UNIVERSIDAD TÉCNICA DE AMBATO

MAESTRÍA ACADÉMICA (MA) CON TRAYECTORIA PROFESIONAL (TP) EN MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN SEGURIDAD DE REDES Y COMUNICACIONES
COHORTE 2021

Tema: POLÍTICAS DE SEGURIDAD INFORMÁTICAS PARA ANALIZAR VULNERABILIDADES Y RESGUARDAR LA INFORMACIÓN DE LAS UNIDADES ADMINISTRATIVAS DE LA DIRECCIÓN DISTRITAL 18D06 – EDUCACIÓN

Trabajo de Titulación, previo a la obtención del grado académico de Magíster en Tecnologías de la Información Mención Seguridad de Redes y Comunicaciones

Modalidad del Trabajo de Titulación: Proyecto de Titulación con Componente de Investigación Aplicada

Autor(a): Ingeniera Cecilia Elizabeth Torres Carrasco

Director(a): Ingeniero Iván Patricio Ortiz Garcés, Mg.

Ambato – Ecuador

2022

A la Unidad Académica de Titulación del Centro de Posgrados

El Tribunal receptor del Trabajo de Titulación, presidido por el Ingeniero Héctor Fernando Gómez Alvarado. PhD, e integrado por los señores: Ingeniero Carlos Alberto Martínez Bonilla, Magister; Ingeniera Wilma Lorena Gavilanes López, Magister, designados por la Unidad Académica de Titulación del Centro de Posgrados de la Universidad Técnica de Ambato, para receptar el Trabajo de Titulación con el tema: *"Políticas de Seguridad informáticas para analizar vulnerabilidades y resguardar la información de las Unidades Administrativas de la Dirección Distrital 18D06 – Educación"* elaborado y presentado por la *señora Ing. Cecilia Elizabeth Torres Carrasco,* para optar por el Grado Académico de Magíster en Tecnologías de la Información Mención Seguridad de Redes y Comunicaciones; una vez escuchada la defensa oral del Trabajo de Titulación, el Tribunal aprueba y remite el trabajo para uso y custodia en las bibliotecas de la UTA.

Ing. Héctor Fernando Gómez Alvarado. PhD.

Presidente y Miembro del Tribunal

Ing. Carlos Alberto Martínez Bonilla. Mg.

Miembro del Tribunal

Ing. Wilma Lorena Gavilanes López, Mg.

Miembro del Tribunal

AUTORÍA DEL TRABAJO DE TITULACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Titulación presentado con el tema: Políticas de Seguridad informáticas para analizar vulnerabilidades y resguardar la información de las Unidades Administrativas de la Dirección Distrital 18D06 – Educación, le corresponde exclusivamente a: Ingeniera Cecilia Elizabeth Torres Carrasco, Autora bajo la Dirección del Ingeniero Iván Patricio Ortiz Garcés, Magister, Director del Trabajo de Titulación, y el patrimonio intelectual a la Universidad Técnica de Ambato.

Ing. Cecilia Elizabeth Torres Carrasco

c.c.: 1803112315

AUTORA

Ing. Iván Patricio Ortiz Garcés, Mg.

c.c.: 0602356776

DIRECTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que el Trabajo de Titulación, sirva como un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los Derechos de mi trabajo, con fines de difusión pública, además apruebo la reproducción de este, dentro de las regulaciones de la Universidad.

Ing. Cecilia Elizabeth Torres Carrasco

c.c.: 1803112315

ÍNDICE GENERAL

ÍNDICE DE TABLAS

Pág.

ÍNDICE DE FIGURAS

Pág.

AGRADECIMIENTO

Mi agradecimiento a mi hijo Mateo Guerrero Torres, a mis hermanos, a toda mi familia, mis maestros, al Ing. Iván Patricio Ortiz Garcés, Mg. Director de Tesis y compañeros de estudio, todos quienes estuvieron en toda esta etapa de estudio apoyándome y dándome el empuje para llegar a este punto; mi agradecimiento por levantarme cuando estuve caída por la partida de mi madre y el brindarme esas fuerzas que necesité para continuar y realizar mi objetivo propuesto.

Cecilia Elizabeth Torres Carrasco

DEDICATORIA

A mi madre Carmita Carrasco que se encuentra descansando a tu lado Padre Dios, te dedico este trabajo, contigo inicié este sueño, me apoyaste en todo momento y me diste el empuje para empezar este reto, pero partiste antes de tiempo y hoy físicamente ya no estas junto a mí, pero sé que desde el cielo tu estas feliz por mi logro alcanzado, a ti mi amor y mi esfuerzo madre mía.

Cecilia Elizabeth Torres Carrasco

UNIVERSIDAD TÉCNICA DE AMBATO
CENTRO DE POSGRADOS
MAESTRÍA ACADÉMICA (MA) CON TRAYECTORIA PROFESIONAL (TP) EN MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN SEGURIDAD DE REDES Y COMUNICACIONES
COHORTE 2021

TEMA:

POLÍTICAS DE SEGURIDAD INFORMÁTICAS PARA ANALIZAR VULNERABILIDADES Y RESGUARDAR LA INFORMACIÓN DE LAS UNIDADES ADMINISTRATIVAS DE LA DIRECCIÓN DISTRITAL 18D06 – EDUCACIÓN

MODALIDAD DE TITULACIÓN: *Proyecto de Titulación con Componente de Investigación Aplicada*

AUTOR: *Ingeniera Cecilia Elizabeth Torres Carrasco*

DIRECTOR: *Ingeniero Iván Patricio Ortiz Garcés, Magister*

FECHA: *Veintitrés de agosto de dos mil veintidós*

RESUMEN EJECUTIVO

En los últimos años la seguridad informática ha tenido un gran avance de manera que, de gasto ha paso a ser vista como una inversión, por parte de los dirigentes de las instituciones a nivel mundial. Es por eso que la investigación tiene como finalidad realizar Políticas de Seguridad informáticas para analizar vulnerabilidades y resguardar la información de las Unidades Administrativas de la Dirección Distrital 18D06 – Educación, esto aportará confidencialidad, integridad y disponibilidad de la información, a través de la utilización de mecanismos, para garantizar que solo aquellas personas autorizadas accedan a la información y a los recursos cada vez que lo requiera, manteniendo la exactitud y totalidad de la información, para ello se utilizó la investigación aplicada, de manera que, este tipo de investigación ayudó en el estudio, debido que se implementó políticas de seguridad informática, es decir en este caso las

políticas fueron establecidas acorde a los problemas identificados y no se pueden aplicar a otra institución. Así también se utilizó la investigación de campo debido, que durante el estudio se asistió al Distrito para la recolección de información mediante entrevistas, cuestionarios, encuestas y observaciones que permitan analizar los factores de riesgo de la seguridad informática. Por otra parte, también se utilizó el enfoque cuantitativo, porque en el estudio se empleó una lista de cotejo la cual se avaluó por los especialistas de la universidad, al igual que también se utilizó el enfoque cualitativo el cual permitió realizar preguntas e hipótesis antes, durante o después de la recolección y el análisis de los datos. Es por eso que en el estudio se trabajó con una muestra conformada por 10 Departamentos Administrativos del Distrito 18D06 Cevallos a Tisaleo. Después de realizar el estudio se concluyó que el establecimiento de políticas de ayudaron a manejar de forma íntegra, confiable y legal toda la información, y también protegerlos de los riesgos que se puedan presentar**,** y el contar con políticas de seguridad que permitirá tener una institución de confianza.

DESCRIPTORES: CUALITATIVO, CUANTITATIVO, ESPECIALISTAS, ENTREVISTAS, FACTORES DE RIESGO, INTEGRIDAD, INVESTIGACIÓN, INFORMACIÓN, POLÍTICAS, SEGURIDAD INFORMÁTICA.

UNIVERSIDAD TÉCNICA DE AMBATO
CENTRO DE POSGRADOS
MAESTRÍA ACADÉMICA (MA) CON TRAYECTORIA PROFESIONAL (TP) EN MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN SEGURIDAD DE REDES Y COMUNICACIONES
COHORTE 2021

THEME:

COMPUTER SECURITY POLICIES TO ANALYZE VULNERABILITIES AND PROTECT THE INFORMATION OF THE ADMINISTRATIVE UNITS OF THE DISTRICT DIRECTORATE 18D06 – EDUCATION

DEGREE MODALITY: *Degree Project with an applied research component*

AUTHOR: *Engineer Cecilia Elizabeth Torres Carrasco*

DIRECTED BY: *Engineer Iván Patricio Ortiz Garcés, Master*

DATE: *August twenty-third, two thousand twenty-two*

EXECUTIVE SUMMARY

In recent years, computer security has made great progress in such a way that, from spending, it has come to be seen as an investment, by the leaders of institutions worldwide. That is why the purpose of the research is to carry out Computer Security Policies to analyze vulnerabilities and protect the information of the Administrative Units of the District Directorate 18D06 - Education, this will provide confidentiality, integrity and availability of information, through the use of mechanisms, to guarantee that only those authorized persons access the information resources whenever required, maintaining the accuracy and completeness of the information, for which applied research was used, so that this type research helped in the study, because computer security policies were implemented, that is, in this case the policies were established according to the problems identified and cannot be applied to another institution. Thus,

due field research was also used, which during the study assisted the District to collect information through interviews, questionnaires, surveys and observations that allow analyzing the risk factors of computer security. On the other hand, the quantitative approach was also used, because in the study a checklist was used, which was evaluated by the specialists of the university, as well as the qualitative approach, which allowed asking questions and hypotheses before, during or after data collection and analysis. That is why the study worked with a sample made up of 10 Administrative Departments from District 18D06 Cevallos to Tisaleo. After carrying out the study, it was concluded that the establishment of policies helped to manage all the information in an integral, reliable and legal way, and also protect them from the risks that may arise and having security policies that will allow to have a trusted institution.

KEYWORDS: QUALITATIVE, QUANTITATIVE, SPECIALISTS, INTERVIEWS, RISK FACTORS, INTEGRITY, RESEARCH, INFORMATION, POLICIES, COMPUTER

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1 Introducción

En los últimos años la seguridad informática ha tenido un gran avance de manera que, de gasto ha paso a ser vista como una inversión, por parte de los dirigentes de las instituciones a nivel mundial. Es por eso por lo que se puede indicar que en varios países el crecimiento ha sido acelerado y en otros ha sido lenta, pero en última instancia todos han convertido en un mundo digital, en el cual el mundo digital es un activo intangible muy valioso, de forma que debe ser custodiado o protegido de posibles robos, mal uso de información, perdidas, daños, etc. (Tirado , Ramos , Álvarez , & Carreño , 2020)

En el caso de Ecuador se ha visto que las redes de computadoras son atacadas y vulneradas, es por eso por lo que año tras año se ha incrementado la facilidad de ejecución, velocidad de programación, y el daño que pueden causar este tipo de ataques, es por eso por lo que se considera necesario tener políticas adecuadas de seguridad informática, las cuales permitan proteger la información.

También se debe reconocer que actualmente la facilidad de conectarse a cualquier red ha ido en aumento, de forma que los software y aplicación son más accesibles y amigables, es por eso por lo que se tienden a conectarse en una sola red para poder compartir sus recursos, pero ese pequeño detalle representa un gran riesgo. Para eso es necesario que las entidades dispongan de medios que permitan mitigar en gran nivel la vulneración de recursos e información. (Vega , 2018)

1.2 Justificación

El presente estudio es importante debido que el desarrollo de Políticas de Seguridad informáticas ayudará analizar vulnerabilidades de la información de las Unidades Administrativas de la Dirección Distrital 18D06 – Educación, debido que la información constituye uno de los recursos principales de una organización, por lo tanto, se la debe proteger, mediante un conjunto de actividades, controles y políticas de seguridad que se deben implementar en base a recursos humanos, hardware y software. La seguridad de la información depende de la gestión y los procedimientos adecuados, de los empleados de la organización, y del nivel de seguridad de los medios técnicos. (Vega , 2018)

Establecer la seguridad informática aportará integridad y disponibilidad de la información en la red, a través de la utilización de mecanismos, para garantizar que solo aquellas personas autorizadas accedan a la información y a los recursos de red cada vez que lo requiera, manteniendo la exactitud y totalidad de la información.

Así también el estudio será de beneficio para los operarios de las Unidades Administrativas de la Dirección Distrital 18D06 – Educación, debido que aportara con información valiosa que permita asegurar la información, y no se vea comprometida voluntaria e involuntariamente, el hecho de trabajar con información errónea puede ser tan dañino para las actividades como perder la información, de hecho, si la manipulación de la información es lo suficientemente sutil puede causar que se arrastre una cadena de errores acumulativos y que sucesivamente se tome decisiones equivocadas. (Castro, 2018)

1.3 Objetivos

1.3.1 General

Realizar Políticas de Seguridad informáticas para analizar vulnerabilidades y resguardar la información de las Unidades Administrativas de la Dirección Distrital 18D06 – Educación.

1.3.2 Específicos

- Fundamentar teóricamente las políticas de Seguridad informática para analizar vulnerabilidades y resguardar la información de las Unidades Administrativas de la Dirección Distrital 18D06 – Educación.
- Establecer políticas de seguridades informáticas para evitar vulnerabilidades y proteger la información de las Unidades Administrativas de la Dirección Distrital 18D06 - Educación.
- Proponer seguridades mediante normas ISO 27001, sugerir el levantamiento de un SERVER y trabajar con carpetas compartidas usando software libre.
- Plantear una propuesta que permita la generación de una guía de procedimientos de Seguridad enfocados a la parte de las Unidades Administrativas para reducir la fuga de información confidencial de la Dirección Distrital 18D06 - Educación.

CAPITULO II

MARCO TEORICO

2.1 Antecedentes Investigativos

Durante mucho tiempo las entidades solo se preocupaban por mejorar los sistemas informáticos, dejando a un lado y sin darle importancia las seguridades, las mismas que con el pasar de los años se han venido perfeccionando la forma de vulnerar la información de las organizaciones siendo estas susceptibles a ser violentas, todo esto con la evolución de los sistemas que nos juega el pro y el contra, en el avance tecnológico tanto en el internet y de las comunicaciones en general han abierto una puerta para que las personas empiecen a descubrir el valor de la información y la facilidad de acceder a los datos.

Actualmente la mayoría de las entidades por no decir todas, tanto en el sector privado como público dan prioridad a respaldar y cuidar su información tomando medidas y brindando seguridad a la información, la misma que es considerada como uno de los bienes más preciados para la continuidad de procesos.

El desarrollo del estudio propuesto nace de la necesidad de la seguridad de la información que maneja el distrito objeto de estudio, debido que no cuenta con políticas de seguridad informática, necesitando ser investigado para obtener una alternativa de solución, ya sea preventiva o correctiva, sobre seguridades; además, es imposible encontrar métodos de seguridad que completamente seguros, ya que cada día aparecen nuevos riesgos en distintos niveles. Por los riesgos que surgen día a día en la administración de datos y posteriormente en su actividad, es importante ejecutar un análisis de amenazas basándonos en la normatividad ISO 27001 o más, para controlar mejor los procedimientos y neutralizar las amenazas que puedan causar debilidades y ser vulneradas la información. (Catuto, 2021)

Ante lo indicado se presentan investigaciones que han realizado estudios similares:

El estudio de Vega (2008), de la Universidad La Salle en Bolivia**,** indica que **l**as facilidades para conectarse a las redes han aumentado; además, las aplicaciones y el software son cada vez más amigables y accesibles, de esto modo todos tienden a conectarse en una red para compartir los recursos, pero esa facilidad de conexión también representa un aumento en los riesgos de que la información y los recursos de una organización puedan ser vulnerados. Es por eso por lo que se deben implementar medidas de seguridad para proteger la información y los activos de la Empresa. Seguridad significa disponer de medios que permitan reducir lo más que se pueda, la vulnerabilidad de la información y de los recursos; aunque no se puede alcanzar el 100% de seguridad, la tendencia debe ser llegar a ese valor extremo.

Los hackers, crackers están vigilando permanentemente las redes con el fin de encontrar las vulnerabilidades o debilidades de un sistema de información, el desarrollo del software ha permitido hacer cada vez más fácil la configuración y su utilización, Internet también permite la conectividad de todo tipo de usuario, de esta forma las amenazas a la seguridad de la Información están latentes y en cualquier momento un servidor o dispositivo de red puede ser atacado con fines negativos a la imagen de la Empresa o Institución, a su funcionalidad y otros aspectos

Es por eso por lo que el autor concluye que la información constituye uno de los recursos principales de una organización, por lo tanto, se la debe proteger, mediante un conjunto de actividades, controles y políticas de seguridad que se deben implementar en base a recursos humanos, hardware y software. La seguridad de la información depende de la gestión y los procedimientos adecuados, de los empleados de la organización, proveedores, clientes, accionistas y del nivel de seguridad de los medios técnicos.

Por su parte Romero y otros (2018) enfatiza que el términos de seguridad informática se debe entender a las bases que conforman los cimientos de esta ciencia, para las partes

más complejas de esta disciplina, una de estas bases es el concepto de seguridad, la cual consiste en un estado de bienestar, es la ausencia de riesgo por la confianza que existe en alguien o algo, si la seguridad se aborda desde el tema disciplinario el concepto se puede definir como una ciencia interdisciplinaria para evaluar y gestionar los riesgos a los que se encuentra una persona, un animal, el ambiente o un bien. Existen países en donde la seguridad es un tema nacional, aunque depende del tipo de seguridad, existen muchos tipos de ésta, por ejemplo, la seguridad ambiental, la seguridad económica, la seguridad sanitaria y en casi la mayoría de los países cuando se hace un análisis de la palabra seguridad, se hace referencia a la seguridad de las personas, por ejemplo, evitar el estado de riesgo de un robo, de un daño físico o de un bien material.

Mientras que Departamento de Tecnología Organización Inca (2016), presentado en Lima Perú enfatiza que las políticas de seguridad informática que es una manera de comunicarse con los usuarios, de manera que las mismas crean un canal de comunicación en relación con los recursos informáticos de la institución. Así también se puede resaltar que las políticas de seguridad informática no se considera como una técnica o expresión legal que involucre sanciones a empleados, sino más bien son descripciones de lo que se desea resguardar, de manera que una política que permite reconocer a la información como uno de los principales activos, así como un motor de intercambio y desarrollo en el ámbito de sus negocios. Por tal razón, las políticas de seguridad deben concluir en una posición consciente y vigilante del personal.

2.2 Desarrollo de Variables de Estudio

2.2.1 La seguridad

Al hablar de términos de seguridad informática se debe entender a las bases que conforman los cimientos de esta ciencia, para las partes más complejas de esta disciplina, una de estas bases es el concepto de seguridad, la cual consiste en un estado de bienestar, es la ausencia de riesgo por la confianza que existe en alguien o algo, si la seguridad se aborda desde el tema disciplinario el concepto se puede definir como

una ciencia interdisciplinaria para evaluar y gestionar los riesgos a los que se encuentra una persona, un animal, el ambiente o un bien. Existen países en donde la seguridad es un tema nacional, aunque depende del tipo de seguridad, existen muchos tipos de ésta, por ejemplo, la seguridad ambiental, la seguridad económica, la seguridad sanitaria y en casi la mayoría de los países cuando se hace un análisis de la palabra seguridad, se hace referencia a la seguridad de las personas, por ejemplo, evitar el estado de riesgo de un robo, de un daño físico o de un bien material.

La seguridad siempre busca la gestión de riesgos, esto quiere decir que se tenga siempre una forma de evitarlo o prevenirlo y que se pueda realizar ciertas acciones para evitar esas situaciones de la mejor forma. Se definió que la seguridad podría ser catalogada como la ausencia de riesgo, la definición de este término involucra cuatro acciones que siempre están inmersas en cualquier asunto de seguridad como son:

- Prevención del riesgo
- Transferir el riesgo
- Mitigar el riesgo
- Aceptar el riesgo

Así que, cuando se está buscando hacer algo más seguro, estas acciones son algo que se debe de considerar sin importar el área, se aplica a cualquier intento de tener mejor o mayor seguridad en cualquier tema que se requiera.

2.2.2 Seguridad informática

Hay que tener en cuenta que en varios casos se suelen confundir dos conceptos, los cuales son la seguridad informática y la seguridad de información, aunque las dos palabras son similares son muy diferentes de manera que seguridad informática es la que se encarga de las técnicas, procesos, que procesan transmiten y almacenan la información, por su parte la seguridad de información no solo se preocupa del medio informático, además se preocupa de todo lo que tenga información, en si abarca todo.

Según Figueroa (2021), puntualiza la protección de la información en especial, al proceso que se le realiza, con la prioridad de evitar la manipulación de datos y procesos por personas no autorizadas. Su finalidad es que tanto personas como equipos tecnológicos y datos estén protegidos contra daños y amenazas hechas por terceros.

Ante el criterio emitido por el autor Figueroa se puede indicar que en la actualidad la informática está siendo ahogada por todo tipo de información posible, aunque la información sigue siendo un universo complejo, de modo que los procesos en varias ocasiones son más visibles.

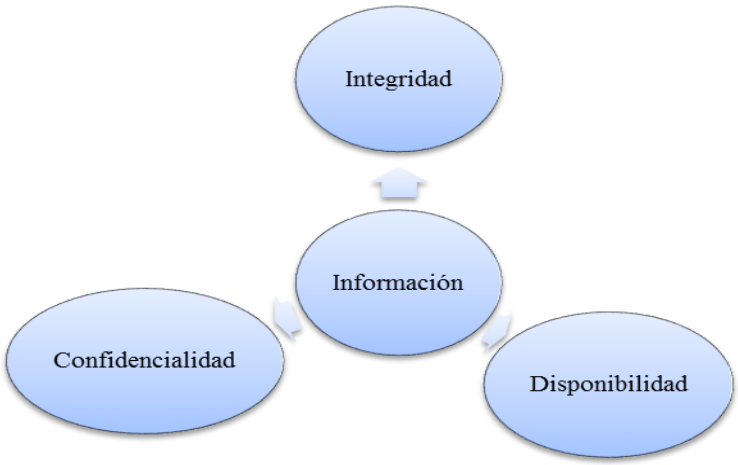
La función principal de la seguridad informática es la que se encarga de minimizar los riesgos, en este caso también puede ser por el ingreso de información, de los usuarios, del hardware e incluso de todos los protocolos de seguridad que se implementan, pero el fin es reducir los riesgos.

2.2.3 Pilares de la seguridad

Los datos son valores, números, medidas, textos, documentos en bruto, la información es el valor de esos datos, es lo que aporta conocimiento. Los manuales de procedimientos, los datos de los empleados, de los proveedores y clientes de la empresa, la base de datos de facturación son datos estructurados de tal forma que se convierten en información, que aportan valor como compañía.

Los pilares de la SI, se basan en la necesidad que todos tienen para obtener información, de su integridad disponibilidad e importancia, lo que ayude a obtener su mayor rendimiento con el mínimo riesgo.

***Figura 1**: Pilares de Seguridad*



Nota: Aquí se muestra los pilares que debe tener la seguridad informática.

Como se puede observar en la figura 1, la seguridad debe contener tres pilares base de información, de modo que, si alguno de los tres lados pierde usabilidad, o seguridad, la institución quedará expuesta a diversos ataques, es por eso por lo que es necesario conocer la función que tiene cada uno de sus lados para que sufra ningún desfase.

2.2.4 Confidencialidad:

En términos de seguridad de la información, la confidencialidad hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos. El objetivo de la confidencialidad es, entonces, prevenir la divulgación no autorizada de la información. (Calderón , 2020)

En general, cualquier empresa pública o privada y de cualquier ámbito de actuación requiere que cierta información no sea accedida por diferentes motivos. Uno de los ejemplos más típicos es el de la inteligencia de un país. Además, es sabido que los logros más importantes en materia de seguridad siempre van ligados a temas estratégicos militares.

Los principios de confidencialidad no solo deben aplicarse para proteger la información sino todos aquellos datos e información de los que sea responsables. La información

puede tener carácter confidencial no solo por ser de alto valor para la organización, sino por ejemplo porque puede estar amparada por legislación de protección de datos de carácter personal, un ejemplo de violación de la confidencialidad son las filtraciones sufridas por entidades bancarias, grandes empresas y gobiernos para exponer públicamente algunas de sus actividades.

2.2.5 La integridad:

Este es uno de los principales pilares de seguridad, debido que se encarga de que la información sea respaldada y no se comprometa de ninguna manera, de manera que el hecho de trabajar con información errónea puede resultar tan complicado en el caso de perder información.

2.2.6 Disponibilidad:

Para poder considerar que se dispone de una seguridad mínima en lo que a la información respecta, se tiene a la disponibilidad, de nada sirve que solo el usuario acceda a la información y que sea incorruptible, si el acceso a la misma es tedioso o imposible, la información para resultar útil y valiosa debe estar disponible para quien la necesita, se debe implementar las medidas necesarias para que tanto la información como los servicios estén disponibles, por ejemplo un ataque distribuido de denegación de servicio o DDoS puede dejar inutilizada una tienda online impidiendo que los clientes accedan a la misma y puedan comprar. Otro ejemplo de perdida de disponibilidad sería que la dirección de correo electrónico sea utilizada para lanzar campañas de spam y en consecuencia añadida a listas negras, impidiendo que ninguno de los destinarios de los emails legítimos los reciba.

2.2.7 La ISO 27001 seguridad de información

La norma ISO 27001 es una normativa internacional que tiene como objetivo llegar a la protección de la confidencialidad de la información y los datos de la entidad. Es una norma desarrollada como modelo para el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora de un SGSI para cualquier tipo de

organización. Permite diseñar e implantar un SGSI, en base a las necesidades, objetivos, requisitos de seguridad, los procesos, los empleados, el tamaño, los sistemas de soporte y la estructura de la organización. (Mantilla , 2018)

La norma ISO 27001 es:

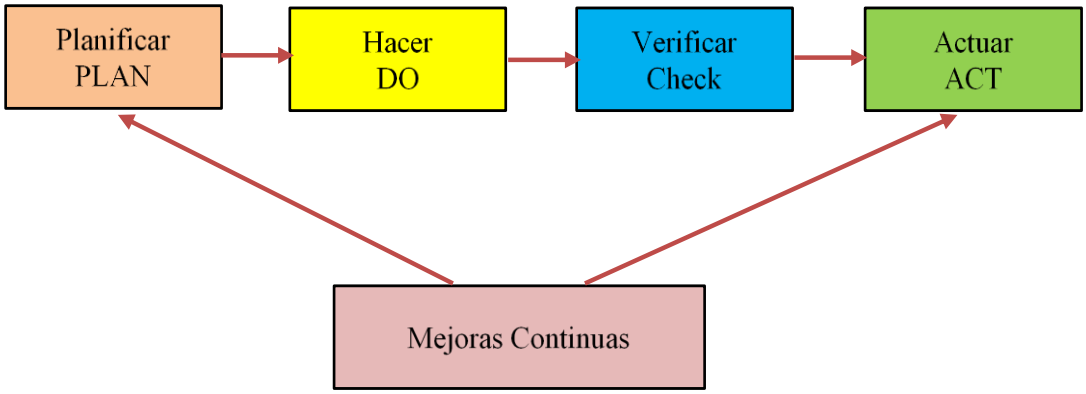
- Se puede recalcar que la ISO 27001 es una norma internacional que permite la confidencialidad, aseguramiento, e integridad de la información y datos, así como de los sistemas que la procesan.
- La aplicación de ISO-27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización.
- La Gestión de la Seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002. (Ministerio de Industria, Comercio y Turismo, 2017)

Dentro de la organización el tema de la seguridad de la información es un capítulo muy importante que requiere dedicarle tiempo y recursos. La organización debe plantearse un Sistema de Gestión de la Seguridad de la Información (SGSI). El objetivo de un SGSI es proteger la información y para ello lo primero que debe hacer es identificar los “activos de información” que deben ser protegidos y en qué grado. (Calderón , 2020)

Luego debe aplicarse el plan PDCA ('PLAN – DO – CHECK – ACT'), es decir Planificar, Hacer, Verificar, Actuar y repetir el ciclo. Es decir, este proceso es entendido que nunca termina, de manera que los riesgos a los que se encuentran expuestos son interminables, pero se pueden tratar. (Calderón , 2020)

Ante lo indicado se puede indicar que los problemas de seguridad no son únicamente de naturaleza tecnológica, es por esa razón que son imposibles eliminarlos en su totalidad, es por eso por lo que un SGSI cumple con cuatro niveles repetitivos, estos ayudan a mejorar la seguridad en la institución.

Figura 2: *Sistema de Gestión de Seguridad informática*



Nota. Se muestra los niveles del SGSI, para mejorar el proceso que ayudan a mejorar la seguridad.

- **PLANIFICAR (Plan):** esta etapa es la que se encarga de la creación de políticas, selección de controles, análisis de riesgos, así como también se analiza la situación de la entidad.
- **HACER (Do):** en esta fase se realiza la implementación del SGSI, así como también los controles, y la seguridad informática.
- **VERIFICAR (Check):** mediante el proceso de verificación se realiza auditorías internas, los cuales ayudan a constatar si los procesos realizados están correctamente ejecutados.
- **ACTUAR (Act):** consiste en ejecutar tareas de mantenimiento, propuestas de mejora, acciones preventivas y acciones correctivas. (Calderón , 2020)

Porque se trabaja con ISO 27001

Aquí podemos discernir observando las ventajas y desventajas de las normas ISO 27001.

Tabla 1: Ventajas y desventajas de las normas ISO 27001

Ventajas	Desventajas
Certificado de confianza y calidad empresarial	Modificación de rutinas y procesos internos
El mejor sistema de seguridad interna	Delegación de responsabilidades
Reducción de los casos de riesgo	
Aumenta la conciencia y el compromiso	

Nota. Se puede observar las ventajas y desventajas al trabajar con las normas ISO 27001

2.2.8 La ISO 27002

Esta ISO permite proteger la información, la cual constituye el código de las mejores prácticas en lo que se refiere a la implementación del Sistema de Gestión de Seguridad de la Información. Así también se puede observar que establece principios y directrices, de manera que puede mejorar el SGSI en la empresa.

2.2.9 Sistemas Operativos Libres

Son un grupo muy pequeño de personas con conocimiento más profundo de la tecnología, podría utilizar la alternativa de un software libre, ya que muy pocas personas se adaptan en utilizar y trabajar como por ejemplo en Linux, conociendo que es un sistema operativo totalmente libre con un código abierto adaptándolo a nuestras necesidades.

Este Sistema Operativo respeta totalmente la necesidad del usuario para lo que quiera hacer uso con el software sea este en su modificación y en su redistribución, es por eso la palabra Libre.

Características de los S.O. Libres

Las características que definen un sistema operativo libre son:

- Puede usarse para cualquier propósito.

- Las fuentes pueden ser estudiadas y cambiadas.
- El SO puede distribuirse arbitrariamente.

Samba

Es una herramienta de red extremadamente útil sea para un sistema Windows y Unix en su red, permite que Windows comparta archivos e impresoras y también permite a los usuarios acceder a los recursos compartidos por los sistemas Windows.

Samba se ejecuta en plataformas Unix, pero se dirige a los clientes de Windows como un nativo, este permite que un sistema Unix se mueva a un entorno de red de Windows sin causar problemas. Los usuarios de Windows pueden acceder con gusto a los servicios de archivos e impresión sin saber ni preocuparse de que esos servicios los ofrezca un host Unix.

Samba ofrece varios servicios:

- Permite compartir uno o algunos sistemas de archivos
- Permite compartir uno o diversos sistemas de archivos distribuidos
- Permite compartir las impresoras que se encuentran instaladas en el servidor entre todos los clientes Windows que están en la red
- Permite a los clientes navegar por la red
- Uno de los mayores beneficios es que permite autentificar a los clientes que ingresan en un dominio Windows.

Cuentas de usuario

Samba es un servicio que requiere de “administración de usuarios” para poder realizar los permisos correspondientes. En función del usuario que acceda, samba se comportará de una forma u otra ya que cuando accede un usuario normal, estos tienen unos permisos limitados por cuestiones de seguridad y cuando accede un usuario como

administrador, este dispondrá de todos los permisos acorde a las funciones que desempeñe.

Para que la administración sea posible samba dispone de su propia base de datos de “usuarios samba” pero como los usuarios utilizan otros recursos del servidor como carpetas e impresoras, es necesario que estén creados en el sistema Unix - Linux.

Carpetas compartidas

El protocolo Samba nos permite conectar Windows con el sistema de archivos Linux y de esta forma ver discos y carpetas Linux como unidades de red en Windows.

Las carpetas compartidas son un recurso útil que nos permite trabajar con documentos en común dentro de un grupo o grupos de trabajo, con seguridades entre ellos los permisos que se les da a cada uno del usuario que ingrese a la carpeta.

2.2.9.1 Linux

Linux es un software libre, y este recibe el nombre de una serie de sistemas operativos de tipo Unix en su gran mayoría son gratuitos, con la particularidad de que podemos instalar un sistema muy ligero e ir agregando todo lo necesario posteriormente o según lo vayamos necesitando.

Linux es multiusuario, multitarea y multiplataforma, es de código libre del cual podemos utilizarlo, copiarlo, modificarlo y redistribuirlo libremente para cualquier uso que queramos darle o adaptarlo.

Linux está hecho para funcionar todo el hardware de un PC, ya que un ordenador no puede funcionar sin un sistema operativo y Linux es un sistema operativo gratuito, este sistema operativo también es conocido por controlar servidores que es donde en realidad Linux toma importancia gracias a sus tareas específicas y a sus capacidades de personalización.

2.2.9.2 Centos

Es un sistema operativo Linux para empresas, proporciona una plataforma informática gratuita y de código abierto, compatible con su fuente ascendente, Red Hat Enterprise Linux.

Centos es uno de los Sistemas Operativos más elegidos a la hora de montar un servidor Linux, es el dominante entre las empresas que brindan servicios de hosting y servidores. Esto es gracias a una excelente estabilidad y seguridad, soportada por una comunidad representada en manuales foros y demás que se encuentran en una constante actualización para las particularidades de este sistema operativo.

2.9.10 Sistemas Operativos Licenciados.

Estos sistemas operativos se basan al pago de la licencia del software que se requiere utilizar en una organización, empresa, entidad u otra, es el derecho a utilizar el software de forma específica, los términos de la licencia describen el uso permitido del software, los derechos del autor el mismo que limita como una persona puede utilizar el software. Estos Sistemas Operativos licenciados están en igualdad de condiciones frente a la seguridad que los sistemas operativos libres.
La única diferencia entre un Software licenciado y uno libre es que el pagado tiene la ventaja que el fabricante da soporte técnico y las garantías de seguridad de sus sistemas a utilizar

2.9.10.1 Windows Server

Windows Server dio inicio a principios de siglo con Windows 2000, un sistema que continuaba con el legado de Windows NT que unía bajo una misma denominación tanto las versiones de escritorio como servidores.

El ecosistema de Windows Server no es solo el sistema operativo sino también todas las herramientas que lo rodean y que lo ayudan a cumplir su misión.

Dentro de Windows Server podemos encontrar herramientas para realizar las mismas tareas que en un Unix o Linux. Este Sistema Operativo está desarrollado en C++ y Assembler, entre una de sus características más destacadas para equipos de trabajo es que es un sistema multiusuario. Por lo tanto, es un sistema que pueden utilizar todos los empleados de una determinada compañía, centralizando así la gestión y administración de archivos.

Las ventajas que ofrece Windows Server como Sistema Operativo son relevantes para favorecer el trabajo de los programadores y desarrolladores y, por tanto, mejorar los resultados corporativos, además tiene una administración muy sencilla, de modo que el sistema se puede manejar de forma rápida y eficiente. Además, y resalta por ser muy flexible.

2.2.11 Políticas de seguridad informática

Se puede resaltar que la seguridad informática en los últimos años ha tomado gran auge, debido a que el mundo posee un nivel de desarrollo tecnológico importante, debido que la forma de conexión mediante redes abierto nuevos horizontes de comunicación, lo cual ha traído nuevas amenazas para los sistemas de información, es por eso por lo que se ve en la necesidad de desarrollar un documento que ayude a mitigar la diversidad de riesgos que se presentan en la seguridad informática.

2.2.12 Malware

Para García (2017), malware o malicious software (software malicioso), se refiere a cualquier tipo de aplicación o programa informático, que después de infectar el sistema, daña de diferentes formas los sistemas informáticos acorde al tipo de malware, de manera intencional o sin que el usuario se dé cuenta.

Este tipo de aplicación puede clasificarse como spyware, gusanos, ransomware, troyanos, y otros los cuales se detallan posteriormente; por lo anterior se podría decir

que malware se refiere a cualquier tipo de código malicioso o amenaza informática de tipo lógico, aunque se le llame solo virus. (García , 2017)

2.2.13 Ransomware

Ransomware se forma al unir ransom (rescate, en inglés) con ware (producto o mercancía, en inglés). Ya que en este caso el malware pide un rescate (ransom) a la víctima, a través de un mensaje o una ventana emergente, de ahí el nombre. Es un «secuestro virtual» de nuestros recursos por el que nos piden un rescate. (Instituto Nacional de Ciberseguridad, 2017)

Mediante un mensaje, que suele ser intimidante, avisan a la víctima de que la única forma en que puede descifrar sus archivos o recuperar el sistema es pagar al cibercriminal. Es habitual que incluyan un límite de tiempo para pagar el rescate o amenacen con la destrucción total de los archivos secuestrados o con incrementar el valor del rescate si no se paga a tiempo.

El ransomware (secuestro de información) es el término genérico para referirse a todo tipo de software malicioso que le exige al usuario del equipo el pago de un rescate. (López, 2016)

2.2.14 Virus informáticos

Unos de los primeros conceptos cuando se habla de seguridad informática, es el de virus informático. Las computadoras solo entienden código binario como ceros y unos, en el mundo de las computadoras y de la informática existen muchos conceptos como el de programas, videojuegos, sistemas operativos y cualquier clase de software.

El software es uno de los conceptos más abstractos, se lo define como todo lo intangible de la computadora, son instrucciones que el ordenador espera que se realicen, las cuales pueden ser instrucciones complejas o instrucciones sencillas.

Según Beynon-Davies (2015), el término software o programa es utilizado para describir una secuencia de varias instrucciones que es leído por un computador, los cuales son escritos en un determinado lenguaje de programación que pueden ser clasificados de la siguiente manera:

- Lenguaje de máquina
- Lenguaje ensamblador
- Lenguajes de alto nivel

Analizado el tema clave sobre el software, un virus informático es un programa que tiene como objetivo dañar o cambiar el funcionamiento de la computadora. Esta es una definición bastante clara, pero el virus informático no siempre tiene que ser un programa completo, puede ser hasta cierto punto fragmentos de un programa.

Según Vieites (2016), se define al virus informático, como un programa desarrollado en un determinado lenguaje de programación (C++, C, ensamblador, etc.) con el objetivo de infectar uno o varios sistemas informáticos, utilizando varios mecanismos de propagación o auto replicación, el cual trata de reproducirse de forma acelerada para extender su alcance.

Un virus informático puede hacer muchas cosas, por ejemplo, eliminar archivos, evitar accesos a las computadoras, robo de información, bloqueo de funciones de un sistema operativo o de programas dentro de una computadora. También Vieites (2016), indica que existen varios tipos de virus que se los puede definir de la siguiente manera:

- Virus de sector de arranque (BOOT)
- Virus de archivos ejecutables
- Virus de macros
- Virus de lenguajes de Script
- Gusanos
- Troyanos
- Spyware

- Keyloggers
- Adwares
- Dialers
- Backdoors
- Rootkits

Se mencionó algunos, ya que la lista es bastante grande pero la mayoría son programados para causar daños relacionados con la red y tener la capacidad de auto propagación, esto quiere decir que se multiplica el mismo muchas veces y se posiciona en partes automatizadas del sistema operativo infectado.

Las bombas de tiempo son virus que se activan al pasar un determinado tiempo o al producir un evento, el que puede ser, por ejemplo, abrir el navegador, pero los eventos suelen ir relacionados con ciertos cálculos matemáticos y registros de memoria, aunque también existen los que se activan con tareas sencillas, estos son solamente algunos de los tipos que se podrían mencionar.

2.2.15 Concepto de autenticación

La autenticación se puede definir como un proceso en el que se busca confirmar algo como verdadero, no se busca verificar un usuario, ya que la autenticación no siempre está relacionada con estos, en muchos casos se quiere saber si un cambio o un dato es correcto, no se debe cometer el error en pensar que solamente las personas necesitan este proceso, este puede ser para cualquiera, un sistema, un dispositivo o una persona.

La autenticación es bastante usada en el mundo de la computación, sólo que actualmente la contraseña del correo o de una red social ha hecho olvidar que este método de validación era ya muy común, por ejemplo, todas las credenciales que expiden para realizar una votación en determinado país es un método de autenticación, otro ejemplo es cuando se ingresa a un país y solicitan un documento como la visa o pasaporte, también es un método de autenticación, otro caso es cuando se asigna un número de cuenta o ID de identificación en el trabajo para acceder a ciertas áreas o

también para llevar un registro de los movimientos y en caso de ser necesario poder validar esos movimientos. (Vega, Politicas y Seguridad de la informacion, 2008)

Existen diversos tipos de autenticación, se va a conocer algunos de ellos los más implementados ya que todos los días se trabaja en encontrar más y mejores métodos. Se tiene los tipos de autenticación en los que se tiene algo conocido, en teoría únicamente por el usuario, por ejemplo, una contraseña, eso es lo más común, pero en teoría, ya que, si se proporciona el usuario y la contraseña del correo electrónico, también puede entrar otro usuario y no significa que sea la persona dueña de la cuenta.

Otro tipo de autenticación es la que se basa en algo de propiedad del usuario, por ejemplo, la tarjeta de crédito, pasaportes o también son los Tokens que generan números aleatorios o palabras claves. También existen las tarjetas conocidas como inteligentes o que contienen cierta información, se pueden parecer a una tarjeta de crédito, pero el comportamiento o información puede variar.

Se tiene también los tipos de autenticación basados en una característica física, este tipo en comparación con lo que ya se mencionó se puede decir que son los más nuevos. Cuando se habla de características físicas se puede mencionar a:

- La voz
- Las huellas dactilares
- El ojo
- La escritura

La autenticación se puede considerar como parte de un método de control de acceso, la mayoría de las ocasiones esto se complementa con otras partes de un sistema, ya que hoy en día debido al manejo de la información y la personalización de los gadgets que se tiene disponibles, se vuelve una labor compleja la de tener control y manejo dentro del sistema.

Los tipos de autenticación no son excluyentes, así que, si se usa un método, no es una barrera para usar otro, de hecho, en sistemas complejos el usuario se puede encontrar

con sistemas que utilizan tres tipos de autenticación, obviamente se tiene que pensar en el usuario, a veces es muy molesto siempre y cuando analizando el costo vs el beneficio

2.2.16 Mecanismos preventivos en seguridad informática

Los mecanismos preventivos en la seguridad informática son los más olvidados, los cuales son vistos como una pérdida de tiempo, la parte administrativa en la mayoría de los casos lo ve como un costo extra, es algo parecido como por ejemplo, con los seguros médicos o seguros de vehículos, se puede pagar 10 años el seguro de un carro y nunca tener un accidente, en primera instancia se podrá analizar que es algo muy bueno, pero después en algún momento se podrá pensar que es un desperdicio haber pagado una cantidad 10 años y sin usarla (Departamento de Tecnología Organización Inca, 2016).

La definición de los mecanismos preventivos consiste en una serie de revisiones periódicas, algunos cambios o mejoras de diferentes aspectos que pueden ser de hardware, software o de cualquier elemento involucrado en los sistemas y procesos, por eso es por lo que las revisiones dependen de los procesos de la empresa y cada una tiene sus propios procesos. Los mecanismos preventivos en realidad son a largo plazo y por esta razón son considerados por la mayoría como una pérdida de tiempo y dinero.

Hay que resaltar que el mayor número de ataques informáticos se puede evitar, siempre y cuando se utilicen mecanismos preventivos, se podría evitar gracias al buen trabajo. La Barrera más fuerte a la que se enfrenta una empresa al querer aplicar los mecanismos preventivos, es la aceptación y el compromiso de todos los involucrados, hacer entender que no es una carga, es parte de los procesos y de lo que se debe hacer bien en la organización. (Figueroa S. J., 2021)

Entre los elementos que se pueden aplicar en los mecanismos preventivos se puede mencionar a:

El respaldo de información: Es uno de los procesos más comunes que se pueden realizar en las compañías y que gozan de cierta aceptación general, las empresas entienden que

los problemas con información son muy costosos, parece muy fácil pero seleccionar los mecanismos de respaldo no es tan sencillo como se analizar, se tiene que considerar los siguientes factores: Qué formatos de archivo se tienen, por ejemplo, MP3, archivos de texto, bases de datos y otros, las imágenes y vídeos por ejemplo, son archivos que normalmente necesitan atención especial.

- Horario de respaldo: Otro reto es a qué hora se puede hacer el respaldo, es común seleccionar las horas de menos tráfico.
- Control de los medios: El tener acceso a respaldos es algo de alto riesgo, se puede robar la información, manipular, perder, así que, el respaldo es una solución, pero también es otro problema que se debe resolver.
- La comprensión de la información: No toda la información se puede comprimir, pero existe alguna que, sí lo necesita, así que se deben hacer las valoraciones respectivas (Figueroa, Rodríguez, Bone, & Saltos, 2017).

Estos son sólo algunos de los procesos, pero la organización puede personalizar lo que quiere considerar en los mecanismos preventivos.

2.2.17 Mecanismos correctivos en seguridad informática

Los mecanismos correctivos tienen una gran diferencia en tiempo con los mecanismos preventivos, estos se aplican cuando, después de que algo sucedió y la función principal es corregir las consecuencias. Entre las características que tienen los mecanismos correctivos normalmente son muy caros, esto se debe a que el problema ya se lo tiene encima y no se puede tenerlo durante mucho tiempo, así que, contratar expertos para resolver el problema o el tiempo que le dedicara a el equipo de trabajo siempre va a costar mucho, en un porcentaje muy alto se acaban pagando servicios de solución a otras empresas, adquiriendo soluciones o comprando software y parches de actualización que logran resolver el problema. (Agustina , 2019)

Otra característica de los mecanismos correctivos es que el tiempo es limitado, así que el tiempo se vuelve algo muy apreciado en estos casos, pero también es muy escaso.

Probablemente la empresa o la persona puede poder obtener dinero, pero tiempo es casi imposible.

Dentro de los mecanismos de corrección se tienen diferentes pasos de ejecución para enfrentar este problema serio en los que se puede mencionar:

- Catalogación y asignación de problemas: En este paso se hace un catálogo de los problemas a los que se pueden enfrentar, detectar y clasificar es algo muy recurrente en todo lo relacionado con la seguridad informática, ya que es una forma para poder saber cómo abordar las situaciones y buscar alguna respuesta o solución a lo que se presenta.
- Análisis del problema: En este paso es muy evidente que la actividad que se hace es analizar el problema que se ha presentado, en muchos casos esta parte se realiza por los expertos, ya no, por las personas involucradas en el problema.
- Análisis de la solución: Antes de intentar solucionar el problema se debe de analizar la propuesta de la solución, se ha cometido un error, puede ser que no de forma directa, pero es un error, el impacto no va a ser más o menos, si es culpa del usuario o de un tercero, así que la solución tiene que estar bien planteada y ejecutada. Antes de empezar a realizar los cambios, actualizaciones y movimientos se debe tratar de analizar y de predecir qué es lo que va a suceder.
- La documentación: Este componente es vital, ya que los cambios que se hacen probablemente son algo que se hizo con un tiempo limitado, rápido y que involucraron muchos recursos, así que la documentación es muy importante, ya que puede ser que por las velocidades no se recuerden todos los pasos y cambios que se han realizado. En caso de encontrar algún problema se puede consultar la documentación para detectar si la solución era correcta (Montero , 2013).

2.2.18 Mecanismos detección de seguridad informática

Los mecanismos de detección son los más complejos y son en los que se necesita tener alto grado de conocimientos técnicos dependiendo de la materia que se aborde, por ejemplo, seguridad de plataformas en línea, en específico de un tipo de bases de datos o tecnología como Wordpress, esto depende del sistema, aplicación o el ecosistema que tenga funcionando.

Los mecanismos de detección parten de que se tiene la idea de que un atacante es capaz de violar la seguridad y puede haber realizado una intrusión total o parcial a un determinado recurso. Siempre que se trabaja en los mecanismos de detección se tiene la premisa en mente, se debe de trabajar como si lo que se fuera a encontrar es lo peor y se debe estar preparados para la peor de las situaciones posibles (Alvarez, 2015).

Estos mecanismos de detección tienen dos objetivos:

- Poder detectar el punto exacto del ataque para poder llegar a una solución y recuperarse del mismo, pero no siempre es posible esto, depende de los problemas que se afrontan.
- Detectar la actividad que se considera sospechosa y conocer lo sucedido, ya que si no se encuentra donde fue el ataque, lo mínimo que se necesita es saber qué fue lo que sucedió y partir de esa parte.

2.2.19 Medios de seguridad de respaldo

Las medidas y procedimiento de respaldo que se implementen garantizarán mantener la integridad y disponibilidad de la información y de las instalaciones de procesamiento de la información frente a cualquier eventualidad. (Castro , 2018)

Para alcanzar un nivel de respaldo adecuado se harán las copias de seguridad de la información y del software que se determinen en cada caso y se comprobarán regularmente.

2.2.19.1 DAS

Este tiene una conexión directamente desde el ordenador a los datos, es decir son discos duros que ayudan a compartir datos entre los usuarios.
El acceso al almacenamiento puede ser directo

- Direct Attached Storage (DAS)
- En ese caso cada servidor necesita su sistema de almacenamiento
- Estos sistemas de almacenamiento externos están infrautilizados
- Pueden ser por ejemplo para llevar a cabo backups
- Un backup nocturno significa que el resto del día esos discos están inutilizados. (Navarro , 2017)

Figura 3: *Almacenamiento directo de DAS.*

Nota: Conexión directamente desde el ordenador a los datos

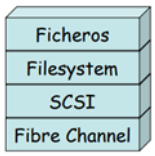
2.2.19.2 SAN

Este es un dispositivo que permite el intercambio de datos, mediante la utilización de una red de alta velocidad, así también permite trabajar con conectividad al disco duro.

- Se accede de forma serie a bloques de disco
- Normalmente mediante comandos SCSI-3
- Los protocolos están optimizados para baja latencia y nulas pérdidas
- La solución de transporte más habitual es Fibre Channel

- Acceso de varios servidores al mismo volumen requiere sistemas de ficheros especiales. (Navarro , 2017)

Figura 4: *Almacenamiento SAN*



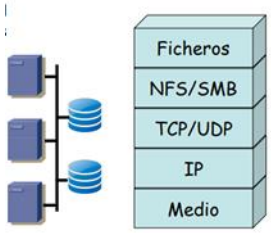
Nota. SAN trabaja en una red de alta velocidad para almacenar datos.

2.2.19.3 NAS

Es un tipo de disco duro el cual se encuentra ligado o conectado a una red LAN, permitiendo trabajar con toda la información receptada y guardada, dando la facilidad de compartir información entre los usuarios que se encuentre conectados.

- En una solución NAS
- Se accede a ficheros
- Se suele transportar sobre una tecnología LAN (o LAN + IP)
- Los protocolos no garantizan baja latencia ni nulas pérdidas (su recuperación aumenta la latencia)
- NFS, SMB/CIFS, AFP, etc.

Figura 5: *Almacenamiento NAS*



Nota. NAS el dispositivo de almacenamiento conectado a una red LAN.

2.2.20 Servicio de almacenamiento en línea

Cada vez con más frecuencia, personas e instituciones están optando por utilizar servicios de respaldo en línea, utilizando servicios en la nube. Ante esta alternativa, es importante considerar sus ventajas y desventajas y estudiar de qué manera estas apoyan o difieren de las necesidades de la institución o grupo de investigadores.

Ventajas

Algunas de las ventajas son:

- Pueden realizar respaldos de datos de forma automática, según se programe
- No requieren la intervención directa de las personas en la realización de tareas manuales asociadas al respaldo
- Permite que se mantengan copias de los datos en otras locaciones
- Pueden incluir servicios de encriptado. (Comisión Económica para América Latina y el Caribe, 2020)

CAPITULO III

MARCO METODOLOGICO

3.1. Ubicación

3.1.1 Datos informativos

Nombre de la Empresa: Dirección Distrital 18D06 - Educación.
Provincia: Tungurahua
Cantón: Quero
Ubicación: Mariano Benítez y Juan Benigno Vela
Beneficiarios: Personal administrativo
Responsables: Líderes Departamentales
Tiempo Estimado: Durante 2 años

3.1.2 Misión (según acuerdo 020-12)

Garantizar el acceso y calidad de la educación inicial, básica y bachillerato a los y las habitantes del territorio nacional, mediante la formación integral, holística e inclusiva de niños, niñas, jóvenes y adultos, tomando en cuenta la interculturalidad, la plurinacionalidad, las lenguas ancestrales y género desde un enfoque de derechos y deberes para fortalecer el desarrollo social, económico y cultural, el ejercicio de la ciudadanía en la diversidad de la sociedad ecuatoriana.

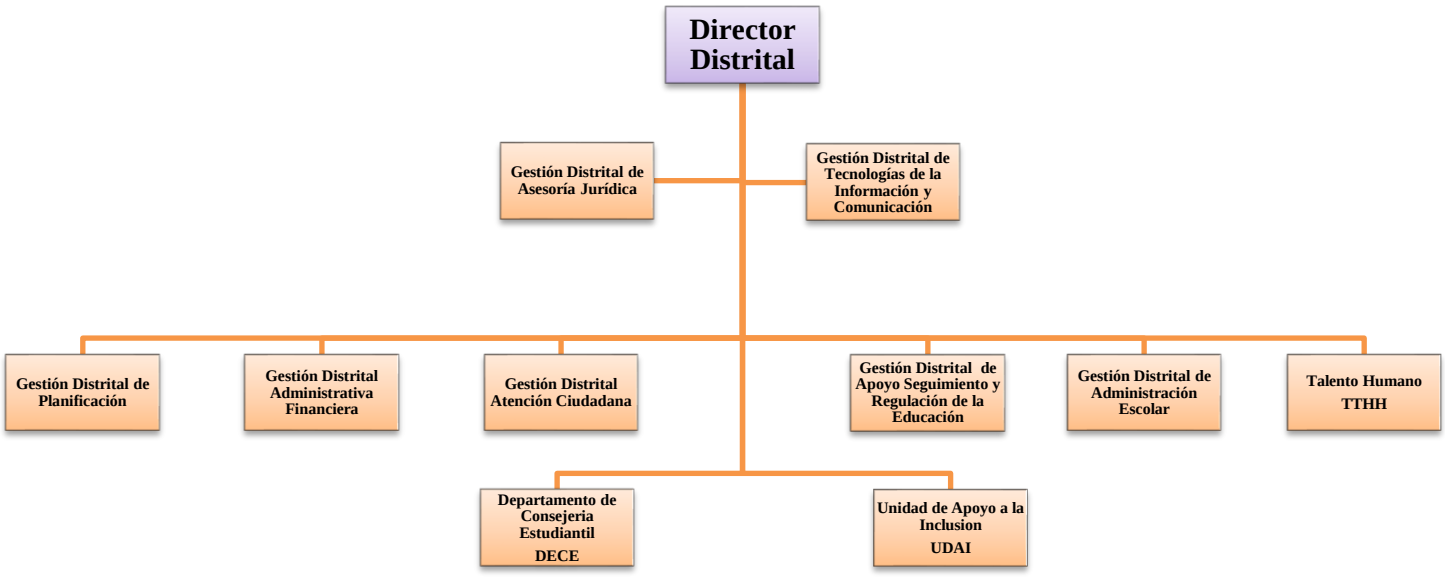
3.1.3 Visión

El Sistema Nacional de Educación brindará una educación centrada en el ser humano, con calidad, calidez, integral, holística, crítica, participativa, democrática, inclusiva e interactiva, con equidad de género, basado en la sabiduría ancestral, plurinacionalidad, con identidad y pertinencia cultural que satisface las necesidades de aprendizaje individual y social, que contribuye a fortalecer la identidad cultural, la construcción de ciudadanía, y que articule los diferentes niveles y modalidades de 4 los sistemas de educación.

3.1.4 Organigrama del distrito

Aquí encontramos los Departamentos con los que cuenta la Dirección Distrital 18D06 - Educación.

Figura 6: *Departamentos Administrativos del Distrito 18D06 - Educación*



Nota. Organigrama de los Departamentos Administrativos que dispone el Distrito 18D06 – Educación.

3.1.5 Política de calidad

Proporcionar servicios efectivos de atención ciudadana, a la comunidad educativa, logrando la satisfacción del usuario a través de un proceso de mejora continua.

3.1.6 Objetivos de calidad

a) Estandarizar los procesos de Atención Ciudadana en todas las Direcciones Distritales.
b) Incrementar la satisfacción del usuario en los procesos de Atención Ciudadana.
c) Disminuir las quejas ciudadanas en las Direcciones Distritales.

3.2 Equipos y Materiales

Los equipos y materiales que se utilizaron en la investigación son los que se detallan en la tabla 2 a continuación:

Tabla 2: *Equipos y materiales utilizados*

Orden	Descripción	Unidad	Cantidad	Costo Unitario	Costo Total
1	Equipo	Unidad	1	850	$ 850
2	Router	Unidad	1	45	$ 45
3	Internet	horas	700	0.10	$ 70.00
				Costo Total	**$ 965**

Nota. Esta tabla muestra los materiales que se utilizó en la investigación del trabajo

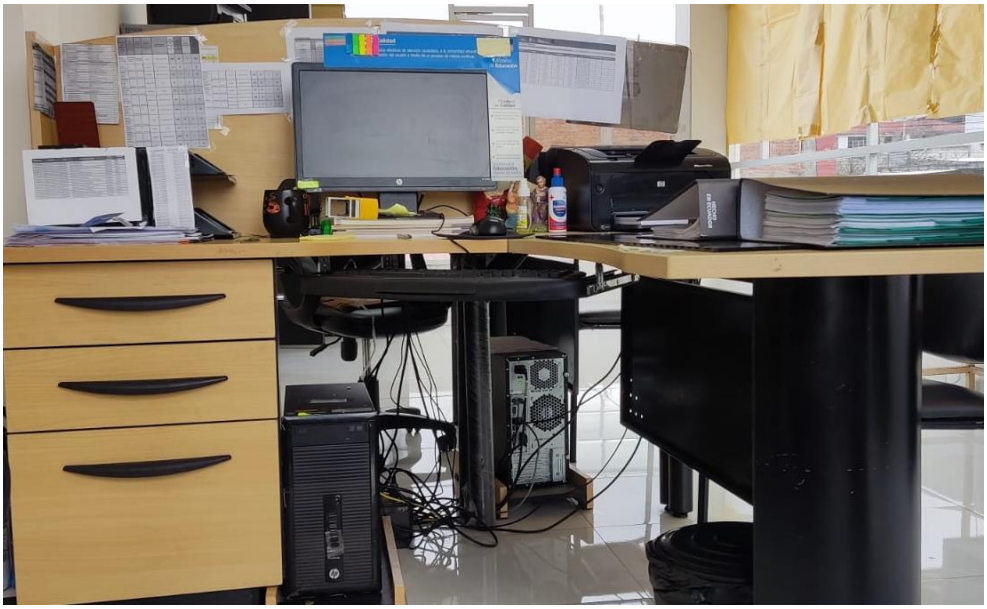
3.2.1 Tecnología

Actualmente las entidades demandan que deben tener confidencialidad con la información registrada, debido que es información general de docentes, personal administrativo, comunidad educativa. Es por eso por lo que el distrito para su desarrollo de funciones cuenta con los siguientes equipos que se detallan a continuación:

Se trabaja con equipos personales de escritorio con carpetas compartidas por red, a continuación, se presenta las características de los equipos que se cuenta en el distrito.

- Procesador Intel Core(M) I7-4770 CPU, 3.40GHz
- 2 disco Duros (1 Disco sólido de 256 GB este como ejecutable o disco de arranque, y 1 Disco mecánico de 500GB este como almacenamiento)
- Memoria RAM de 12,0 GB
- Sistema Operativo de 64 bits
- Windows 10 PRO

Figura 7: *Equipos informáticos del Distrito 18D06 – Educación*



Nota. Se puede observar los equipos informáticos con los que trabajan los funcionarios de los Departamentos Administrativos del Distrito 18D06 – Educación.

3.3 Tipo de Investigación

Los tipos de investigación son importantes, debido que es el conjunto de métodos que se aplican para conocer el problema a profundidad, esto permite generar nuevos conocimientos en el área de trabajo.

3.3.1 Investigación aplicada

Este tipo de investigación tiene como fin realizar el estudio de la problemática presentada, debido que ayuda aportar nuevos resultados, esto ayudara a confiar en lo proyectado, es por eso por lo que se puede indicar, que concreta su atención en las posibilidades concretas de llevar a la práctica las teorías generales, y destinan sus esfuerzos a resolver las necesidades que se plantean la sociedad y los hombres. (Baena , 2015)

Ante lo indicado, este tipo de investigación ayudará en el estudio, debido que se implementaran políticas de seguridad informática ISO 27001, es decir en este caso las políticas serán establecidas acorde a los problemas identificados y no se pueden aplicar a otro departamento institución.

3.3.2 Investigación de campo

Este tipo de investigación tiene como finalidad recolectar los datos relativos en cuento al tema presentado, es decir este tipo permite el estudio en el campo de estudio donde se presenta el problema. (Baena , 2015)

Como se Baena ha indicado en el apartado anterior se puede indicar que esta investigación será útil debido, que durante el estudio se asistirá al Distrito para la recolección de información mediante entrevistas, cuestionarios, encuestas y observaciones que permitan analizar los factores de riesgo de la seguridad informática.

3.3.3 Alcance de investigación correlacional

Para Hernández, Fernández, y Baptista (2015), la investigación será correlacional debido que, permitirá ver la relación de las variables de estudio, de tal forma que la asociación y la correlación son lo mismo, la diferencia es que la asociación es para las variables categóricas y la correlación para las variables numéricas, para ello se detalla la formula en la siguiente ecuación 1.

$$r = \frac{N\sum xy - \sum x \sum y}{\sqrt{[N\sum x^2 - (\sum x)^2][N\sum y^2 - (\sum y)^2]}}$$

Ecuación 1: Formula de correlación de Pearson
Fuente (Hernández, Fernández , & Baptista, 2015)

Donde:

r= coeficiente de correlación de Pearson

$\sum xy$= sumatoria de los productos de ambas variables

$\sum x$= sumatoria de los valores de la variable independiente

$\sum y$= sumatoria de los valores de la variable dependiente

$\sum x^2$= sumatoria de los valores al cuadrado de la variable independiente

$\sum y^2$= sumatoria de los valores al cuadrado de la variable dependiente

N = tamaño de la muestra en función de parejas

La correlación de Pearson es una prueba de hipótesis y también es medida de correlación a través de su índice R de Pearson, lo que detalla su valoración a continuación en la tabla 3.

Tabla 3: *Valoración de correlación de Pearson*

Índices R y Rho	Interpretación
0.00-0.20	Intima correlación
0.20-0.40	Escasa Correlación
0.40-0.60	Moderada Correlación
0.60-0.80	Buena Correlación
0.80-1.00	Muy Buena Correlación

Nota. Aquí se observa la escala de interpretación de los valores de Pearson a través del índice R.

3.3.3.1 El enfoque culi-cuantitativo

Enfoque cuantitativo

Este enfoque se basa en los aspectos numéricos para investigar, analizar y comprobar información y datos, es decir permite el manejo estadístico de la información que posean valores iguales, de manera que este estudio está orientado a verificar o comprobar de manera deductiva las proposiciones planteadas en la investigación, esto es mediante la construcción de hipótesis en base a la relación de variables para posteriormente someterlas a medición logrando así su confirmación o refutación. (Neill & Cortez, 2017)

En este caso el enfoque cuantitativo según lo comentado en el apartado anterior porque en el estudio se emplea una lista de cotejo la cual es avalada por los especialistas de la universidad.

Enfoque cualitativo

Este enfoque se basa en preguntas e hipótesis antes, durante o después de la recolección y el análisis de los datos. (Hernández, Fernández , & Baptista, 2015). Es decir, este tipo de investigación permitió establecer políticas de seguridades informáticas para evitar vulnerabilidades y proteger la información de las Unidades Administrativas de la Dirección Distrital 18D06 – Educación.

3.4 Prueba de Hipótesis

El estudio al ser inferencial, en particular la prueba de hipótesis, que ayuda a la toma de decisiones al examinar el atributo de la población a partir de la muestra. Es por eso que la prueba de hipótesis es necesaria debido que ayuda a medir el grado de fiabilidad de los resultados del estudio.

3.4.1 Hipótesis de investigación

Las políticas de seguridad informática ISO 27001 reducirá el riesgo de la seguridad de la información en las Unidades Administrativas de la Dirección Distrital 18D06 – Educación.

3.4.2 Hipótesis Nula

Las políticas de seguridad informática ISO 27001 no reducirá el riesgo de la seguridad de la información en las Unidades Administrativas de la Dirección Distrital 18D06 – Educación.

3.5 Población Muestra

En el estudio se trabaja con el total de población, debido que la población es inferior a 50 personas, es por eso por lo que se utiliza el muestreo regulado, este permite que todos los elementos formen parte de la muestra, es por eso que no se utilizará ningún tipo de cálculo para la muestra debido que la población es finita, así también se puede

enfatizar que no existe limitación de información de forma que todos los recursos están a nuestra disposición para poder realizar el estudio propuesto.

Ante lo indicado anteriormente se puede indicar que la muestra para el estudio es el personal Administrativo del Distrito 18D06 Cevallos a Tisaleo la misma que está conformada por 10 Departamentos con los siguientes funcionarios que se presentan a continuación en la tabla 4:

Tabla 4: *Población y muestra*

Detalle	Número	Porcentaje
Departamento de TTHH	2	14.29%
Departamento de UDAI	2	14.29
Departamento de DECE	1	7.14%
Departamento de Atención Ciudadana	1	7.14%
Departamento Jurídico	1	7.14%
Departamento de ASRE	1	7.14%
Departamento de Planificación	1	7.14%
Departamento de Administración Escolar	2	14.29%
Departamento Administrativo Financiero	2	14.29%
Departamento de TICs	1	7.14%
TOTAL	**14**	**100%**

Nota. En esta tabla se puede observar al personal a ser considerado para el muestreo de la población del Distrito

3.6 Recolección de Información

Para la recolección de información se utilizará las siguientes técnicas y herramientas de investigación que se detallan a continuación:

Observación directa: esta permite estar relacionado directamente con las personas involucradas con el problema de investigación. (Diaz, 2017)

Lista de verificación: este tipo de técnica permite constatar de forma visible como se está realizando los procesos que son parte dentro de la empresa, de forma que son formatos que permiten recabar información de manera sistemática y de forma ordenada. (Morán & Ramos , 2018)

Instrumentos de recopilación de información

Ficha de observación: este tipo de instrumento permite recolectar de forma sistemática toda la información necesaria para el estudio mediante la visita a la entidad de estudio.

Cuestionario En la tabla 5 se puede observar las técnicas e instrumentos de investigación como se detalla a continuación.

Tabla 5: *Técnicas e Instrumentos de Investigación*

Técnica	Instrumento
Observación	Ficha de Observación
Lista de verificación	Cuestionario

Nota. Podemos ver las técnicas de muestreo para recopilar la información.

3.7 Procesamiento de la Información y Análisis Estadístico

Para poder procesar la información recabada, se trabajará con el sistema estadístico SPSS (Statistical Package for the Social Sciences - Paquete Estadístico para las Ciencias Sociales) versión 23, esto permitirá la comprobación de hipótesis realizada mediante la media porcentual, obteniendo con esto los resultados de la investigación.

Para lo mencionado se realizó el siguiente procedimiento:

- Elaboración del instrumento de recolección de información
- Validación del instrumento
- Organización de la información
- Tabulación de la información
- Resultados

3.8 Variables Respuesta o Resultados Alcanzados

Los posibles resultados que se espera alcanzar con la aplicación de la propuesta de implementación de las políticas de seguridad informática, es lograr un cambio

significativo en el cuidado que mantienen los funcionarios en el manejo de información, siguiendo disciplinadamente las políticas implantadas en la institución.

Los criterios utilizados en la lista de verificación según ANEXO 1 la que se va a aplicar a la Unidades Administrativas de la Dirección Distrital 18D06 – Educación, se eligió debido a los problemas que se presentan en la institución, esto ayudará a conocer la situación real de la misma, para poder diseñar políticas que ayuden a la seguridad informática.

CAPITULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

A continuación, se validarán los resultados obtenidos después de la encuesta realizada, antes y después de la implementación de Políticas de Seguridad informáticas para analizar vulnerabilidades y resguardar la información de las Unidades Administrativas de la Dirección Distrital 18D06 – Educación.

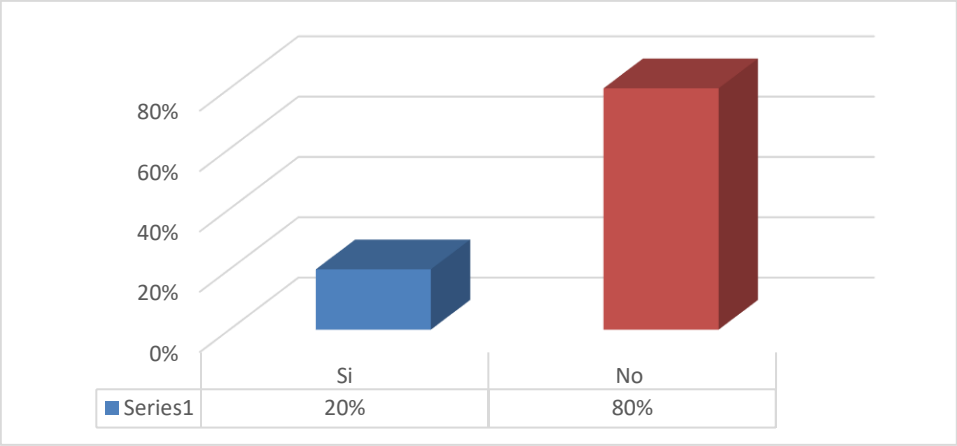
4.1 Análisis de Resultados

A continuación, se describirá los resultados que se obtuvieron en la aplicación de encuestas, datos que permitirán conocer la situación actual de la institución en estudio, así como también la evolución o cambio que tuvo después de la implementación de las políticas de seguridad informática.

4.2 Tabulación de los Resultados

1. Cuentan con políticas de seguridad informática las Unidades Administrativas de la Dirección Distrital 18D06 – Educación.

Figura 8: *Políticas de seguridad*



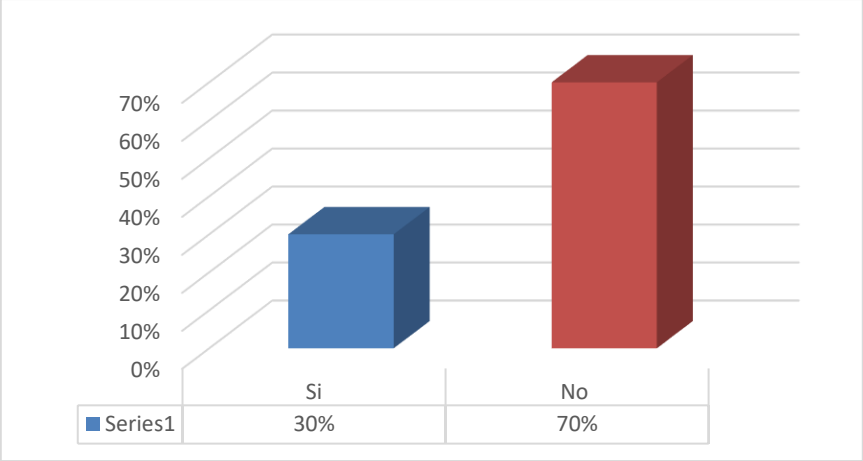
Nota: Nos permitirá observar que no cuentan con políticas de seguridad el Distrito

Análisis:

El 20% de los encuestados indicaron que cuentan con políticas de seguridad informática en la Unidades Administrativas de la Dirección Distrital 18D06 – Educación, y el 80% menciona que no, enfatizando que el distrito no cuenta con tácticas para manejar la información de la unidad de estudio.

2. Los equipos informáticos están resguardados en lugares seguros.

Figura 9: *Equipos informáticos resguardados*



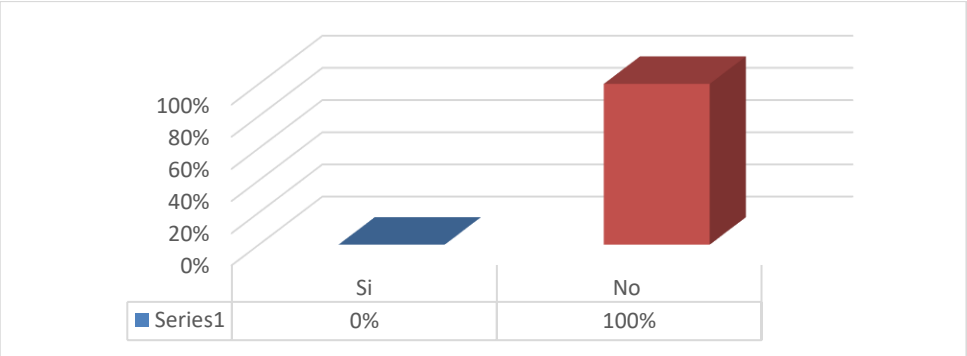
Nota: Este gráfico nos muestra que no están resguardados los equipos

Análisis:

El 30% indican que los equipos informáticos están resguardados en lugares seguros, mientras que el 70% indica que no, señalando que existe un inconveniente en contar con lugares seguros para guardar los equipos informáticos del distrito.

3. Se registran los usuarios que manipulen los equipos de los distritos.

Figura 10: *Registro de usuarios que manipulen los equipos*



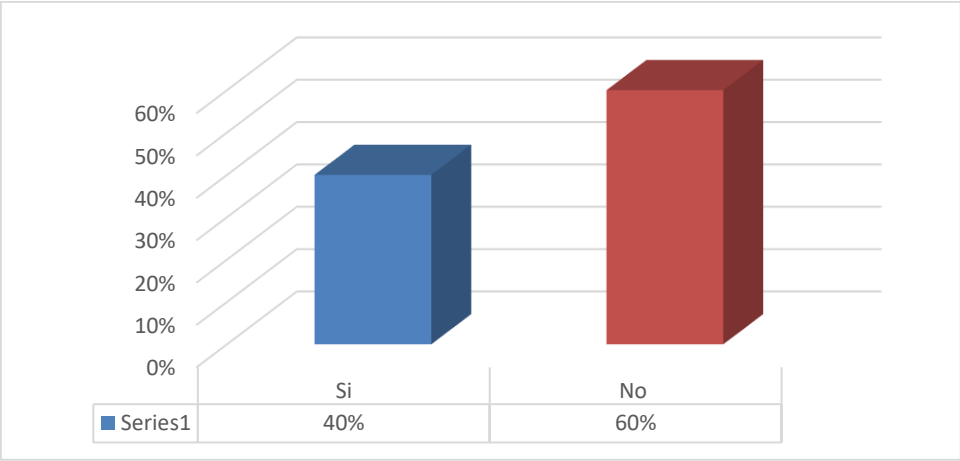
*Nota***:** Nos visualiza que los funcionarios manipulan los equipos del Distrito

Análisis:

El 100%, de encuestados indica que el funcionario no se registra cuando manipulan los equipos del distrito, indicando que en ningún área del distrito se está realizando el registro de funcionarios, siendo un problema relevante el cual se debe tomar acciones de corrección inmediatas, debido que, al no contar con un registro no se puede verificar que persona tuvo acceso al equipo.

4. Los equipos informáticos cuenta con áreas seguras.

Figura 11: *Áreas seguras*



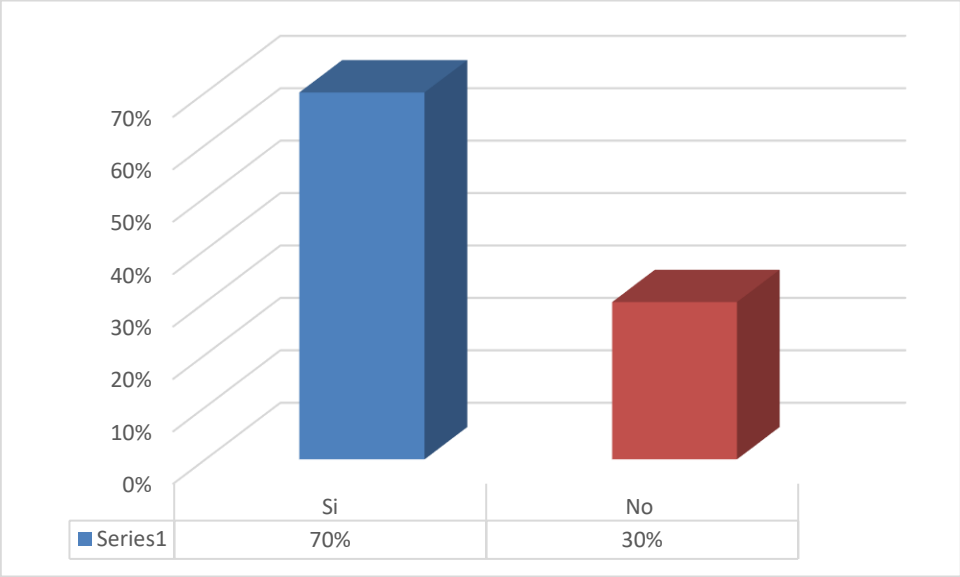
Nota: Verificamos que los equipos del Distrito no cuentan con áreas seguras

Análisis:

EL 40% de operarios, menciona que los equipos informáticos cuentan con áreas seguras, mientras que el 60% de operarios indica que no cuenta con área seguras, esto indica que el distrito no cuentas con áreas seguras.

5. Se realizan mantenimientos de los equipos informáticos.

Figura 12: *Mantenimientos de equipos informáticos*



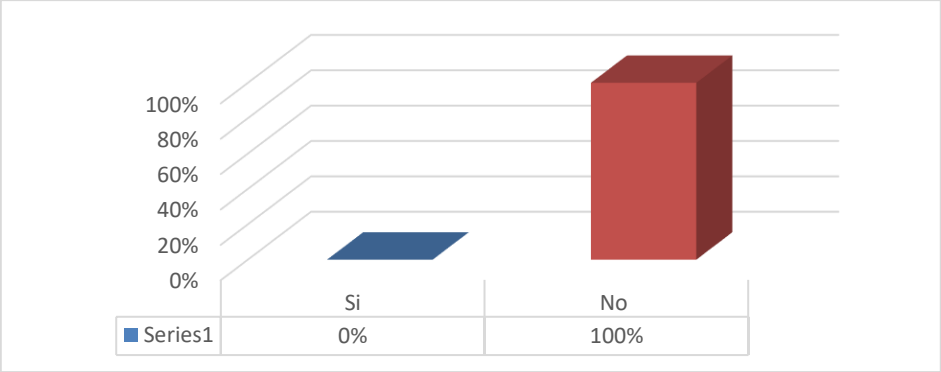
Nota: No se da mantenimiento constante a los equipos del Distrito

Análisis:

El 70% de encuestados indica que se realizan mantenimientos de los equipos informáticos en el distrito, mientras que el 30% indica que no, resaltando que se dan mantenimientos a los equipos del distrito.

6. Las Unidades Administrativas de la Dirección Distrital 18D06 – Educación cuentan con un servidor.

Figura 13: *Cuenta con un servidor*



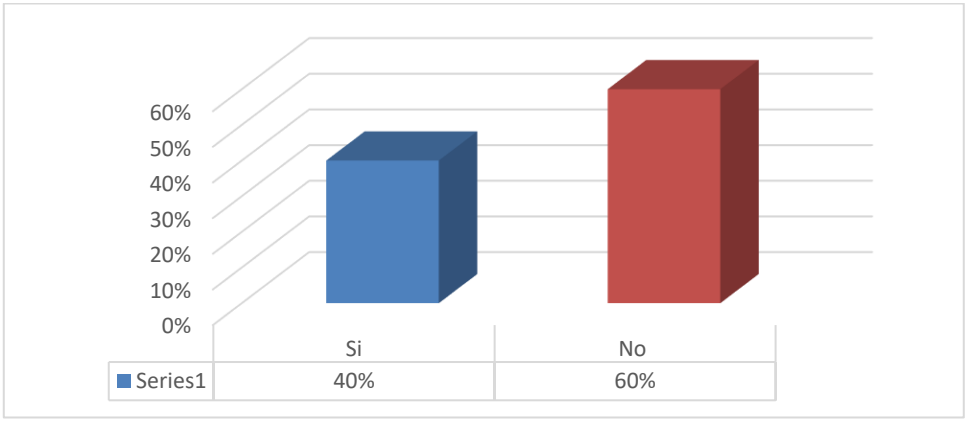
Nota: No se cuenta con un servidor dentro de la entidad

Análisis:

El 100% indica que las Unidades Administrativas de la Dirección Distrital 18D06 – Educación no cuentan con un servidor, esto es un problema importante, debido que, es una herramienta que es sumamente necesario porque en la institución de trabaja en grupo, y este ayuda a guardar datos y estos puedan ser compartidos fácilmente.

7. Tienen instalados sistemas de alimentación eléctrica ininterrumpida en los equipos.

Figura 14: *Sistema de alimentación eléctrica ininterrumpida*



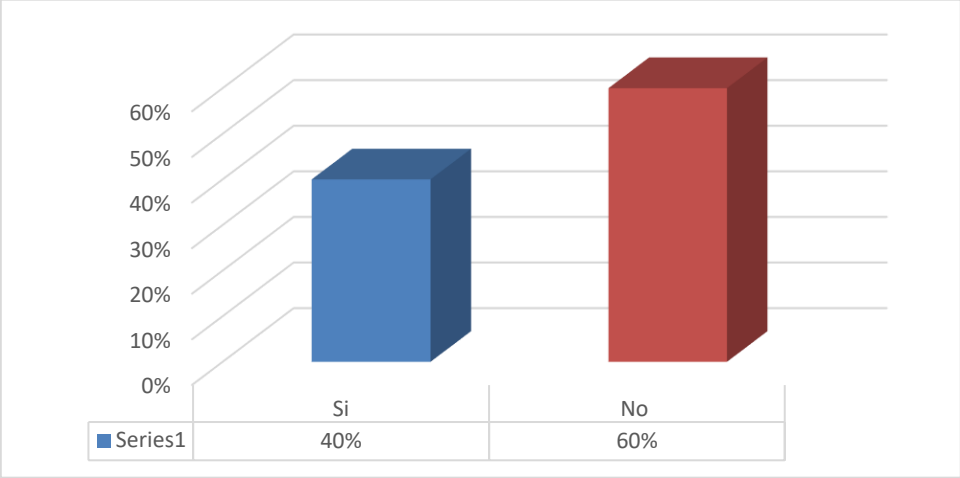
Nota: No cuentan con sistemas de alimentación eléctrica en todos los equipos

Análisis:

El 40% indica que tienen instalados sistemas de alimentación eléctrica ininterrumpida en los equipos, mientras que el 60% menciona que no cuenta con ese tipo de sistema, se recomienda a la unidad a optar el mismo mecanismo para todo el distrito, debido que el sistema de energía ininterrumpida ayuda a proteger a los equipos.

8. Cuentan con copias de seguridad informática periódicas.

Figura 15: *Copias de seguridad informática*



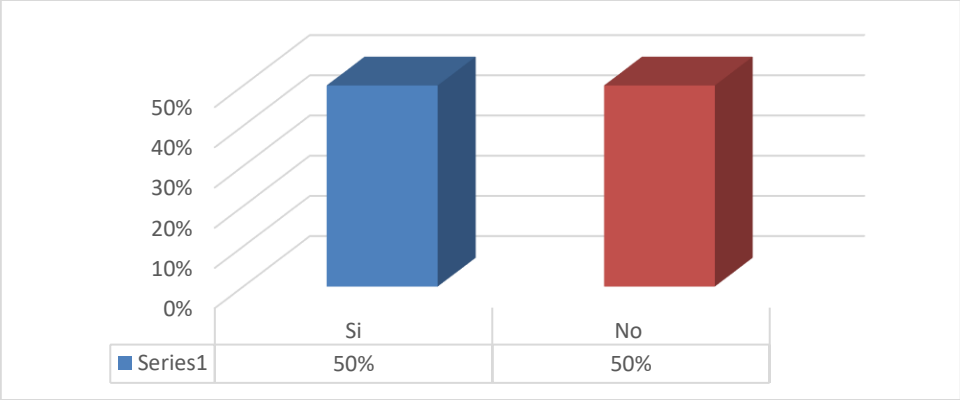
Nota: No cuentan con copias de seguridad informática periódica

Análisis:

El 40% indica que cuentan con copias de seguridad informática periódica, mientras que el 60% indica que no cuenta con esta herramienta, esto recalca que el distrito debe contar con un sistema que respalde su información.

9. Existe un responsable del área de informática.

Figura 16: *Responsable del área informática*



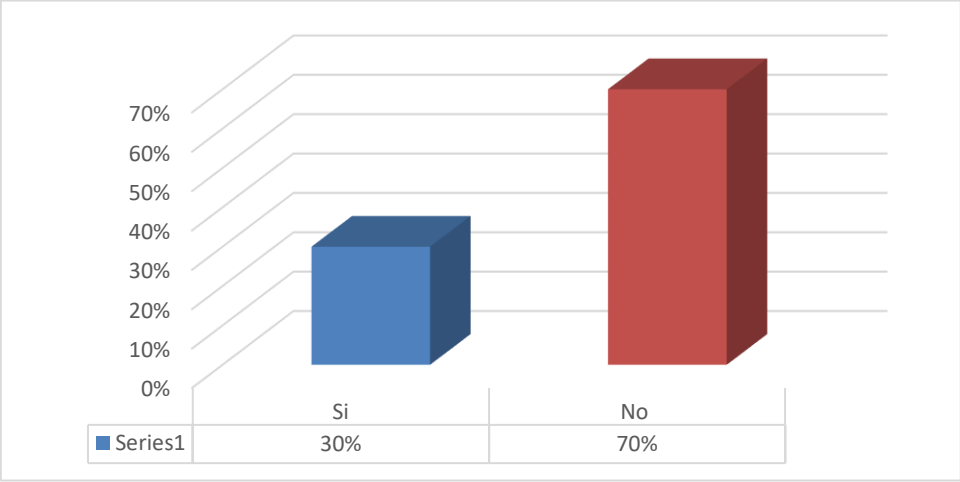
Nota: Aquí muestra que no tienen claro si cuentan o no con un responsable del área informática

Análisis:

El 50% indica que existe un responsable del área de informática, mientras que el otro 50% indica que no, enfatizando que el mayor número de empleados desconoce de la existencia del responsable informático.

10. Las claves son manejadas personalmente por cada usuario.

Figura 17: *Manejo de claves*



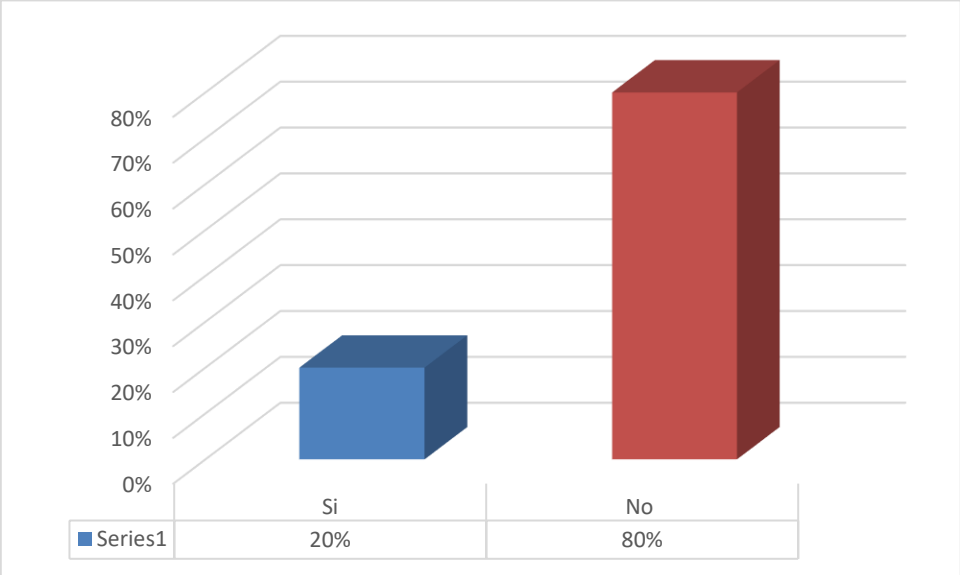
Nota: Las contraseñas no son manejadas correctamente por el funcionario

Análisis:

El 30% de operarios indica que las claves son manejadas personalmente por cada usuario, mientras que el 70% indica que no, esto indica que el distrito debe manejar internamente cada usuario de cada equipo su clave de usuario, porque al no ser de esa manera está corriendo el riesgo de mala manipulación de información por otros usuarios.

11. Existen políticas de grupo aplicables para el acceso a la información.

Figura 18: *Políticas de acceso de información*



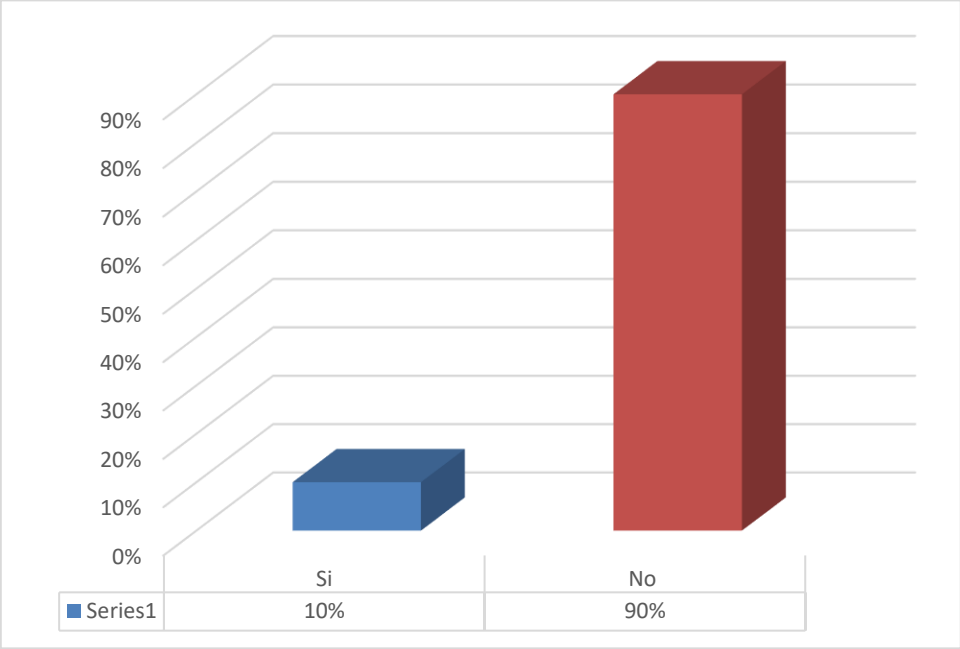
Nota: No cuenta con políticas de grupo aplicables para el acceso a la información

Análisis:

El 20% indica que existen políticas de grupo aplicables para el acceso a la información, mientras que el 80% indica que no, esto muestra que existe deficiencia con las políticas de información, problema que hay que dar solución lo más pronto posible.

12. Existe un procedimiento de identificación y autenticación de las personas externas e internas que manipulan los equipos de cómputo de la institución.

Figura 19: *Procedimiento de identificación y autenticación*



Nota: No cuenta con procedimiento de identificación y autenticación de las personas que ingresan

Análisis:

EL 10% indica que existe un procedimiento de identificación y autenticación de las personas externas e internas que manipulan los equipos de cómputo de la institución, mientras que el 90%, indica que no existen procedimientos adecuados para todas las áreas administrativas del distrito.

4.3 Verificación de hipótesis

Para la aplicación de la correlación R de Pearson se consideraron las variables estructurales Políticas de seguridad informáticas para analizar vulnerabilidades y resguardar la información de las unidades administrativas de la dirección distrital 18D06 – educación, dándonos una buena correlación lineal positiva con un resultado

del 0,8245235 de acuerdo a la concentración de mercado lo que significa que es muy favorable para esta investigación ya que se aproxima a 1, además es importante hacer mención que si una de las variables tiende a aumentar también lo hará la otra.

Tabla 6: Medidas Simétricas

Descripción	Valor	Error típ. asint.[a]	T aproximada[b]
Intervalo por Intervalo R de Pearson	0,8245325	0,048	5,35
Ordinal por Ordinal Correlación de Spearman	0,735	0,204	4,256
Nº de Casos Válidos	10		

Nota.. SPSS Stadistics Versión 23

El resultado del modelo acepta la hipótesis, es decir las políticas de seguridad informática ISO 27001 reducirá el riesgo de la seguridad de la información en las Unidades Administrativas de la Dirección Distrital 18D06 – Educación, por lo tanto, se rechaza la hipótesis nula (Ho) para quedarse con la hipótesis alterna del investigador (H1). Se recuerda que la H1 es aquella que busca la correlación.

H1= Las políticas de seguridad informática ISO 27001 reducirá el riesgo de la seguridad de la información en las Unidades Administrativas de la Dirección Distrital 18D06 – Educación.

Se puede concluir a través de la prueba de hipótesis que sí existe correlación porque el $p > 0,05$, y esta correlación representa un índice de 0,8245325, por lo que se puede definir una correlación significativa. Entonces con la correlación de Pearson se prueba la hipótesis y se mide su índice R de Pearson.

4.4 Establecer las políticas de seguridades informáticas para evitar vulnerabilidades y proteger la información que reposan en las Unidades Administrativas de la Dirección Distrital 18D06.

Una vez conocido los resultados del ex ante evaluación sin contar con políticas de seguridad; se implementa las políticas de seguridad en el Distrito.

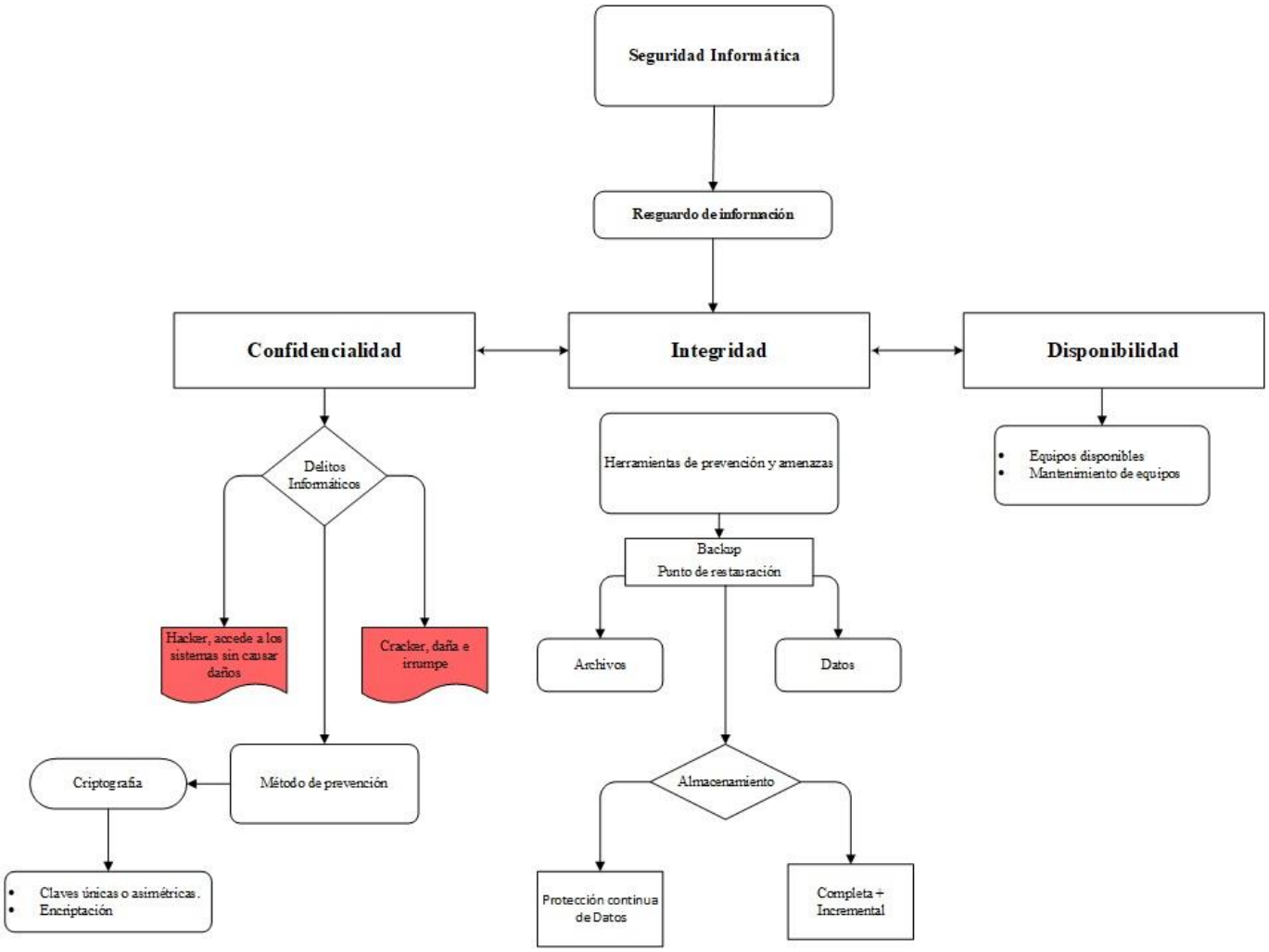
El diseño de políticas permitirá garantizar la calidad y excelencia en el tratamiento de información, permitiendo asegurar la continuidad de los procesos de las Unidades Administrativas del distrito a través de un Sistema de Gestión de Seguridad de la Información que constituye el marco de referencia para lograr la consecución de este compromiso, garantizando confidencialidad, integridad y disponibilidad de la información.

Objetivos: Con la finalidad de llevar a cabo la política establecida para la organización se establecen los siguientes:

- Considerar la seguridad de la información como un proceso de mejora continua, que permita alcanzar niveles de seguridad cada vez más avanzados.
- Generar una adecuada gestión de riesgos que puedan detectar las vulnerabilidades posibles en los activos de información.
- Definir, desarrollar e implementar los controles de seguridad organizativos que resulten necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada en Unidades Administrativas de la Dirección Distrital 18D06 – Educación.

Para generar una adecuada gestión de riesgos que puedan detectar las vulnerabilidades posibles en los activos de información, se sugiere a los departamentos administrativos seguir con el siguiente flujograma que presenta a continuación:

Figura 20: *Flujograma de manejo de seguridad informática*



Nota: Elaboración propia

4.4.1 Acceso a las áreas o zonas controladas

4.4.1.1 Áreas seguras

Se consideran áreas seguras los lugares que ayudan a resguardar adecuadamente los equipos tecnológicos, esto ayudará a evitar incidentes que afecten a la integridad física de la información o interferencias no deseadas. Estas áreas contribuirán a tener los equipos salvaguardados, lejos de la manipulación de cualquier persona que no esté autorizada.

4.4.1.2 Política:

Proteger los equipos tecnológicos contra el acceso de personas no autorizadas o cualquier daño a la información del sistema.

4.4.1.3 Perímetro físico

Cuando el Distrito disponga de un servidor, se debe considerar que el área donde se encuentre el servidor debe mantenerse cerrada desde el piso hasta el techo, con una adecuada ventilación (cuarto frio con sistema de ventilación adecuado), así como también debe tener sus respectivas instalaciones eléctricas, donde el acceso lo tendrán solo el personal que labora en el distrito. Es por eso por lo que se considera que el departamento administrativo debe crear normas que se puedan seguir para cualquier actualización de información o algún tipo de notificación el hardware, es por eso por lo que en el distrito se entrega un computador por cada empleado, de manera que cada empleado se hará responsable de su máquina, por lo que ningún empleado o visitante podrá manipular cualquier computador sin autorización.

Este tipo de medida será la primera barrera de protección del sistema de seguridad informática e introducen un retardo que incrementa el tiempo de materialización de un acto doloso o accidental. Esto se aplicará al lugar donde se encuentra los equipos tecnológicos e incluyen: medios técnicos, físicos, alarma.

4.3.2 Controles de acceso físico

Para control de ingreso de personas externas a la entidad se deberá registrar a la entrada presentando su cedula de identidad, donde el guardia tomará toda la información como: nombres, apellidos, motivo de la visita, hora de ingreso, el uso de bitácoras será esencial para el registro de las personas que ingresan y salen del distrito (ANEXO 3).

Mientras que la información sensible como respaldo de información fuentes de sistemas, códigos serán almacenados en lugares de en lugares seguros y de condiciones ambientales adecuadas, el lugar será de acceso únicamente para el personal autorizado.

4.3.3 Protección de oficinas

Cada departamento deberá contar con un acceso principal con cerradura, el responsable del cuidado del edificio cerrará cada acceso principal con llave luego de que todo el personal del área se haya retirado, además deberá revisar las ventanas que se encuentren también cerradas.

Se debe instalar un sistema de detección de intrusos en todas las puertas y ventanas accesibles y que será activado después de cerrar los departamentos.

Cada departamento debe tener un extintor de CO2 o espuma para que el personal pueda sofocar cualquier pequeño incendio si existiere.

Debido a que el hardware de cada usuario esta desprotegido por estar en las estaciones de trabajo, el departamento de Sistemas deberá organizar a los sistemas para que los usuarios finales puedan acceder a su información a través de la red local y trabajar directamente con el servidor cuando este sea implantado y así mantener a los datos importantes de la Institución a salvo de errores o manipulaciones del hardware.

4.3.4 Seguridad de los equipos

Objetivo: Proteger a los equipos físicamente para reducir toda clase de daño, pérdida o acceso no autorizado a los datos y que ocasionen la interrupción a las actividades de la Institución.

4.3.5 Ubicación y protección de los equipos

En cada departamento los equipos deberán ser ubicados en lugares que no afecten al mismo, que no sea esta cerca de ventanas donde puedan ser afectados por la lluvia, polvo o por robo.
No deben comer, beber o fumar sobre o cerca de los equipos especialmente en el área de procesamiento de información.

Se deberá realizar por los menos dos veces al año un monitoreo de las condiciones ambientales de los departamentos que es el lugar donde se procesa datos para prevenir cualquier problema en los equipos.

4.3.6 Seguridad de los servidores

4.3.6.1 Política

Una vez implementado el servidor se debería aplicar la política de protección física de los servidores, aplicativos y web, con el fin de reducir la perdida, daño o acceso no autorizado de datos que provoquen la paralización de las actividades del distrito.

4.3.6.2 Ubicación y protección de los servidores

En el departamento administrativo los equipos deberán ser ubicados estratégicamente en lugares que no afecten ni causen molestias en el desarrollo de las actividades, como por ejemplo debe estar ubicado donde haya suficiente ventilación y no llegue líquidos, o polvos.

El distrito tendrá políticas sobre el comportamiento del empleado dentro de las instalaciones, como comer, beber o fumar.

El distrito deberá realizar por lo menos una vez al año un monitoreo de las instalaciones y condiciones ambientales, en especial en el área de equipos con el fin de prevenir daños y salvaguardar el área.

4.3.6.3 Política de contraseñas en el Servidor

Se deberá establecer la política de contraseñas para exigir contraseñas complejas, que contienen una combinación de letras mayúsculas y minúsculas, números y símbolos, y son típicamente un mínimo de ocho caracteres o más para todas las cuentas, incluidas las cuentas administrativas, como el administrador local, de dominio administrador y administrador de la empresa. De esta manera, cuando los usuarios requieran de una nueva contraseña, la política de contraseñas determina si reúne los requisitos de complejidad establecidos.

4.3.6.4 Suministros de energía

Cuando se implante los servidores se sugiere que deben contar con un UPS para que brinde el tiempo de autonomía necesaria, esto ayudara a proteger el equipo, de forma que se podrá apagar el equipo con las recomendaciones indicadas por el fabricante.

4.3.7 Seguridad del cableado de las instalaciones

El cableado de las instalaciones debe ser cubierto por canaletas, y deben ser cableados por lugares que no interrumpan el libre acceso, con el fin de evitar daños en los usuarios o trabajadores al momento de movilizarse.

Las instalaciones de cableado eléctrico deberán ser independiente del cableado de red para evitar interferencias.

4.3.8 Seguridad en redes inalámbricas

Todo tipo de información que se realice al router inalámbrico, debe ser almacenada. El nombre que se lo asigne, la dirección IP, contraseña usuario, deberá ser guardado y entregadas únicamente al departamento de seguridad informática de la institución.

4.3.9 Seguridad informática

Las seguridades informáticas nos permiten proteger de las amenazas externas e internas como: ataques informáticos, virus, robos de información, errores humanos, exposición pública de credenciales, fallos o desactualizaciones en el software y fallos en el hardware, para ello se toma de medidas para dar seguridad a la información.

4.3.10 Medidas de Seguridad

Las actividades referentes a la seguridad informática serán coordinadas por el departamento de sistemas de la institución, pudiendo incluir personal de diferentes partes de la organización con funciones y roles específico. Para ello se propone el siguiente flujograma el cual ayudará al mejor desarrollo de información informática en el distrito.

Figura 21: *Flujograma de medidas de seguridad*

Nota: Elaborado a partir de (Romero , y otros, 2018)

Para cumplir con el flujograma presentado en la figura 13 se deberá desarrollar lo siguiente:

a) Asegurar que las actividades referentes a la seguridad sean ejecutadas de acuerdo con las políticas establecidas.

b) Identificar cómo manejar los incumplimientos.

c) Aprobar metodologías y procedimientos para la seguridad informática, por ejemplo, de evaluación de riesgos, respaldo de la información y tratamiento de incidentes.

d) Identificar cambios significativos en las amenazas y la exposición de la información y de las instalaciones de procesamiento de la información a las amenazas.

e) Evaluar la adecuación y coordinación de la implementación de los controles de seguridad informática.

f) Promover en forma efectiva la educación, la formación y la concienciación en seguridad informática a través de la organización.

g) Evaluar la información resultante del tratamiento y análisis de los incidentes de seguridad informática y las acciones recomendadas en respuesta a los mismos.

4.3.11 Manejo de seguridad informática

El Ministerio de Educación utiliza la plataforma office 365, el mismo que incluye la nube o llamado también OneDrive con una disponibilidad de almacenamiento de 1 Terabyte, este es totalmente pagado por la planta central del Ministerio de Educación.

Todos los funcionarios deben tener una cuenta de correo institucional, al momento de crear la cuenta, automáticamente puede hacer uso de los beneficios que brinda el office 365, la nube es uno de los más utilizados para almacenar la información con la que se trabaja en la unidad a la que presta servicios.

En este punto cuando el funcionario cesa sus funciones, el lineamiento a seguir es que debemos proceder con el cierre de la cuenta de correo institucional esto se maneja por medio de disposiciones que emiten de forma escrita por medio de Gestión Documental – Quipux en el que solicita el Departamento de Talento Humano al Departamento de TICs la inhabilitación de la cuenta de servicio de correo institucional; el cual toda información que reposa en la nube del office 365 queda inactivo de todo tipo de ingreso

por el cierre de la cuenta antes mencionada, información que si no es descargada a su debido tiempo, se perderá la información que reposa en la nube en el caso de cerrarse la cuenta del funcionario.

4.3.12 Asignación de responsabilidades sobre Seguridad Informática

- Para el manejo de claves de seguridad, o acceso existirá únicamente un responsable, el cual será el líder de unidad, este tendrá acceso, permisos de creación y demás, mientras que el analista y funcionario tendrá únicamente acceso a la lectura de información, esto ayudará a obtener segura la información y no se filtre a personas externas.
- La asignación de las responsabilidades de seguridad informática se hará en correspondencia con las políticas de seguridad informática, definiéndose claramente las responsabilidades asociadas con la protección de los bienes informáticos y para la ejecución de procesos específicos de seguridad.
- La persona con responsabilidad de seguridad asignada puede delegar tareas de seguridad a otras, sin embargo, siguen manteniendo la responsabilidad y deberán poder garantizar que cualquier tarea delegada se ha cumplido correctamente.
- Se asegurará que cada cual conozca su responsabilidad con relación al mantenimiento de la seguridad y que cada clase de problema tenga alguien asignado para tratarlo, involucrando a todo el personal relacionado con los bienes informáticos. Por ejemplo, los usuarios serán responsables del uso adecuado de sus identificadores y contraseñas y los administradores de redes y sistemas están obligados a cubrir las brechas de seguridad y corregir los errores. Para alcanzar una seguridad efectiva es conveniente lograr una participación lo más amplia posible de todo el personal (o al menos la ausencia de una oposición activa).
- Se establecerán niveles de responsabilidad asociados con las políticas de seguridad. Por ejemplo, en una red se puede definir un nivel con los usuarios de esta, donde cada uno tendrá la responsabilidad de proteger su cuenta. Un

usuario que permita que su cuenta sea comprometida incrementa la posibilidad de comprometer otras cuentas o recursos. Los administradores de redes y sistemas forman otro nivel de responsabilidad, implementando los mecanismos de seguridad que se requieran.

- Debe quedar claro que los usuarios son individualmente responsables de la comprensión y aplicación de las políticas de seguridad de los sistemas que ellos emplean y del uso apropiado de los recursos que les han sido asignados.

Con este objetivo se concluye las seguridades para la información que maneja el Distrito, cumplimiento el objetivo planteado en el que se establece las políticas de seguridad informáticas para evitar las vulnerabilidades y proteger la información que reposan en las Unidades Administrativas de la Dirección Distrital 18D06.

4.4 Proponer seguridades mediante normas ISO 27001 y sugerir el levantamiento de un SERVER y trabajar con carpetas compartidas usando software libre.

Antes de proponer medidas de seguridad con la norma ISO 27001 se puede indicar lo siguiente: Esta ISO es una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada juntamente con la ITU (Unión Internacional de telecomunicaciones) que está especialmente creada para los organismos de telecomunicaciones, instalaciones de telecomunicaciones, redes y líneas y para los que éstos suponen importantes activos empresariales.

Esta ISO permite establecer políticas, procedimientos y controles que tienen que ver con los objetivos de negocio de la organización en este caso la de brindar información segura a las Unidades Administrativas de la Dirección Distrital 18D06 - Educación. Se ha visto necesario la implementación de está ISO debido a que la gestión de la seguridad de la información es sumamente necesaria con el fin de gestionar adecuadamente la información del distrito y continuar con éxito su desarrollo.

4.4.1 Políticas que regulan actividades relacionadas uso de tecnologías

Finalidad

Las Políticas de Tecnología de la Información y Comunicación tienen como finalidad el proteger la información del distrito y buscar un aumento en la seguridad y aprovechamiento de la tecnología, lo que contribuye de manera determinante a aumentar la eficiencia en el trabajo y garantizar la continuidad de las actividades distritales.

Ámbito

Las Políticas de Tecnología de la Información y Comunicación serán aplicadas de manera obligatoria por las y los empleados, servidores públicos y trabajadores que integran el distrito en estudio, que utilicen el hardware, software y comunicaciones, para el cumplimiento de sus actividades diarias.

Responsable

El departamento de Tecnología de la Información será la encargada de administrar y ejecutar estas políticas a través de procedimientos, asimismo las políticas deben cumplirse a nivel nacional por las dependencias que tienen a su cargo el uso de recursos tecnológicos.

Recursos Tecnológicos

Las Políticas de Tecnología de la Información regularán y estandarizarán el uso de los recursos informáticos que el distrito pone a disposición de todo el personal para desarrollar sus actividades y cumplir con la misión de la entidad.

4.4.2 Política para el uso adecuado de las tecnologías de información y comunicaciones

Responsables Personal con el cargo de: Gestor de Hardware y Software, Analista de Seguridades TI, Soporte Técnico.

Generales

Los usuarios internos para el uso adecuado de los recursos tecnológicos tomarán en cuenta las siguientes indicaciones:

1. Para el hardware (equipos, impresoras, escáner, servidores y demás recursos tecnológicos) de propiedad del distrito, el departamento de Tecnología de la Información es la única autorizada para realizar las actividades de soporte técnico, mantenimiento y cambios de configuración en el equipo de cómputo. En el caso de trabajos de mantenimiento efectuadas por terceros, éstas serán previamente autorizadas por el departamento de Tecnología de la Información.

2. En caso de equipos tecnológicos en estado de arrendamiento, la empresa proveedora es la única autorizada a realizar los trabajos de mantenimiento y cambio de hardware o en su caso autorizar dichas labores, previa coordinación con el departamento de Tecnología de la Información.

3. El acceso al área de infraestructura informática es restringido y únicamente ingresará personal autorizado.

4. Se restringirá el acceso a los equipos tecnológicos, a aquellos usuarios que no cuenten con una autorización previa del encargado en sistemas para laborar fuera de horario.

5. Las/os usuarios autorizados de los sistemas informáticos del distrito, no harán uso indebido de suministro, información, datos en general y datos considerados como confidenciales.

6. Los sistemas de información desarrollados internamente o aquellos adquiridos a terceros, estarán instalados en la infraestructura disponible en el departamento de Tecnología de la Información (licenciamiento, software, código fuente, hardware).

8. La identidad de los usuarios externos y los derechos de acceso otorgados, se mantendrán en un repositorio central, sea un documento que contenga al menos los

siguientes campos como: nombres/apellidos, cédula de ciudadanía/identidad, empresa o entidad en la que labora, nombre del proyecto, responsable del proyecto, fecha de solicitud de los permisos, fecha de expiración de los permisos, sitios a los que se otorgó el acceso, dirección IP de la máquina, dirección MAC de la máquina, persona que autoriza y persona que otorga el acceso.

9. Se prohíbe a los usuarios utilizar los permisos otorgados para fines diferentes a los especificados en la solicitud de acceso, así como también se prohíbe el intercambio de direcciones IP con otros usuarios que no estén incluidos en la solicitud.

10. En caso de que el usuario tenga la sospecha que sus accesos han sido comprometidos, solicitará de manera inmediata su bloqueo al departamento de Tecnología de la Información.

11. Para el caso de conexiones inalámbricas, por defecto se otorgará acceso a la red de visitantes de la entidad. Si se especifican accesos puntuales, se otorgará acceso a la red corporativa con un perfil de navegación de acuerdo con sus necesidades.

12. Se mantendrá un inventario actualizado de los activos tecnológicos.

14. En ninguna circunstancia las/os empleados/as de la entidad, podrán utilizar los activos informáticos para realizar actividades que están prohibidas por las políticas.

4.4.3 Políticas para el uso del equipo de cómputo

- El uso del equipo será exclusivamente del funcionario contratado para realizar las actividades relacionadas con las funciones asignadas.
- La instalación o reubicación del equipo al interior de una misma área o fuera de ella, ya sea independiente o conectado a la red, será realizada únicamente por la persona del área de Informática.
- No podrán hacer uso de los equipos informáticos del Distrito ningún usuario externo.
- Los equipos no podrán ser sacados fuera del Distrito por ningún motivo.

4.4.4 Vulnerabilidad de seguridad informática

Las vulnerabilidades que se presentan en la seguridad informática acorde a la norma ISO 27001, se detallan a continuación:

- Falta de controles de seguridad
- Aplicaciones desactualizadas.
- Contraseñas modificadas.
- Inadecuada seguridad de cableado.
- Falta de información
- Falta de capacitación en seguridad informática
- Falta de políticas de seguridad informática
- Falta de control sobre datos de entrada y salida.

4.4.5 Políticas de Contraseñas

Todos los funcionarios deberán:

a) Cumplir con las debidas normas de seguridad establecidas en la institución.
b) El usuario tiene la responsabilidad de realizar el cambio de clave cada tres meses.

Generales

Para proteger la información del Distrito 18D06 en los ordenadores se deberá tomar las siguientes consideraciones:

- La contraseña y usuario asignado son personales, de manera que en ningún caso se debe compartir con terceros.
- Las contraseñas establecidas por cada usuario para los diversos sistemas que maneja serán de su única responsabilidad.
- La Unidad de TIC, será el encargado de realizar las debidas configuraciones de los equipos para que tenga un numero límite de intentos erróneos cuando

ingrese la contraseña, después de los intentos el equipo automáticamente se bloqueara.

- La unidad de TIC desbloqueara el equipo únicamente cuando el usuario lo solicite.

Para poder establecer contraseñas seguras se recomienda cumplir con lo siguiente:

- Tener mínimo 8 caracteres
- Los caracteres deben estar compuestos por letras mayúsculas, minúsculas y números.
- No debe tener palabras como el nombre del usuario, familiares, u algo relacionado a información personal, que sea fácil identificar.
- Tampoco es recomendable utilizar números con alguna fecha especial o número de teléfono, o fecha de nacimiento.
- La contraseña debe ser renovada mínimo cada tres meses.
- Estará prohibido entregar cualquier tipo de contraseña mediante llamadas telefónicas.
- En el caso de necesitar información de algún computador que el usuario se encuentre de vacaciones o fuera de la entidad se pedirá al jefe de TIC que autorice dicho proceso.

4.4.6 Política

Sugerir el levantamiento de un SERVER y trabajar con carpetas compartidas usando software libre.

Debemos mencionar que el Distrito 18D06 – Educación no cuenta actualmente con un servidor que nos permita administrar la información que maneja cada Departamento administrativo de la institución, es por esa razón que se sugiere se levante un servidor para el manejo de información, donde repose los archivos más relevantes en el servidor y se guarde, crea o abra la información por medio de carpetas compartidas por cada

Departamento con un manejo individual, otorgando los permisos según las funciones de cada funcionario.

El distrito por ser una entidad pública y del cual depende de los recursos del estado hasta el momento no dispone de un servidor que es necesario para la seguridad de la información; por esta razón se está sugiriendo el levantamiento de un server el mismo que quede plasmada en documentos todas las políticas para mantener un servidor; de igual manera para abaratar costos se sugiere Sistemas Operativos libres para evitar pagar licencias y genere más gastos al estado.

4.4.6.1 Levantamiento del servidor para almacenamiento de información

Aquí en este punto se recomienda dentro del servidor crear carpetas compartidas en el cual cada Departamento que conforma la Dirección Distrital tendrá su propia carpeta compartida como por ejemplo "DEPARTAMENTO DE TTHH", "DEPARTAMENTO DE ATENCIÓN CIUDADANA", "DEPARTAMENTO ADMINISTRATIVO FINANCIERO", este tipo de carpetas se ocupara en cada uno de los departamentos, solo los funcionarios de esa unidad podrá acceder a la información de ese departamento (no podrán acceder a carpetas de otras unidades), (cada carpeta compartida tendrá un usuario y contraseña para el ingreso a la carpeta); de igual forma los accesos podrán tenerlos con todos los permisos solo el líder Departamental mismo que será custodio de la información permisos de lectura, escritura y permisos de NTFS; y los analistas según su labor o requerimiento de la máxima autoridad se procederá con dar los permisos para el funcionario.

4.4.7 Sistemas operativos

A continuación, se detallan los sistemas operativos que se recomienda utilizar al distrito acorde a sus necesidades, debido que tienen accesibilidad libre y gratuita, ente ellos son:

- **Linux** que es un sistema operativo con alto rendimiento, confiables y flexibles. Tiene base estable con cargas de trabajo e implementaciones de TI, ya sea con servidores, virtual, de nube.

- **Centos** Sistema Operativo conocido por la estabilidad que brinda, la consistencia, la administración que es muy fácil de usar y la replicación directa, la versión Centos del sistema operativo es de código abierto.

- **Windows Server** sistemas enfocado a los servidores y los centros de datos, el S.O. dispone de un gran número de funciones y muchas características para permiten a los ordenadores el trabajar en un entorno centralizado y el efectuar medidas de seguridad a toda la red de tal forma que todos los datos que se transportan en la red estarán siempre seguros.

Cuadro Comparativos de los Sistemas Operativos sugeridos

Tabla 7: *Cuadro Comparativo*

	LINUX	CENTOS	WINDOWS SERVER
VENTAJAS	• Tiene seguridad contra virus. • Es configurable y adaptable a la necesidad del usuario. • Es un código libre. • Soluciones de errores instantáneos. • Soporte para muchas plataformas de hardware. • Hay más seguridad y fiabilidad. • Su costo es totalmente gratuito. • El usuario no depende del creador del software.	• En los últimos tiempos este sistema operativo en muy utilizados en servidores debido a seguridades. • Es un sistema operativo sin costo. • Las actualizaciones de seguridad son realizadas rápidamente. • CentOs tiene un alto nivel de estabilidad y de eficacia en el consumo de recursos, sobre todo se ha optimizado para correr Apache, PHP, MySQL. • Es un sistema Operativo muy liviano	• Es fácil de usar y configurar. • Cuenta con garantía. • Cuenta con soporte técnico. • Cuenta con una interface amigable. • Es fácil de administrarlo. • Menor tiempo de desarrollo.
DESVENTAJAS	• No es muy fácil de usar como el Windows • Interface compleja de manejar. • Se necesita conocimientos técnicos, conocimientos de comandos.	• Solución válida únicamente para usuarios con pocas necesidades de procesamiento. • Limitaciones para audio y video sincronizado • Si falla el servidor falla todo	• No es adaptable a las necesidades del usuario. • Limitación de configuración para el usuario. • El software no es gratuito. • Vulnerable a virus. • Muy hackeable. • El costo es muy elevado. • Las nuevas versiones requieren de muchos recursos. • Es el sistema operativo que tiene muchos fallos de seguridad. • Hay que reiniciar después de una actualización.

Nota: Cuadro comparativos de los Sistemas Operativos a ser considerados, en donde se puede observar las ventajas y desventajas.

Como conclusión una vez estudiado los Sistemas Operativos y de acuerdo a la realidad del Distrito 18D06 – Educación y siendo esta una entidad del estado que depende del presupuesto que se le asigne y por cuestiones de austeridad que vive el País, no se puede levantar un servicios con licenciamiento pagado; es por esta razón que el Sistema Operativo que nos va a brindar las características necesarias para poder diseñar, implementar las comparticiones de las carpetas por Departamentos dentro del Distrito es un S.O. libre como el Centos de la mano con el Samba siendo los más idóneos y el que se acoge a la realidad de la necesidad de la entidad, para trabajar con carpetas compartidas y con las autentificaciones.

Aquí se ha propuestas seguridades mediante las normas ISO 27001, y de igual manera se está sugiriendo para beneficio del Distrito el levantamiento de un SERVER y poder manejar de mejor manera la información más sensible para el Distrito mediante el manejo de carpetas compartidas usando un software libre el que permitirá abaratar costos, siempre trabajando en beneficio del Distrito, cumpliendo con el objetivo.

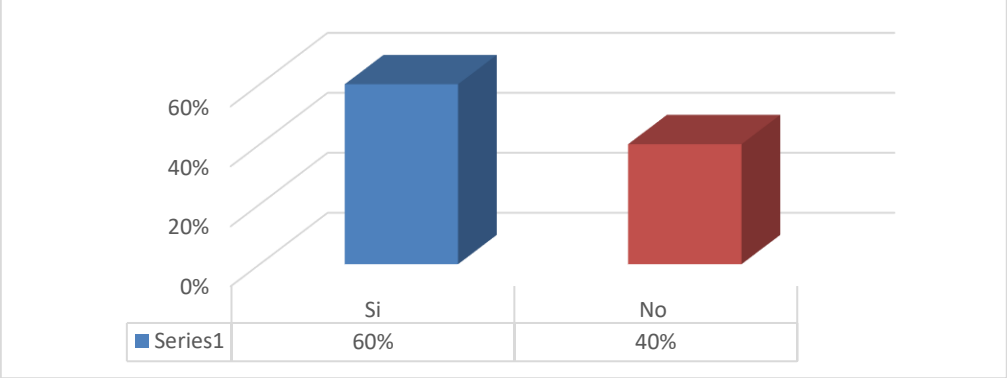
Para la implementación de las políticas se realizó tres reuniones con el departamento Administrativo del Distrito en estudio la primera reunión se mostró y se identificó las falencias en la seguridad informática, en la segunda reunión se socializó las políticas que podrían plantearse como plan piloto; y en la tercera reunión se fijó el tiempo para la implementación de una prueba piloto de aplicación para poder obtener los resultados y conocer si era factible la propuesta planteada, es por eso que a continuación en los resultados post se pueden identificar lo siguiente:

4.5 Análisis de post resultados

Después de haber establecido e implementado las políticas y medidas de seguridad dentro del Distrito en cada una de las unidades administrativas con todo el personal, se evaluó nuevamente a los funcionarios del distrito con el fin de conocer si existió mejoras, es por eso por lo que se detalla a continuación los siguientes resultados a continuación:

1. **Cuentan con políticas de seguridad informática las Unidades Administrativas de la Dirección Distrital 18D06 – Educación.**

Figura 22: Políticas de seguridad



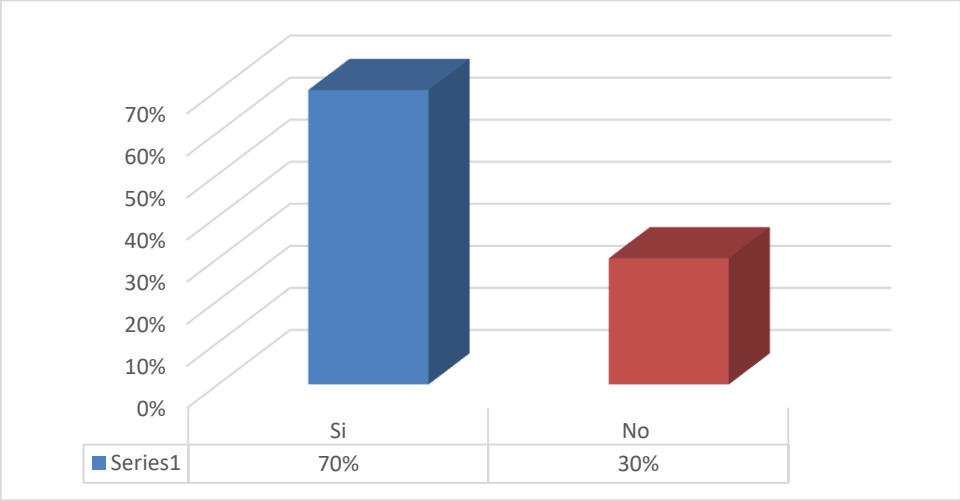
Nota: Nos permitirá observar si cuentan con políticas de seguridad el Distrito.

Análisis:

El 60% de los encuestados indicaron que cuentan con políticas de seguridad informática en la Unidades Administrativas de la Dirección Distrital 18D06 – Educación, y el 40% menciona que no, enfatizando que el distrito cuenta con tácticas para manejar la información de la unidad de estudio.

2. Los equipos informáticos están resguardados en lugares seguros.

Figura 23: *Equipos informáticos resguardados*



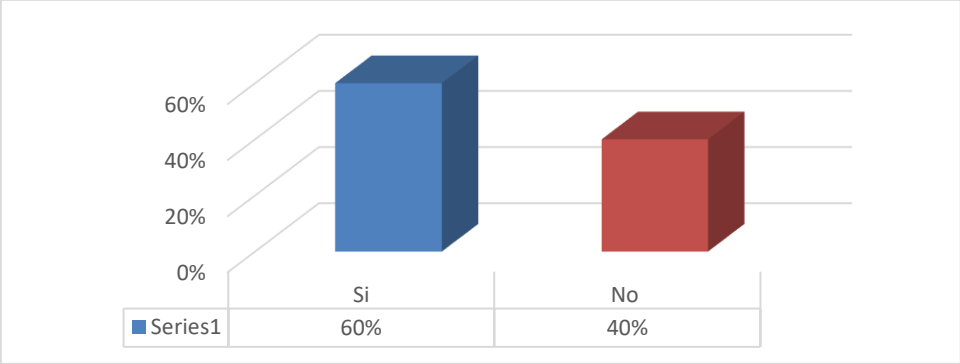
Nota: Este gráfico nos muestra si los equipos están siendo resguardados en lugares seguros

Análisis:

El 70% indican que los equipos informáticos están resguardados en lugares seguros, mientras que el 30% indica que no, señalando que el distrito después de la aplicación de las políticas adecuó las áreas para mantener los equipo.

3. Se registran los usuarios que manipulen los equipos de los distritos.

Figura 24: *Registro de usuarios que manipulen los equipos*



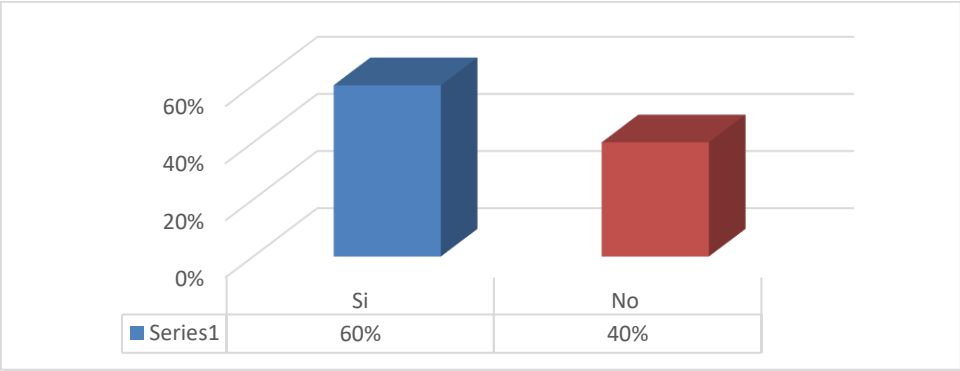
Nota: Nos visualiza que los funcionarios se registran para él uso de los equipos del Distrito

Análisis:

El 60%, de encuestados indica que el funcionario se registra cuando va a utilizar los equipos del distrito, y el 40% indican que no, recalcando que se están registrando a los usuarios, pero por falta de cultura no se cumple con el 100% de registros..

4. Los equipos informáticos cuenta con áreas seguras.

Figura 25: *Áreas seguras*



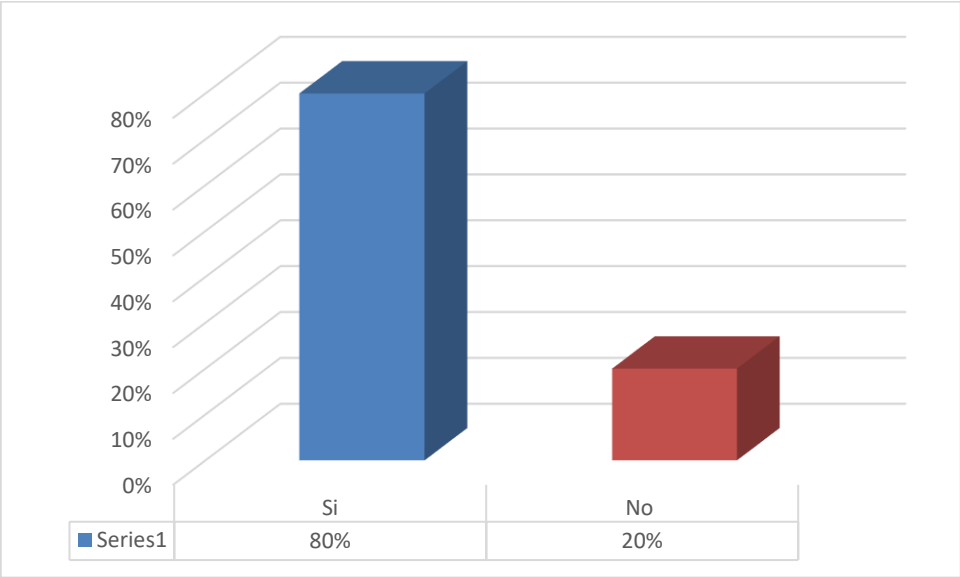
Nota: Verificamos que los equipos del Distrito cuentan con áreas seguras

Análisis:

EL 60% de operarios, menciona que los equipos informáticos cuentan con áreas seguras, mientras que el 40% de operarios indica que no cuenta con áreas seguras, esto indica que el distrito ahora cuenta con lugares seguros para almacenamiento de equipos tecnológicos.

5. Se realizan mantenimientos de los equipos informáticos.

Figura 26: *Mantenimientos de equipos informáticos*



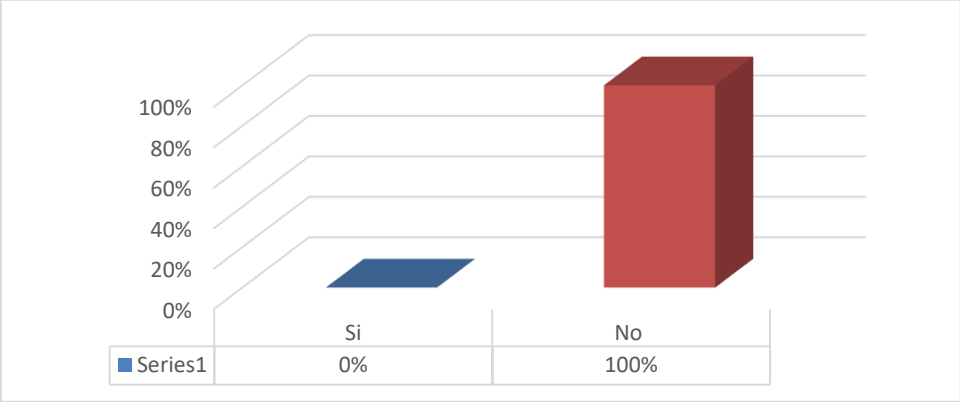
Nota: Se constata que se está dando mantenimiento constante a los equipos del Distrito

Análisis:

El 80% de encuestados indica que se realizan mantenimientos de los equipos informáticos en el distrito, mientras que el 20% indica que no, resaltando que se dan mantenimientos a los equipos del distrito.

6. Las Unidades Administrativas de la Dirección Distrital 18D06 – Educación cuentan con un servidor.

Figura 27: *Cuenta con un servidor*



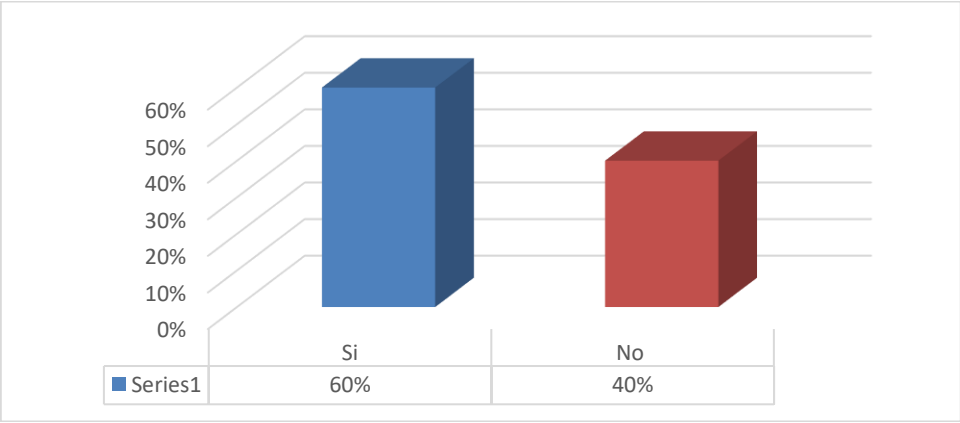
Nota: Aquí se muestra que aun no se cuenta con un servidor dentro de la entidad

Análisis:

El 100% indica que las Unidades Administrativas de la Dirección Distrital 18D06 – Educación aun no cuentan con un servidor, se está en proceso de adquisición de un servidor desde planta central; al implementar nos permitirá manejar con más seguridad la información, con las políticas planteadas.

7. Tienen instalados sistemas de alimentación eléctrica ininterrumpida en los equipos.

Figura 28: *Sistema de alimentación eléctrica ininterrumpida*



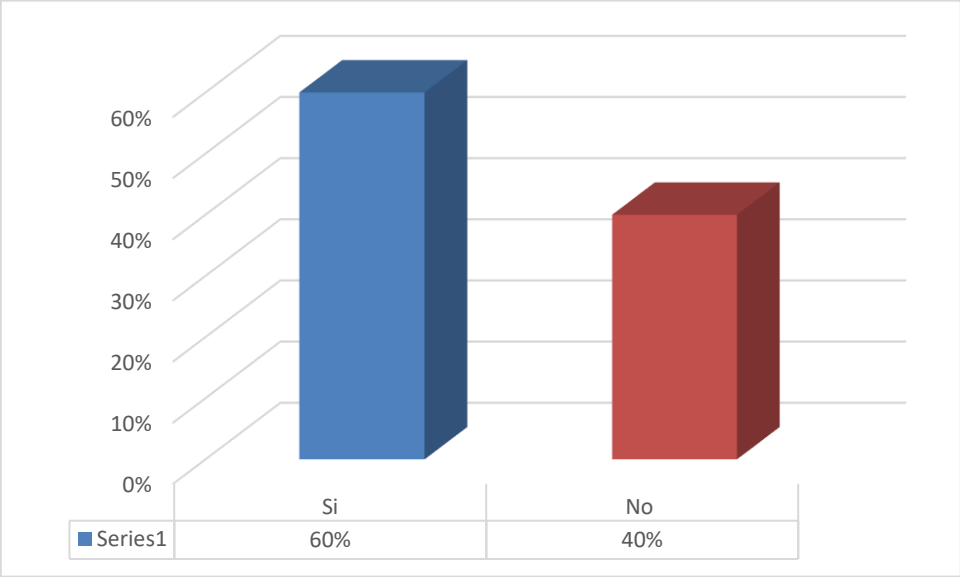
Nota: El sistema eléctrico esta de forma ininterrumpida

Análisis:

El 60% indica que tienen instalados sistemas de alimentación eléctrica ininterrumpida en los equipos, mientras que el 40% menciona que no cuenta con ese tipo de sistema, ayudando al distrito a cuidar del equipo debido que al contar con este tipo herramienta garantiza la seguridad de información.

8. Cuentan con copias de seguridad informática periódicas.

Figura 29: *Copias de seguridad informática*



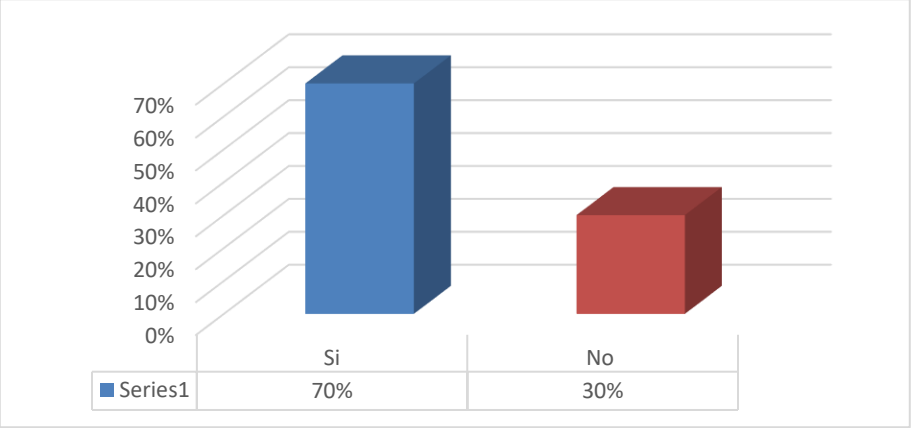
Nota: cuentan con copias de seguridad informática periódica

Análisis:

El 60% indica que cuentan con copias de seguridad informática periódica, mientras que el 40% indica que no cuenta con esta herramienta, indicando que se cuenta con respaldo de información, esto da seguridad al empleado y al ciudadano, debido que se podrá contar con información de años atrás.

9. Existe un responsable del área de informática.

Figura 30: *Responsable del área informática*



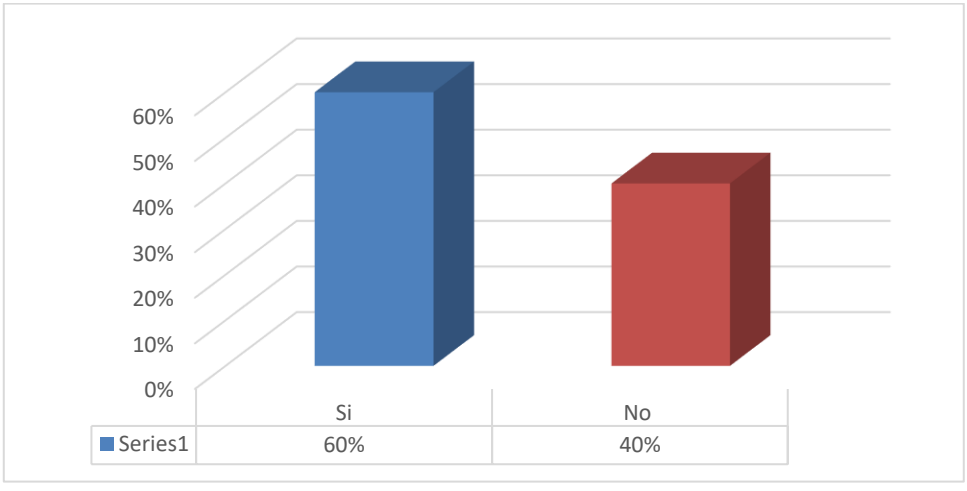
Nota: Aquí muestra que cuenta con responsables del área informática

Análisis:

El 70% indica que existe un responsable del área de informática, mientras que el otro 30% indica que no, enfatizando que cierta cantidad de empleados desconoce de la existencia del responsable informático.

10. Las claves son manejadas personalmente por cada usuario.

Figura 31: *Manejo de claves*



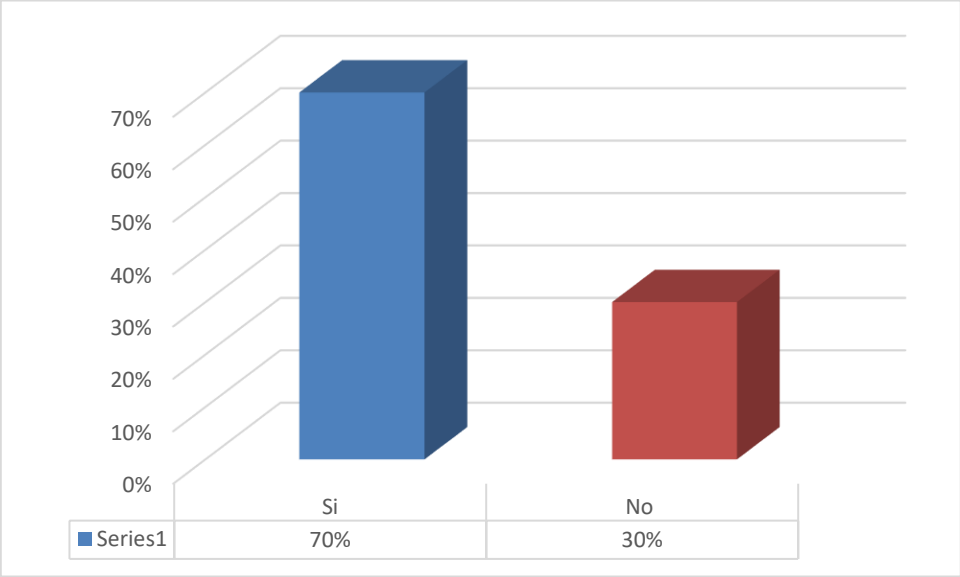
Nota: Las contraseñas son manejadas por el funcionario

Análisis:

El 60% de operarios indica que las claves son manejadas personalmente por cada funcionario, mientras que el 40% indica que no, esto indica que el distrito está manejando las claves de cada usuario personalmente, esto ayuda a proteger la información.

11. Existen políticas de grupo aplicables para el acceso a la información.

Figura 32: *Políticas de acceso de información*



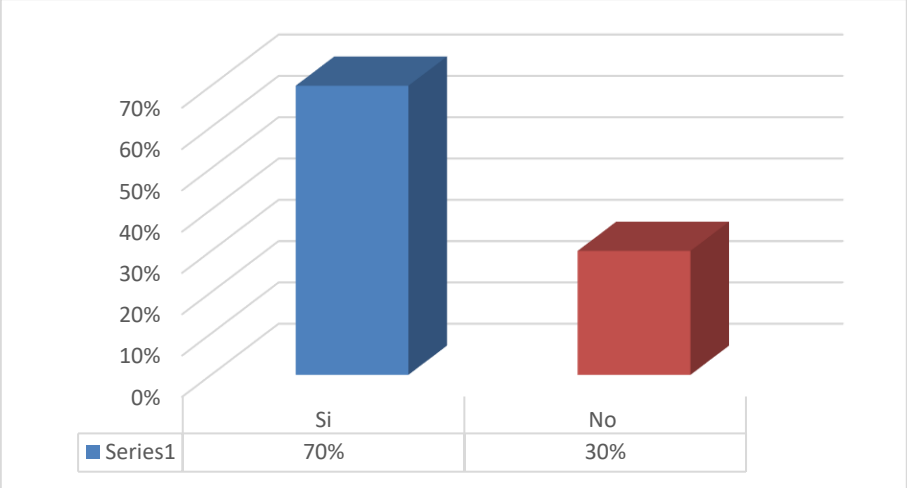
Nota: Cuenta con políticas de grupo aplicables para el acceso a la información

Análisis:

El 70% indica que existen políticas de grupo aplicables para el acceso a la información, mientras que el 30% indica que no, esto muestra que las políticas de información han contribuido con la seguridad informática de la institución.

12. Existe un procedimiento de identificación y autenticación de las personas externas e internas que manipulan los equipos de cómputo de la institución.

Figura 33: *Procedimiento de identificación y autenticación*



Nota: Cuenta con procedimiento de identificación y autenticación de las personas externas e internas

Análisis:

EL 70% indica que existe un procedimiento de identificación y autenticación de las personas externas e internas que manipulan los equipos de cómputo de la institución, mientras que el 30%, indica que no existen procedimientos adecuados para todas las áreas administrativas del distrito.

Como se puede observar en el antes y el después en los resultados con la implementación de las políticas de seguridad, se puede visualizar una mejora significativa, como muestra los resultados expuestos.

Una vez conocido los resultados se procede a realizar una nueva reunión con la autoridad y funcionarios que conforman el Distrito quedando implementado las políticas de seguridad de información (ANEXO 4), quedando como compromiso adicional la adquisición del servidor para completar con la implementación con las seguridades que cuentan en este trabajo en beneficio de la institución.

CAPÍTULO V

CONCLUSIONES, RECOMENDACIONES, BIBLIOGRAFÍA Y ANEXOS

5.1 CONCLUSIONES

- Se puede indicar que el tener conocimiento de mecanismos y metodologías de seguridad informática es necesario, debido que el desarrollo de la tecnología avanza de manera acelerada, y la información que se transmite por los diferentes canales de comunicación son de igual importancia, es por eso por lo que es necesario resguardarlo de una forma segura. Fusionándolo con políticas de Seguridad informática, será una herramienta de gran utilidad para el distrito debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información.
- Mediante el establecimiento de políticas de seguridad en las Unidades Administrativas de la Dirección Distrital 18D06 – Educación, ayudaran a manejar de forma íntegra, confiable y legal toda la información, y también protegerlos de los riesgos que se puedan presentar, y el contar con políticas de seguridad bajo esta norma permitirá tener una institución de confianza.
- El trabajo de investigación se crea con el objetivo de plantear e implementar políticas de seguridad informáticas en las Unidades Administrativas de la Dirección Distrital, con el fin de evitar riesgos de pérdida de información por distintas formas y protegerlas, proponiendo seguridades mediante normas ISO 27001 la que me permita evaluar y controlar los riesgos que se hayan identificado en la investigación, y sugiriendo el levantamiento de un SERVER

para trabajar con carpetas compartidas y fomentar de mejor manera las seguridades y el manejo de información, a más de las políticas que ya se están propuestas.

- El distrito al no contar con un servidor, que permita el acceso a datos y aplicaciones que se encuentran en la oficina, será de gran utilidad la generación de una guía de procedimientos de Seguridad enfocados a la parte de las Unidades Administrativas, debido que ayudará a reducir la fuga de información confidencial de la Dirección Distrital 18D06 – Educación, de manera que esta detalla las medidas preventivas que se pueden realizar para mitigar este riesgo en la entidad, así como también posee un detalle de cómo gestionar ciertos inconvenientes presentado.
- En la pre evaluación, se pudo conocer un 70% de equipos informáticos no están resguardados en lugares seguros, señalando que existe un inconveniente en contar con lugares seguros para guardar los equipos informáticos del distrito, por otra parte, el 60% indica que no cuenta con copias de seguridad informática periódica, así también el 70% no maneja personalmente las claves de usuarios.
- En la post evaluación después de la implementación de políticas de seguridad se pudo observar que se mejoró el resguardo de los equipos, debido que el 70% está cumpliendo con esa medida, por otra parte, el 60% el usuario está registrándose cuando manipula los equipos, por otra parte, también mejoró, porque antes no contaba con una copia de seguridad informática y con la implementación la entidad empezó a contar con un sistema.

5.2 RECOMENDACIONES

- Se recomienda que el Distrito 18D06 maneje a cabalidad las políticas de seguridad basadas en la ISO 27001, pero como responsabilidad directa serán los líderes Departamentales quienes será los entes directos de llevar a cabo la ejecución de las políticas de seguridad en conjunto con sus analistas a cargo.
- Se recomienda al Distrito adquirir de un servidor para completar con la implementación de seguridades, ya que esta nos permitirá trabajar con las carpetas compartidas que será uso exclusivo de los líderes departamentales, este server servirá para almacenar la información de cada departamento, con el ingreso a cada una de ellas con su usuario y contraseña según estipula en las políticas planteadas en el documento.
- Así también se recomienda al usuario utilizar contraseñas seguras, es decir, aquellas compuestas por ocho caracteres, como mínimo, y que combinen letras, números y símbolos. Es conveniente, además, que modifique sus contraseñas con frecuencia. En especial, le recomendamos que cambie la clave de su cuenta de correo si accede con frecuencia desde equipos públicos. Navegue por páginas web seguras y de confianza. Para diferenciarlas identifique si dichas páginas tienen algún sello o certificado que garanticen su calidad y fiabilidad. Extreme la precaución si va a realizar compras online o va a facilitar información confidencial a través de internet

5.3 BIBLIGRAFÍA

Agustina , S. M. (2019). *Seguridad informática la protexión de la información en una empresa vitivinicola de mendoza.* Tesis de grado , Universidad Nacional de Cuyo , Mendoza. Obtenido de https://bdigital.uncu.edu.ar/objetos_digitales/15749/sistimariaagustina.pdf

Alvarez, B. L. (2015). *Seguridad en informática.* tesis de grado, Universidad Iberoamericana , México. Obtenido de http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf

Avenía , D. C. (2017). Fundamentos de Seguridad Informática. 29. Obtenido de https://digitk.areandina.edu.co/bitstream/handle/areandina/1367/Fundamentos%20de%20seguridad%20inform%C3%A1tica.pdf?sequence=1&isAllowed=y

Baena , P. G. (2015). *Metodología de la investigación.* México: Grupo editorial patria . Obtenido de https://editorialpatria.com.mx/pdffiles/9786074384093.pdf

Castro , R. (2018). *Las medidas y procedimiento de respaldo que se implementen garantizarán.* México. Obtenido de https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf

Comisión Económica para América Latina y el Caribe. (2020). *Medios de seguridad de r4espaldo de informaciòn.* Mèxico. Obtenido de https://biblioguias.cepal.org/c.php?g=495473&p=4398069

Departamento de Tecnología Organización Inca. (2016). *Politicas de seguridad informática.* Lima. Obtenido de https://www.centroinca.com/centro_inca/documentos/politica_seguridad_informatica.pdf

Diaz, S. L. (2017). *La observación.* México. Obtenido de http://www.psicologia.unam.mx/documentos/pdf/publicaciones/La_observacion_Lidia_Diaz_Sanjuan_Texto_Apoyo_Didactico_Metodo_Clinico_3_Sem.pdf

Figueroa, S. J., Rodríguez, A. R., Bone, O. C., & Saltos, G. J. (2017). La seguridad informática y la seguridad de la información. 29. Obtenido de file:///C:/Users/Usuario/Downloads/420-1655-2-PB.pdf

García , M. R. (2017). *Seguridad informática y el malware.* Universidad Piloto de Colombia, Colombia . Obtenido de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2641/00004128.pdf?sequence=1&isAllowed=y

Hernández, S. R., Fernández , C. C., & Baptista, L. M. (2015). *Metodología de lainvestigación* (Sexta ed.). México: Mc Graw Hill Education . Obtenido de https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf

Hernandez, Sampieri, Fernandez, & Collado. (2015). *Metodologia de la Investigacion.* México: McGRAW-HILL.

Instituto Nacional de Ciberseguridad. (2017). *Ransomware: una guía de aproximación para el empresario.* Lima. Obtenido de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ransomware_metad.pdf

López, C. (2016). *Todo sobre el ransomware: Guìa bàsica de preguntas frecuentes.* Lima. Obtenido de http://www.eset-la.com/pdf/kit-antiransomware/Guia-Todo_Sobre_Ransomware.pdf

Mantilla , G. A. (2018). Gestión de seguridad de la información con la norma ISO 27001: 2013. *Espacios*, *39*(18), 7. Obtenido de https://www.revistaespacios.com/a18v39n18/a18v39n18p05.pdf

Ministerio de Industria, Comercio y Turismo. (2017). Sistemas de Gestión de la Seguridad de la Información Requisitos (ISO/IEC 27001:2013 incluyendo Cor 1:2014 y Cor 2:2015). 34. Obtenido de file:///C:/Users/Usuario/Downloads/une-en_iso-iec_27001.pdf

Montero , B. J. (2013). El concepto de seguridad en el nuevo paradigma de la normatividad mexicana. *Scielo*, 29. Obtenido de http://www.scielo.org.mx/pdf/regsoc/v25n58/v25n58a7.pdf

Morán , P. J., & Ramos , M. V. (2018). *El checklist como herramienta del sistema de gestión de calidad y la competitividad en la operadora de transporte terrestre urbano del cantón milagro.* Milagro. Obtenido de http://repositorio.unemi.edu.ec/bitstream/123456789/4023/1/EL%20CHECKLIST%20COMO%20HERRAMIENTA%20DEL%20SISTEMA%20DE%20GESTI%C3%93N%20DE%20CALIDAD%20Y%20LA%20COMPETITIVIDAD%20EN%20LA%20OPERADO.pdf

Navarro , S. (2017). *San y Nas.* Universidad Pública de Navarro , México. Obtenido de https://www.tlm.unavarra.es/~daniel/docencia/rng/rng14_15/slides/Tema1-11-SANyNAS.pdf

Neill, D. A., & Cortez, S. L. (2017). *Procesos y fundamentos de la investigación científica.* Tesis de grado , Universidad Técnica de Machala, Machala . Obtenido de http://repositorio.utmachala.edu.ec/bitstream/48000/14232/1/Cap.4-Investigaci%C3%B3n%20cuantitativa%20y%20cualitativa.pdf

Organización Internacional de Normalización. (2015). Guía de implementación para la seguridad de la información ISO 27001:2013. 30. Obtenido de https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Romero , C. M., Figueroa , M. G., Vera , N. D., Álava , C. J., Parrales , A. G., Álava , M. C., . . . Castillo , M. M. (2018). *Introducción a laseguridad informatica y el analisis de vulnerabilidad.* Tesis de grado , Universidad Estatal del Sur Manabí, Manabí. Obtenido de https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Tirado , R. N., Ramos , R. D., Álvarez , M. E., & Carreño , S. S. (2020). Seguridad informática, un mecanismo para salvaguardar la información de las empresas. *Revista Publicando, 4*(10), 12. Obtenido de https://revistapublicando.org/revista/index.php/crv/article/view/367/pdf_332

Vega , V. W. (2018). Políticas y seguridad de la información. *Scielo, 2*(2), 29. Obtenido de http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2008000100008

Vega, V. W. (2008). Politicas y Seguridad de la informacion. *Scielo*. Obtenido de http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2008000100008

5.4 ANEXOS

ANEXO 1: Modelo de lista de verificación

ANEXO 2: Marco Propositivo

ANEXO 3: Control de ingreso de usuarios (bitácora)

ANEXO 4: Documento de aprobación de políticas de Seguridad

ANEXO 1.

Modelo de lista de verificación

Objetivo: Determinar las falencias de las Unidades Administrativas de la Dirección Distrital 18D06 – Educación, en el manejo de seguridad informática.

Con esta lista de verificación nos permitirá comprobar si contamos o no con políticas de seguridad, si conocen o no el cómo proteger la información, el mantenimiento y los lugares seguros que deben encontrarse los equipos informáticos.

Tabla 8: *Lista de Verificación*

Pregunta	SI	NO	Observación
1. Cuentan con políticas de seguridad informática las Unidades Administrativas de la Dirección Distrital 18D06 – Educación			
2. Los equipos informáticos están resguardados en lugares seguros.			
3. Se registran los usuarios que manipulen los equipos de los distritos.			
4. Los equipos informáticos cuenta con áreas seguras.			
5. Se realizan mantenimientos de los equipos informáticos.			
6. Las Unidades Administrativas de la Dirección Distrital 18D06 – Educación cuentan con un servidor.			
7. Tienen instalados sistemas de alimentación eléctrica ininterrumpida en los equipos			
8. Cuentan con copias de seguridad informática periódicas.			
9. Existe un responsable del área de informática			
10. Las claves son manejadas personalmente por cada usuario.			

11. Existen políticas de grupo aplicables para el acceso a la información.			
12. Existe un procedimiento de identificación y autenticación de las personas externas e internas que manipulan los equipos de cómputo de la institución.			

Nota**:** ***C****omprueba si contamos o no con políticas de seguridad, cómo proteger la información, mantenimientos de los equipos informáticos.*

ANEXO 2.

MARCO PROPOSITIVO

5.1 PROPUESTA

Tema: Guía de procedimientos de Seguridad enfocados a la parte de las Unidades Administrativas para reducir la fuga de información confidencial de la Dirección Distrital 18D06 - Educación.

5.1.1 Introducción

Una vez que se pudo establecer las políticas y medidas de seguridad, es necesario que la entidad cuente con el principio del mínimo privilegio, es decir el usuario deberá tener acceso a información estrictamente necesaria las cuales le permita desarrollar sus actividades diarias, debido que, se puede identificar que el factor humano es uno de los principales componentes de la fuga de información, de manera que se es necesario concientizar a los operarios en materia de ciberseguridad dentro de la entidad.

Hay que enfatizar que la prevención no será suficiente, debido que la fuga de información puede resultar muy negativa y tener un fuerte nivel de dispersión, afectando a terceros y usuario. La urgencia por preservar la imagen de la empresa hace que en ocasiones no se tomen las decisiones adecuadas cuando no se dispone de un procedimiento básico que sirva de guía y que permita minimizar adecuadamente el impacto y evitar un empeoramiento de la situación, es por eso por lo que es necesario realizar una guía que ayude a mitigar el riesgo de fuga de información confidencial de la Dirección Distrital 18D06- Educación.

A lo largo del desarrollo de la guía se detallarán diferentes aspectos con relación a la gestión del incidente, es decir, cuando la situación ya se ha producido en varias ocasiones de forma que hay que gestionar las posibles consecuencias, con el objetivo de minimizar el impacto del incidente de fuga de información sobre la organización y sobre otros actores externos.

La guía se basa en torno a protección de tres principios fundamentales los cuales se detalla a continuación:

- **Confidencialidad:** este principio maneja que la información que se maneja es solamente para el personal autorizado.
- **Integridad:** se encarga de que la información sea correcta y esté libre de errores, de forma que la información puede ser alterada de forma intencional.
- **Disponibilidad:** permite que la información este accesible tanto para el operario o personas debidamente autorizadas.

5.1.2 Gestión para la fuga de información

Al ser diversas las situaciones y aspectos dentro de este tipo de incidentes, una inadecuada gestión puede causar efectos adversos al deseado, es por eso por lo que, la guía para la fuga de información que se propone detalla los principales aspectos y puntos que se tendrá en cuenta.

Figura 34: *Gestión para la fuga de información*

Nota. Guía para la fuga de información indica los principales aspectos que se tendrá en cuenta.

5.1.2.1 Fase inicial

Dentro de esta fase se detectará de forma temprana los incidentes presentados, de manera que una vez que se ha tenido conocimiento del incidente, en primer lugar, debemos de informar internamente de la situación, junto con el lanzamiento del protocolo de actuación. Dentro de la información que debemos transmitir internamente es importante incidir en la prudencia y redirigir a un interlocutor previamente designado cualquier duda o pregunta tanto de los propios empleados como si la misma procede de terceros el exterior. Además, se deberá de informar de la puesta en marcha del proceso de gestión de la incidencia.

Origen y motivos

El origen de las amenazas que provocan las fugas de información puede ser tanto internas como externas.

Figura 35: *Origen de motivos y amenazas*

Nota. Las amenazas de información pueden ser tanto internas como externas

Origen interno

Dentro de este factor se encuentra la fuga de información por parte del empleado de la institución, ya sea de forma inconsciente por desconocimiento o error o también puede ser de forma dolosa, es decir el empleado proporciona información sin autorización conocido como insider.

Origen externo

Dentro de este grupo se encuentran todas las organizaciones que se encuentran fuera del alcance de la organización, y estas tienen como objetivo acceder de manera ilícita a información confidencial, dentro de ellos se tiene a los siguientes que se detallan a continuación:

El hackitivismo: son terceros que no están de acuerdo con la actividad que realiza la institución.

Venganza de personas que se encuentren descontentas con el servicio prestado: el acceso no consentido a información confidencial por usuarios mal atendidos criminales o ciberdelincuentes que persiguen sustraer datos buscando un fin económico.

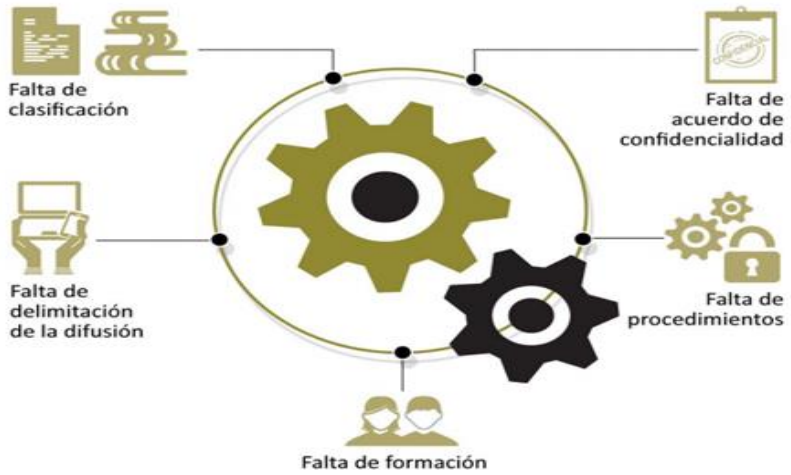
Robo de información confidencial: el acceso de información interna, en este caso expedientes.

Ataque de terceros: buscan únicamente dañar la imagen de la institución.

Causas de la fuga de información

Causas organizativas

Figura 36: *Causas de fuga de información*



Nota. Causas que la organización para la fuga de la información

Falta de clasificación

Uno de los primeros errores que se comete durante la protección de la información es la falta de clasificación de esta. Esta clasificación se puede realizar en base a su nivel de confidencialidad y en función de diversos parámetros como el valor que tiene para

la organización, el impacto que puede generar su filtración, su nivel de sensibilidad o si se trata de información personal o no.

Falta de delimitación del ámbito de difusión

Hay que tener en cuenta que se debe delimitar de forma correcta el alcance de la información, la cual ayudara a difundir la información y su nivel de confidencialidad.

Falta de conocimiento y formación

Este tipo de circunstancias son las que producen errores por parte de los empleados de la institución, debido que deben utilizar los recursos que les proporcione, de manera que es una institución pública y se basa en recursos del estado. Es por eso por lo que se debe manejar los recursos proporcionados de forma diligente y responsable como es el caso de los servicios en la nube, los dispositivos móviles, el correo electrónico, las redes sociales o la simple navegación por Internet.

Ausencia de procedimientos

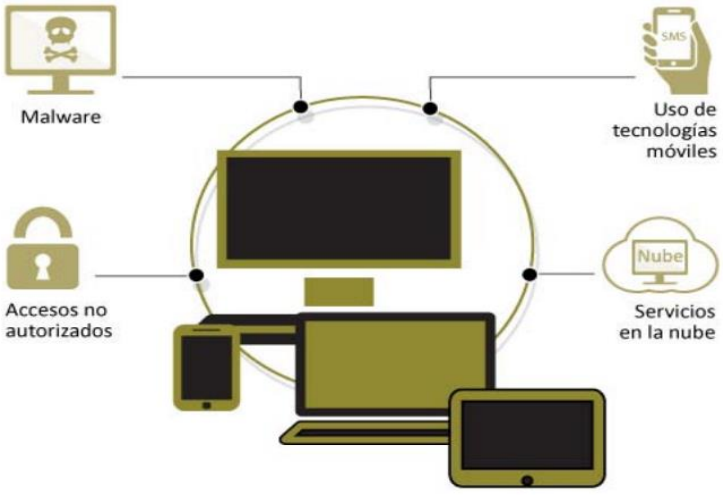
Esta es una de las causas más comunes de la fuga de información de la institución, debido que no cuenta con procedimientos específicos en el área administrativa, siendo sumamente importantes, debido que ayudan a cumplir con las políticas establecidas.

Inexistencia de acuerdos de confidencialidad

La inexistencia de este tipo de acuerdos es sumamente importante, debido que ayuda a que el empleado divulgue la información fuera de la institución, además, hay que tener en cuenta que la legislación laboral permite establecer límites a las actividades de sus trabajadores, ofreciendo canales para ayudar a los empresarios a evitar un uso inadecuado o malintencionado de la información de la que es responsable el distrito.

Causas técnicas

Figura 37: *Causas técnicas*



Nota. Las causas técnicas para la fuga de información

Códigos maliciosos

Este es uno de los más comunes debido que debido que representa una de las amenazas de robo de información, mientras que el malware está muchas veces diseñado utilizando técnicas que permiten mantener oculto su código en un sistema, mientras recoge y envía información, lo que dificulta su localización.

Acceso no autorizado a sistemas e infraestructuras

Para no tener este tipo de inconvenientes es importante actualizar los sistemas, debido que es parte fundamental de la gestión y responsabilidad de la empresa, puesto que aporta mayor seguridad y denota un trabajo de mejora continua que redunda en beneficio de la aplicación y, por extensión, del usuario.

Generalización del uso de servicios en la nube

Al ser una entidad pública y no contar con el presupuesto adecuado el uso de esta herramienta ayuda al almacenamiento debido que ayuda a tener segura la información, cuando lo cierto es que no sólo depende de eso. El nivel de seguridad que tiene depende

de la robustez de las contraseñas de los propios usuarios y de su formación en ciberseguridad.

Como mitigar la fuga de información

Visto que el factor humano es uno de los principales motivos de fugas de información, es muy importante llevar a cabo campañas de concienciación en materia de ciberseguridad dentro de la entidad, sin perjuicio de que podamos hacerlas extensivas a terceros con los que mantengamos relaciones comerciales o profesionales.

Además, conviene desarrollar y mantener actualizadas políticas claras y completas de acceso a la información, debiéndonos asegurar de que son bien conocidas por todos los miembros de la organización y, en su caso, terceros ajenos a la misma que deban acceder a información del distrito en base a algún tipo de relación contractual. Con relación a este extremo, es importante que la organización siga el principio del mínimo privilegio, el cual se traduce en que un usuario sólo debe tener acceso a aquella información de carácter sensible estrictamente necesaria para desempeñar sus funciones diarias. Dicho de otro modo, nadie de la organización deberá tener permiso de acceso a información que no necesite por razón de su cargo o funciones.

Dentro de esta imprescindible labor de prevención, es importante conocer los productos y servicios que la industria de ciberseguridad ofrece, muchas veces de forma gratuita, para mitigar esta amenaza. Por citar algunos, podemos destacar aquellos destinados a la gestión del ciclo de vida de la información (ILM, del inglés Information Life-cycle Management), productos para el control de dispositivos externos, u otros destinados específicamente a evitar la fuga de información (DLP, del inglés Data Loss Prevention).

No obstante, la implantación de medidas preventivas técnicas y organizativas, sigue existiendo la posibilidad de que se produzca un incidente de seguridad relacionado con la información que se maneja en el distrito. Por eso, además de estar continuamente implementando nuevas medidas de protección, siempre se debe estar preparado por si

se produce tal incidente: disponer de un plan de riesgos adecuado, de un programa de compliance y de haber implementado medidas tecnológicas apropiadas son actuaciones esenciales de cara a dificultar la producción de incidentes, a minimizar su impacto dentro de la organización, y a graduar eventuales responsabilidades legales que pudieran afectar.

5.1.2.2 Fase de lanzamiento

Una vez que se activa el protocolo interno de gestión del incidente, el primer paso es el de convocar a los miembros administrativos del distrito, entendido como aquel equipo de gestión responsable de tomar las decisiones durante este proceso.
Mantener la calma y actuar coordinada y organizadamente es fundamental para evitar decisiones incorrectas o que pueden provocar consecuencias negativas adicionales.

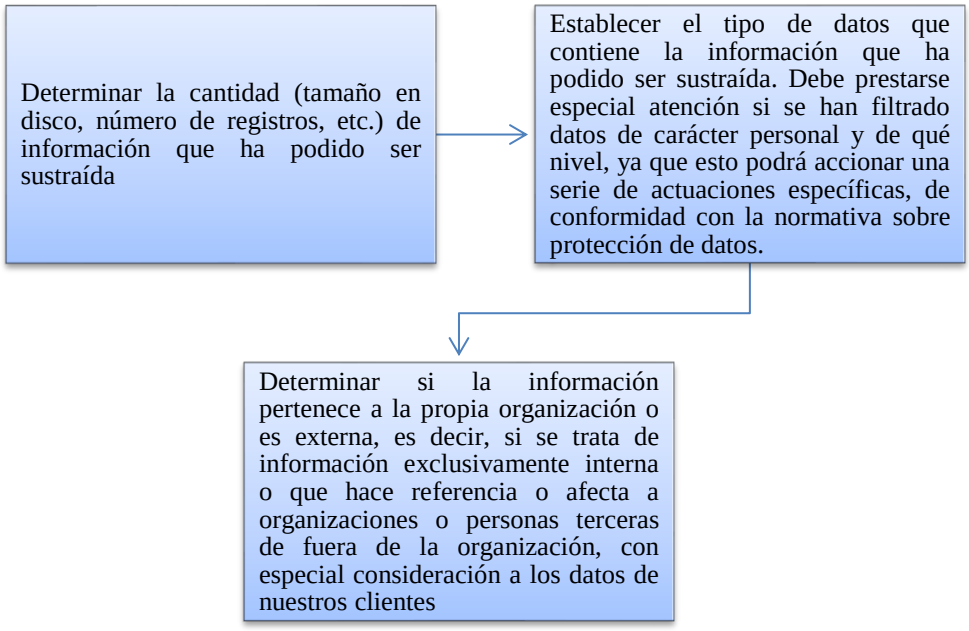
5.1.2.3 Fase de auditoria

Figura 38: *Fases de la auditoria*

Nota. Se visualiza las cuatro fases de una auditoría

Una vez se han iniciado los pasos anteriores, daría comienzo la fase de obtención de información sobre el incidente. Para ello, será necesario iniciar una auditoría interna, con el objetivo de determinar con exactitud y en el menor tiempo posible lo siguiente:

Figura 39: *Obtención de información de auditoria*



Nota. Por medio de una auditoría interna se obtendrá de forma rápida la información

5.1.2.4 Fase de la evaluación

Con la información recopilada se podrá iniciar el proceso de valoración del incidente, así como sus posibles consecuencias e impacto. Para ello es recomendable establecer las tareas a emprender, así como una planificación detallada para cada una de ellas. Se debe considerar que al tratarse de una evaluación inicial las tareas se diseñan en función de la información disponible, que puede ser incompleta. Por otro lado, también hay que tener en cuenta la ventana de tiempo de respuesta disponible, puesto que se debe actuar con agilidad. Dentro de las principales tareas que será necesario llevar a cabo se encuentran las siguientes:

a) Actuaciones para cortar la filtración y evitar nuevas fugas de información.
b) Tareas de revisión de la difusión de la información y mitigación de esta, en especial si ésta contiene datos de carácter personal o se trata de información confidencial.

c) Tareas de actuación con los afectados por la fuga de información, ya sean internos o externos.
d) Tareas para la mitigación de las consecuencias legales: posibles incumplimientos de normativa en materia de protección de datos de carácter personal o de otra normativa. También aquellas tareas encaminadas a la preparación de toda la información necesaria ante posibles denuncias por los afectados, otras organizaciones, etc.
e) Tareas para la determinación de las consecuencias económicas, que puedan afectar a la organización y su posible mitigación.
f) Tareas a acometer en los activos de la organización afectados, y su alcance, en relación con los activos de información, infraestructuras, personas, etc.
g) Planificación del contacto y coordinación con fuerzas y cuerpos de seguridad, denuncia y otras actuaciones, en caso de ser necesario.
h) Planificación de comunicación e información del incidente, tanto a nivel interno como externo, a medios de comunicación, y afectados, en caso de ser necesario.

5.1.2.5 Fase de mitigación

Junto con el paso anterior, se llevará a cabo la comunicación pertinente a los medios. Los medios de comunicación pueden aportar un mecanismo muy eficaz para hacer llegar tranquilidad a los afectados.

Debe de existir un único punto de contacto exterior desde la organización para evitar descoordinación.

En caso de existir personas afectadas por la fuga de información, si se han filtrado datos personales de terceros, deberá seguirse el procedimiento establecido por el distrito, así como seguir las indicaciones y protocolos que establezca el organismo de control.

5.1.2.6 Fase de seguimiento

Una vez completadas las principales acciones del plan, se procederá a evaluar el resultado y la efectividad de las acciones realizadas, en relación con las consecuencias y su impacto. Además, en caso de ser necesario, se deberá hacer frente a otros aspectos que hayan podido generarse durante la fase de mitigación del incidente, como puedan ser consecuencias legales, económicas, reputacionales.

ANEXO 3: Control de ingreso de usuarios (bitácora)

CONTROL DE INGRESOS DE USUARIOS DISTRITO 18D06 CEVALLOS A TISALEO
COORDINACIÓN ZONAL DE EDUCACIÓN 3
BITÁCORA

Ministerio de Educación

Nº	FECHA	CEDULA	NOMBRES Y APELLIDOS	TELÉFONO	HORA DE INGRESO	UNIDAD VISITADA	TRÁMITE A REALIZAR	HORA DE SALIDA	FIRMA

Firma

.....
Nombre: (Responsable de AT)

ANEXO 4: Documento de aprobación de políticas de Seguridad

DISTRITO 18D06 CEVALLOS A TISALEO – EDUCACIÓN
Quero

ACTA

En reunión mantenida con los funcionarios líderes de las unidades y Analista del Distrito 18D06 Cevallos a Tisaleo, se trata puntos relevantes en beneficio de la institución; temas tratados por el Departamento de TICs, propuesta expuesta por la Ingeniera Cecilia Torres Carrasco sobre las políticas de seguridades informáticas para evitar vulnerabilidades y proteger la información de las Unidades Administrativas del Distrito según estudio realizado en base a las vulnerabilidades.

Una vez escuchada la propuesta queda aceptada por unanimidad las políticas de seguridades informáticas para evitar vulnerabilidades y proteger la información de las Unidades Administrativas en beneficio del Distrito, para lo cual se firma y se sella en constancia de esta.

Quero, abril del 2022,

Firmado electrónicamente por:
SEGUNDO LUIS CHUGCHILAN RAMOS

Director Distrital
18D06 - Educación