno de los pasos importantes para la realización del SGSI es el análisis y gestión de riesgos de los activos que participan en los procesos de la Institución.

Para cada activo identificado se asignó un código dependiendo del tipo de activo ya sea físico, de tipo software o sistema de información.

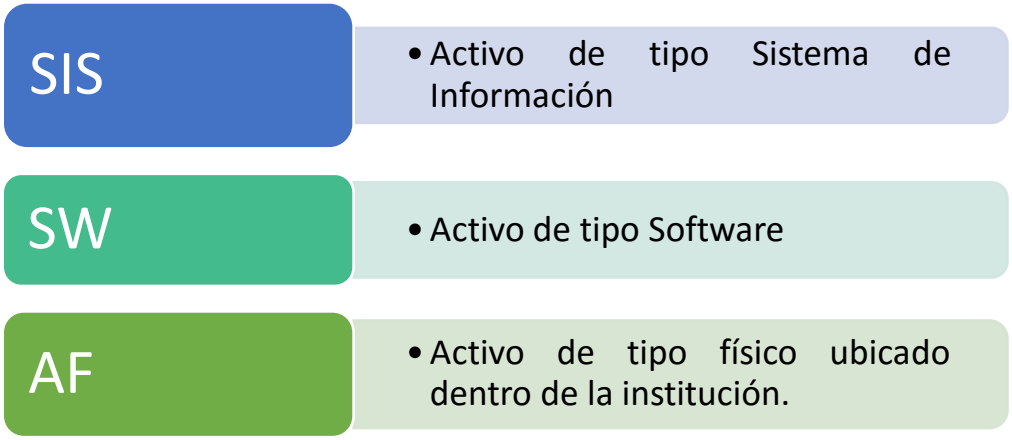


Fig. 4 Nomenclatura Activos de Información

- IDENTIFICACIÓN DE ACTIVOS INFORMÁTICOS:

Id	Activo	Características
AF-01	Servidor de Archivos	• Marca: HP • Procesador: Intel XEON • Memoria RAM: 16 GB • Disco duro: 640 GB
AF-02	Ordenadores	• Cantidad: 55 • Procesador: Intel Core I3 • Memoria RAM: 2 GB • Disco duro: 500 GB
AF-03	Switch	• Marca: TP Link • Cantidad de puertos: 24
AF-04	Router	Marca: Mikrotik
AF-05	Central Telefónica IP	SIP PBX (Private Branch Exchange)

AF-06	Impresoras Multifunción	• Modelo: Xerox Phaser 3635MFP • Velocidad de impresión: 35 x minuto • Funciones: Copia, Correo electrónico, Impresión, Escaneado
SIS-01	QUIPUX (Sistema de Gestión Documental)	Para la elaboración de memorando, oficios, circulares y todo lo que implica comunicación formal dentro y fuera de la institución.
SIS-02	MOGAC (Módulo de Gestión de Atención Ciudadana Inicio de Sesión)	Permite acceder a los trámites de las Direcciones Distritales del Ministerio de Educación de educación de forma virtual.
SIS-03	Sistema de Activos Tecnológicos	• Manejo de inventarios de hardware y software. • Medición del uso de software. • Análisis de licenciamiento.
SW-01	Correo Institucional	• Microsoft Exchange Server • Microsoft Outlook 2010
SW-02	Cuentas de Usuario	Cuentas de usuario en el servidor con Sistema Operativo Windows Server 2012.

Tabla 2 Identificación de Activos Informáticos

Elaborado por: Investigador

Para identificar los riesgos se procede a evaluar cada uno de los activos según el nivel tanto de confidencialidad, disponibilidad e integridad que brindan para el aseguramiento de la información en un rango entre 1 y 5.

Activo	Confidencialidad	Disponibilidad	Integridad	Total
Servidor de Archivos	4	4	3	4
Ordenadores	3	4	2	3
Switch	2	4	3	3
Router	2	3	3	3

Central Telefónica IP	4	4	4	4
Impresoras Multifunción	3	4	2	3
QUIPUX (Sistema de Gestión Documental)	3	3	4	3
MOGAC (Módulo de Gestión de Atención Ciudadana)	4	3	4	4
Sistema de Activos Tecnológicos	4	4	3	4
Correo Institucional	2	3	2	2
Cuentas de Usuario	4	4	3	4

Tabla 3 Identificación de riesgos

Elaborado por: Investigador

A partir de la tabla anterior se determinan aquellos activos cuyo valor es mayor o igual a 3 para realizar la evaluación de riesgos.

Activo	Total
Servidor de Archivos	4
Ordenadores	3
Switch	3
Router	3
Central Telefónica IP	4

Impresoras / Copiadoras	3
QUIPUX (Sistema de Gestión Documental)	3
MOGAC (Módulo de Gestión de Atención Ciudadana)	4
Sistema de Activos Tecnológicos	4
Cuentas de Usuario	4

Tabla 4 Activos de mayor importancia

Elaborado por: Investigador

Activo	Amenazas	Vulnerabilidades	Valoración del activo (1-5)	Probabilidad de ocurrencia de la amenaza (1-5)	Total Riesgo
Servidor de Archivos	Alteración de información	Ausencia de medidas de seguridad	4	3	12
	Robo de información	Falta de Mantenimiento			
Ordenadores	Apagones del ordenador	Daño fuente de alimentación	3	4	12
	Virus	Falta de Mantenimiento			
	Malware	Falta de control en la red			
		Uso inadecuado de internet			
	Phishing	Falta de capacitación a los usuarios sobre técnicas de ataques informáticos			
		Falta de herramientas anti-phishing			
	Denegación de servicio	Falta de monitoreo de routers y firewall			

Activo	Amenazas	Vulnerabilidades	Valor del activo	Probabilidad de ocurrencia (1-5)	Total Riesgo
Switch	Recalentamiento	Cambios del suministro eléctrico	3	3	9
	Daño o pérdida total				
	Bajo rendimiento	Falta de mantenimiento			
Router	Recalentamiento	Cambios del suministro eléctrico	3	3	9
	Bajo rendimiento	Falta de Mantenimiento			
	Conexión intermitente	Mala ubicación del dispositivo			
Central Telefónica IP	Pérdida de conexión	Mala administración de la central telefónica	4	3	12
Impresoras / Copiadoras	Daño de cartuchos	Falta de mantenimiento	3	4	12
	Daño de cabezales				
	Atascamiento de papel	Carga incorrecta de papel			
		Uso de papel inadecuado			

Activo	Amenazas	Vulnerabilidades	Valor del activo	Probabilidad de ocurrencia (1-5)	Total Riesgo
QUIPUX (Sistema de Gestión Documental)	Robo de información	Falta de políticas de seguridad	3	3	9
		Falta de control de acceso			
MOGAC (Módulo de Gestión de Atención Ciudadana)	Robo de información	Falta de políticas de seguridad	4	3	12
		Falta de control de acceso			
Sistema de Activos Tecnológicos	Robo de información	Falta de políticas de seguridad	4	3	12
		Falta de control de acceso			
Cuentas de Usuario	Alteración o eliminación de cuentas	Falta de control de acceso	4	3	12
		Mala administración			

Tabla 5 Activos de mayor importancia

Elaborado por: Investigador

Luego de realizar el análisis y evaluación de riesgo de los principales activos de la institución identificando además las amenazas con su probabilidad de ocurrencia se pueden determinar aquellos con mayor probabilidad de afectación, ya sea por motivo de daños, ataques, vulnerabilidades, etc.

Selección de objetivos de control:

El siguiente paso para el desarrollo del SGSI es relacionar los controles definidos por la norma ISO 27001 con los activos de mayor valoración en cuanto al factor riesgo reflejados en las tablas anteriores.

A continuación se enuncian las 11 áreas o dominios que conforman la norma ISO27001 [14]:

A.1 Políticas de seguridad.

A.2 Organización de seguridad.

A.3 Administración de activos.

A.4 Seguridad de los recursos humanos.

A.5 Seguridad física y ambiental.

A.6 Gestión de comunicaciones y operaciones.

A.7 Sistema de control de accesos.

A.8 Adquisición, desarrollo y mantenimiento de sistemas de información.

A.9 Administración de incidentes de seguridad de la información.

A.10 Plan de continuidad del negocio.

A.11 Cumplimiento.

La columna “Objetivo de control” contiene el dominio que se relaciona con la posible amenaza de cada activo informático detallado:

Activo	Amenazas	Vulnerabilidades	Valoración del activo (1-5)	Probabilidad de ocurrencia de la amenaza (1-5)	Total Riesgo	Objetivo de Control
Servidor de Archivos	Alteración de información	Ausencia de medidas de seguridad	4	3	12	• A.11 CONTROL DE ACCESO
	Robo de información	Falta de Mantenimiento				
Ordenadores	Apagones del ordenador	Daño fuente de alimentación	3	4	12	• A.7 GESTIÓN DE ACTIVOS • A.9 SEGURIDAD FÍSICA Y AMBIENTAL • A.10 GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES.
	Virus	Falta de Mantenimiento				
	Malware	Falta de control en la red				
		Uso inadecuado de internet				
	Phishing	Falta de capacitación a los usuarios sobre técnicas de ataques informáticos				
		Falta de herramientas anti-phishing				
	Denegación de servicio	Falta de monitoreo de routers y firewall				

Activo	Amenazas	Vulnerabilidades	Valor del activo	Probabilidad de ocurrencia (1-5)	Total Riesgo	Objetivo de Control
Switch	Recalentamiento	Cambios del suministro eléctrico	3	3	9	• A.7 GESTIÓN DE ACTIVOS • A.8 SEGURIDAD FÍSICA Y AMBIENTAL
	Daño o pérdida total					
	Bajo rendimiento	Falta de mantenimiento				
Router	Recalentamiento	Cambios del suministro eléctrico	3	3	9	• A.7 GESTIÓN DE ACTIVOS • A.8 SEGURIDAD FÍSICA Y AMBIENTAL
	Bajo rendimiento	Falta de Mantenimiento				
	Conexión intermitente	Mala ubicación del dispositivo				
Central Telefónica IP	Pérdida de conexión	Mala administración de la central telefónica	4	3	12	• A.10 GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES
Impresoras / Copiadoras	Daño de cartuchos	Falta de mantenimiento	3	4	12	• A.9 SEGURIDAD FÍSICA Y AMBIENTAL.
	Daño de cabezales					
	Atascamiento de papel	Carga incorrecta de papel				
		Uso de papel inadecuado				

Activo	Amenazas	Vulnerabilidades	Valor del activo	Probabilidad de ocurrencia (1-5)	Total Riesgo	Objetivo de Control
QUIPUX (Sistema de Gestión Documental)	Robo de información	Falta de políticas de seguridad Falta de control de acceso	3	3	9	• A.6 GESTIÓN DE COMUNICACIONES Y OPERACIONES. • A.7 SISTEMA DE CONTROL DE ACCESOS.
MOGAC (Módulo de Gestión de Atención Ciudadana)	Robo de información	Falta de políticas de seguridad Falta de control de acceso	4	3	12	• A.6 GESTIÓN DE COMUNICACIONES Y OPERACIONES. • A7 SISTEMA DE CONTROL DE ACCESOS.
Sistema de Activos Tecnológicos	Robo de información	Falta de políticas de seguridad Falta de control de acceso	4	3	12	• A.6 GESTIÓN DE COMUNICACIONES Y OPERACIONES. • A.7 SISTEMA DE CONTROL DE ACCESOS.
Cuentas de Usuario	Alteración o eliminación de cuentas	Falta de control de acceso Mala administración	4	3	12	• A.7 SISTEMA DE CONTROL DE ACCESO

Tabla 5 Selección de controles

Elaborado por: Investigador

4.2.4 Declaración de Aplicabilidad

A continuación se desarrolló la declaración de aplicabilidad (SOA) donde se detallan los controles relevantes y aplicables a la situación actual del Distrito de Educación, apoyados en la norma ISO/IEC 27002, la misma es la versión mejorada en cuanto a controles que la ISO 27001.

El proceso consiste en listar aquellos controles de seguridad que resulten factibles implementar en la institución, así como la justificación de aquellos que no lo sean. En la declaración de aplicabilidad se incluyen:

- El dominio o control de la norma ISO 27001.
- Los objetivos de control así como los controles que se llevan a cabo o se encuentran implementados.
- Los objetivos de control que se han seleccionado y su debida justificación.
- Los objetivos de control que se han excluido y la debida justificación para tomar dicha decisión.

El encargado de revisar y aprobar la declaración de aplicabilidad es el director del departamento de tecnología, en este caso el Ing. Diego Silva.

Es importante mencionar que se ha utilizado el formato de la declaración de aplicabilidad (SOA) de la misma norma ISO.

5. Políticas de Seguridad					
Objetivo	**Apoyar y proporcionar la guía para gestionar adecuadamente la seguridad de la información en base a políticas y normativas apropiadas.**				
SECCIÓN	**CONTROLES ISO 27001**	**APLICABILIDAD**		**JUSTIFICACIÓN APLICABILIDAD**	**JUSTIFICACIÓN DE EXCLUSIÓN**
		SI	**NO**		
5.1	Políticas de seguridad de la información				
5.1.1	Documentar políticas de seguridad de información.	x		Es imprescindible documentar las políticas de seguridad. Para ello la dirección distrital debe aprobar un documento sobre ellas y comunicar a todos los funcionarios de la institución.	
5.1.2	Revisión de la política de seguridad de la información.	x		Se debe realizar una revisión periódica de las políticas para garantizar que es adecuada y eficaz.	
6. Organización De La Seguridad De La Información					
Objetivo	**Establecer un modelo o estructura de gestión el cual facilite el proceso de organización y control de la información.**				
SECCIÓN	**CONTROLES ISO 27001**	**APLICABILIDAD**		**JUSTIFICACIÓN APLICABILIDAD**	**JUSTIFICACIÓN DE EXCLUSIÓN**
		SI	**NO**		
6.1	Organización interna				
6.1.1	Compromiso de la gerencia con la seguridad de la información	x		Debe existir un comprometimiento por parte de la gerencia respecto a gestionar adecuadamente la seguridad de la información a través de una dirección clara y precisa.	

6.1.2	Coordinación de la seguridad de información	x		Las actividades para llevar a cabo la gestión de seguridad de la información deben ser coordinadas por el departamento de tecnologías bajo supervisión de la dirección.	
6.1.3	Asignación de responsabilidades de la seguridad de la información	x		Es imprescindible definir y documentar las diferentes responsabilidades sobre seguridad de la información.	
6.1.4	Proceso de autorización para los medios de procesamiento de información	x		Es necesario establecer un procedimiento donde se gestionen las autorizaciones para la utilización de recursos donde se procese información.	
6.1.5	Acuerdos de confidencialidad	x		En los contratos laborales se deben establecer acuerdos sobre la no divulgación de información garantizando así la confidencialidad de la misma.	
6.1.6	Contacto con autoridades	x		Se debe mantener un contacto periódico con la dirección a fin de monitorizar y regular los procesos que se llevan a cabo.	
6.1.7	Contacto con grupos de interés especial		x		No aplica debido a que la institución no mantiene contacto con terceros, es decir la información se maneja internamente.
6.1.8	Revisión independiente de la seguridad de la información	x		Es necesario revisar de manera individual políticas, objetivos de control y demás procesos de seguridad de forma periódica, más aun cuando se realice algún cambio significativo.	

SECCIÓN	CONTROLES ISO 27001:2005	APLICABILIDAD		JUSTIFICACIÓN APLICABILIDAD	JUSTIFICACIÓN DE EXCLUSIÓN
		SI	NO		
6.2	***Entidades Externas***				
6.2.1	Identificación de riesgos relacionados con entidades externas.		x	Es necesario definir controles y normativas respecto al acceso tanto de proveedores de servicios o artículos como de los usuarios que solicitan un determinado requerimiento en la institución.	
6.2.2	Tratamiento de la seguridad cuando se trabaja con clientes		x		
6.2.3	Tratamiento de la seguridad en contratos con terceras personas		x		

7: Gestión de Activos					
Objetivo*:*	**Mantener un nivel óptimo respecto a la protección de activos informáticos de la institución lo cual garantice la continuidad de las actividades institucionales además de salvaguardar la integridad, confidencialidad y disponibilidad de la información.**				
SECCIÓN	**CONTROLES ISO 27001:2005**	**APLICABILIDAD**		**JUSTIFICACIÓN APLICABILIDAD**	**JUSTIFICACIÓN DE EXCLUSIÓN**
		SI	**NO**		
7.1	Responsabilidad por los activos				
7.1.1	Inventarios de activos	x		Todos los activos deben estar identificados y a partir de ello mantener un inventario actualizado de los mismos.	
7.1.2	Propiedad de los activos	x		El departamento de sistemas tiene a su cargo la responsabilidad de los activos informáticos por lo que debe llevar un control adecuado de los mismos.	
7.1.3	Uso aceptable de los activos	x		Es importante para los intereses de la institución que se establezcan controles para promulgar el correcto uso de los recursos y por ende de la información.	

SECCIÓN	CONTROLES ISO 27001:2005	APLICABILIDAD		JUSTIFICACIÓN APLICABILIDAD	JUSTIFICACIÓN DE EXCLUSIÓN
		SI	NO		
7.2	Clasificación de la información				
7.2.1	Lineamientos de clasificación		x		En el distrito de educación todos los procesos tienen el mismo propósito por lo cual no es prioritario clasificar la información para obtener mejores resultados. No es posible detener o dejar en segundo plano o cola de espera un proceso por más pequeño que este parezca.
7.2.2	Etiquetado y manejo de la información		x		

8: Seguridad de los recursos humanos					
Objetivo:	**Asegurar que los funcionarios comprendan sus responsabilidades y obligaciones respecto al uso de activos y recursos de la institución, evitando así posibles problemas como robo o alteración de la información.**				
SECCIÓN	**CONTROLES ISO 27001:2005**	**APLICABILIDAD**		**JUSTIFICACIÓN APLICABILIDAD**	**JUSTIFICACIÓN DE EXCLUSIÓN**
		SI	**NO**		
8.1	Prioridad a los empleados.				
8.1.1	Selección		x		La contratación de personal es en parte ajena a la institución debido a que ésta se realiza a través de la plataforma *socio empleo* por parte de planta central donde son seleccionados los aspirantes a un determinado cargo.
8.1.2	Términos y condiciones del empleo		x		
8.2	Durante el empleo				

8.2.1	Responsabilidades de gestión		x		En los acuerdos contractuales no tiene participación el distrito, los realiza la coordinación zonal.
8.2.2	Formación de la seguridad de la información		x		
8.2.3	Proceso disciplinario		x		
8.3	Terminación o cambio de empleo				
8.3.1	Cese o cambio de puesto de trabajo	x		Se deben establecer pautas para asegurar que el abandono de la institución por parte de un empleado no conlleve consecuencias. Es decir comprobar que se eliminen derechos de acceso además de la devolución de recursos o equipamiento proporcionado por parte de la institución.	

9: Seguridad Física y Ambiental					
Objetivo**:**	**Evitar la interrupción de las actividades del Distrito 18D01 de Educación debido a daño o pérdida del equipamiento informático ya sea por acceso físico no autorizado de personal o desastres ambientales.**				
SECCIÓN	**CONTROLES ISO 27001:2005**	**APLICABILIDAD**		**JUSTIFICACIÓN APLICABILIDAD**	**JUSTIFICACIÓN DE EXCLUSIÓN**
		SI	**NO**		
9.1	Áreas seguras				
9.1.1	Perímetro de seguridad física	x		Se deben establecer perímetros de seguridad para proteger aquellas áreas con equipamiento importante o con instalaciones donde se procesa información.	

9.1.2	Controles físicos de entrada	x		Para evitar mal uso del equipamiento es importante que se definan controles de entrada para asegurar el acceso de solo personal autorizado.	
9.1.3	Seguridad de oficinas, despachos y recursos		x		No aplica debido a que los funcionarios no disponen de oficinas, todos se encuentran situados en cubículos en el área central de las instalaciones.
9.1.4	Protección frente a amenazas externas	x		Debe existir un plan de gestión de riesgos ante eventualidades externas como sismos, incendios, ataques, etc., para evitar el daño de equipos y mucho menos la pérdida de información.	
9.1.5	El trabajo en áreas seguras		x		Los funcionarios cuentan únicamente con un espacio reducido de trabajo por lo que no es posible trasladarse a áreas consideradas como seguras o de menor riesgo para el desarrollo de sus actividades.
9.1.6	Áreas de acceso público		x		No aplica debido a que existe una sola entrada a la institución la misma que sirve tanto para funcionarios como para personas externas por lo que no es posible cumplir este apartado.
9.2	Seguridad de equipos				
9.2.1	Emplazamiento y protección de equipos	x		Una correcta ubicación de los equipos disminuirá el riesgo de amenazas y peligros ambientales.	

9.2.2	Instalaciones de suministro		x		El distrito cuanta con una planta propia de electricidad por lo que no se ve afectado por falta de electricidad.
9.2.3	Seguridad del cableado	x		Se debe proteger el cableado de energía y telecomunicaciones para evitar tanto daños como interferencias.	
9.2.4	Mantenimiento de los equipos	x		Programar un mantenimiento periódico de los equipos a fin de mantener la disponibilidad de la información.	
9.2.5	Salida de activos fuera de las dependencias de la empresa		x		No aplica debido a que no existe justificación alguna para la salida de equipamiento fuera de la institución.
9.2.6	Seguridad de los equipos y activos fuera de las instalaciones		x		

10: Administración de comunicaciones y operaciones					
Objetivo**:**	**Asegurar la protección de la información que se transmite a través de la red y garantizar una adecuada operación de los recursos de tratamiento de información institucional.**				
SECCIÓN	**CONTROLES ISO 27001:2005**	**APLICABILIDAD**		**JUSTIFICACIÓN APLICABILIDAD**	**JUSTIFICACIÓN DE EXCLUSIÓN**
		SI	**NO**		
10.1	Procedimientos y responsabilidades de operación				
10.1.1	Documentación de procedimientos de operación	x		Se deben documentar los procedimientos operativos y ponerlos a disposición de los demás.	

10.1.2	Gestión de cambios		x		No aplica debido a que el distrito no tiene permisos para modificar ninguno de los sistemas que se manejan, los privilegios para ello los tiene planta central.
10.1.3	Gestión de capacidad	x		Para alcanzar un nivel óptimo respecto a la productividad de los sistemas es importante que se realice un seguimiento continuo del uso de recursos pata tomar medidas correctivas si fuese necesario.	
10.1.4	Separación de entornos de desarrollo, prueba y producción		x		No aplica debido a que en el distrito no se desarrolla ningún tipo de sistema.
10.2	Protección contra código malicioso				
10.2.1	Controles contra códigos maliciosos	x		Es vital para garantizar la integridad de la información que se establezcan mecanismos o herramientas de detección de ataques y código malicioso.	
10.3	Copias de respaldo				
10.3.1	Copias de respaldo de la información			Con la realización de copias de respaldo se garantiza que la información esté disponible a todo momento especialmente en caso de que ocurran incidentes que la comprometan.	
10.4	Registro de actividad y supervisión				
10.4.1	Registro y gestión de eventos de actividad	x		Es importante registrar los problemas que ocurren relacionados con la seguridad de la información a fin de analizarlos y brindar soluciones más eficaces.	

10..4.2	Protección de los registros de información			Debe existir un área donde se resguarden archivos de importancia para la institución.	
10.5	Gestión de Vulnerabilidad técnica				
10.5.1	Gestión de las vulnerabilidades técnicas	x		Al obtener oportunamente información de ataques o vulnerabilidades la dirección está en la capacidad de tomar las medidas correctivas apropiadas.	
10.5.2	Restricciones en la instalación de software		x		No aplica debido a que existe una prohibición respecto a la instalación de software ajeno a los que maneja la institución.
10.6	Gestión de la seguridad en las redes				
10.6.1	Controles de red	x		Un aspecto importante para garantizar la integridad y confidencialidad de la información es una administración adecuada de las redes que se manejan.	
10.7	Intercambio de información con partes externas				
10.7.1	Políticas y procedimientos de intercambio de información		x		No aplica, la información se maneja explícitamente de manera interna. No existe motivo alguno para compartirla con terceras personas.
10.7.3	Mensajería electrónica	x		Toda información relacionada con los procesos internos pasan por servidores de mensajería y sistemas propios del Ministerio de Educación, por lo que es indispensable asegurar la integridad de la misma.	
10.7.4	Acuerdos de confidencialidad	x		Es importante documentar acuerdos de confidencialidad de la información con lo cual se garantiza la no divulgación y por tanto el uso inadecuado de la misma.	

11: Control de Accesos					
Objetivo*:*	**Gestionar el acceso de los funcionarios hacia los recursos donde se maneja información importante para la institución.**				
SECCIÓN	**CONTROLES ISO 27001:2005**	**APLICABILIDAD**		**JUSTIFICACIÓN APLICABILIDAD**	**JUSTIFICACIÓN DE EXCLUSIÓN**
		SI	**NO**		
11.1	Requisitos de negocios para el control de acceso				
11.1.1	Política de control de accesos	x		La documentación de una política de control de acceso tanto a las instalaciones como a los recursos informáticos por parte de personas no autorizadas permitirá mantener un nivel más óptimo de la integridad de la información.	
11.1.2	Control de acceso a las redes y servicios asociados	x		Se debe impedir el acceso de todo funcionario o persona externa a excepción del director del departamento de sistemas a los recursos de red a fin de impedir la interceptación o robo de información	
11.2	Gestión de acceso de usuario.				
11.2.1	Gestión de altas/bajas en el registro de usuarios	x		Es necesario que exista un procedimiento formal para la asignación de usuario como de contraseñas tanto de equipos como de plataformas a aquellos funcionarios que lo requieran.	
11.2.2	Gestión de información confidencial de autenticación de usuarios	x		Se debe gestionar adecuadamente la entrega de información personal para la autenticación de cada funcionario,	
11.2.3	Retirada o adaptación de los derechos de acceso	x		Deben ser retirados los privilegios o derechos de acceso a la información a aquellos funcionarios que terminen su contrato laboral en la institución debido a que ya no tiene razón alguna para ingresar o hacer uso de los recursos.	

11.3	Responsabilidades del usuario				
11.3.1	Uso de información confidencial para la autenticación	x		Es importante que se concientice a cada funcionario sobre la importancia de mantener la confidencialidad en cuanto la información que se le es otorgada para la autenticación respectiva.	
11.4	Control de acceso a sistemas y aplicaciones				
11.4.1	Restricción del acceso a la información	x		Es necesario que se restrinja la accesibilidad a los funcionarios ajenos a los procesos donde se maneja información. Únicamente debe tener acceso aquellos que intervengan en los procesos.	
11.4.2	Procedimientos seguros de inicio de sesión	x		Se debe asegurar el acceso hacia los sistemas y aplicaciones que se manejan mediante un método de autenticación que impida que personas no autorizadas hagan uso de información vital.	
11.4.3	Gestión de contraseñas de usuario	x		Un aspecto importante respecto a la seguridad, es que se utilicen “contraseñas fuertes” lo cual garantice que no se vulneren los sistemas que se manejan.	
11.4.4	Uso de herramientas de administración de sistemas		x		No aplica debido a que está prohibido tanto la instalación como el uso de herramientas o software externo al que se maneja.
11.4.5	Control de acceso al código fuente de los programas	x		Se debe restringir el acceso hacia el código fuente de las aplicaciones existentes ya que dicha acción puede conllevar al daño de una aplicación o sistema.	

12: Adquisición, desarrollo y mantenimiento de los sistemas de información					
Objetivo:	**Garantizar la calidad de los sistemas de información que se adquieran o desarrollen mediante la inclusión de controles y políticas de seguridad.**				
SECCIÓN	**CONTROLES ISO 27001:2005**	**APLICABILIDAD**		**JUSTIFICACIÓN APLICABILIDAD**	**JUSTIFICACIÓN DE EXCLUSIÓN**
		SI	**NO**		
12.1	Requerimientos de seguridad de los sistemas				
12.1.1	Análisis y especificación de los requisitos de seguridad		x		No aplica debido a que el distrito 18D01 de Educación no se encarga del desarrollo de ningún sistema de información. Todos los distritos únicamente hacen uso de los sistemas que le proporciona planta central
12.2	Seguridad en los procesos de desarrollo y de soporte				
12.2.1	Política de desarrollo seguro		x		
12.2.2	Procedimiento de control de cambios en sistemas		x		
12.2.3	Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones		x		
12.2.4	Restricciones sobre los cambios de paquetes de software		x		
12.2.5	Principios de construcción de sistemas de seguros		x		
12.2.6	Ambiente de desarrollo seguro		x		
12.2.7	Desarrollo contratado externamente		x		
12.2.8	Pruebas de seguridad de sistemas		x		

12.2.9	Pruebas de aceptación de sistemas		x		
12.3	Datos de Prueba				
12.3.1	Protección de los datos utilizados en prueba		x		

13: Gestión de incidentes en la seguridad de la información					
Objetivo**:**	**Garantizar una solución efectiva y a tiempo por parte de la dirección y departamento de sistemas ante la aparición u ocurrencia de incidentes o contratiempos relacionados con la seguridad de la información.**				
SECCIÓN	**CONTROLES ISO 27001:2005**	**APLICABILIDAD**		**JUSTIFICACIÓN APLICABILIDAD**	**JUSTIFICACIÓN DE EXCLUSIÓN**
		SI	**NO**		
13.1	Gestión de incidentes y mejoras en seguridad de la información				
13.1.1	Responsabilidades y procedimientos	x		Se deben establecer responsabilidades para garantizar una respuesta eficaz e inmediata a un determinado problema de seguridad.	
13.1.2	Notificación de los eventos de seguridad de la información	x		Ante la ocurrencia de cualquier eventualidad, la notificación del problema a las autoridades por parte del funcionario permitirá brindar una solución inmediata.	
13.1.3	Valoración de eventos de seguridad de la información y toma de decisiones	x		La clasificación de incidentes de seguridad permitirá dar una solución eficaz a aquellos con mayor afectación para la institución.	

14: Gestión de la continuidad comercial					
Objetivo:	**Asegurar la restauración y continuidad de los procesos de la institución mediante un análisis previo de incidentes, fallas de seguridad, desastres, y demás eventos suscitados.**				
SECCIÓN	**CONTROLES ISO 27001:2005**	**APLICABILIDAD**		**JUSTIFICACIÓN APLICABILIDAD**	**JUSTIFICACIÓN DE EXCLUSIÓN**
		SI	**NO**		
14.1	Aspectos de la seguridad de la información				
14.1.1	Planificación de la continuidad de la seguridad de la información	x		Es necesario para garantizar la continuidad de las actividades institucionales documentar los procesos y controles que permitan solucionar inconvenientes en un futuro cercano.	
14.1.2	Implantación de la continuidad de la seguridad de la información	x			
14.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	x		Periódicamente es necesaria una revisión de los controles documentados a fin de verificar su validez y vigencia.	
15: Cumplimiento					
Objetivo:	***Cumplir tanto los controles, políticas y normas establecidas así como las disposiciones normativas y contractuales a fin de garantizar una adecuada gestión de la seguridad de la información en el Distrito de Educación.***				
SECCIÓN	**CONTROLES ISO 27001:2005**	**APLICABILIDAD**		**JUSTIFICACIÓN APLICABILIDAD**	**JUSTIFICACIÓN DE EXCLUSIÓN**
		SI	**NO**		
15.1	Cumplimiento con requerimientos legales				
15.1.1	Identificación de la legislación aplicable		x		La institución no manejo sistemas de información por lo que no mantiene relaciones contractuales por la adquisición o uso de los mismos.
15.1.2	Derechos de propiedad intelectual (DPI)		x		La institución utiliza software libre por lo que no mantiene relación alguna con instituciones de venta o alquiler de software que exijan el pago por licencias.

15.1.3	Protección de los registros de la organización	x		Deben promoverse buenas prácticas respecto a la protección de registros importantes de la institución.	
15.1.4	Protección de datos y privacidad de la información personal	x		De acuerdo a los acuerdos contractuales por ética se debe garantizar la privacidad y la protección de la información de carácter "personal".	
15.1.5	Regulación de los controles criptográficos	x		Mediante la aplicación de mecanismos de cifrado se asegura en parte la protección de la información de la institución.	
15.2	Cumplimiento con las políticas y estándares de seguridad y el cumplimiento técnico				
15.2.1	Revisión independiente de la seguridad de la información	x		Es necesario revisar de manera individual políticas, objetivos de control y demás procesos de seguridad de forma periódica, más aun cuando se realice algún cambio significativo.	
15.2.2	Cumplimiento de las políticas y normas de seguridad	x		El director o responsable del área de seguridad de información debe revisar periódicamente el cumplimiento de políticas, procesos, normas y demás mecanismos de seguridad implementados.	
15.2.3	Comprobación del cumplimiento	x		Es preciso la realización de una auditoría interna para garantizar que se cumplen adecuadamente los procesos de seguridad.	

Tabla 6 Declaración de aplicabilidad
Elaborado por: Investigador

A partir de la declaración realizada se analiza su aplicación actual en la institución y se determina su nivel de cumplimiento para posteriormente elaborar la propuesta de mejora en cada uno de los controles relevantes de la norma ISO 27001.

Luego de realizar el análisis de cada control, en conjunto con el director del departamento de tecnología se determina el porcentaje de cumplimiento de cada uno de ellos para obtener una representación cuantitativa del cumplimiento.

1. Políticas De Seguridad De La Información

1.1.Documentación de políticas de seguridad de la Información

El distrito de Educación no cuenta con un documento específico referentes a políticas de seguridad. Los diferentes procesos que se llevan a cabo no se los realiza en base a lineamientos establecidos, únicamente se aplican ciertas normativas para gestionar la información pero éstas son hasta cierto punto básicas las cuales no son suficientes para garantizar que la información esté asegurada.

Es necesario que el departamento de tecnología en conjunto con la dirección establezca políticas de seguridad factibles y de carácter obligatorio.

Las mismas deben ser documentadas y socializadas a todo el personal del Distrito de Educación sin excepción ya que todos participan activamente en los procesos institucionales.

Además deben considerarse las sanciones correspondientes en caso de detectar el incumplimiento de las políticas establecidas.

1.2.Revisión y evaluación

Como se mencionó anteriormente debido a que el Distrito no cuenta con políticas establecidas mucho menos documentadas, no se cumple con este control.

Luego de definir las políticas será necesario que la dirección del Distrito se comprometa en realizar una revisión periódica de las mismas con el fin de determinar su efectividad y cumplimiento lo cual garantice la seguridad de los procesos que se llevan a cabo.

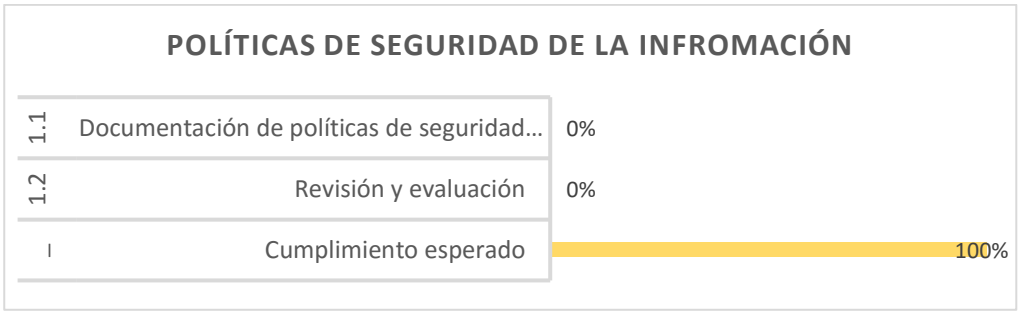


Fig. 5 Cumplimiento-políticas de seguridad
Elaborado por: Investigador

Como se puede observar en el gráfico anterior, no se cumple ninguno de los apartados relacionados con las políticas de seguridad. Es decir no se lleva a cabo la documentación ni revisión periódica de las mismas.

2. Organización De La Seguridad De La Información

2.1.Organización Interna

a. Compromiso de la gerencia

La dirección tiene un papel importante en cuanto a la seguridad de la información

Actualmente la dirección está comprometida para salvaguardar la información que se genera a nivel interno de la dirección distrital conjuntamente con las áreas respectivas.

Entre sus principales obligaciones se encuentran:

- Autorizar la capacitación al personal sobre la importancia de brindar seguridad a la información que maneja en cada uno de los procesos internos.

- Verificar de manera periódica con el responsable del área que las actividades relacionadas con la seguridad de la información que se lleven a cabo cumplan de manera obligatoria las políticas establecidas anteriormente.

- Ejecutar acciones rápidas y eficaces ante un problema o percance relacionado con la seguridad de la información previa una evaluación minuciosa de dicho riesgo.

- Determinar las medidas de sanción en caso de verificar el no cumplimiento de las mismas.

El compromiso con los procesos informáticos de parte de la gerencia tiene un nivel aceptable. Ante un evento o petición del analista de sistemas la atención y gestión por parte del director distrital ha sido oportuna.

b. Asignación de responsabilidades de la seguridad de la información

Un aspecto relevante para garantizar la seguridad de la información es la definición de responsabilidades.

- En nuestro caso existe corresponsabilidad entre el departamento de tecnología el cual realiza las tareas de control y monitoreo de los diferentes procesos de cada unidad que conforman la dirección y el funcionario responsable de cada proceso.

- Además el departamento de tecnología tiene a su cargo informar a la dirección sobre problemas suscitados y presentar posibles soluciones para juntos poder tomar las medidas correctivas adecuadas y a tiempo.

- Es importante mencionar la responsabilidad que existe respecto a los activos de información debido a que a través de ellos se realiza el procesamiento de información, esto se explicará detalladamente en el apartado referente a la Propiedad de los activos.

c. Proceso de autorización para los medios de procesamiento de información

El departamento administrativo lleva un control sobre la asignación de equipos a cada usuario o funcionario de la institución.

Dichos funcionarios necesitan tener acceso a la red para el procesamiento y manejo de información; esto conlleva a lidiar con el riesgo de que se vulnere, no solamente la integridad de la red interna sino también de los activos informáticos.

Uno de los problemas que se presentan en la dirección es al momento de asignar privilegios de acceso en la red, los cuales son autorizados por el jefe inmediato y el director distrital luego de ser solicitados documentos legalmente suscritos (formulario de solicitud donde se detallen los sitios requeridos para el desarrollo de su trabajo). Al realizar dicha asignación

quedan expuestos a ser fácilmente vulnerados tanto la red como los activos utilizados.

A partir de ello se han presentado casos donde se pudo detectar el uso inadecuado de los privilegios asignados en la red, realizando actividades completamente ajenas a los procesos institucionales específicamente para entretenimiento personal, causando que los demás usuarios de la red tengan inconvenientes al momento de realizar su trabajo en las páginas oficiales del ministerio debido a que no tienen todo el ancho de banda disponible.

d. Acuerdos de confidencialidad

Al momento en que un funcionario suscribe su contrato, la unidad de talento humano realiza el procedimiento y explicación para que el nuevo funcionario suscriba el acuerdo de confidencialidad. Este acuerdo es un modelo específico enmarcado a nivel del Ministerio de Educación.

Dicho acuerdo no es de carácter público, es decir no es visible para personas externas o ajenas a la institución, debido a que es un instrumento técnico interno que tiene como fin salvaguardad información de uso exclusivo para fines únicamente de la institución.

Dicha actividad se la realizó a partir del presente año como directriz a nivel nacional por parte de la máxima autoridad es decir el Ministro de Educación.

e. Contacto con autoridades

En la institución actualmente se cumple con este control conforme a la estructura organizacional que tiene el Distrito de Educación. En nuestro caso el área de TICS cumple con sus funciones, es decir salvaguardar la información que se maneja; de darse el caso de encontrarse ante un problema grave o que comprometa la seguridad interna, el departamento de tecnología debe acudir a su jefe inmediato (Jefe administrativo financiero) quien a su vez emite la alerta al director Distrital para en conjunto dar una solución a dicho problema.

El único problema detectado es la ausencia del director distrital debido a que el mismo tiene obligaciones fuera de la institución como la realización de seguimientos y visitas a las diferentes unidades educativas a su cargo según la agenda del despacho distrital con lo cual en ocasiones no es posible tomar medidas correctivas a tiempo.

f. Revisión independiente de la seguridad de la información

Todos los apartados relacionados con la seguridad de la información dentro del Distrito de Educación, entre ellos políticas, controles y dominios, objetivos de control y procesos, se deberán analizar y evaluar de forma independiente en periodos de tiempo establecidos.

Dicha revisión se la realizará de manera individual con el propósito de evaluar y garantizar el cumplimiento y funcionalidad de cada uno de los ítems mencionados.

Si en la revisión se identifican irregularidades o procedimientos no adecuados o que no cumplen con el objetivo de gestionar adecuadamente la seguridad de la información se deberá tomar las acciones correctivas oportunas, es decir realizar los cambios pertinentes para el mejoramiento de los mismos.

Lamentablemente en el distrito de Educación el área de tics no puede cumplir con una hoja ruta para cumplir con revisiones independientes en toda la dirección distrital. Esto se debe a que a diario el funcionario satisface las necesidades que se suscitan de manera ocasional en cada área. Además existen ocasiones que el jefe de la unidad de Sistemas tiene que salir a "territorio", es decir a realizar revisiones a las unidades educativas.

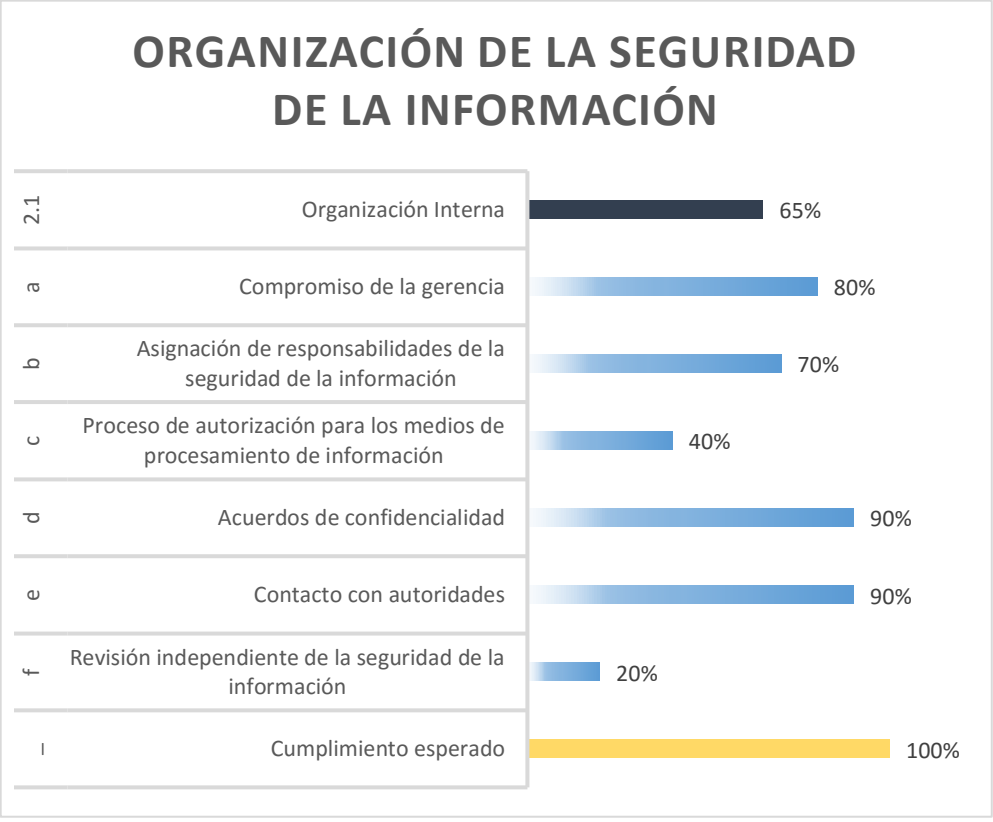


Fig. 6 Cumplimiento - Seguridad de la información
Elaborado por: Investigador

En el cuadro referente a los controles relacionados con la organización de la seguridad de la información, se puede observar que los controles con mayor índice de cumplimiento son “acuerdos de confidencialidad” y “contacto con autoridades” con un porcentaje del 90%. Los demás controles tienen un índice aceptable a excepción de la “revisión independiente”, cuyo cumplimiento es prácticamente nulo.

3. Gestión De Activos

3.1.Responsabilidad por los activos

a. Inventario de los Activos

De manera general quien tiene a su cargo el inventario de los activos institucionales es el departamento administrativo financiero. Ellos son los encargados de realizar el proceso de transición entre el funcionario saliente y quien ingresa a la institución. Por ejemplo en nuestro caso el departamento administrativo realizó la entrega de los activos informáticos al Ing. Diego Silva al momento de su ingreso al Distrito de Educación.

Cabe mencionar que la Unidad de Sistemas no tiene a su cargo la custodia de todos los equipos informáticos que se encuentran al interior de la institución ya que el proceso anteriormente mencionado de entrega de equipos se lo hace también con cada funcionario al que se le asigne un activo informático para el cumplimiento de sus funciones. Por ejemplo el ordenador de un determinado analista se encuentra bajo responsabilidad del mismo, más no del departamento de sistemas.

Respecto al proceso de “baja” de activos se realiza el siguiente proceso:

- La unidad de Sistemas emite un informe donde se detallen los motivos para que el bien ingrese al proceso de “baja”.
- Una vez que el jefe de unidad de tics presente el informe el área administrativa moviliza el bien para el proceso de baja hacia las bodegas de la institución.

b. Propiedad de los Activos

Los bienes son propiedad del Distrito de Educación ya que son adquiridos con el presupuesto designado según las necesidades institucionales.

En el Distrito de Educación existen definidas responsabilidades para el cuidado de los mismos. Este proceso lo realiza la unidad de talento humano y administrativa, quienes mediante documentos legales designan como

custodios de los activos a utilizar a los diferentes funcionarios al momento de su ingreso a la Institución. Con esto el distrito de Educación da cumplimiento al reglamento General para Administración, Utilización y Control de Bienes del sector público.

c. Uso aceptable de los activos

Luego de identificar, documentar y establecer políticas para la adecuada gestión de la información que se maneja, además de los activos informáticos de la institución relacionados con el procesamiento de datos, se deberá garantizar que los empleados, en este caso los funcionarios del Distrito de Educación se acojan y cumplan responsablemente con dichas normativas para el uso aceptable de la información.

Se ha detectado casos donde se ha podido evidenciar que tanto activos como recursos son utilizados de manera impropia o inadecuada. Por ejemplo el acceso a internet así como los ordenadores asignados a cada funcionario son utilizados de manera hasta cierto punto irresponsable. En ocasiones desperdician energía dejando encendidos los ordenadores lo cual causa un llamado de atención al jefe de la Unidad de Sistemas y en otros casos ciertos usuarios los utilizan con fines de carácter personal o para su entretenimiento lo cual ocasiona retrasos en las actividades laborales.

De esta manera es importante que los funcionarios con acceso a los activos informáticos tengan conocimiento de los parámetros y límites respecto a su uso. Además deberán estar conscientes que ellos son los responsables de la información que manejan además de los activos a su cargo.

En caso de detectar el mal uso respecto a lo anteriormente mencionado el director de la institución deberá tomar medidas adecuadas para su corrección inmediata.

En las tareas de control que se llevarán deberán incluirse:

- Normativas para el uso de sistemas institucionales.
- Lineamientos para controlar el acceso a la red institucional.

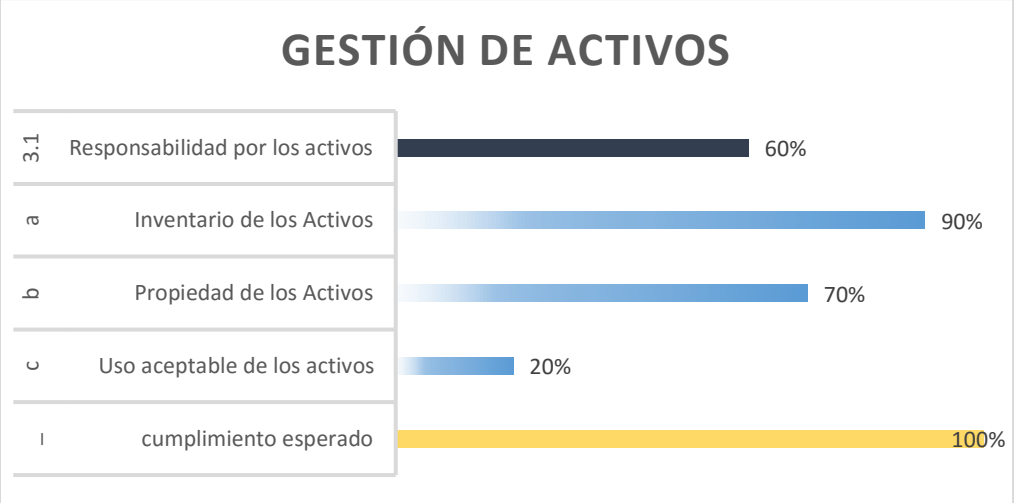


Fig. 7 Cumplimiento - Gestión de Activos
Elaborado por: Investigador

En la figura 7 referente a la Gestión de Activos, se puede percibir que el control con mayor porcentaje de cumplimiento es "Inventario de Activos", al contrario del control relacionado con el uso aceptable de los mismos, ya que prácticamente no se lo lleva a cabo en el Distrito de Educación.

4. Seguridad De Los Recursos Humanos

4.1.Seguridad después del empleo

a. Cese o cambio de puesto de trabajo

El distrito de Educación si cumple con este apartado debido a que cuando un funcionario de la institución cesa en sus funciones debe dejar legalizada toda la documentación, procesos, archivos, devolución de activos para su salida conforme a la LOSEP reglamento General para Administración, Utilización y Control de Bienes del sector público.

El problema que se percibe es que no existe una adecuada inducción respecto al nuevo funcionario que ingresa a la institución debido a que una vez que asume su cargo no tiene un hilo de continuidad adecuado para seguir con las actividades institucionales. Lo correcto sería que el funcionario saliente guíe o capacite a quien ingresa para beneficio del Distrito de Educación.

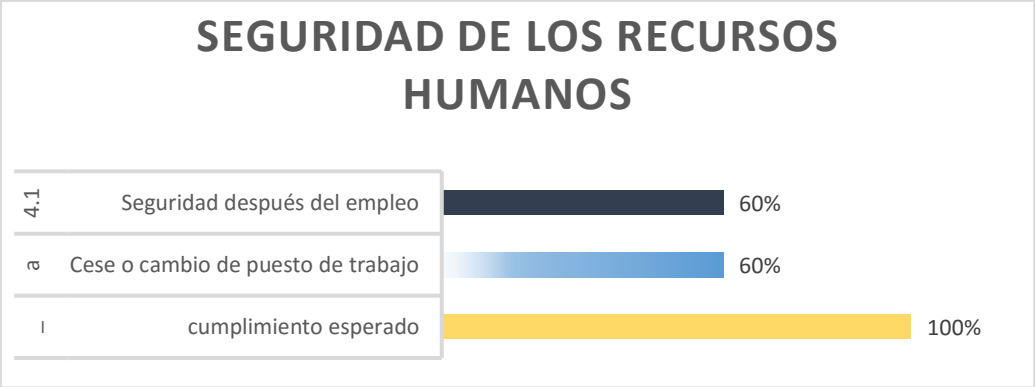


Fig. 8 Cumplimiento - Recursos humanos
Elaborado por: Investigador

En la figura anterior se observa que el control relacionado con la seguridad después del empleo se lo lleva a cabo de forma aceptable, obviamente es necesaria la aplicación de lineamientos para su funcionamiento óptimo.

5. Seguridad Física Y Ambiental

5.1. Áreas Seguras

a. Perímetros de seguridad física

Por un pedido realizado por parte de la coordinación zonal 3 de educación, El Instituto Tecnológico Superior “Bolívar” facilito parte de su infraestructura para que se la misma sea ocupada por los funcionarios del Distrito 18D01 de Educación. Dichas instalaciones se encuentran ubicadas en el centro de la ciudad.

Actualmente no existe un monitoreo dentro de la institución. El distrito contrató los servicios de guardianía privada para las noches con el objeto de salvaguardar los activos al interior de la institución.

La información procesada es guardada en los equipos de las estaciones de trabajo de cada funcionario. Es importante mencionar que la dicha información se encuentra respaldada en el sistema de gestión documental QUIPUX y en el sistema de carpetas compartidas, y en el Módulo de Gestión de Atención Ciudadana (MOGAC).

Respecto a documentos físicos hay que mencionar que los mismos se encuentran en "Archivo" del distrito. Este puede ser de talento humano o del departamento administrativo.

Los departamentos no están divididos sino que tienen un solo ambiente, es decir son salas compartidas por todos los profesionales, lo cual en parte resulta inseguro debido a que hay podrían acceder sin restricción alguna a los demás ordenadores.

b. Controles físicos de entrada

La forma de ingreso al distrito se lo realiza en información en donde le solicitan el número de Cédula del usuario y le permiten el ingreso al departamento solicitado.

Debido a que hace aproximadamente dos meses personas no autorizadas accedieron hasta las instalaciones del Distrito y sustrajeron un ordenador con información de suma importancia para la institución por la falta de control en canto al acceso físico, existe mayor control en las puertas principal y lateral.

Dicho control consistió en la colocación de una cámara de video vigilancia para identificar quienes acceden hacia las instalaciones del Distrito y las actividades que realizan al interior de la institución.

c. Asegurar las oficinas, habitaciones y medios

EL responsable de la seguridad del Distrito es del conserje, el mismo que llega dos horas antes que el personal para cumplir con sus actividades y es quien al final de la jornada laboral cierra el distrito verificando que todo se encuentre en orden.

De comprobar que exista pérdida o daño de algún activo institucional lo notifica a las autoridades Distritales. De esta manera el guardia es responsable únicamente de la parte externa más no de las oficinas ya que no tiene acceso hacia el interior de la institución, únicamente salvaguarda las instalaciones puertas afuera de la misma.

d. Protección contra amenazas externas e internas

El distrito de Educación si cumple con lo estipulado en gestión de riesgos.

- En lo concerniente a vías de evacuación, éstas se encuentran definidas y socializadas a los funcionarios.

- El distrito cuenta con áreas consideradas seguras en caso de ocurrir una emergencia; éstos son el parqueadero de vehículos y la cancha deportiva ubicados en la parte posterior del edificio los cuales son accesibles desde todas las dependencias.

  El problema detectado es que no existen señaléticas donde se indique la ruta de evacuación por lo que en caso de darse una emergencia, para personas externas que se encuentren al interior de la institución resultaría casi imposible realizar una adecuada evacuación.
  Otro de los problemas percibidos es que no existen las facilidades de evacuación para personas con discapacidad. Ya se realizó un simulacro y para los funcionarios con discapacidad y que se encuentran en los pisos altos del Distrito resultó sumamente dificultoso la realización de la misma.

- Respecto al uso y manejo de extintores en caso de incendio, estos se encuentran ubicados en zonas estratégicas de la institución. Existe un extintor en cada piso a la llegada de los escalones por lo que está al alcance de cualquier persona.

e. Áreas de acceso público, entrega y carga

Se lleva un proceso cuidadoso en cuanto a la entrega de suministros y materiales por parte de los proveedores al distrito:

- En primer lugar los proveedores se anuncian en información.

- Luego el funcionario responsable de ese proceso les permite el ingreso hacia el parqueadero.

- Finalmente los suministros son descargados en la bodega respectiva.

5.2.Seguridad de los Equipos

a. Ubicación y protección de los equipos

En este apartado el Distrito de Educación tiene sumo cuidado. El servidor así como el equipamiento informático importante se encuentra instalado en una habitación independiente, protegido de la humedad y el calor.

Dicha habitación se encuentra en el tercer piso del edificio y cuenta con la seguridad necesaria para que personal no autorizado no pueda acceder al mismo. La única manera de acceder a ella es a través de dos puertas de seguridad a las cuales solo tiene acceso el analista de la unidad de sistemas.

b. Servicios públicos de soporte

- Respecto al servicio de eléctrico éste es suministrado por la empresa pública local. Es importante mencionar en este apartado que no todos los ordenadores cuentan con UPS, únicamente cuentan con dicho equipamiento aquellos funcionarios que lo solicitaron.

  Ese fue el principal problema detectado lo cual podría afectar la integridad física de los equipos si existieran problemas como cortes de suministro eléctrico

- En cuanto a las herramientas de comunicación el distrito de Educación se maneja tanto Voz IP el cual permite la comunicación entre funcionarios dentro de las instalaciones y por telefonía fija pagada con la empresa CNT, quien además es el proveedor del servicio de internet del Distrito.

  El ancho de banda es de 10 Mb sin embargo se ha detectado que la conexión es inestable y lenta en ciertas ocasiones.

c. Seguridad del cableado

Para el cableado de datos se utiliza en el Distrito cable UTP categoría 6 con conectores RJ45. EL cableado está protegido por canaletas correctamente adecuadas dentro la institución, éstas no impiden ni dificultan las actividades de los funcionarios. Por su correcta ubicación pasan desapercibidas.

d. Mantenimiento de equipos

Existe un plan de mantenimiento de los equipos que se lleva a cabo cada cuatro meses. El encargado de realizar dicha actividad es el ingeniero David Silva con la ayuda de sus asistentes quienes son los encargados de velar por el correcto funcionamiento y operación del equipamiento tecnológico.

Lamentablemente la mayoría de las veces no se ejecuta dicho mantenimiento preventivo por las múltiples ocupaciones del personal de sistemas con lo cual se presentan incidentes con los ordenadores o equipos. Ante esto surge la necesidad de dar soluciones correctivas las cuales generan incluso gastos a la institución.

e. Seguridad de los equipos fuera de las instalaciones

Todos los equipos que se encuentran en las instituciones educativas pertenecientes al distrito #1 de educación están bajo la administración del Distrito 18D01 de educación.

Los responsables directos de la custodia de dichos equipos son las mismas instituciones quienes cuentan con actas de entrega / recepción de los mismos.

Ante un incidente con cierto activo informático el responsable de la institución reporta al distrito sobre el percance suscitado mediante u informe detallado para brindar soluciones adecuadas.

f. Seguridad de la eliminación o re-uso del equipo

El distrito de educación está a cargo de la eliminación o baja de los equipos tanto externos como los que se manejan en las instalaciones distritales.

Respecto a la eliminación de equipos externos es decir aquellos que se encuentran en las instituciones educativas del sector, el proceso es el siguiente:

- El responsable, es decir el docente informático a cargo realiza un análisis del equipo en cuestión.

- En caso de que el activo informático hubiese cumplido su vida útil el funcionario realiza un informe dirigido al distrito de educación para continuar con el procedimiento de eliminación.

En cuanto tiene que ver a los equipos que se encuentran dentro del distrito el informe anteriormente mencionado lo realiza el departamento del área tecnológica.

En ambos casos luego de realizar el informe se procede enviar los equipos dados de baja hacia la empresa recicladora con la que mantiene convenio el distrito de Educación para la eliminación física de los mismos.

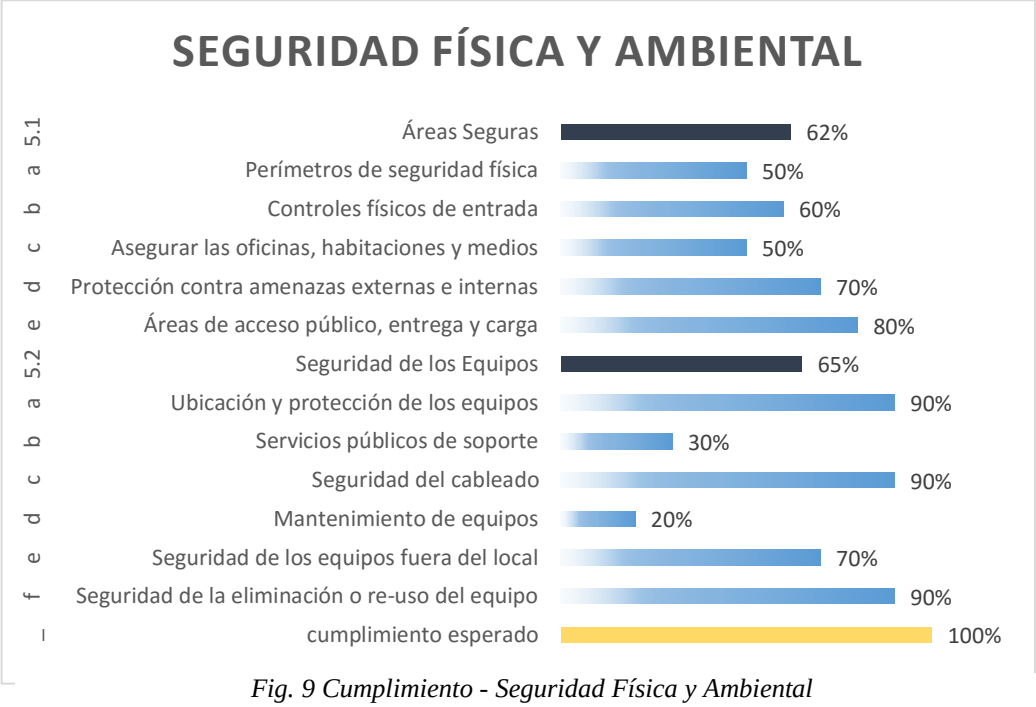


Fig. 9 Cumplimiento - Seguridad Física y Ambiental
Elaborado por: Investigador

En la figura anterior se puede apreciar los porcentajes de cumplimiento de los controles referentes a la seguridad física y ambiental, donde la ubicación y protección de los equipos son los tópicos donde el departamento de tecnologia hace mayor énfasis en cuanto a su cuidado y aplicación.

Los controles donde es necesario mejorar el índice de aplicabilidad son los servicios públicos y mantenimiento de los equipos. Éste último debido a la falta de un cronograma de revisiones periodicas.

6. Administración De Comunicaciones Y Operaciones

6.1.Procedimientos y responsabilidades operacionales

a. Documentación de procedimientos de operación

Existen documentos donde se detallan los parámetros respecto al manejo de los sistemas institucionales como MOGAC, QUIPUX, etc.

El problema es que no existe documentación para los procesos relacionados con la seguridad de la información, únicamente se realizan socializaciones para dar a conocer a los funcionarios responsables de determinados procesos

la forma de llevarlos a cabo por lo que la mayoría de veces se genera dependencia del director de tecnología debido la ocurrencia de imprevistos o sucesos inesperados.

b. Gestión de cambios

No existe la autorización por parte de planta central para que el distrito realice la gestión de cambios por su parte.

Las veces en las que se realiza cambios ya sea referente a hardware o software es por disposición de planta central previo un estudio donde se procura la mejora de las actividades institucionales.

Es importante mencionar que uno de los problemas más graves que se pudo detectar es que el distrito no cuenta con licencias respectivas de los programas que utiliza con lo cual se corre el riesgo de que se generen incluso problemas legales a la institución.

6.2.Protección contra código malicioso

a. Controles contra códigos maliciosos

No existen controles establecidos para identificar ni combatir códigos maliciosos.

Existe un alto grado de probabilidad de ocurrencia de ataques, inyección de código o robo de información ya que no se toman las medidas adecuadas para contrarrestar dichos problemas en caso que se efectivicen.

El único mecanismo de protección con que cuenta la institución es el antivirus actualizado para evitar la propagación de virus tanto en los ordenadores como en la red, sin embargo esto no es suficiente debido a que la mayoría de funcionarios no utilizan dicha herramienta al momento de introducir sus dispositivos de almacenamiento.

Otra medida preventiva que se lleva a cabo es el bloqueo de sitios web riesgosos.

6.3.Copias de seguridad

a. Copias de seguridad de la información

Se lleva a cabo el respaldo de información sin embargo dicho proceso no se encuentra documentado ni se lo realiza en base a políticas.

El proceso de backups o respaldo de información de todos los ordenadores se lo realiza cada dos meses mediante tareas programadas en el servidor.

Como se mencionó anteriormente el servidor se encuentra ubicado en el cuarto de equipos correctamente asegurado.

Cuando un funcionario necesita información respaldada de su ordenador solicita al responsable de sistemas en esta caso el Ing. David Silva tener acceso a la misma.

6.4. Registro de actividad y supervisión

a. Registro y gestión de eventos de actividad

No se lleva a cabo un control preventivo, es decir no se realiza una revisión periódica sobre los procesos relacionados con la seguridad de la información. Debido a ello ante la ocurrencia de problemas el departamento de tecnología se ve en la necesidad de brindar soluciones efectivas lo cual genera un mayor gasto de recursos ya que el daño tiene un mayor grado de afectación.

b. Protección de los registros de información

La información digital se encuentra alojada en los sistemas institucionales. Un respaldo de las mismas se encuentra en el servidor ya que se realizan backups cada dos meses de toda la información en caso de que se suscite una emergencia.

No existen controles para salvaguardar la información mencionada, por lo que existe siempre el riesgo de que ocurran alteraciones o pérdida de la misma.

Respecto a la información física, ésta se encuentra almacenada y resguardada en los diferentes archivos del Distrito. Sólo personal autorizado tiene acceso a la misma.

6.5.Gestión de vulnerabilidad técnica

a. Restricción en la instalación de software

Si existe restricción para todos los funcionarios en lo que respecta a la instalación de software.

Lo que se realiza por parte del departamento de tecnología a más de socializar e indicar la prohibición que existe para la instalación de software sin autorización del personal de sistemas es restringir los permisos administrativos a cada usuario con lo cual se impide que puedan realizar dicha actividad que en la mayoría de las veces es con el fin de llevar a cabo actividades completamente ajenas a las requeridas en la institución.

Cuando un funcionario necesita utilizar software con el que no cuenta en su ordenador debe realizar una solicitud al analista de sistemas el cual se encarga de realizar la instalación del mismo a través de la cuenta de administrador.

6.6.Gestión de la seguridad en las redes

a. Control de red

No se lleva a cabo ningún control en la red por lo que el Distrito está expuesto a sufrir alteraciones o incluso el robo de la información que maneja a través de la misma.

El problema se hace más crítico debido a que la mayoría de procesos que llevan los funcionarios se los realiza a través de plataformas institucionales en red como QUIPUX, MOGAC, entre otros.

6.7.Intercambio de información con partes externas

a. Políticas y procedimientos de intercambio de información; b. Mensajería electrónica

El intercambio de información se lo realiza a través de las plataformas institucionales que se manejan como Quipux, Mogac además de correos institucionales (MINEDUC).

Referente a la información que se entrega a "clientes", en el caso del distrito de educación son las personas y estudiantes que gestionan algún proceso o solicitan cierto documento, el proceso que se sigue es entregar una copia del documento físico ya que el original se queda en custodia de la institución. Dicho documento tiene la firma y sello del director distrital o del encargado del proceso además de la firma de la persona que solicita el documento para que quede constancia de dicho proceso.

Es importante mencionar que para realizar dicho trámite las personas tienen acceso a la institución pero su estadía se encuentra sumamente controlada por el personal.

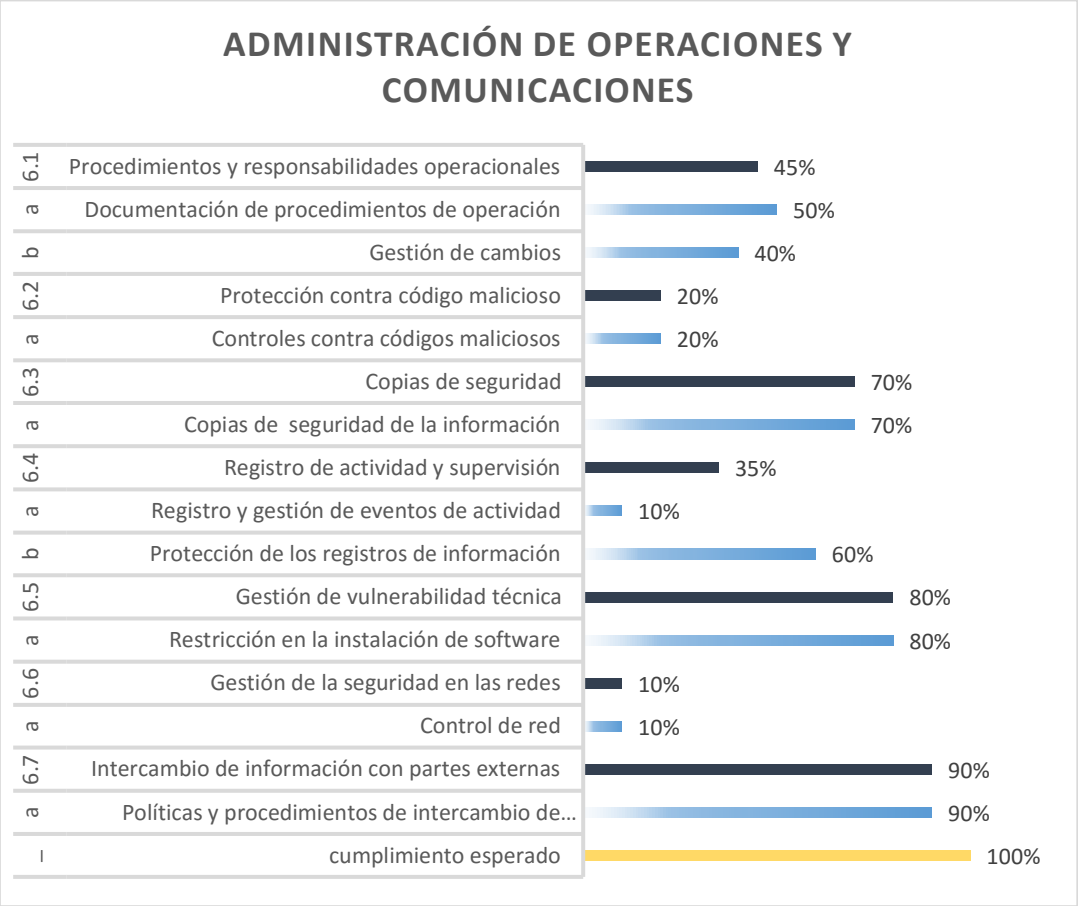


Fig. 10 Cumplimiento - Gestión operaciones y comunicaciones
Elaborado por: Investigador

En la figura 10 referente a la gestión de operaciones y comunicaciones, se detallan los porcentajes de los controles que conforman el mismo, siendo el punto crítico el control en la red, además del registro y gestión de eventos de actividad. En general el dominio en cuestión tiene un nivel sumamente bajo en cuanto a cumplimiento por lo que se deberán tomar las medidas correctivas apropiadas. El único apartado que deja cierto grado de satisfacción es el intercambio de información con partes externas.

7. Control De Acceso

7.1.Requisitos de negocio para el control de acceso

a. Política de Control de accesos

No existen políticas definidas para gestionar el control de acceso, sin embargo se llevan a cabo los siguientes controles.

- Ningún funcionario tiene acceso a un ordenador que no se encuentre bajo su cargo ni mucho menos acceder a las plataformas institucionales si no cuenta con los permisos para hacerlo. Este proceso se lo controla mediante la asignación de claves las cuales son otorgadas por el analista de sistemas. En el apartado de "Gestión de altas/bajas en el registro de usuarios" se detallará el proceso de asignación de usuarios y contraseñas.

- Además existe restricción en cuanto al uso de impresoras, plotter, etc. con excepción del personal administrativo quienes disponen de una impresora personal.

b. Control de acceso a las redes y servicios asociados.

El departamento de sistemas restringe el acceso del personal hacia sitios web ya que pueden ser peligrosos, además de que no son necesarios para el desarrollo y cumplimiento de las actividades laborales.

Respecto a la red interna los funcionarios tienen acceso únicamente a la sección de carpetas compartidas. Sólo personal de sistemas tiene privilegios para acceder a configuración de la red.

7.2.Gestión de acceso de usuario

a. Gestión de altas/bajas en el registro de usuarios.

Cuando se produce el ingreso a la institución de un nuevo funcionario, el procedimiento para la asignación de usuarios y claves es el siguiente:

- Respecto a las plataformas institucionales, el departamento de talento humano solicita al departamento de sistemas la creación y asignación de una cuenta y clave para el nuevo empleado.

- El analista de sistemas hace la entrega de dicho requerimiento al funcionario en cuestión, el cual se encarga de modificar la contraseña a su conveniencia. Las plataformas mencionadas al cabo de tres meses solicitan que se gestione la contraseña de manera obligatoria para continuar utilizándolas lo cual brinda un alto grado de confianza y seguridad para el procesamiento de la información a través de las mismas.

- En cuanto a la gestión de usuarios y claves para los ordenadores asignados a los funcionarios, el analista de sistemas crea un usuario en el pc y le asigna la contraseña correspondiente. El problema percibido es que dichas claves

no se gestionan periódicamente. Se explicará el problema de manera más detallada en el control “gestión de contraseñas”.

b. Retirada de los derechos de acceso

El departamento de sistemas cumple a cabalidad con este control. Cuando finaliza el contrato de un determinado funcionario o se retira de la institución por cierto motivo, el director del departamento de tecnología se encarga personalmente de cerrar todas las cuentas y eliminar contraseñas tanto del ordenador como de las plataformas que utilizaban en el Distrito.

7.3.Responsabilidades del usuario

a. Uso de información confidencial para la autenticación

Este control hace relación única y específica al nivel de compromiso del personal con el manejo de sus claves o contraseñas.

En el Distrito de Educación se ha socializado sobre la importancia de gestionar adecuadamente las mismas con el objetivo de evitar la vulneración de la seguridad de la información.

Cada funcionario debe estar consciente que es responsable de su equipo, cuentas que manejan y de la información que procesan. El uso inadecuado como la difusión o socialización de claves debe ser controlado y sancionado por parte de las autoridades.

7.4.Control de acceso a sistemas y aplicaciones

a. Gestión de contraseñas

En el Distrito de educación cada equipo tiene claves de acceso las cuales hasta el momento no se han gestionado. Únicamente se realizó la asignación de las mismas hacia los funcionarios al momento de su ingreso por lo que existe un nivel elevado de inseguridad en cuanto se refiere a este apartado.

Es recomendable que se realice una gestión adecuada de las mismas a través de políticas establecidas. La forma más efectiva de gestionarlas es a través de gestores los cuales generen claves aleatorias a las que se accede mediante la clave maestra de la aplicación. Con ello se disminuye el riesgo de que personas

no autorizadas o incluso los mismos empleados accedan a información no autorizada.

b. Uso de herramientas de administración de sistemas

Es importante controlar que el personal no tenga autorización o privilegios para la instalación de aplicaciones las cuales puedan anular o vulnerar claves o incluso los sistemas que se utilizan.

Como se mencionó anteriormente el personal de sistemas restringe los permisos para la instalación de todo tipo de software externo por lo que se puede asegurar que este control se cumple a cabalidad.

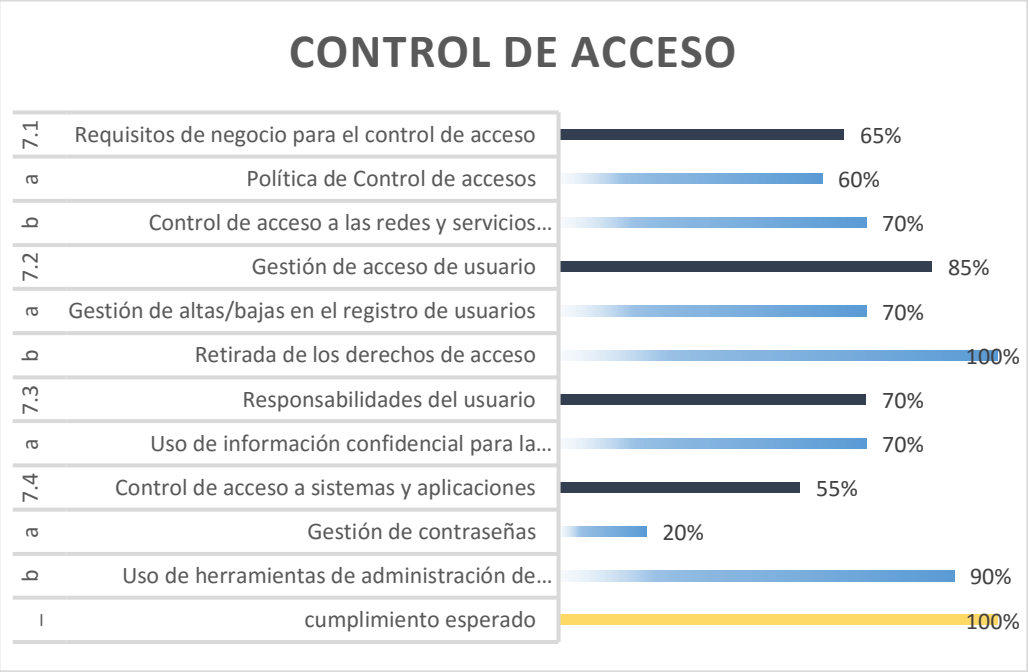


Fig. 11 Cumplimiento - Control de Acceso
Elaborado por: Investigador

Como se observa en la figura anterior, la mayoría de controles tiene un cumplimiento aceptable con un porcentaje mayor al 55%, excepto el control relacionado a la gestión de contraseñas cuyo índice de cumplimiento es 20% y está por debajo de lo esperado por lo cual hay que tomar medidas correctivas en relación a dicho control.

8. Adquisición, Desarrollo Y Mantenimiento De Los Sistemas De Información.

No aplica debido a que el distrito 18D01 de Educación no se encarga del desarrollo de ningún sistema de información. Todos los distritos únicamente hacen uso de los sistemas que le proporciona planta central.

9. Gestión De Incidentes En La Seguridad De La Información

9.1.Gestión de incidentes y mejoras en seguridad de la información

- Responsabilidades y procedimientos

El departamento de sistemas tiene la obligación de dar solución no solamente a problemas relacionados con la seguridad de la información, sino a todos aquellos que afecten el cumplimiento de las actividades institucionales relacionadas al área de tecnología.

Ante la presencia de un suceso, el analista del departamento de sistemas realiza un informe detallando el problema y las causas que lo provocaron. Cuando éste tiene un nivel elevado de afectación para los intereses del Distrito el reporte es presentado de manera urgente al Director Distrital para en conjunto tomar las medidas correctivas y dar solución a dicho problema.

- Notificación de los eventos de seguridad de la información

Únicamente se ha socializado por parte de las autoridades y el personal de sistemas hacia los empleados la importancia de que los mismos reporten cualquier problema ocurrido relacionado con la seguridad de la información ya sea en su puesto de trabajo o en cualquier instalación del distrito de educación.

El problema es que no existe una política definida para llevar a cabo dicho procedimiento.

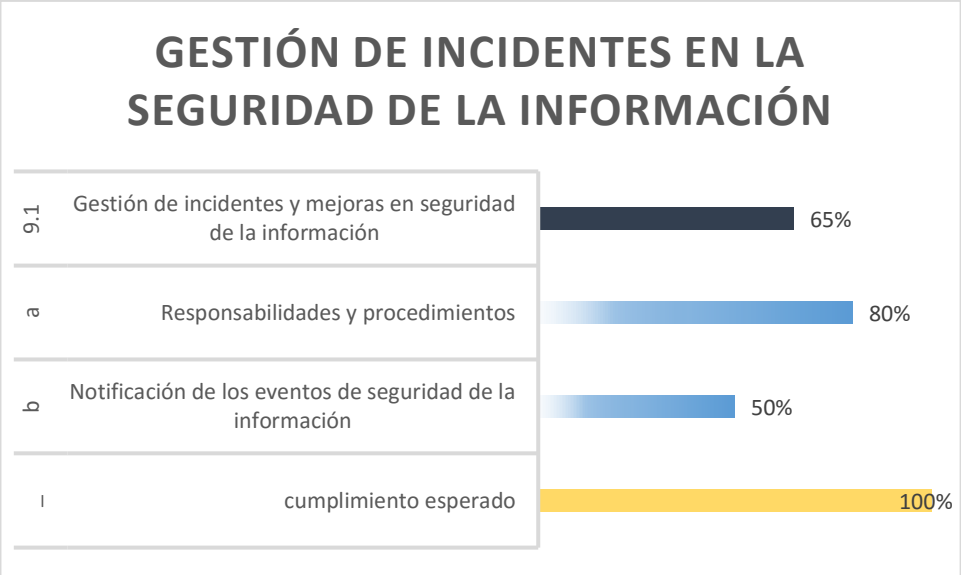


Fig. 12 Cumplimiento - Gestión de Incidentes
Elaborado por: Investigador

Lo mencionado anteriormente se plasma en la figura 12 relacionada a la gestión de incidentes. En promedio los controles que conforman el dominio "Gestión de incidentes y mejoras en seguridad de la información" tienen un porcentaje de cumplimiento del 65%, lo cual da la pauta de la correcta aplicabilidad de ambos controles en la institución.

4.3 Implementación de procedimientos y controles para la gestión de incidentes de seguridad de la información.

En base al análisis realizado mediante la aplicación de los controles de la norma ISO 27001 y tomando en cuenta los diferentes escenarios que maneja el Distrito de Educación para llevar a cabo las diferentes actividades tanto operativas como comerciales se ha podido determinar que la probabilidad de ocurrencia de incidentes relacionados con la seguridad de la información en Distrito 18D01 de Educación es elevado.

Para ello es necesario establecer políticas de seguridad coherentes y enmarcadas dentro de los límites de cumplimiento institucional, cuyo objetivo será apoyar y proporcionar la guía para gestionar adecuadamente la seguridad de la información. Las mismas deberán ser aprobadas por la dirección, a partir de ello socializarlas a todo el personal y posteriormente verificar su cumplimiento.

Las políticas definidas a continuación cubren las necesidades de seguridad: ***organizacional, lógica, física y legal*** del Distrito de Educación en lo referente al

manejo adecuado para salvaguardar la información. Por su puesto las mismas siguen la línea de cumplimiento de los controles de la norma ISO 27001.

- Seguridad Organizacional (Gestión de activos – Recursos humanos)

  Se establecerá un marco formal a través del cual se maneje la institución incluyendo aspectos relacionados como servicios, gestión de activos, recursos humanos, físicos, responsabilidades y actividades complementarias ante situaciones o eventualidades relacionadas a la seguridad de la información.

- Seguridad Lógica (Control de acceso – gestión de las operaciones y comunicaciones)

  Se establecerán los lineamientos y normativas para la gestión de control de acceso por parte de los usuarios tanto a sistemas institucionales como a equipamiento para evitar cambios o alteraciones en la configuración de los mismos. Además se definen normativas para el control de vulnerabilidades por causa de software malicioso.

- Seguridad Física

  Se establecen límites en cuanto a la definición de perímetros de seguridad.

  Además se implementarán controles relacionados con el manejo, mantenimiento y soporte técnico de los equipos

- Seguridad Legal - Cumplimiento

  Se deben integrar las políticas y normativas de seguridad establecidas bajo el régimen o reglamentación interna del Distrito de Educación a fin de verificar el cumplimiento de las mismas y a partir de ello definir sanciones al personal de la institución ante faltas cometidas y que vulneren la seguridad de la información.

1. GESTIÓN DE ACTIVOS

Objetivo:

Garantizar la continuidad operacional del distrito de Educación, evitando posibles riesgos referentes a los activos informáticos, los mismos que pueden ser causados de manera intencional o accidental provocando la interrupción de actividades.

A. RESPONSABILIDAD POR LOS ACTIVOS :

- Se deberán establecer acuerdos de confidencialidad que comprometa al personal a la utilización de los activos entregados por el Distrito de Educación única y exclusivamente para beneficio de la institución y no para otros fines.

- Cada funcionario será el responsable y custodio de los activos recibidos por parte de talento humano para llevar a cabo sus actividades laborales según la normativa del reglamento General para Administración, Utilización y Control de Bienes del sector público. Dicha actividad deberá ser documentada para en un fututo realizar la devolución y constatación de activos.

- Cada área del distrito de Educación tendrá un responsable a cargo de los activos considerados de "mayor importancia".

- El/los responsable(s) de cada área a más de salvaguardar los activos a su cargo deberán mantener un documento actualizado de los mismos con información relevante para su adecuada gestión.

2. RECURSOS HUMANOS (PERSONAL)

Objetivo:

Minimizar los riesgos de error humano mediante la definición de mecanismos para el correcto manejo de los recursos.

A. DURANTE EL EMPLEO:

- Todo el personal a su ingreso a la institución recibirá capacitación adecuada sobre buenas prácticas referentes a la seguridad de la información según sea su área operativa y en función de las actividades que llevan a cabo, con el propósito de mantener la integridad, disponibilidad y confidencialidad de la misma.

- La información procesada por personal de la institución es propiedad única y exclusiva del Distrito 18D01 de Educación. En ningún caso un funcionario tiene la potestad de tomar, modificar o eliminar información sin la autorización respectiva.

- Los funcionarios deberán comprometerse y firmar un compromiso de confidencialidad o no divulgación referente a la información mencionada anteriormente.

- Cada funcionario tiene la obligación de reportar incidentes de cualquier índole que se presenten en sus actividades diarias.

- Ante problemas suscitados relacionados con la seguridad de la información en las distintas estaciones de trabajo del personal de la institución, el departamento de sistemas deberá dar solución a los mismos en el menor tiempo posible.

- Se deberá realizar un monitoreo continuo de las cuentas de usuarios, que presenten un comportamiento sospechoso o hayan presentado cierto antecedente relacionado con la vulneración de parámetros relacionados a la seguridad de la información.

B. FINALIZACIÓN O CESE DE FUNCIONES:

- Al término de la relación laboral de cualquier funcionario con el Distrito 18D01 de Educación, el usuario deberá realizar la devolución y traspaso de los recursos y activos entregados para el desarrollo de sus actividades laborales.

- Todas las novedades o problemas relacionados con la devolución de activos deberán ser registradas en un documento, el cual servirá de respaldo para elaborar las sanciones correspondientes.

- Si existen recursos o activos que sean propiedad del funcionario y exista información relacionada con los procesos o actividades que se llevan a cabo en el Distrito, el personal de sistemas deberá realizar la transferencia de dicha información y posteriormente eliminarla del dispositivo en mención.

- Dicha entrega y recepción de información deberá ser respaldada mediante un documento formal.

- Una vez que un determinado funcionario deje de formar parte del Distrito 18D01 de Educación se procederá a cerrar todas las cuentas y eliminar las contraseñas tanto del ordenador como de las plataformas institucionales a las que tenía acceso de forma inmediata.

3. CONTROL DE ACCESO

Objetivo:

Evitar el acceso a personas no autorizadas tanto internas como externas a los diferentes sistemas que se manejan además del equipamiento para impedir la manipulación o pérdida de información.

A. CONTROL DE ACCESO A REDES Y SERVICIOS ASOCIADOS

- Se deberá implantar un sistema de autenticación robusto para los usuarios conectados.

- Mediante un análisis se deberá determinar las amenazas y vulnerabilidades en la red. Además se determinarán los puntos a proteger y los usuarios de los cuales se protegerán los recursos.

- El firewall deberá estar correctamente configurado determinando los servicios de la red que pueden ser accesados y quienes pueden utilizar dichos recursos, dejando al margen a usuarios no autorizados.

- La política utilizada será de carácter restrictivo, es decir en base al uso de un cortafuegos, el cual tenga la misión de denegar todo el tráfico a través de la red y habilitar expresamente el tráfico de los servicios que se necesiten.
- Por ningún motivo se permitirá el acceso a la red por parte de terceros. Cabe mencionar que se consideran usuarios externos o terceros a personas o entidades que mantienen relación con el Distrito 18D01 de Educación fuera del marco laboral institucional como proveedores de servicios y suministros y personas naturales que solicitan determinado requerimiento como estudiantes y padres de familia.

- Los datos que se transmitan a través de la red deberán ser encriptados.

- Se deberá ejecutar y documentar la configuración de routers, switches y demás dispositivos de red para garantizar la seguridad de la misma.

B. GESTIÓN DE ACCESO DEL USUARIO:

- Las claves entregadas por el personal de sistemas al personal deberán ser lo suficientemente fuertes. Deberán ser gestionadas a través de un gestor el cual genere claves aleatorias a las que se acceda mediante la clave maestra de la aplicación.

- Se asignarán cuentas de acceso a los diferentes equipos así como a los sistemas institucionales a todo usuario siempre y cuando se informen por parte de talento humano hacia el departamento de sistemas los objetivos de uso así como los privilegios o permisos a los que el usuario en mención tendrá acceso en dependencia de las actividades específicas que va a desarrollar.

- En caso de extravío o pérdida de la cuenta principal por parte de cierto funcionario, éste deberá presentar la respectiva justificación e identificación personal para que el personal de área de sistemas proceda con la creación de una cuenta temporal para dicho usuario.

- Queda estrictamente prohibido el acceso a archivos o documentos almacenados en ordenadores que no se encuentren a cargo del funcionario en mención.

- Se deberá realizar una revisión periódica de los controles de acceso para determinar el cumplimiento del mismo debido a que existen casos donde se realizan cambios de puestos de trabajo o delegación de nuevas funciones hacia los funcionarios.

- La única persona que podrá realizar tareas con privilegios de administrador o acceder a todos los recursos informáticos será el Director del departamento de tecnologías, en este caso el Ing. Diego Silva.

C. RESPONSABILIDAD DE LOS USUARIOS

- Todo usuario que tenga acceso tanto a equipamiento como a los diferentes sistemas que se manejan debe poseer una cuenta de usuario con la clave respectiva. Dicho usuario será el responsable de mantener a salvo la cuenta en mención.

- Se restringe rotundamente la compartición de claves y cuentas personales con otros funcionarios.

- Por seguridad los usuarios deberán evitar dejar constancia de las claves a su cargo en lugares físicos que no sean seguros como por ejemplo papeles o superficies cercanas a su estación de trabajo lo cual pueda facilitar a un tercero obtener información sobre la clave personal.

- Cada funcionario será responsable de la gestión sobre su cuenta y clave asignada por el departamento de sistemas. En caso de detectar la mala utilización de las mismas deberá ser investigado y acatar las sanciones correspondientes por parte de la dirección distrital.

- Todos los funcionarios son responsables del ordenador a su cargo y por ende de la información almacenada en el mismo. En caso de que el usuario debiera ausentarse de su estación de trabajo por cierto motivo, este deberá cancelar las sesiones activas en su ordenador, el mismo que además deberá estar configurado con una herramienta de bloqueo la cual solicite la contraseña de acceso para evitar que terceros puedan ingresar a la información que contiene el ordenador a su cargo.

- En caso de comprobar que una cuenta ha sido violada, el funcionario debe reportar dicha situación al departamento de sistemas para tomar las medidas correspondientes.

D. RESPONSABILIDAD RESPECTO AL USO DE CORREO ELECTRÓNICO Y SISTEMAS INSTITUCIONALES:

- El personal deberá comprometerse y garantizar la correcta utilización de ambas herramientas a fin de salvaguardar la información que se procesa y transmite a través de las mismas.

- Tanto el correo institucional como los sistemas informáticos son de uso exclusivo para los funcionarios del Distrito 18D01 de Educación. Por ende cada usuario será responsable de la información que se envíe o procesa de su cuenta.

- Toda actividad relacionada con el uso indebido de cualquiera de las herramientas en cuestión será motivo de sanción por parte de la dirección ya que se pone en peligro la integridad de la información institucional.

E. SEGURIDAD EN EL CONTROL DE ACCESO AL SISTEMA OPERATIVO Y APLICACIONES:

- Únicamente el personal de sistemas tendrá acceso como administrador a los ordenadores y recursos.

- El personal Distrital tendrá acceso únicamente a las aplicaciones, módulos y sistemas a su cargo donde llevará a cabo sus funciones.

- Será necesario definir y estructurar el nivel de acceso hacia las diferentes aplicaciones mediante la creación de cuentas restrictivas dependiendo obviamente del cargo o funcionario en cuestión.

- Se deberá implementar un registro o LOG donde se detallen las actividades del personal en cuanto se refiera a conexiones, intentos fallidos, número de horas y terminal donde realizó la conexión a fin de tener respaldada información referente a posibles violaciones de acceso.

F. SEGURIDAD EN EL CONTROL DE ACCESO DE TERCEROS

- Ninguna persona ni entidad externa a la institución tendrá acceso a los recursos y mucho menos a los sistemas donde se procesa información de importancia para el distrito.

G. POLÍTICAS DE ACCESO A INTERNET

- Se deberá concientizar a los funcionarios sobre el peligro que implica la navegación por sitios sospechosos o de dudosa procedencia con lo cual se corre el riesgo de sufrir ataques informáticos.

- Solamente personal administrativo tendrá acceso a Internet, además de funcionarios que soliciten hacer uso del mismo para tareas específicas con la justificación respectiva. En caso de verificar el uso de dicha herramienta con fines completamente ajenos o que no estén relacionados con las actividades laborales se deberá emitir un informe para determinar las sanciones correspondientes.

- Se deberá hacer un análisis de los navegadores permitidos para hacer uso de esta herramienta, dependiendo de las especificaciones y requerimientos de los sistemas que se manejan. La mayoría de ellos funcionan adecuadamente en Mozilla Firefox.

- Los funcionarios con acceso a Internet tendrán ciertas restricciones como por ejemplo la no visualización o descarga de música, videos o material de índole personal, el acceso a páginas que contengan software malicioso además de contenido no licenciado.

- Se deberá capacitar a los funcionarios sobre la no divulgación de información a través de la red para no comprometer la confidencialidad de la información interna.

- Se deberá restringir la participación de los usuarios en foros, grupos de discusión, además del uso o acceso a redes sociales o cuentas de correo que no pertenezcan a la institución.
- El responsable del departamento de sistemas deberá realizar un seguimiento sobre las buenas prácticas de esta herramienta.

- Respecto a los funcionarios que no tengan acceso a internet y lo soliciten para una determinada tarea, el responsable del área de sistemas deberá definir procedimientos para la solicitud y aprobación del uso de Internet.

H. GESTIÓN DE CONTRASEÑAS RESPECTO AL PERSONAL

- Los funcionarios una vez recibida la clave de acceso para los diferentes sistemas tienen la potestad de modificar la contraseña de acuerdo a su conveniencia y comodidad. Sin embargo deberán evitar el uso de información personal al momento de definir dichas contraseñas como nombres, números telefónicos, fechas de nacimiento, etc.

- Deberá evitar el uso de la misma contraseña tanto para fines personales como laborales.

4. GESTIÓN DE OPERACIONES Y COMUNICACIONES

Objetivo:

Asegurar la protección de la información que se transmite a través de la red y garantizar una adecuada operación de los recursos de tratamiento de información institucional.

A. RESTRICCIÓN EN LA INSTALACIÓN DE SOFTWARE

- El software instalado en los ordenadores del distrito de Educación es el dispuesto por planta central del ministerio de Educación en la ciudad de Quito.

- Se deberá utilizar dicho software bajo los parámetros de seguridad establecidos.

- Se prohíbe a los funcionarios sin importar su área laboral la instalación de software externo. Deberán realizar una solicitud al departamento de tecnología en el cual se detallen los motivos por el que solicitan la instalación del/los programas en mención en su estación de trabajo.

B. PROTECCIÓN CONTRA SOFTWARE MALICIOSO

- El servidor al igual que los ordenadores dispuestos a los funcionarios deberán tener instalado y configurado adecuadamente un software antivirus. El mismo deberá estar actualizado y brindando protección en tiempo real.

- En casos explícitos en los cuales sea necesaria la instalación de software externo, se deberá verificar que el mismo sea procedente de fuentes confiables.

C. FIREWALL

- Se deberá implantar un sistema de autenticación robusto para los usuarios conectados.

- Establecer los elementos de la red que se pretenden proteger entre ellos equipos informáticos, datos y sistemas que se manejan.

- Se aplicará una política restrictiva, es decir denegar todo el tráfico a través de la red y habilitar expresamente el tráfico de los servicios que se necesiten.

- El director del departamento de tecnologías deberá establecer un nivel de monitoreo y respuesta permanente ante eventualidades en la red institucional o en las conexiones hacia sitios externos.

D. Copias de Seguridad

- Definir el software adecuado con el que se realizarán los respaldos de información.

- Se establecerá un cronograma donde se detallan los períodos de tiempo en que se realizarán los respaldos o backups.

- El director del departamento de Sistemas será el encargado analizar y determinar la información crítica o de mayor importancia para proceder con los respaldos de información y en dado caso la restauración de la misma para garantizar la disponibilidad de la información y la continuidad de las actividades laborales.

- Se deberá documentar la posible causa por la que pérdida de la información, ya sea por falla de un componente físico o manipulación inadecuada.

- El director de sistemas deberá determinar los componentes más óptimos para almacenar los respaldos de información además de una adecuada ubicación de los mismos.

5. SEGURIDAD FÍSICA

Objetivo:

Proteger el equipamiento y por ende la información que contiene el mismo mediante medidas de contingencia ante desastres naturales además de daños provocados por personas malintencionadas.

A. ÁREAS SEGURAS:

- Cada piso de la institución deberá contar con herramientas auxiliares es decir extintores, alarmas de emergencia y lámparas para salvaguardar la integridad física tanto de los funcionarios como de los recursos ante una eventualidad de índole física o ambiental.

- Se deberá designar un responsable el cual será el encargado de realizar el monitoreo de las condiciones ambientales como temperatura, humedad, etc. a fin de garantizar que los equipos y estaciones de trabajo operen en condiciones adecuadas.

- El responsable de todos activos y en general de las instalaciones al interior del edificio será el conserje quien al ingreso a su jornada laboral (1 hora antes que el resto de personal) verificará el estado de la instalaciones y recursos. De presentarse algún incidente deberá notificar inmediatamente a las autoridades Distritales para tomar las medidas correspondientes.

- La seguridad al exterior de la institución estará a cargo del guardia privado contratado por el Distrito de Educación.

B. CONTROLES FÍSICOS DE ENTRADA

- Los funcionarios a más de registrar su ingreso a la institución a través del sensor biométrico deberán contar con una identificación para el ingreso a la institución con el propósito de evitar acceso de personas externas a la misma.

- Por zonas establecidas como “de alto riesgo” únicamente deberá transitar o tener acceso personal autorizado.

- Se prohíbe al personal institucional el acceso hacia el cuarto de servidores. En caso de tener algún requerimiento únicamente tendrán acceso al departamento de tecnología para que el analista de sistemas le brinda atención inmediata.

C. SEGURIDAD DE EQUIPOS

- Se prohíbe totalmente al personal del distrito de Educación, a excepción de miembros del departamento de sistemas la intervención o manipulación física de los recursos o activos informáticos.

- El cuarto de servidores donde se encuentran los equipos considerados "de mayor importancia" como el servidor, la central de voz IP, y los equipos de red deberán estar situados en una zona segura, aislada completamente de oficinas, departamentos o cualquier unidad del Distrito para evitar toda clase riesgo ya sea peligros ambientales o manipulación de personas no autorizadas.

- Únicamente tendrá acceso a la sala donde se encuentra el equipamiento mencionado en el ítem anterior el responsable de los mismos, es decir el administrador de sistemas con su respectiva identificación.

D. INSTALACIONES DE SUMINISTRO

- Se deben establecer perímetros de seguridad con el objetivo de proteger áreas donde se encuentre cableado, instalaciones equipo de suministro eléctrico, entre otros.

- El cableado de red deberá estar aislado físicamente de los demás tipos de cable especialmente del de corriente o energía eléctrica con el propósito de evitar interferencias.

- Las estaciones de trabajo deberán contar con una adecuada instalación del suministro eléctrico la cual provea energía mediante una fuente de alimentación ininterrumpida o UPS para garantizar la integridad del equipamiento y por ende la información.

E. MANTENIMIENTO DE LOS EQUIPOS

- Se deberá implementar y llevar a cabo un plan de mantenimiento preventivo trimestral de los equipos, el cual permita detectar amenazas para prevenir fallos y problemas futuros.

- De presentarse casos de daños o fallos en el equipamiento del personal deberá realizarse un mantenimiento de índole correctivo en el menor tiempo posible para asegurar la continuidad de las actividades y procesos laborales.

- Ningún funcionario tiene la facultad para intervenir físicamente ni lógicamente ninguna estación de trabajo aunque la misma amerite o necesite

reparación. El usuario deberá reportar el problema al departamento de sistemas para su solución inmediata.

F. SEGURIDAD DE LA ELIMINACIÓN O RE-USO DE EQUIPOS

- En caso de que un activo informático hubiese cumplido su vida útil el departamento de tecnología realizará un informe dirigido a la dirección distrital para continuar con el procedimiento de eliminación.

- Una vez aprobado el informe se procederá a movilizar el bien hacia las bodegas de la institución y posteriormente hacia la empresa recicladora con la que mantiene convenio el distrito de Educación para la eliminación física de los activos.

G. SEGURIDAD DE LOS EQUIPOS Y ACTIVOS FUERA DE LAS INSTALACIONES

- Cada docente informático de las instituciones educativas que conforman el Distrito Nº 1 de Educación deberán mantener un informe detallado sobre el estado y uso de los activos informáticos hacia el departamento de sistemas del Distrito 18D01 de Educación.

- En caso de que los activos en mención necesiten mantenimiento o soporte técnico el docente responsable deberá brindar la solución adecuada. Si el problema tiene un nivel de complejidad elevado, el departamento de sistemas asistirá personalmente para solucionar el problema.

6. CUMPLIMIENTO

Objetivo:

Verificar el cumplimiento de las políticas y normativas establecidas para garantizar la integridad de la información y procesos institucionales.

- La unidad de sistemas realizará un monitoreo y revisión periódica del cumplimiento de las políticas y buenas prácticas de seguridad establecidas.

- Toda violación a las políticas definidas anteriormente será motivo de sanciones aplicables de ley por parte de la dirección al personal que incurra en dicha falta previa investigación y sustento del personal de sistemas.

- El presente SGSI busca abrir el camino a una posible certificación, debido a ello podrá ser actualizado para beneficio de la institución siempre y cuando se respeten los lineamientos de la norma ISO 27001.

4.3 Monitorización e implementación de mejoras

Una vez implementado el Sistema de Gestión de Seguridad de la Información la institución debe llevar a cabo un control y monitoreo periódico sobre el mismo con el propósito de mantener un nivel elevado se seguridad garantizando en todo momento la integridad, confidencialidad y disponibilidad de la información. A partir de ello el Distrito de Educación tiene la obligación de mejorar constantemente la eficacia y productividad en cuanto a resultados del SGSI.

La institución deberá identificar los cambios en relación a los riesgos y vulnerabilidades encontrados y definidos en el presente sistema de gestión y evitar la ocurrencia de los mismos en base a acciones preventivas.

Para plasmar lo anteriormente mencionado se plantea la implementación de un "Plan de Mejora"; una herramienta cuya finalidad será la recolección de todas las acciones denominadas como "de no conformidad" del presente proyecto, el cual deberá ser implementado y puesto en marcha luego de un tiempo prudencial respecto a la implantación del SGSI (2 años mínimo).

El plan de mejora será anual, al inicio del año se procederá con la apertura del mismo y estará constituido por las actividades definidas a continuación:

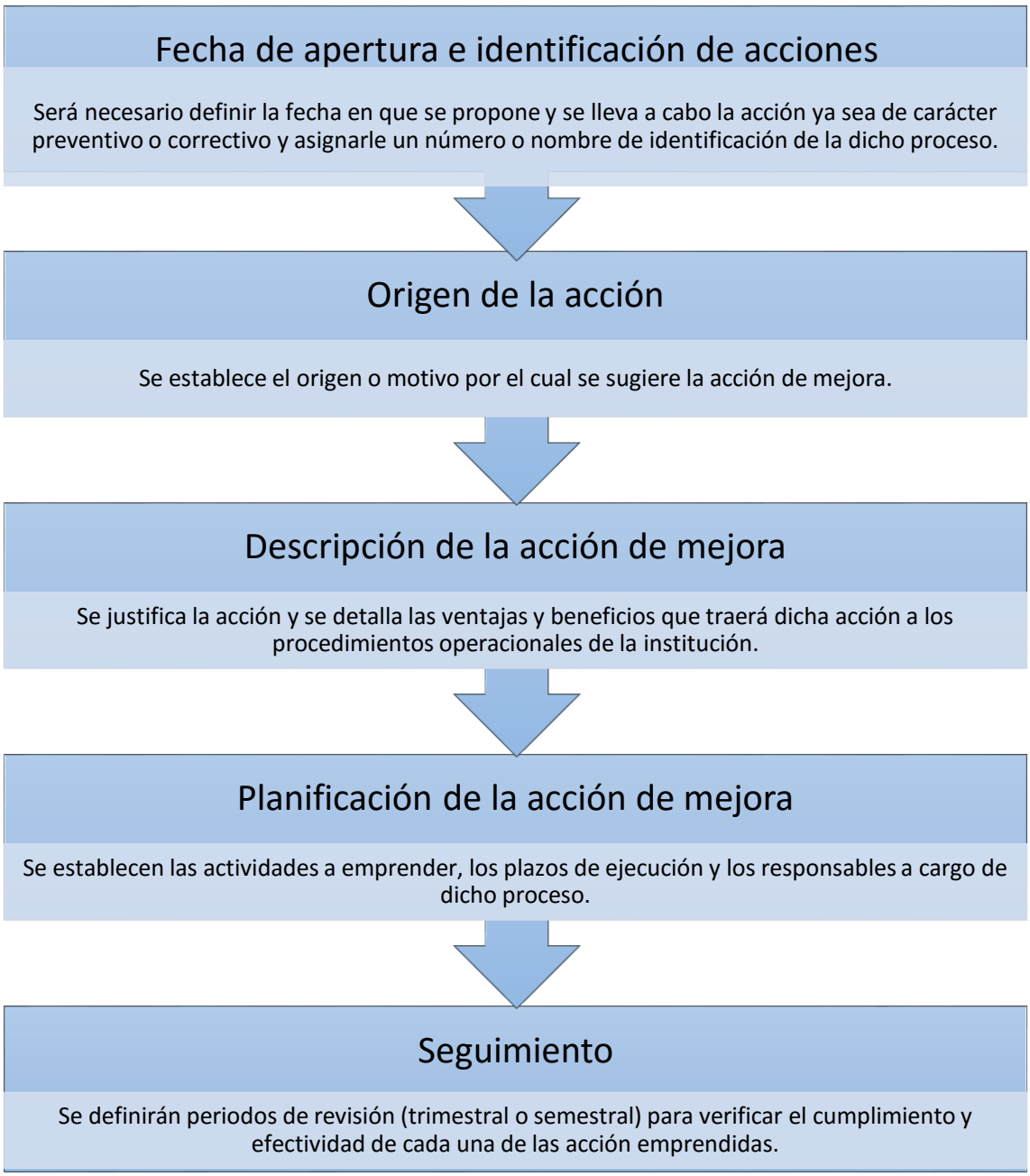


Fig. 13 Metodología de monitoreo y mejoras
Elaborado por Investigador

Es importante mencionar que los procesos de mejora deberán ser propuestos por el personal y de ser el caso aprobados por el Director Distrital durante una reunión o comité con el personal de sistemas y los miembros involucrados en dichos procesos.

CAPÍTULO 5
CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Al término del presente proyecto se concluyó lo siguiente:

- El Distrito 18D01 de Educación no cuenta actualmente con procedimientos relacionados a la salvaguardia de la información. Los diferentes procesos que se llevan a cabo no se los realiza en base a políticas establecidas, únicamente se aplican ciertas normativas para gestionar la información las cuales no son suficientes para garantizar que la información esté asegurada.

- Al no contar con un sistema preventivo para gestionar adecuadamente la información, todas las acciones que emprende la institución en lo referente a la seguridad de la misma son de carácter correctivo lo cual genera un desperdicio de recursos para el Distrito de Educación.

- Se evidenció que no se gestionan adecuadamente los activos informáticos por lo que la información que se procesa a través de los mismos está expuesta en gran medida ante amenazas y vulnerabilidades.

- En cuanto se refiere a la protección física y ambiental existen procedimientos que se llevan a cabo por disposición de planta central pero están enfocados en ciertos aspectos como ubicación y protección de equipos pero se descuidad en gran medida apartados como el mantenimiento de equipos, perímetros de seguridad físico, controles físicos de entrada, etc. con lo cual se expone tanto la integridad de los equipos como del personal.

- Referente a la gestión de comunicaciones y operaciones se gestiona parte la misma. Gracias a las diferentes restricciones y parámetros de seguridad de los sistemas institucionales, los archivos y documentos se encuentran correctamente respaldados y documentados. El problema radica en la falta de seguridad a la red interna convirtiéndose en blanco fácil ante ataques informáticos.

- No se gestiona adecuadamente el control de accesos. Por una parte las claves de usuarios proporcionadas por el departamento de sistemas no modifican periódicamente y por otra no es posible verificar si las claves personales administradas por los mismos funcionarios para el manejo de los sistemas institucionales son lo suficientemente fuertes y confiables.

Recomendaciones

- Implementar el Sistema de Gestión de Seguridad de la información el cual sea supervisado o monitoreado periódicamente a fin de normar delimitar toda actividad relacionada con la seguridad de la información.

- Es necesario concientizar a todo el personal inmerso en el manejo de información dentro del Distrito de Educación sobre la importancia de salvaguardar la información que se procesa a fin de disminuir significativamente la ocurrencia de eventos que comprometan la continuidad institucional.

- La dirección deberá trabajar en conjunto y apoyar al departamento de sistemas en temas relacionados con la seguridad de la información a fin de garantizar la confidencialidad, integridad y disponibilidad de la misma en los diferentes procesos que se llevan a cabo.

- Aprobar, poner en marcha y verificar el cumplimiento de las políticas de seguridad implementadas en el presente proyecto de investigación.

- Realizar un monitoreo y evaluación del SGSI y a partir de ello proponer mejoras de acuerdo a las necesidades institucionales.

Referencias Bibliográficas

[1] «La seguridad informática es un problema internacional,» TechNet, Microsoft, 12 Abril 2007. [En línea]. Available: https://www.microsoft.com/latam/technet/articulos/tn/2007/abr-19.mspx.

[2] K. I. T. Guayta, «Propuesta de Políticas de Seguridad de la información para la CORPAIRE,» Enero 2012. [En línea]. Available: http://bibdigital.epn.edu.ec/bitstream/15000/7790/1/CD-4072.pdf.

[3] S. V. Z. Manosalvas, «Politicas de seguridad y los riesgos informaticos en industria Catedral s.a. de la ciudad de Ambato durante el año 2010,» 2011. [En línea]. Available: http://repo.uta.edu.ec/bitstream/123456789/2381/3/Tesis_t731mrt.pdf.

[4] J. H. MAZZINGHI, «Gestión del riesgo en la seguridad informática: el nuevo escenario del control,» Febrero 2011. [En línea]. Available: http://webcache.googleusercontent.com/search?q=cache:s_BoACRkLP8J:www.cidemconsult.cl/biblioteca/doc/40/raw+&cd=13&hl=es-419&ct=clnk&gl=ec.

[5] J. J. Cano, «Inseguridad Informática: Un concepto dual ·en seguridad informática,» 2004. [En línea]. Available: https://webcache.googleusercontent.com/search?q=cache:TLg9fLP7JRkJ:https://ojsrevistaing.uniandes.edu.co/ojs/index.php/revista/article/download/437/640+&cd=1&hl=es&ct=clnk&gl=ec

[6] M. B. G. C. C. Guerrero, «Plan Maestro de Seguridad Informática para la UTIC de la ESPE con lineamientos de la norma ISO/IEC 27002,» [En línea]. Available: http://repositorio.espe.edu.ec/bitstream/21000/6026/1/AC-GS-ESPE-034491.pdf.

[7] E. p. d. I. 27001, «ISO 27000.ES,» 2005. [En línea]. Available: http://www.iso27000.es/sgsi.html.

[8] S. C. Y. D. V. Leslie Chilán Rodríguez, «Análisis para la integración de un Sistema de Gestión de Seguridad de Información (SGSI) ISO-27001 Utilizando OSSIM para empresa Industria,» Diciembre 2014. [En línea]. Available: http://docplayer.es/1147293-Universidad-politecnica-salesiana-sede-guayaquil-carrera-ingenieria-de-sistemas.html.

[9] P. A. López, «Seguridad Informática,» Editex, 2010, 2016, p. 30.

[10] S. C. d. D. e. S. Estratégica, «Seguridad de la Información,» Ambato, 2014, p. 99.

[11] S. G. d. ISO, «Organismos Nacionales de Normalización en Países en Desarrollo,» 2010. [En línea]. Available: http://www.iso.org/iso/fast_forward-es.pdf.

[12] M. D. P. A. A. G.-C. H. RAMOS, «Seguridad Informática,» Paraninfo, 2011, p. 19.

[13] Federico Alonso Atehortua Hurtado, Ramón Bustamante «Sistema de gestión integral. Una sola gestión, un solo equipo,» Universidad de Antioquía, 2008.

[14] J. C. R. Rico, «Gestión de la Seguridad,» [En línea]. Available: http://www.fundaciondedalo.org/archivos/ACTIVIDADES/SSI07/GestionDeLaSeguridad.pdf.

[15] J. A. B. AREITIO J, Seguridad de la información. Redes, informática y sistemas de información, Paraninfo, 2008.

[16] Allan Silva, « Determinando la población y la muestra,» [En línea]. Available: https://allanucatse.files.wordpress.com/2011/01/tipo-de-muestreo.pdf

ANEXOS

ANEXO A:

FORMATO DE PREGUNTAS REALIZADAS EN LA ENTREVISTA AL DIRECTOR DEL DEPARTAMENTO DE SISTEMAS.

1. ¿Se aplican actualmente políticas de seguridad para gestionar la información? Si ( ) Enúncielas No ( )

. . . . . .

. . . . . .

. . . . . .

2. ¿Están definidas responsabilidades del personal en cuanto al uso adecuado de los recursos?

. . . . . .

. . . . . .

. . . . . .

3. ¿Existe un control sobre el acceso no autorizado de personal, con la finalidad de proteger el equipamiento y sistemas que se manejan en la institución?

. . . . . .

. . . . . .

. . . . . .

4. ¿Se realiza un mantenimiento periódico de los equipos de la institución?

. . . . . .

. . . . . .

5. ¿Han realizado simulacros frente a la caída de los sistemas de información y de comunicación. Si…. De qué manera se lo ha realizado; No….. Porque?

. . . . . .

. . . . . .

. . . . . .

6. ¿Se realizan tareas de monitoreo a los sistemas de información que se manejan?

. . . . . .

. . . . . .

. . . . . .

. . . . . .

7. ¿Se realiza gestión de riesgos en cuanto a la seguridad de la información?

. . . . . .

. . . . . .

. . . . . .

8. ¿Qué mecanismo, técnicas y/o herramientas de seguridad se aplican en los sistemas de información y de comunicación?

. . . . . .

. . . . . .

. . . . . .

9. ¿Dispone de un control sobre el inventario de los activos existentes en toda la institución?

. . . . . .

. . . . . .

. . . . . .