PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

Trabajo de Titulación como requisito previo para la obtención del título de Magíster en Tecnologías de Información mención Gestión y Administración de TI

ANALISIS DE VULNERABILIDADES DE LA SEGURIDAD INFORMÁTICA UTILIZANDO ISO 27001 CASO DE ESTUDIOS UNIDADES ADMINISTRATIVAS DE LA DIRECCIÓN DISTRITAL 05D01 LATACUNGA - EDUCACIÓN

Autor: Nelson Ivan Soria

Director: Charles Edisson Escobar Terán

Quito, 21 de marzo de 2024

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

DECLARACIÓN Y AUTORIZACIÓN

Autorizo a la Pontificia Universidad Católica del Ecuador, 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.

Nelson Ivan Soria
C.I. 0201703105
Autor

APROBACIÓN DEL TUTOR

En mi carácter de Director (a) – Tutor (a) del Trabajo de Posgrado Titulado: "ANALIZAR LAS VULNERABILIDADES DE LA SEGURIDAD INFORMÁTICA UTILIZANDO ISO 27001 CASO DE ESTUDIOS UNIDADES ADMINISTRATIVAS DE LA DIRECCIÓN DISTRITAL 05D01 LATACUNGA - EDUCACIÓN", presentado por el maestrante NELSON IVAN SORIA, titular de la Cédula de Identidad Nº 0201703105 para optar al Grado de Magíster en Educación mención gestión del aprendizaje mediado por TIC, considero que dicho Trabajo de Investigación reúne los requisitos y méritos suficientes para ser sometido a la evaluación por parte de los Lectores – Evaluadores que se designen para tal fin por parte de las autoridades de la Facultad de Ciencias de la Educación.

En la ciudad de Quito, a los 20 días de marzo de 2023

Charles Edisson Escobar Terán C.I. 1202812549

cescobar637@puce.edu.ec

NOTA:

Se comunica que en el servicio de análisis Turnitin, el referido trabajo de titulación alcanzó el siguiente resultado: **8 %** índice de similitud con otras fuentes.

TURNITIN: INCLUIR HOJA DEL INFORME CON EL PORCENTAJE

Tesis_Soria_N_rev

ORIGINALITY REPORT

8%	8%	2%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	repositorio.uta.edu.ec Internet Source	4%
2	www.educacionyfp.gob.es Internet Source	1%
3	repo.uta.edu.ec Internet Source	1%
4	es.slideshare.net Internet Source	1%
5	Submitted to Pontificia Universidad Catolica del Ecuador - PUCE Student Paper	1%
6	creativecommons.org Internet Source	1%

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Titulación presentado con el tema: Analizar las vulnerabilidades de la seguridad informática utilizando ISO 27001 caso de estudios Unidades Administrativas de la Dirección Distrital 05D01 Latacunga - Educación, le corresponde exclusivamente a: Nelson Ivan Soria, Autor bajo la Dirección del Ingeniero Charles Edisson Escobar Terán, Director del Trabajo de Titulación, y el patrimonio intelectual a la Pontificia Universidad Católica del Ecuador.

Nelson Ivan Soria
C.I. 0201703105
Autor

Charles Edisson Escobar Terán
C.I. 1202812549
Director

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

RESUMEN

El presente proyecto de investigación abordó la seguridad informática de la Dirección Distrital 05D01 Latacunga - Educación, enfocándose en establecer políticas de seguridad conforme a las normas ISO 27001. El estudio reveló la carencia de políticas adecuadas de seguridad informática en la institución, lo que implicaba riesgos significativos. El objetivo principal fue elaborar políticas robustas de seguridad informática, complementado por objetivos secundarios como identificar riesgos, elaborar procedimientos actualizados y formular un cronograma para su implementación. La metodología del estudio integró enfoques cualitativos y cuantitativos, aplicando observación, entrevistas y cuestionarios al personal administrativo para alcanzar un panorama detallado de la situación en la actualidad de seguridad informática. Este enfoque mixto facilitó la identificación precisa de necesidades y desafíos. Es así que, el análisis de los datos recolectados mostró problemas significativos en la seguridad informática, incluyendo inconsistencias en la aplicación de políticas, deficiencias en la protección de equipos, gestión de accesos y respaldo de información. Estos hallazgos destacaron la necesidad de adoptar medidas mejoradas en seguridad informática. Finalmente, La propuesta del estudio consistió en una serie de políticas detalladas y una guía de procedimientos actualizada, centradas en proteger los recursos de la información, mitigar los posibles riesgos y establecer medidas de seguridad efectivos. La adopción de las normas ISO 27001 fue crucial para asegurar la integridad, confidencialidad y disposición de la información, reforzando la infraestructura de la seguridad informática de la institución. El estudio resaltó la relevancia de conservar prácticas de seguridad informática efectivas y actualizadas en el ámbito educativo.

Palabras clave: Seguridad informática, políticas, vulnerabilidades, ISO 27001, información.

ABSTRACT

This research project addressed the computer security of the District Directorate 05D01 Latacunga - Education, focusing on establishing security policies in accordance with ISO 27001 standards. The study revealed the lack of adequate computer security policies in the institution, which implied risks significant. The main objective was to develop robust information security policies, complemented by secondary objectives such as identifying risks, developing updated procedures and formulating a schedule for their implementation. The study methodology integrated qualitative and quantitative approaches, applying observation, interviews and questionnaires to administrative staff to achieve a detailed overview of the current computer security situation. This mixed approach facilitated the accurate identification of needs and challenges. Thus, the analysis of the data collected showed significant problems in computer security, including inconsistencies in the application of policies, deficiencies in equipment protection, access management and information backup. These findings highlighted the need to adopt improved cybersecurity measures. Finally, the study proposal consisted of a series of detailed policies and an updated procedural guide, focused on protecting information resources, mitigating potential risks, and establishing effective security measures. The adoption of ISO 27001 standards was crucial to ensure the integrity, confidentiality and disposition of information, reinforcing the institution's computer security infrastructure. The study highlighted the relevance of maintaining effective and up-to-date information security practices in the educational field.

Keywords: Computer security, policies, vulnerabilities, ISO 27001, information.

INTRODUCCIÓN

La seguridad informática es un aspecto de gran relevancia en la actualidad, ya que la información es la parte más fundamental de una organización. La norma ISO 27001 se considera una herramienta útil para garantizar la seguridad de la información. Según la Escuela Europea de Excelencia, la oportuna identificación de las vulnerabilidades es elemento esencial de un sistema de seguridad de la información en la operación de evaluación de riesgos (Escuela Europea de Excelencia, s.f.).

Las vulnerabilidades y amenazas en ISO 27001 en donde su oportuna identificación es un aspecto esencial de un sistema de seguridad de la información dentro del ámbito de evaluación de los riesgos. Las amenazas y vulnerabilidades en ISO 27001 van en conjunto por este motivo, se tratan en un solo capítulo y tienen que ser tratadas en su conjunto (Saeckel, 2023). Sin embargo, entre ellas existe una diferencia que casi siempre no es clara. La diferencia que existe entre amenazas y vulnerabilidades en ISO 27001 es importante. Es indispensable diferenciar claramente entre los dos atributos de un riesgo, debido a que la existencia del riesgo, dependerá de la coexistencia de una amenaza y una vulnerabilidad.

La metodología utilizada para utilizar en el proceso de análisis y evaluación de los riesgos en la parte inicial de conocimiento del sistema, la fase donde se identifica las vulnerabilidades, amenazas y riesgos de seguridad y así de determina el nivel de riesgo a la que está expuesta la organización, por medio de la probabilidad e impacto en los ámbitos de confidencialidad, integridad y disponibilidad de la información, para posteriormente establecer un sistema de control en base a los hallazgos obtenidos.

La gestión de vulnerabilidades en el contexto de ISO 27001 como un proceso constante sirve para asegurar su infraestructura de TI de la mejor manera posible. La norma ISO/IEC 27001 es una norma internacional para la Gestión de Seguridad de la Información. Con el uso de esta norma, las organizaciones tienden a determinar los riesgos de seguridad y definir controles para su gestión o eliminación, pueden captar la confianza de sus clientes y mejorar su imagen de marca.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Formulación del problema

Actualmente las empresas a nivel mundial están expuestas a ataques cibernéticos, donde la seguridad informática es un argumento crucial en la actualidad y debido a la dependencia de la tecnología en la vida cotidianas.

Con los grandes avances tecnológicos la seguridad informática paso a ser de un gasto al ser considerada como una inversión por medio de los directores o jefes de las empresas en todo el mundo. Por tal motivo se podría señalar que en diferentes países el crecimiento se ha ido acelerando y en otros es de forma lenta, pero últimamente todos han transformado en un mundo digital, lo cual el mundo digital es un activo intangible muy valioso, por lo cual tiene que ser custodiado o protegido de robos, uso inadecuado de información o perdidas de datos.

"Según el Índice Global de Ciberseguridad (IGC), de la Unión Internacional de Telecomunicaciones (UIT), de julio del presente año, en el que se mide el compromiso de los Estados frente al tema de seguridad informática, Ecuador se encuentra en el sexto puesto de 19 países de América Latina." (MINTEL, SN)

Una vez que se hizo una comprobación visual y verificando que la Dirección Distrital 05D01 Latacunga – Educación; no cuenta con políticas de seguridad implantadas, se procede con un análisis para proponer la aplicaccion de un reglamento autónomo de las políticas de seguridad según las Norma ISO 27001.

Los datos de la Dirección Distrital 05D01 Latacunga - Educación se ha tornado importante e indispensable, en el sentido que se encuentran vulnerables a perdidas, mala manipulación, robo de datos, borrado de información; por lo cual se busca la creación de un reglamento interno autónomo para precautelar la seguridad de los antecedes.

En temas de seguridad las redes informáticas se han visto violentas y vulneradas, debido a que anteriormente ha ido aumentando la facilidad de ejecución, rapidez de programación, y el daño que provoca estos sucesos; en tal sentido, es esencial el contar con políticas de seguridad informática, mismas que permitirán resguardan la información.

De esta discusión se puede identificar el problema principal:

- La Dirección Distrital 05D01 Latacunga - Educación, no cuentan con una política o normativa vigente autónoma para la protección de la seguridad informática, la confiabilidad e integridad de los datos y la información mediante las normas ISO 27001.

Y los siguientes problemas secundarios:

- No se han Identificado los activos o equipos servidores de la información de las Unidades Administrativas de la Dirección Distrital 05D01 Latacunga – Educación"
- No se han obtenido los riesgos que pueden dañar a los activos de la información de las Unidades Administrativas de la Dirección Distrital 05D01 Latacunga – Educación"
- No se han definido las políticas autónomas de seguridad de la información por medio de las normas ISO 27001 para la Dirección Distrital 05D01 Latacunga - Educación.
- No se cuenta con una guía actualizada de procedimientos para promocionar la cultura de la seguridad informática en las Unidades Administrativas para minimizar la filtración de información sencible de la Dirección Distrital 05D01 Latacunga – Educación.

1.2. Objetivos de la Investigación

1.2.1. Objetivo General

- Desarrollar las políticas de seguridad de la información para la Dirección Distrital 05D01 Latacunga – Educación mediante normas ISO 27001

1.2.2. Objetivos Específicos

- Identificar los riesgos que pueden afectar a los activos de la información de las Unidades Administrativas de la Dirección Distrital 05D01 Latacunga – Educación"
- Elaborar la guía actualizada de procedimientos para la seguridad informática enfocados a las Unidades Administrativas para reducir la fuga de información

confidencial de la Dirección Distrital 05D01 Latacunga – Educación.

- Formular un cronograma de implementación de las políticas de seguridades informáticas mediante normas ISO 27001 para la Dirección Distrital 05D01 Latacunga - Educación.

1.3. Justificación de la Investigación

Actualmente los sistemas informáticos están utilizando una gran área en el ámbito empresarial, institucional entre otros, el cual demanda que la información que es similar debe ser confidencial, además que se tiene políticas de seguridad para acceder a la misma.

La información que maneja la Dirección Distrital 05D01 Latacunga - Educación, los equipos de computación, los sistemas informáticos, son de uso importante en el trabajo diario de cada funcionario, la información antigua como los que se van generando se almacenan en cada uno de los equipos como base de datos considerada como un almacenamiento empírico, sin tener un control de la información la misma que es vulnerada constantemente y es por la falta de seguridades informáticas.

"La prioridad es la seguridad, y consiste en asegurar que la información no se pierda ni 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." (Romero Castro y otros, 2018)

Por medio de las seguridades informáticas se manejará información adecuada y correcta la que permitirá brindar datos certeros, y con beneficios gigantescos como el fácil manejo de información que reposará como base de datos, agilitará los procesos, respuestas a corto plazo a los usuarios.

Para todo este proceso se recomendará tomar como prioridad la capacitación a todo el personal sobre el manejo de documentos digitales y la ejecución de las políticas de seguridad normas ISO 27001 y 27002.

Viendo la problemática y con el objetivo de resguardar la información con la que se trabaja en la Dirección Distrital 05D01 Latacunga - Educación y por ser de mucha relevancia se propone

también plantear políticas autónomas de seguridad por medio de las normas ISO 27001, 27002 la cual permite reducir gastos, considerando que la seguridad de la información tiene un costo sin conllevar una evidente ganancia financiera.

Sugerir que se implemente y se resguarde la información en un server con un SO de software libre (Es un sistema operativo de código abierto) que en la actualidad con el uso de códigos abiertos brinda muchos beneficios directos, como resguardar la información por medio de almacenamiento; se deberá crear carpetas dentro del Servidor por cada Unidad y líder Departamental, quienes serían los custodios directos del manejo de información (carpetas que servirá como repositorio).

Para esto y por cuestiones de seguridad tendría un usuario y contraseña las que tendrían permisos y restricciones, cada carpeta manejaría procesos de entrada y salida de información de cada unidad departamental, más las políticas de seguridad normas ISO 27001 que serán incluidas.

La Dirección Distrital 05D01 Latacunga - Educación debe emplear normativas para trabajos de diagnóstico, tanto para la implementación como la implantación de sistemas de seguridad de la información – SGSI alineado con el estándar ISO/IEC 27001 y el sistema de control establecido en la norma ISO/IEC 27002.

Se obtienen los resultados de una experiencia al momento de aplicar las fases de auditoría, la metodología de análisis y evaluación de riesgos mediante el diseño y ejecución de varios instrumentos como cuestionarios que se aplicaron a los administradores, clave de seguridad, entrevistas a los empleados del área informática y usuarios de los sistemas, pruebas de intrusión y testeo que ayuden a obtener el diagnóstico de seguridad actual. (Francisco Nicolás Javier Solarte Solarte1, Edgar Rodrigo ENRIQUEZ ROSERO2, Mirian del Carmen Benavides Ruano3 - Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001, 2015)

CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA

2.1. Antecedentes de la Investigación

Durante mucho tiempo, las empresas e instituciones públicas han descuidado la seguridad de la información, centrándose únicamente en mejorar sus sistemas informáticos. Sin embargo, con el paso del tiempo, se ha perfeccionado la manera de vulnerar la información que tienen estas organizaciones, lo que las hace susceptibles a ataques. La mejora tecnológica, principalmente en Internet y las comunicaciones, ha dado paso para que las personas reconozcan lo importante de la información y la facilidad de acceso a los datos.

En la actualidad, gran parte, si no todas, de las instituciones públicas y privadas, como puede ser en el sector privado como en el público, otorgan importancia a la protección y el respaldo de su información. Reconocen que la información es uno de los activos más indispensables para la continuidad de los procesos. Para lograr esto, se toman medidas y se implementan protocolos de seguridad.

La seguridad de la información abarca varios aspectos, entre estos esta el control de acceso, la seguridad de los dispositivos, la gestión de contraseñas y el control de las vulnerabilidades, entre otros (Catuto Pilay, 2021). Todos estos aspectos necesitan un estudio, un presupuesto y una implementación adecuada, estas pueden ser de forma preventiva o correctiva. Es importante tener en cuenta que no existe un método de seguridad totalmente seguro, ya que todos los días surgen nuevos riesgos en diferentes niveles. Por lo tanto, es fundamental realizar un análisis de todas las amenazas basado en normativas como la ISO 27001, con el objetivo de mejorar los procedimientos y neutralizar las amenazas que tiendan a debilitar la seguridad de la información (Catuto Pilay, 2021) .

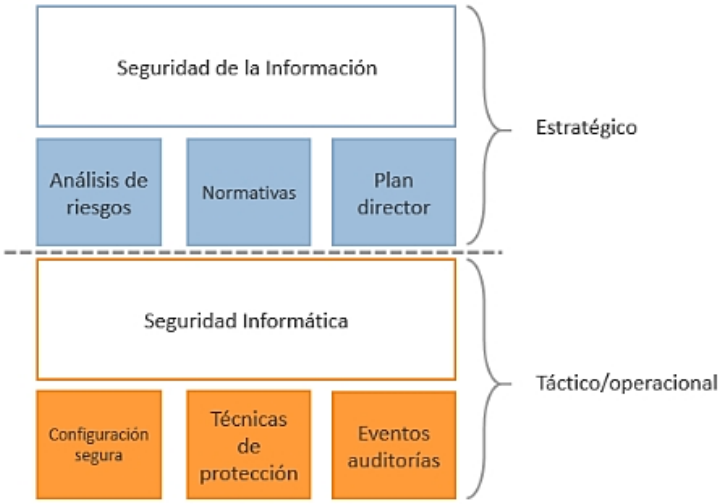
Aunque la seguridad informática y la seguridad de la información tienden a parecer similares debido al desarrollo y la constante evolución de la tecnología, en realidad son áreas distintas con objetivos y actividades diferentes que deben trabajar en conjunto. La seguridad informática se centra en aspectos tácticos y operativos de la seguridad, por otro lado la seguridad de la información se considera la línea estratégica de la seguridad (ISO 27001, 2017).

La seguridad de la información abarca diversos aspectos, como la gestión de riesgos, las amenazas, los análisis de escenarios, las buenas prácticas y los marcos normativos. Estos elementos requieren niveles que aseguren los procedimientos y la tecnología utilizada, con el

fin de aumentar la seguridad en la elaboración, utilización, almacenamiento, transmisión, recuperación y disposición final de la información (ISOTools, 2017)

Figura 1

Seguridad de la Información



En Ecuador, son escasas las instituciones y organizaciones que cuentan con la certificación de la Norma ISO 27001, lo que refleja una falta de conciencia acerca de los riesgos potenciales. Teniendo en cuenta que los procesos organizacionales dependen en amplia cantidad de los sistemas de información, es importante reconocer que estos se encuentran expuestos a diversas amenazas que pueden explotar vulnerabilidades y colocar en peligro los activos más críticos que albergan información

Para asegurar la seguridad de la información en las instituciones y organizaciones, es necesario considerar las potenciales amenazas que puedan afectarla. El hacking y los virus informáticos son riesgos comunes que pueden provocar incidentes involuntarios y colocar en peligro la seguridad de la información (Valdeviezo Troya & Rodriguez Poveda, 2015).

Ante esta situación, resulta imperativo realizar un análisis de seguridad de la información en la Dirección Distrital 05D01 Latacunga - Educación. Este análisis debe incluir la identificación de potenciales vulnerabilidades y riesgos a los que se enfrenta, utilizando métodos, así como la observación, la investigación, encuestas y entrevistas. Por medio de este análisis, se deben determinar las causas y efectos de los obstaculos existentes y buscar soluciones, incluyendo el establecimiento de políticas de seguridad que resguarden adecuadamente la información.

2.2. Bases Teóricas

La Norma ISO 27001, una norma internacional, su objetivo garantizar la seguridad, privacidad e integridad de los datos, la información y los sistemas que los procesan (Grupo ESGINNOVA, 2022). Mediante el estándar ISO 27001:2013 para los Sistemas de Gestión de la Seguridad de la Información, las organizaciones tienen a analizar los riesgos y realizar los controles requeridos para reducirlos o eliminarlos (Intedya, 2018). La implementación de la norma ISO-27001 se traduce en una diferenciación respecto a otras organizaciones, lo que mejora su competitividad y su imagen.

Además, la Gestión de la Seguridad de la Información se mejoran con las excelentes prácticas y los controles propuestos en la norma ISO 27002 (ESGinnova, 2021). Hoy en día, la seguridad informática tiene un papel indispensable, ya que previene el hurto de datos sensibles como pueden ser los números de cuentas bancarias, información de tarjetas de crédito, contraseñas, documentos, hojas de cálculo y bases de datos, entre otros.

Sin embargo, no solo se trata del robo de datos, sino también del mal uso de la información almacenada en los ordenadores. Otro individuo puede alterar los códigos fuente de los programas o emplear imágenes y cuentas de correo electrónico para obtener contenido malicioso. Además, existen ciberdelincuentes con la intención de ingresar a los sistemas informáticos y llevar a cabo ataques contra otros equipos, sitios web o redes, con el único propósito de causar cao (Vazquez Reyna, 2018).

La seguridad informática incorpora varias medidas de protección, como programas antivirus, firewalls y otras formas que requieran del usuario, estas pueden ser la activación o desactivación de ciertas funciones de software (Kiuwan, 2023). Además, los ciberdelincuentes pueden recurrir a ataques DDoS para impedir el acceso a sitios web y provocar el fallo del servidor (Netec, 2023).

Figura 2

¿Qué es seguridad informática?

Nota. Tomado de (Netec, 2023)

La Norma ISO 27001:2013 se ha desarrollado para ser implementada en organizaciones y empresas de cualquier tipo, con el fin de proporcionar pautas que impulsen la evolución de la seguridad de la información. Dicha norma define niveles de soporte para los Sistemas de Gestión de Seguridad de la Información (SGSI) y se alinea con las tecnologías de la información de cada empresa. Se destacan cambios significativos en comparación con la versión de 2005, como la reducción de 17 controles, pasando de 133 a 114, y la eliminación de requisitos redundantes, lo que resulta en una menor documentación y la inclusión de secciones de acción (Montalvo Cisneros, 2021)

La aplicación de esta normativa ha sido modificada por numerosas organizaciones tanto públicas como privadas en todo el mundo. Determine un enfoque sistemático para el manejo de la información privada de la organización y garantiza su protección y disponibilidad. En resumen, se considera un estándar integral que abarca la seguridad técnica, física, del personal y de los procesos dentro de la empresa (Riveros, 2020).

2.3. Desarrollo de Variables de Estudio

2.3.1. La Seguridad

El término seguridad tiene múltiples usos y se deriva del latín "securitas". En el ámbito de la informática, se distinguen dos tipos de seguridad: la física, que implica obstaculos físicas para restringir el acceso sin autorización al sistema, y la lógica, que se enfoca en la encriptación de códigos y el uso de autenticación, antivirus y cortafuegos para evitar que los intrusos superen las barreras físicas (Jacha Rojas, 2019).

En su sentido más amplio, el término "seguridad" se relaciona con la ausencia de riesgos o peligros y está estrechamente vinculado a la confianza y la prevención. Su significado puede variar según el campo de conocimiento desde el cual se aborde (Editorial Etecé, 2023)

La protección de la información se trata de los métodos y procesos utilizados para resguardar los archivos de información en varias formas y estados. Por otro lado, la seguridad informática se centra en los métodos y procesos técnicos para garantizar la confidencialidad, disponibilidad e integridad de la información (Figueroa Suárez et al., 2018).

En resumen, la seguridad abarca distintos aspectos y se aplica tanto a la protección física como a la protección lógica de la información. La seguridad de la información se centra en la protección de los archivos de información, mientras que la seguridad informática se enfoca en los métodos técnicos para obtener la confidencialidad, disponibilidad e integridad de la información. Ambos conceptos son fundamentales para asegurar la protección y la fiabilidad en los sistemas informáticos.

2.3.2. Seguridad informática

La seguridad informática se ocupa de anticipar los ataques dañinos dirigidos a computadoras, servidores, dispositivos móviles, sistemas electrónicos, redes y datos, entre otros (Figueroa Suárez et al., 2018). Se refiere a la capacidad de resistir accidentes o acciones ilícitas que afecten la disponibilidad, autenticidad, integridad y confidencialidad de los datos que están almacenados o transmitidos, así como de los servicios establecidos por las redes y sistemas informáticos (Postigo Palacios, 2020).

En la actualidad, la seguridad informática se han transformado en una parte esencial para los negocios y las operaciones de las organizaciones, ya que se encarga de resguardar la privacidad

de los datos en los sistemas informáticos. Aunque no existen sistemas infalibles al 100%, las empresas que se relacionan a través de medios digitales requieren buscar mecanismos especializados para respaldar la seguridad de sus datos mediante la implementación de los diferentes tipos de seguridad informática (UNIR, 2021).

Es importante destacar que la seguridad informática se encarga de la protección del entorno informático, por lo que la protección de la información conlleva cualquier cosa que pueda contener información. La informática se ocupa de procesar, almacenar y transmitir la información, mientras que la seguridad de la información está preocupada por la protección integral de esa información en diversos contextos. Aunque existen diferencias entre ambos conceptos, lo más relevante es el alcance y la amplitud de cada uno en el entorno informático (Romero Castro et al., 2018).

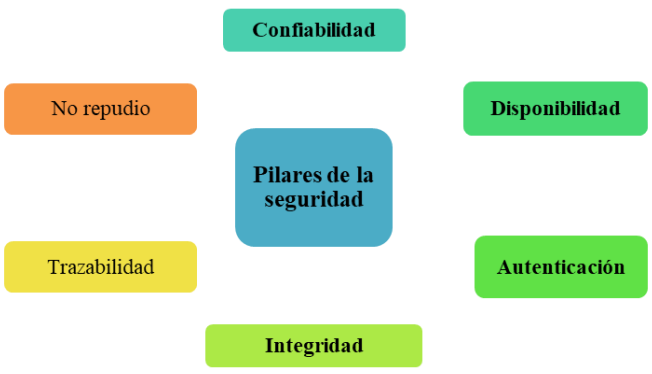
2.3.3. Pilares de la seguridad

Los datos representan valores, números, medidas, textos y documentos sin procesar, mientras que la información es el valor que se obtiene a partir de esos datos, aportando conocimiento. Los manuales de procedimientos, los datos de empleados, proveedores y clientes, así como la base de datos de facturación, son ejemplos de datos estructurados que se transforman en información y proporcioan valor a una empresa (Romero Castro et al., 2018).

En el ámbito de la seguridad de la información, existen tres pilares fundamentales: confidencialidad, integridad y disponibilidad. Estos requisitos se consideran esenciales para asegurar la protección de la información. Además, existen otros pilares complementarios, como la autenticación, el no repudio y la trazabilidad, que refuerzan los aspectos de seguridad mencionados anteriormente (Postigo Palacios, 2020).

Figura 3

Pilares de la Seguridad de la Información



2.3.3.1. Confiabilidad

La confidencialidad es una variable importante en la seguridad de la información, ya que establece condiciones para evitar que la información esté disponible o sea indispensable a personas, entidades o procesos no autorizados (Bojacá Garavito, 2021). Este principio implica que solo las personas que están autorizadas deben poder acceder al control de un sistema. La confidencialidad está estrechamente relacionada con la escalada de privilegios que un hacker puede lograr mediante un ciberataque. Al obtener una debilidad, el ciberdelincuente buscará obtener privilegios de administrador en el equipo, lo que le permitirá causar daños más graves en los sistemas informáticos (KeepCoding, 2022).

Para asegurar la confidencialidad de la información, se emplean diversos recursos (Postigo Palacios, 2020). Uno de ellos es la gestión de privilegios, que garantiza que las personas autorizados operen solo con la información necesaria y no tengan acceso a más datos de los requeridos. Otro recurso fundamental es el cifrado de la información, que impide que los usuarios no autorizados puedan leerla en caso de que intercepten la información almacenada o transmitida.

2.3.3.1. Integridad

La integridad este definido como la variable que busca preservar la exactitud y la completitud de los activos, asegurando la integridad de la información y sus métodos de procesamiento a través de controles (Bojacá Garavito, 2021). En el contexto de la seguridad informática, este pilar está relacionado con la escalada de privilegios y se refiere a la manipulación o alteración no autorizada del software o hardware por parte de un ciberdelincuente. La capacidad de modificar un sistema según sus propios deseos es una de las opciones disponibles para un atacante (KeepCoding, 2022).

En otras palabras, la integridad tiene como objetivo garantizar la autenticidad de la información, asegurando que los datos no sean alterados sin autorización previa. Sin embargo, en momento de producirse un cambio no autorizado, inesperado o no planificado, la información tiende sufrir daños irreversibles (DocuSign, Inc, 2021).

Existen diversas formas eficientes de fortalecer el pilar de la integridad, entre las cuales son importantes las siguientes acciones.

En primer lugar, es importante definir permisos adecuados para acceder a los archivos. Esto implica establecer niveles de autorización que limiten el acceso solo a las personas autorizadas, evitando modificaciones no autorizadas por parte de usuarios no autorizados.

Además, se recomienda aplicar sistemas de verificación que detecten cambios en los datos, ya sea en la red o que contenga de daños en los equipos u otros eventos que no tengan relación con la actividad humana. Estos sistemas permiten detectar cambios no deseados en la información, lo que contribuye a mantener la integridad de los datos (DocuSign, Inc, 2021).

Otra medida importante es el uso de checksum para corroborar la integridad de la información almacenados en varios medios durante un período establecido o enviados por canales con ruido. El checksum es un mecanismo que permite detectar cualquier modificación o alteración en los datos, garantizando su integridad durante el proceso de almacenamiento o transmisión (DocuSign, Inc, 2021).

Por lo que las situaciones de integridad quieren asegurar que el intercambio de instrucciones, mensajes y orientaciones entre los funcionarios y sectores logre que los destinatarios sin cambiar su contenido principalmente así evitar afectar la comunicación de carácter interno como externo (DocuSign, Inc, 2021).

2.3.3.1. Autenticidad

La autenticidad es otro pilar fundamental en el ámbito de la ciberseguridad. Este pilar se centra en la capacidad de un software para confirmar la identidad veridica de un usuario o del remitente de un mensaje (KeepCoding, 2022).

En otras palabras, la autenticidad se relaciona con la verificación de la identidad y la garantía de que un usuario o entidad sea realmente quien afirma ser. En el contexto de la seguridad informática, este pilar es esencial para evitar suplantaciones de identidad y asegurar la confianza en las transacciones y comunicaciones digitales.

2.3.3.1. Disponibilidad

La disponibilidad es otro aspecto crucial que puede verse afectado durante un ciberataque. Este pilar hace referencia a la capacidad de los usuarios para ingresar a las

funciones y recursos a los que tienen permiso (KeepCoding, 2022). Se establecen parámetros para permitir el acceso y el uso de la información y los sistemas por parte de individuos, entidades o procesos autorizados cuando sea necesario (Bojacá Garavito, 2021).

Es fundamental desarrollar e implementar ideas para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en los tiempos y la escala requeridos, especialmente después de interrupciones o fallos en los procesos críticos del proyecto (Bojacá Garavito, 2021). La disponibilidad es un aspecto esencial para considerar que se cuenta con un nivel mínimo de seguridad con respecto a la información. No sirve de nada tener información veraz si el acceso a ella es difícil o imposible. La información debe estar disponible para aquellos que la necesiten para que sea útil y valiosa. Por ejemplo, un ataque distribuido de denegación de servicio (DDoS) puede dejar sin utilizar una tienda en línea, impidiendo que los clientes accedan a ella y realicen compras. Del mismo modo, si una dirección de correo electrónico se usa para enviar correos no deseados y se añade a listas negras, se afectará la disponibilidad de los correos legítimos (Romero Castro et al., 2018).

Para garantizar la disponibilidad, se crea políticas de control, como acuerdos de nivel de servicio (SLA), pueden balancear la carga de tráfico para mitigar el impacto de los ataques DDoS y copias de seguridad para la recuperación de información perdida. Además, es importante contar con recursos alternativos a los primarios para evitar interrupciones en caso de fallos (Romero Castro et al., 2018).

2.3.3.1. Trazabilidad

La trazabilidad es una variable fundamental en el desarrollo de un sistema de gestión de seguridad informática, ya que permite establecer procedimientos que ayudan a seguir el proceso de evolución de un producto por todas sus etapas (Bojacá Garavito, 2021).

Esto quiere decir que la trazabilidad consiste en mantener un registro completo y detallado de las etapas y actividades involucradas en el desarrollo de un producto o proyecto. Proporciona la capacidad de rastrear y documentar todos los eventos y cambios que ocurren a lo largo del proceso.

2.3.3.1. No repudio

El principio del no repudio es considerado como el último de los pilares básicos de la ciberseguridad. Este concepto se suma al de la autenticidad y tiene como finalidad respaldar la verificación de la identidad de un usuario. En términos simples, el no repudio se refiere a la función que impide que un usuario niegue haber sido el emisor de la información que envía. Por ejemplo, en el caso de un correo electrónico, el no repudio asegura que el remitente no pueda negar haber enviado el mensaje. (KeepCoding, 2022).

2.3.4. La ISO 27001 seguridad de información

La Norma proporciona los requisitos necesarios para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información, adaptado a los requerimientos y necesidades de la organización (Gómez Torres, 2018).

En términos generales, la Norma deduce de forma genérica cómo se planifica, implementa, verifica y controla un Sistema de Gestión de Seguridad de la Información, sin importar los riesgos ambientales tanto internos y externos de la organización ni los activos de los procesos (UNIR, 2019). Esto significa que toda empresa u organización puede adoptar un SGSI siguiendo este estándar.

La Norma se compone de 10 cláusulas. Las cláusulas 1 a 3 abordan aspectos generales, como los resultados anhelados del sistema de gestión, las normas de referencia importantes y las definiciones aplicables (Gómez Torres, 2018). Las cláusulas 4 a 10 establecen los requisitos fundamentales para una correcta implementación del Sistema de Gestión de Seguridad de la Información (Gómez Torres, 2018)

Cláusula 4: Contexto de la organización

Se enfoca en comprender la organización y su contexto, incluyendo el conocimientos de las necesidades y expectativas de las entidades interesadas y también la determinación del alcance del SGSI.

Cláusula 5: Liderazgo

Se centra en el liderazgo y el acuerdo de la alta dirección, lo que implica establecer políticas de seguridad de la información y definir los roles, responsabilidades y autoridades dentro de la organización.

Cláusula 6: Planificación

Se establecen métodos para abordar los riesgos y oportunidades identificados, así como la definición de objetivos de seguridad de la información y la planificación para alcanzarlos.

Cláusula 7: Soporte

Se refiere al soporte necesario para el funcionamiento del SGSI, donde se incluye la determinación de recursos, la evaluación de la competencia del personal y la concienciación sobre las políticas de seguridad de la información, así como la documentación requerida por la norma.

Cláusula 8: Operación

Se enfoca en las operaciones, donde se establecen los controles operacionales indispensable para cumplir con lo que pide la seguridad de la información, se evalúan los riesgos de seguridad y se implementan medidas para tratar dichos riesgos.

Cláusula 9: Evaluación del desempeño

Se relaciona con la evaluación del desempeño del SGSI, incluyendo la realización de auditorías internas y la revisión del SGSI por parte de la alta dirección.

Cláusula 10: Mejora

Se centra en la mejora de todos los días, abordando las inconformidades, la ejecución de acciones correctivas y el establecimiento de estrategias para la mejora continua del SGSI.

Es importante destacar que la certificación en esta norma necesita que se cumplan las cláusulas 4 al 10, lo cual demuestra el compromiso de la organización con la seguridad de la información y su disposición a continuar las mejores prácticas establecidas en la norma.

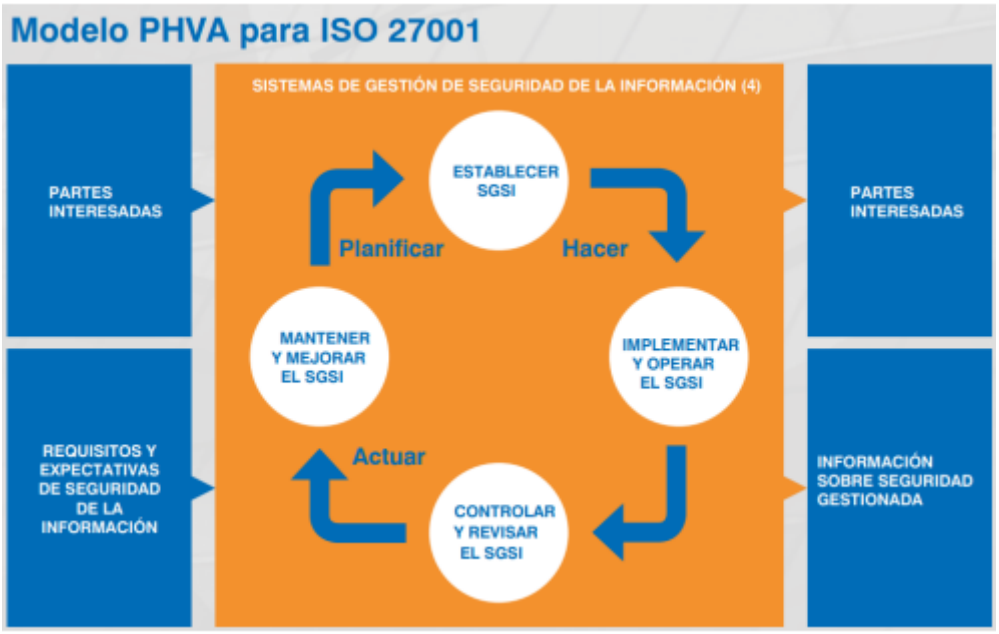
La norma ISO 27001 está basado en el ciclo PHVA, se lo conoce como el ciclo de Deming. Este ciclo no solo se aplica al sistema de gestión en su conjunto, pero también a cada uno de los elementos individuales, lo que proporciona un enfoque para la mejora progresiva (Chávarry

Bonilla, 2021).

El ciclo PHVA, que significa Planificar, Hacer, Verificar y Actuar, es una metodología reconocida internacionalmente para la gestión de procesos. En el contexto de la norma ISO 27001, este ciclo se utiliza para planificar y verificarlos controles de seguridad de la información, implementar dichos controles, verificar su eficacia y realizar las acciones correctivas y preventivas necesarias (Chávarry Bonilla, 2021).

Figura 4

Modelo PHVA para ISO 27001



Nota. Se muestra los niveles del SGSI, para mejorar el proceso que ayudan a mejorar la seguridad. Tomado de (Chávarry Bonilla, 2021)

- Planificar (Plan): se realiza un análisis de riesgos para identificar las riesgos y vulnerabilidades en la seguridad de la información. En relación a este análisis, se seleccionan y diseñan como controlar adecuadamente para disminuir los riesgos identificados.

- Hacer (Do): se implementan los controles definidos en la etapa anterior. Esto implica la adopción de políticas y procedimientos, la distribución de responsabilidades y la implementación de medidas técnicas y organizativas para proteger la información.

- Verificar (Check): se realiza una evaluación y revisión periódica del desempeño del SGSI.

Esto implica medir la eficacia y eficiencia de los controles implementados, así como identificar los posibles brechas o áreas de mejora continua.

- Actuar (Act): se toman acciones correctivas y preventivas para abordar las brechas o deficiencias identificadas durante la fase de verificación. También se realizan ajustes y mejoras continuas en el SGSI para conservarlo actualizado y adaptado a las modificaciones en el entorno de seguridad de la información (Alvarado, 2023)

Este ciclo PHVA permite un enfoque sistemático y cíclico para la gestión de la seguridad de la información, garantizando que se establezcan, implementen, verifiquen y mejoren continuamente los controles indispensables para resguardar los activos de información de una organización

2.3.5. Porque se trabaja con ISO 27001

Al analizar las ventajas y desventajas de las normas ISO 27001, se obtiene una comprensión de forma completa de su impacto y utilidad en las organizaciones. En la siguiente tabla se describen.

Tabla 1

Ventajas y desventajas de las normas ISO 27001

Ventajas	Desventajas
Sistema de gestión estructurado	Es una abstracción y un elevado nivel, debiudo a que no está muy detallado
Menor riesgo de tener un incidente de seguridad	Los requisitos tienden a ser difíciles de interpretar, ya que tienen nuevos conceptos
Las empresas cumplen con la legislación aplicable	No tiene una descripción muy detallada a la hora de reconocer los riesgos.
Mayor prestigio de la empresa	En ciertas instituciones o empresas puede existir cierta resistencia cultural al cambio cuando se implementa la norma ISO 27001
Incrementar la confianza de los clientes	Para implementar y conservar un SGSI basados según establecido de la norma ISO 27001 puede involucrar costos significativos.
Obtener la homologación como	

proveedor de forma más fácil

Nota. Se puede observar las ventajas y desventajas al trabajar con las normas ISO 27001 (ISO 27001, 2022)

2.3.6. Sistemas Operativos Licenciados y Libres

Los sistemas operativos licenciados, también conocidos como software propietario o de código cerrado, son programas informáticos donde los usuarios tienen limitaciones para usar, modificar o redistribuir el software (Quispe, 2020). Estos sistemas restringen las posibilidades de personalización y modificación por parte del usuario.

Por otro lado, el software libre, también llamado software de código abierto, permite a los usuarios tener plena libertad para utilizar, distribuir y modificar el software (EMERGE AVEZALIA, S.L, 2020) . Esta característica fomenta un mayor desarrollo y mejora del software original.

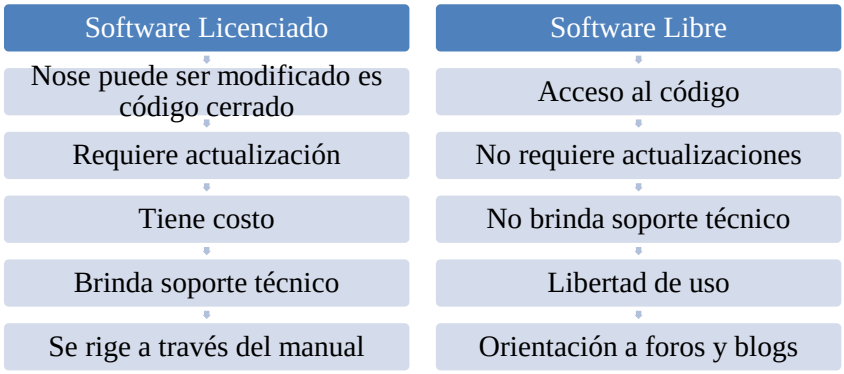
La diferencia principal entre ambos tipos de sistemas operativos radica en las restricciones impuestas por las licencias. En los sistemas operativos licenciados, los términos de la licencia describen los usos permitidos y limitan la forma en que el software puede ser utilizado según las leyes de derechos de auto (Sontay, 2020).

En cuanto a la seguridad, tanto los sistemas operativos libres como los licenciados pueden estar en igualdad de condiciones. Sin embargo, una ventaja tradicional de los sistemas operativos licenciados ha sido el soporte técnico y las garantías de seguridad proporcionadas por los fabricantes (Sontay, 2020).

Ambos tipos de sistemas pueden ofrecer niveles de seguridad similares, aunque los sistemas operativos licenciados a menudo tienen la ventaja adicional del soporte técnico y las garantías proporcionadas por los fabricantes.

Figura 5

Comparación entre sistemas operativos libres y licenciados



Nota. Tomado de (Quispe, 2020)

El término "software libre" fue acuñado por el informático estadounidense Richard Stallman, quien buscaba crear un sistema operativo en el que la libertad de los usuarios fuera primordial (Ixiam, 2022). Las características fundamentales del software libre se basan en una serie de "libertades" que definen su funcionamiento y principios de actuación.

Estas libertades incluyen la posibilidad de analizar y modificar el programa según las necesidades de cada usuario, así como utilizarlo con cualquier propósito deseado (Ixiam, 2022). Además, el software libre permite optimizarlo, corrigiendo errores, realizando mejoras y proponiendo nuevos desarrollos para su avance. Asimismo, se promueve la libertad de entregar copias del programa de manera gratuita, fomentando la colaboración e innovación de otros usuarios.

Algunos ejemplos de sistemas operativos libres son Linux, FreeBSD, OpenBSD y GNU Hurd, los cuales son utilizados en una gran variedad de dispositivos, donde empieza en servidores y computadoras personales hasta llegar a dispositivos móviles y sistemas embebidos. Estos sistemas operativos brindan a los usuarios la posibilidad de utilizar, modificar y distribuir el software de manera libre, fomentando la comunidad y el avance tecnológico (Ixiam, 2022).

Algunos de los ejemplos de sistemas operativos libres se presentan en la siguiente figura

Figura 6

Sistemas Operativos Libres

2.3.6.1. Linux

Linux se defina como un sistema operativo de código abierto que se distingue por su naturaleza completamente libre y gratuito. A diferencia de Windows o macOS, no está sujeto a la propiedad de una única compañía, sino que es resultado de la colaboración de numerosas compañías y personas que ayudan a su desarrollo y tienen sus propias distribuciones de Linux.La gratuidad de Linux significa que los usuarios pueden utilizar en cualquier ordenador sin la necesidad de pagar por su licencia, evitando la necesidad de descargarlo de forma ilegal a través de Internet (Aguilar, 2023).

Las Características de Linux según Aguilar (2023) son:

- **Gratuito:** Linux se destaca por ser un sistema operativo de acceso gratuito, en contraste con otros sistemas como Windows o macOS. Se asigno bajo licencias de código abierto, lo que ayudan a los usuarios acceder al código fuente, modificarlo y distribuirlo libremente.

- **Código abierto:** Linux se define como un sistema de código abierto, lo que implica que su código fuente se lo observa públicamente y se puede descargar, ver, alterar y distribuir libremente. Los usuarios tienen la libertad de utilizar el software como deseen, adaptándolo a sus necesidades sin restricciones ni condiciones impuestas por los propietarios del software.

- **Seguridad:** Linux se lo conoce por su seguridad. Gracias a su naturaleza de

sistema libre, hay menos interés en diseñar un virus o malware para este sistema. Además, su arquitectura para la manipulación de archivos, procesos y memoria evita fácilmente la persistencia de amenazas. La comunidad de usuarios y desarrolladores trabaja en conjunto para identificar y solucionar rápidamente cualquier problema de seguridad que pueda surgir.

- **Multitarea:** Linux es un sistema operativo multitarea, lo que significa que logra la ejecución de muchos programas de forma simultánea. Los usuarios realizaran múltiples tareas por ejemplo navegar por Internet, procesar documentos, escuchar música y ver videos, al igual que en otros sistemas operativos populares.

- **Multiusuario:** Linux es un sistema multiusuario, lo que logra que varios usuarios accedan a todos los recursos y aplicaciones de forma simultánea y segura. Cada usuario cuenta con su propio directorio de inicio y puede acceder solo a los archivos y recursos para los que cuenten con permisos de acceso. Esta característica es especialmente útil en entornos de servidor y en computadoras compartidas.

- **Personalizable:** Linux ofrece una gran capacidad de personalización. Los usuarios pueden modificar casi todos los aspectos del sistema, comenzando con la apariencia visual hasta las configuraciones internas. Hay una variedad de distribuciones de Linux disponibles, con sus propias características y conjuntos de software, lo que ayuda a los usuarios elegir la tenga mayor adaptabilidad a sus necesidades y preferencias.

- **Alto control de dispositivos:** Linux consta de una gran gama de controladores de dispositivos incorporados, lo que facilita la instalación y conexión de diferentes dispositivos sin la exigencia de instalar controladores extras. Además, la comunidad de Linux crea controladores de código abierto para una gran variedad de dispositivos, garantizando una compatibilidad más amplia.

- **Independiente y estable:** Linux se lo considera uno de los sistemas operativos más estables y confiables. En cual se puede cambiar y distribuido libremente, lo que fomenta una respuesta rápida con adaptación a los cambios. Es

ampliamente utilizado en servidores y computadoras que necesitan un funcionamiento continuo sin fallos.

- **Escalable:** Linux tiene gran escalabilidad y puede adaptarse a los requerimientos cambiantes de los usuarios. Su diseño flexible y eficiente en la utilización de recursos permite añadir más usuarios, servicios y dispositivos sin dañar significativamente el rendimiento del sistema (Aguilar, 2023).

2.3.6.1. Centos

CentOS, conocido como Community Enterprise Operating System, es una distribución específica del sistema operativo Linux. Esta distro, como se le conoce comúnmente, se destaca por ser una opción popular entre la comunidad empresarial. CentOS se basa en el código fuente de otro sistema operativo popular, Red Hat Enterprise Linux (RHEL). A través de este enfoque, CentOS proporciona un sistema operativo estable, seguro y de calidad empresarial sin costos de licencia (Ortiz, 2018).

Figura 7

Sistema Operativo CentOS

2.3.6.1. Windows Server

Windows Server es una plataforma que ayuda a construir una infraestructura completa de aplicaciones, redes y servicios web, conectando ambientes locales y Azure, mientras añade capas adicionales de seguridad y ayuda a modernizar las aplicaciones e infraestructura de empresas y organizaciones (Precitool, 2021).

La primera versión de Windows Server, conocida como Windows 2000 Server, fue lanzada en los albores del nuevo milenio. Fue diseñada para convertirse en el servidor de archivos, impresión y web de empresas en crecimiento, ofreciendo una solución eficiente al centralizar todas estas funciones en un único centro.

Con el transcurso del tiempo, Microsoft ha ido implementando avances significativos en Windows Server. La última versión del sistema está especialmente adaptada a las necesidades actuales y se centra en cuatro aspectos clave (Precitool, 2021):

- Seguridad avanzada de varios niveles: Windows Server proporciona una seguridad sólida y sofisticada en múltiples niveles, protegiendo los datos y las aplicaciones de las amenazas cibernéticas.

- **Capacidades híbridas con Azure:** La integración con Azure, la plataforma de servicios en la nube de Microsoft permite una infraestructura híbrida que combina lo mejor de los ámbitos locales y la nube, brindando flexibilidad y escalabilidad.

- **Plataforma de aplicación flexible:** Windows Server ofrece una plataforma versátil para desarrollar y desplegar aplicaciones, permitiendo a las empresas adaptarse a las necesidades cambiantes y aprovechar las últimas tecnologías.

- **Ofertas inmejorables en Azure:** Windows Server en Azure proporciona una gran gama de servicios y soluciones para organizaciones, incluyendo opciones de almacenamiento, análisis de datos, inteligencia artificial y mucho más, impulsando la innovación y el crecimiento empresarial.

Ventajas

- La administración de Windows es sencilla y fácil de realizar.

- Existe una amplia documentación oficial que facilita su uso y proporciona guías y recursos para resolver cualquier problema.

- Permite un menor tiempo de desarrollo, lo que agiliza la implementación de soluciones y aplicaciones.

- El aprendizaje de Windows es relativamente sencillo, lo que facilita su adopción y uso por parte de los usuarios.

- Un aspecto destacado del hosting de Windows en comparación con Linux es su soporte para el framework de alto rendimiento ASP.NET, lo que brinda ventajas adicionales

para el desarrollo de aplicaciones web (Imagar, 2021).

Desventajas

- Se necesita cancelar el pago de una licencia para utilizar Windows, lo que puede suponer un costo adicional para los usuarios.
- Windows es conocido por tener una mayor cantidad de fallos de seguridad en comparación con otros sistemas operativos.
- La instalación y configuración de niveles superiores en Windows necesitan conocimientos avanzados de administración del sistema.
- Windows ocupa más recursos con relación a otros sistemas operativos para servidores, lo que puede afectar el rendimiento en entornos con recursos limitados.
- Después de aplicar una actualización en Windows, es recomendable reiniciar el sistema para que los cambios tengan efecto (Imagar, 2021).

2.3.7. La cultura de seguridad

La cultura de seguridad se refiere al impacto que la cultura organizacional tiene en las formas de actuar y pensar que impactan en la seguridad dentro de una organización (Instituto para una Cultura de seguridad Industrial, 2018). Un enfoque sustentado en la cultura de seguridad no separa la seguridad como un objetivo independiente, sino que destaca:

- El reconocimiento de la cultura de seguridad en las decisiones tomadas por la organización.
- La influencia de la cultura organizacional en los comportamientos y prácticas relacionadas con la seguridad.

Un enfoque fundamentado en la cultura de seguridad no cambiara entonces a la seguridad en una burbuja separada de las demas metas de la organización. Tendrá el énfasis en:

- El lugar asiganado a la cultura de la seguridad en los arbitrajes realizados por la organización.
- La influencia de la cultura de la organización por encima de los

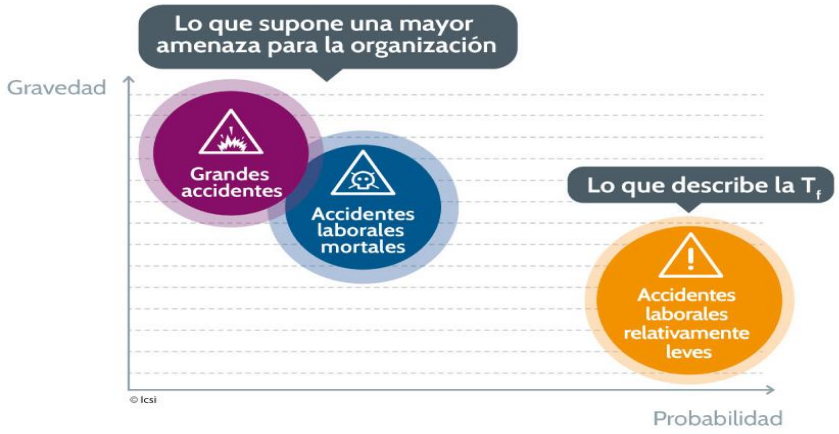
comportamientos y las prácticas en el ámbito de seguridad.

La cultura de seguridad trata del conjunto de actitudes y valores que los usuarios tienen en relación con la seguridad, y cómo se aplican en las labores habituales. En resumen, la cultura de seguridad abarca cómo las personas perciben, valoran y priorizan la seguridad en su vida cotidiana, así como su comportamiento tanto individual como colectivo (SISSA Monitoring Integral, 2023).

Las organizaciones se hacen frente a varios tipos de riesgos, que van desde accidentes leves hasta accidentes laborales graves o mortales, e incluso accidentes que pueden causar varias víctimas y dañar las instalaciones industriales y el medio ambiente. Estos riesgos ocupan varias posiciones según su probabilidad y gravedad (Instituto para una Cultura de seguridad Industrial, 2018):

Figura 8

Los diferentes tipos de riesgos - Crédito: BP graphisme



2.3.8. Malware

El malware se refiere a software o código informático diseñado específicamente para infectar, dañar o acceder a sistemas informáticos. Existen diversos tipos de malware, cada uno con su propio método de corrupción o infección de dispositivos, aunque todos comparten el objetivo común de comprometer la seguridad y privacidad de los sistemas informáticos. El término "malware" se utiliza como una denominación general para cualquier forma de "software malicioso" diseñado para introducirse en un dispositivo sin que el usuario sepa y ocacionar daños, interrupciones en el sistema o robo de datos. Algunos ejemplos de malware incluyen adware, spyware, virus, redes de robots (botnets), troyanos, gusanos, rootkits y ransomware

(Avast Software, 2023).

En el mundo del malware, hay una amplia diversidad de variantes, pero muchos tipos comparten señales de advertencia similares. Es importante monitorear su dispositivo en busca de los siguientes síntomas de infección de malware (Avast Software, 2022):

- **Disminución repentina del rendimiento:** El malware puede utilizar una gran cantidad de potencia de procesamiento, lo que provoca una desaceleración significativa del dispositivo. Por lo tanto, eliminar el malware es una forma de acelerar el rendimiento del PC.

- **Bloqueos y cierres frecuentes del sistema:** Algunos tipos de malware pueden causar cierres repentinos del sistema o bloquear el equipo. Otros malware consumen una gran cantidad de memoria RAM o aumentan la temperatura de la CPU, lo que también puede provocar bloqueos. Un uso constante y alto de la CPU puede ser un indicio de la presencia de malware.

- **Eliminación o daño de archivos:** El malware a menudo elimina o daña archivos como parte de su estrategia para causar caos.

- **Aparición de numerosos anuncios emergentes:** El adware tiene la función de enviar correo no deseado y mostrar ventanas emergentes con anuncios. Otros tipos de malware también pueden generar anuncios y alertas emergentes.

- **Redirecciones del navegador:** Si el navegador continúa dirigiéndote a sitios web no deseados, es posible que un malware haya modificado la configuración de DNS de tu dispositivo.

- **Contactos que reciben mensajes extraños de tu parte:** Algunos tipos de malware se propagan enviando correos electrónicos o mensajes a los contactos de la víctima. Utilizar aplicaciones de mensajería segura puede proteger tus comunicaciones contra espías.

- **Aparición de una nota de rescate:** El ransomware muestra una nota de rescate en tu pantalla, exigiendo un pago para recuperar tus archivos. Esta nota de rescate es un indicador claro de la presencia de ransomware.

- **Presencia de aplicaciones desconocidas:** El malware puede instalar aplicaciones adicionales en tu dispositivo sin tu conocimiento. Si observas nuevos programas que no has

instalado, es posible que sean el resultado de un ataque de malware.

2.3.9. Ransomware

El ransomware se lo considera un tipo de malware que restringe el acceso a la información al cifrar los archivos utilizando algoritmos criptográficos simétricos o asimétricos. Posteriormente, exige un rescate para desbloquear y recuperar los archivos cifrados, siendo común el uso del algoritmo simétrico AES de 256 bits (Moreno et al., 2020).

El ransomware es considerado uno de los problemas con mayor criticidad en el ámbito de la seguridad informática. Se trata de un tipo de malware que bloquea o cifra la información de la víctima y solicita un costo para restaurar el acceso a los datos (Cumbicus Pineda et al., 2022).

Existen dos categorías principales de ransomware, según la forma en que impide el acceso al equipo o a la información:

- Ransomware de cifrado (encrypting ransomware o filecoders): Este tipo de ransomware cifra los archivos del usuario, impidiendo el acceso a los datos. Una vez que el dispositivo está infectado, el atacante solicita un rescate para desencriptar y recuperar los archivos (Bazante Veloz et al., 2019).

- Ransomware que no cifra (lock screen ransomware): Este tipo no puede cifrar los archivos, sino que bloquea el acceso al dispositivo. El ataque realiza cambios en el sistema y modifica la configuración del equipo para mostrar una pantalla con una notificación de rescate, lo que impide toda interacción con el dispositivo comprometido (Bazante Veloz et al., 2019).

2.3.10. Virus informáticos

Los virus informáticos son programas creados con el propósito de propagarse de manera descontrolada y causar daños significativos a los datos electrónicos. Estos programas maliciosos se propagan entre archivos y computadoras, y comparten similitudes sorprendentes en cuanto a su virulencia, métodos de propagación y evolución a lo largo del tiempo con los microorganismos que causan enfermedades infecciosas. Aunque los virus informáticos son una invención humana, su desarrollo sigue una ruta biológica bien conocida. Los ancestros relativamente inofensivos evolucionan gradualmente hasta convertirse en agentes patógenos, desarrollando mecanismos de defensa adaptativos en los sistemas huésped, a la vez que seleccionan

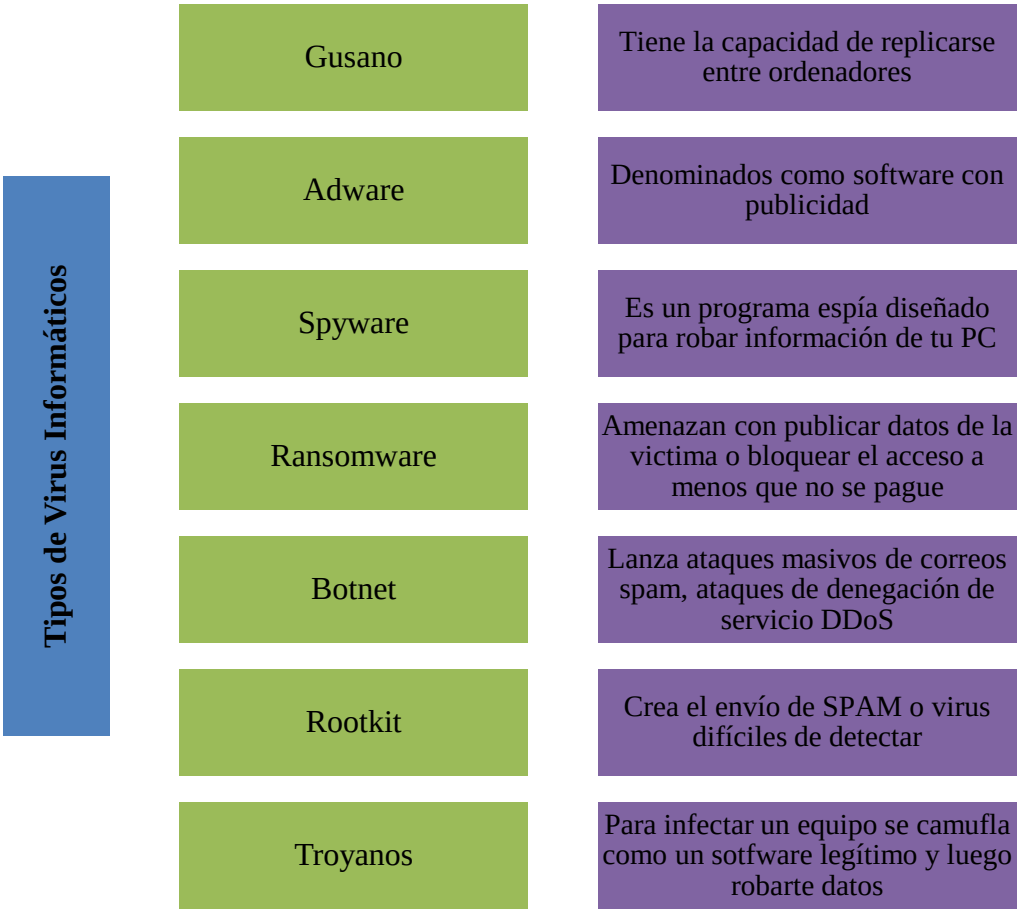
nuevas variantes de virus. Así, se alcanza un equilibrio entre la infección y las defensas del huésped (Guaña Moya et al., 2022).

Según Norton (2018), un virus informático se asemeja a un virus de gripe, ya que está diseñado para infectar a un host y tiene la capacidad de replicarse de manera similar a los virus biológicos.

En la actualidad, existen diversos tipos de virus informáticos, entre los cuales se pueden mencionar los más relevantes:

Figura 9

Tipos de Virus Informáticos



2.3.11. Concepto de autenticación

La autenticación se refiere a la habilidad de identificar de forma exclusiva a un usuario de un sistema o una implementación en funcionamiento. Su objetivo principal es demostrar de manera verificable que un usuario o una aplicación es netamente quien afirma ser (IBM, 2021)

En términos generales, la autenticación implica la presentación de credenciales o pruebas de identidad. Estas pueden ser cosas que el usuario conoce, como una contraseña, algo que posee, como una tarjeta de identificación, o algo inherente a su persona, como su huella dactilar o su rostro. Los recientes avances en este campo inbolucra la autenticación basada en características físicas, como la voz, las huellas dactilares, los ojos y la escritura (IBM, 2021).

En el entorno digital, la autenticación se utiliza ampliamente para tener acceso a diferentes cuentas en línea, como pueden ser correos electrónicos, redes sociales y servicios bancarios en línea. Incluye una capa adicional de seguridad al asegurar que solo los usuarios autorizados puedan ingresar a sus cuentas personales y salvaguardar la información confidencial que contienen (IBM, 2021).

2.3.12. Mecanismos preventivos en seguridad informática

Los mecanismos preventivos en seguridad informática comprenden una variedad de evaluaciones periódicas y mejoras en aspectos técnicos y otros elementos relacionados con los sistemas y procesos de una empresa. Aunque pueden implicar un costo significativo para las organizaciones, se considera una inversión a largo plazo que proporcionará ventajas a la organización (Hernández, 2023).

Figura 10

Mecanismos preventivos de seguridad

Cuando se habla de mecanismos preventivos en seguridad, se hace referencia a la realización de revisiones periódicas y la implementación de cambios y mejoras en diversos aspectos, incluyendo hardware, software y otros componentes periféricos de las computadoras.

Es innegable que muchos ataques informáticos podrían evitarse o al menos reducirse mediante la aplicación oportuna de medidas preventivas. Por esta razón, los mecanismos preventivos tienden a tener gran amplitud, y es crucial tener un plan de eliminación o reducción y llevar a cabo auditorías periódicas para identificar varios problemas y vulnerabilidades en la seguridad informática. Estas estrategias fortalecen la seguridad y ayudan a prevenir riesgos (Hernández, 2023).

Es fundamental entender que la aplicación de la seguridad informática es un proceso permanente y dinámico que necesita atención constante. Este enfoque es el primer paso para reforzar el ingreso, la integridad, la confidencialidad y la disponibilidad de los datos en una organización. Al mantenerse alerta y adoptar un enfoque proactivo, las organizaciones pueden garantizar una protección sólida y actualizada contra las amenazas cibernéticas en constante evolución (Hernández, 2023).

2.3.13. Medios de seguridad de respaldo

Los medios de seguridad de respaldo consisten en crear una copia exacta de todos los archivos y datos que existen en una computadora, y se lo guarda en otro dispositivo de almacenamiento, como puede ser un disco duro externo, una memoria USB o un servidor en la nube. De esta manera, si el equipo principal sufre algún daño o se pierde, es posible obtendrá los archivos a partir de la copia de seguridad (Toledo, 2022).

Existen diferentes tipos de medios para almacenar que se requieran utilizar, y no son excluyentes entre ellos. Algunas de las soluciones más cotidianas incluyen el uso de un almacén de datos que pueden ser personal o del proyecto utilizando discos USB, discos duros de laptops o unidades en red dentro de la institución, un repositorio institucional, un almacén de datos institucional, una infraestructura de almacenamiento nacional, un almacén de datos en la nube y un repositorio disciplinar (CEPAL, 2020).

Los respaldos son de vital importancia para emprendedores y empresas. En motivos de fallos o infecciones por virus, por ejemplo, es crucial arreglar rápidamente los datos de la empresa y de los clientes, al igual que la infraestructura informática, para obtener menos pérdidas económicas. Además, se encuentra en juego la reputación empresarial, que se vería afectada si los clientes experimentaran demoras en la recepción de respuestas, incumplimientos de plazos o una falta de prestación oportuna de los servicios contratados (IONOS, 2020).

CAPÍTULO III: METODOLOGÍA

El presente capitulo está enfocado a detallar la metodología empleada para el proyecto de investigación, la cual tiene como propósito central el analizar las vulnerabilidades de la seguridad informática en las Unidades Administrativas de la Dirección Distrital 05D01 Latacunga - Educación, con el propósito de desarrollar políticas de seguridad de la información basadas en las normas ISO 27001.

Además, este capítulo proporciona una guía sistemática de cómo se esta llevando a cabo el proceso de identificación de riesgos, amenazas y vulnerabilidades, así como la posterior elaboración de procedimientos y guías para la propuesta para implementar las políticas de seguridad. Se describen en detalle las herramientas, técnicas y fuentes de datos empleadas en la investigación, brindando una base sólida para comprender la metodología utilizada en la búsqueda de soluciones efectivas para aumentar la seguridad de la información en la Dirección Distrital.

3.1. Diseño de Investigación

El diseño de la investigación desempeña un papel indispensable en la consecución de los objetivos planteados en este estudio. Implica la estructuración y planificación meticulosa de los métodos y enfoques que se emplearán para abordar la problemática de la seguridad informática en la Dirección Distrital 05D01 Latacunga - Educación. Por lo cual, para el presente proyecto el diseño de la investigación se fundamentó en una perspectiva mixto que combinó elementos cualitativos y cuantitativos.

3.1.1. Enfoque cualitativo

Se empleo un enfoque cualitativo, debido a que se realizó un análisis cualitativo de la situación de seguridad informática en la Dirección Distrital 05D01 Latacunga - Educación, mediante la identificación de riesgos y vulnerabilidades a través de entrevistas y revisión documental. Este enfoque cualitativo permitió una comprensión profunda de los desafíos específicos que enfrentaba la organización en cuanto a la seguridad de la información.

3.1.2. Enfoque cuantitativo

Se empleó un enfoque cuantitativo para cuantificar la magnitud de los riesgos

identificados y establecer métricas para evaluar el impacto potencial de las vulnerabilidades. Esto implicó el uso de herramientas de evaluación de riesgos y la recopilación de datos cuantitativos relacionados con la infraestructura tecnológica y los activos de información.

Se propondrán una serie de políticas de seguridad autónomas en las Unidades Administrativas de la Dirección Distrital 05D01 Latacunga - Educación, basados en la norma ISO 27001, por lo que en este tipo de políticas serán autónomas y determinadas conforme a los problemas identificados para evitar la pérdida de información.

La gestión de la seguridad de la Dirección Distrital 05D01 Latacunga – Educación, según la norma ISO 27001 es competencia de todos los funcionarios que tengan responsabilidades sobre la información, repositorios y cualquier otro dato de la Dirección Distrital.

3.2. Nivel o tipo de Investigación

Los tipos de investigación desempeñan un papel muy importante en la configuración de la metodología utilizada en este estudio. Implican la elección de enfoques específicos que tienen mayor adaptabilidad a los objetivos de la investigación. En este contexto, se han empleado tipos de investigación que abarcan tanto la investigación aplicada, descriptiva y de campo.

3.3.1 Investigación Aplicada

Esta investigación se clasificó principalmente como investigación aplicada, ya que tuvo como objetivo abordar un problema específico en un entorno real, en este caso, la seguridad informática en la Dirección Distrital 05D01 Latacunga - Educación. Se buscó aplicar los conceptos teóricos y las normas ISO 27001 en un contexto práctico para desarrollar políticas y procedimientos de seguridad efectivos.

3.3.2 Investigación descriptiva

Se consideró como investigación descriptiva, ya que se pretendió describir en detalle la situación actual de seguridad informática en la organización, identificando riesgos y vulnerabilidades específicos. También se incluyeron elementos de exploratorios, ya que se exploraron nuevas formas de mejorar la seguridad informática en el contexto educativo.

3.3.3 Investigación de Campo

La investigación de campo recopila los datos directamente de la realidad y permite la obtención de información directa en relación con un problema. (López & Francisco, 2020)

La investigación de campo es un enfoque de investigación que implica la recolección directa de datos en el entorno real donde suceden los eventos que se están estudiando. Por tal motivo se realizará un tipo de investigación exploratorio en la Dirección Distrital 05D01 Latacunga - Educación, para determinar las condiciones actuales de la seguridad de los sistemas de información y de comunicación, para observar, recopilar y analizar datos de primera mano.

3.3. Población

La población objetivo de esta investigación está vinculada a la Dirección Distrital 05D01 Latacunga - Educación, ubicada en la provincia de Cotopaxi, cantón Cotopaxi, con dirección en Antonia Vela 580 y Guayaquil. En este contexto, los principales beneficiarios de la investigación son el personal administrativo que labora en esta entidad educativa. Los encargados de implementar y supervisar las políticas de seguridad informática serán los líderes departamentales de la Dirección Distrital.

La duración estimada de esta investigación abarca un período de 2 años, durante los cuales se llevarán a cabo distintas etapas, desde la identificación de vulnerabilidades hasta la implementación de políticas de seguridad. El número total de personas a ser encuestadas y participantes activos en el proceso es de 29 administrativos, quienes desempeñan roles clave en la gestión de la información y la seguridad informática de la Dirección Distrital 05D01 Latacunga - Educación. Estos individuos serán indispensables para la recopilación de datos, la identificación de riesgos y la implementación de las políticas de seguridad, contribuyendo así al éxito de la investigación.

3.4. Técnicas e instrumentos de recolección de datos (Conforme a ISO)

“Las técnicas de recolección de datos son las distintas formas o maneras de obtener la

información. Son ejemplos de técnicas: la observación directa, el análisis documental, análisis de contenido, etc.

La información será proporcionada por el personal administrativo de la Dirección Distrital 05D01 Latacunga - Educación.

La investigación no tiene sentido sin las técnicas de recolección de datos, que conducen a la verificación del problema planteado. Cada tipo de investigación determinara las técnicas a utilizar y cada técnica establece sus herramientas, instrumentos o medios que serán empleados.

Todo lo que va a realizar el investigador tiene su apoyo en la técnica de la observación. Aunque utilice métodos diferentes, su marco metodológico de recogida de datos se centra en la técnica de la observación y el éxito o fracaso de la investigación dependerá de cual empleó" (Aguiar, s.f.).

Para poder recolectar la información se lo hará mediante la técnica de observación y la entrevista con sus respectivos instrumentos, como son el ingreso de datos y un cuestionario de encuesta.

3.5. Procesamiento y análisis de la Información

3.5.1. Procesamiento y análisis de la información

Como primer punto es realizará a la recopilación de la información seleccionando los datos que se requiere para el desarrollo del presente trabajo, mismos que será revisados en relación con el problema y poder establecer las conclusiones respectivas asegurando que los datos sean lo más reales posibles.

3.5.2. Plan de análisis e interpretación de resultados

Los resultados serán analizados desde el punto de vista descriptivo y estadístico, mismo que permite realizar la interpretación apropiada basada en el marco teórico, relacionado con las variables de investigación y la propuesta lo que servirá para establecer las conclusiones y recomendaciones.

CAPÍTULO IV: PRESENTACIÓN Y ANÁLISIS DE DATOS

4.1. Situación Actual

El presente proyecto de investigación se realizó en la Dirección Distrital 05D01 Latacunga – Educación, una entidad educativa situada en la provincia de Cotopaxi, cantón Cotopaxi, con su sede en Antonia Vela 580 y Guayaquil. Durante un período de 2 años, se dedicó a analizar a fondo la situación de la actualidad en términos de seguridad informática en esta institución educativa.

El enfoque principal de este análisis recayó en el personal administrativo, quienes desempeñan un papel esencial en la gestión de la información y la seguridad informática en la Dirección Distrital. A través de la recopilación de datos y la participación activa de los líderes departamentales, se logró obtener una visión completa de los desafíos y vulnerabilidades que enfrenta la organización con relacion a la protección de la información y la necesidad de desarrollar políticas de seguridad basadas en normas ISO 27001.

A continuación, se presenta la misión y visión de la Dirección Distrital 05D01 Latacunga – Educación:

Misión

"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." (Educación, 2023)

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

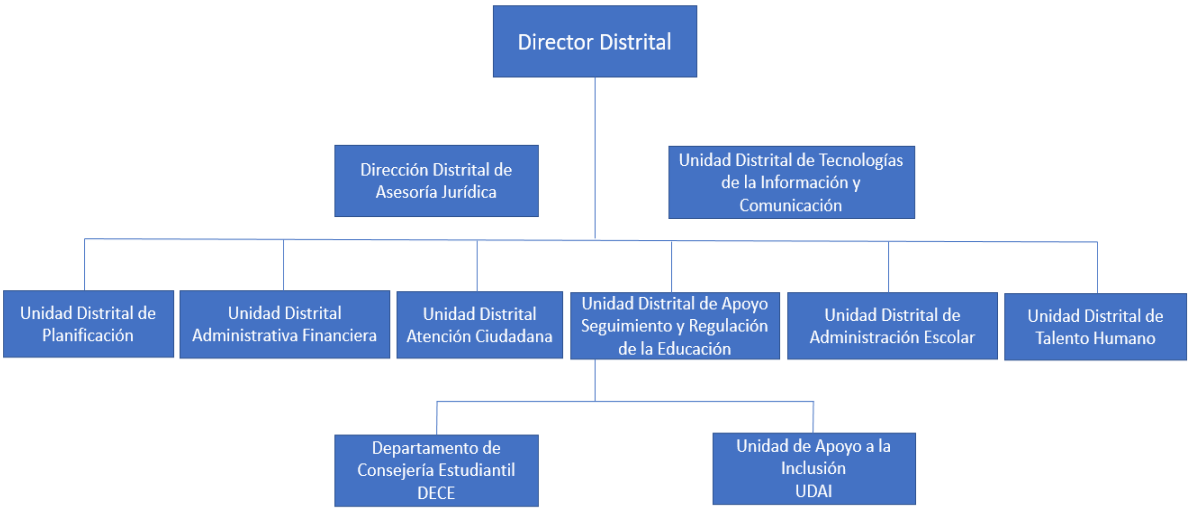
diferentes niveles y modalidades de 4 los sistemas de educación" (Educación, 2023).

Organigrama del distrito

En la figura 11 se muestra los Departamentos con los que cuenta la Dirección Distrital 05D01 Latacunga - Educación.

Figura 11

Departamentos Administrativos de la Dirección Distrital 05D01 Latacunga – Educación



Política de calidad

Es la línea de acción de las organizaciones para ir mejorando continuamente los procesos internos y que son reflejados en la Gestión de Calidad: el cliente, el mercado y la empresa. Para lo cual se busca facilitar los servicios efectivos en la Atención Ciudadana y a la Comunidad Educativa, alcanzando lo requerido por el usuario a través de un proceso de mejora permanente (Nueva ISO 9001, 2017).

Objetivos de calidad

a. Regularizar los procesos de Atención Ciudadana en todas las Direcciones Distritales.

b. Aumentar la complacencia del usuario en los procedimientos de Atención Ciudadana.

c. Reducir las denuncias ciudadanas en las Direcciones Distritales.

4.1.1. Análisis de la necesidad

El análisis de la necesidad es un componente fundamental en la realización de este proyecto de investigación en la Dirección Distrital 05D01 Latacunga – Educación. La necesidad de abordar la seguridad informática se derivó de una serie de factores críticos. En primer lugar, el aumento dependencia de la tecnología en el diario vivir y el incremento de los ataques cibernéticos a nivel global han convertido la seguridad informática en una prioridad tanto para organizaciones como para instituciones educativas. En el contexto específico de la Dirección Distrital, la falta de políticas de seguridad informática y la ausencia de una normativa autónoma para la protección de la información confidencial de la entidad se identificaron como carencias significativas. La ubicación estratégica de la Dirección Distrital en la provincia de Cotopaxi la hace vulnerable a posibles riesgos y amenazas cibernéticas.

En consecuencia, el análisis de la necesidad se centró en la urgente ejecución de políticas de seguridad de la información basadas en las normas ISO 27001, con el propósito de salvaguardar los activos de la información, asegurar la confiabilidad e integridad de los datos y mitigar los riesgos de pérdida o robo de información confidencial. Este análisis, respaldado por datos objetivos y la realidad de la organización, justificó plenamente la necesidad de este proyecto de investigación y la posterior implementación de políticas de seguridad informática en la Dirección Distrital 05D01 Latacunga – Educación.

4.2. Análisis de resultados

Con el objetivo de adquirir información precisa y detallada sobre la situación actual en términos de seguridad informática en la Dirección Distrital 05D01 Latacunga – Educación, se llevó a cabo una encuesta dirigida a las personas de administración de la institución. La encuesta se puede visualizar en el Anexo 1.

La encuesta fue aplicada a un total de 29 administrativos, quienes desempeñan roles cruciales en la gestión de la información y la seguridad informática en la Dirección Distrital. Esta encuesta se diseñó cuidadosamente, abordando aspectos esenciales relacionados con políticas y procedimientos de seguridad informática, protección física de equipos informáticos, respaldo y continuidad del negocio, gestión de accesos y gestión de riesgos.

A través de esta encuesta, se obtuvo una visión integral de la percepción y prácticas de las personas de administración asociado con la seguridad informática en la Dirección Distrital

05D01 Latacunga – Educación, lo que permitió identificar áreas de mejora y definir las bases para la elaboración de políticas de seguridad informática basadas en normas ISO 27001.

Dimensión A: Políticas y procedimientos de seguridad informática

Pregunta 1. ¿Se dispone de políticas de seguridad informática en las Unidades Administrativas de la Dirección Distrital 05D01 Latacunga – Educación?

Tabla 2

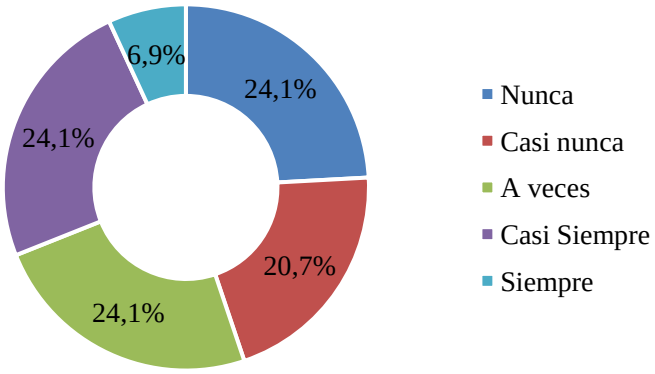
Políticas de seguridad en Unidades Administrativas de la Dirección Distrital 05D01 Latacunga – Educación.

Categoría	Frecuencia	Porcentaje
Nunca	7	24,1%
Casi nunca	6	20,7%
A veces	7	24,1%
Casi Siempre	7	24,1%
Siempre	2	6,9%
Total	29	100%

Nota. Elaboración propia a partir de los datos de la encuesta

Figura 12

Políticas de seguridad en Unidades Administrativas de la Dirección Distrital 05D01 Latacunga – Educación.



Nota. Elaboración propia a partir de los datos de la encuesta

Interpretación:

Según los datos recopilados en la encuesta, la distribución porcentual de las respuestas muestra que el 20,7% de los encuestados afirmó que casi nunca se dispone de políticas de seguridad, mientras que el 24,1% indicó que nunca se cuenta con estas políticas. El 24,1% de los encuestados afirmó que las políticas están presentes a veces en las unidades administrativas. Por otro lado, un 24,1% señaló que casi siempre se dispone de estas políticas y un 6,9% manifestó que siempre están presentes.

Los datos nos indican que la gran parte de los encuestados parece estar experimentando una situación intermedia en términos de disponibilidad de estas políticas, lo que sugiere una inconsistencia en la ejecución de las políticas de seguridad informática en el entorno laboral. La falta de una presencia constante de políticas de seguridad informática podría implicar riesgos para la integridad de los sistemas y la protección de la información sensible.

Pregunta 2. ¿Conoce y comprende las políticas de seguridad informática en las Unidades Administrativas?

Tabla 3

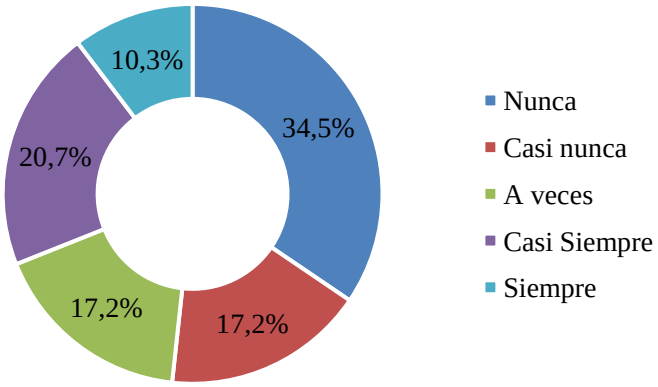
Conocimiento y comprensión de políticas de seguridad informática

Categoría	Frecuencia	Porcentaje
Nunca	10	34,5%
Casi nunca	5	17,2%
A veces	5	17,2%
Casi Siempre	6	20,7%
Siempre	3	10,3%
Total	29	100%

Nota. Elaboración propia a partir de los datos de la encuesta

Figura 13

Conocimiento y comprensión de políticas de seguridad informática



Nota. Elaboración propia a partir de los datos de la encuesta

Interpretación:

Se observa que el 34,5% afirmó Nunca conocer y comprender las políticas de seguridad informática, mientras que un 17,2% respondió Casi nunca. Otro 17,2% indicó A veces tener conocimiento y comprensión, y el mismo porcentaje del 17,2% respondió Casi siempre. Un 10,3% manifestó que Siempre conoce y comprende estas políticas.

El hecho de que más de la mitad de los encuestados (51,7%) haya indicado que Nunca o Casi nunca conoce y comprende las políticas de seguridad informática en las Unidades Administrativas plantea una preocupación significativa. Esto sugiere que existe una falta de comunicación efectiva o de capacitación en términos de las políticas de seguridad informática en el ámbito laboral. Los resultados de la encuesta apuntan a la importancia de fortalecer los esfuerzos de capacitación y comunicación en relación a las políticas de seguridad informática. Esto permitirá mejorar el conocimiento y comprensión del personal, reduciendo los riesgos asociados con la falta de conciencia en temas de seguridad informática y fomentando prácticas más seguras en el manejo de la información.

Pregunta 3. ¿Actualizan y revisan las políticas de seguridad informática en las Unidades Administrativas?

Tabla 4

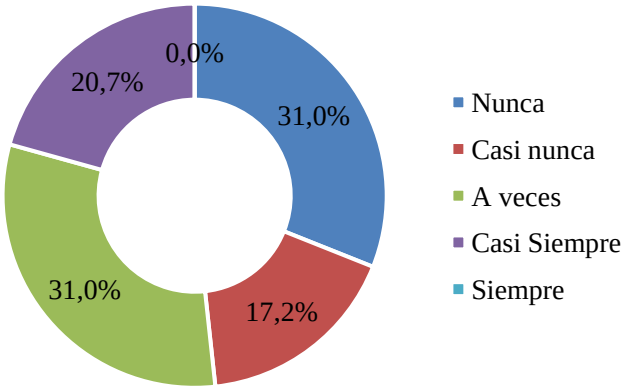
Actualización y revisión de políticas de seguridad en Unidades Administrativas

Categoría	Frecuencia	Porcentaje
Nunca	9	31,0%
Casi nunca	5	17,2%
A veces	9	31,0%
Casi Siempre	6	20,7%
Siempre	0	0,0%
Total	29	100%

Nota. Elaboración propia a partir de los datos de la encuesta

Figura 14

Actualización y revisión de políticas de seguridad en Unidades Administrativas



Nota. Elaboración propia a partir de los datos de la encuesta

Interpretación:

Se observó que el 31,0% respondió Nunca realizan actualización y revisión de las políticas de seguridad, mientras que un 17,2% indicó Casi nunca. Otro 31,0% manifestó que A veces realizan esta actividad, y el mismo porcentaje del 20,7% respondió Casi siempre. No hubo ningún encuestado que respondiera Siempre en esta categoría. El resultado general nos indica que la mayoría de los encuestados (51,7%) parece estar enfrentando desafíos en cuanto a la implementación constante de esta práctica. La falta de una actualización y revisión periódica de las políticas de seguridad informática puede tener implicaciones negativas en la efectividad de las medidas de seguridad. Las amenazas y riesgos en el entorno digital evolucionan constantemente, por lo que la falta de actualización de políticas podría llevar a lagunas de seguridad y vulnerabilidades no identificadas.

El hecho de que un 48,3% de los encuestados haya respondido que no realizan esta actividad de manera constante sugiere la importancia de ir mejorando los procesos y la cultura en torno a la seguridad informática. Es posible que se requieran estrategias más efectivas para promover y establecer prácticas de actualización y revisión regulares de las políticas de seguridad.

Pregunta 4. ¿Comunican y difunden las políticas de seguridad informática al personal de las Unidades Administrativas?

Tabla 5

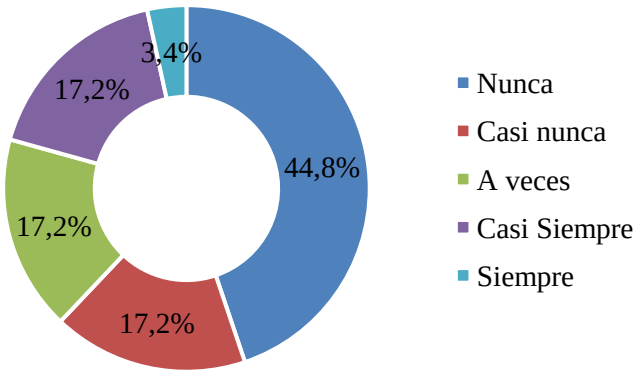
Comunicación y difusión de políticas de seguridad al personal

Categoría	Frecuencia	Porcentaje
Nunca	13	44,8%
Casi nunca	5	17,2%
A veces	5	17,2%
Casi Siempre	5	17,2%
Siempre	1	3,4%
Total	29	100%

Nota. Elaboración propia a partir de los datos de la encuesta

Figura 15

Comunicación y difusión de políticas de seguridad al personal



Nota. Elaboración propia a partir de los datos de la encuesta

Interpretación:

Los resultados de la encuesta referentes a la comunicación y difusión de las políticas de seguridad informática al personal de las Unidades Administrativas de la Dirección Distrital 05D01 Latacunga – Educación indican que el 44,8% respondió que Nunca se comunican y difunden las políticas de seguridad informática, mientras que un 17,2% indicó Casi nunca. Otro 17,2% manifestó que esto se hace A veces, y el mismo porcentaje del 17,2% respondió Casi siempre. Solo un 3,4% de los encuestados afirmó que estas políticas se comunican y difunden Siempre.

Debido a que un reducido porcentaje de los encuestados respondió Siempre en relación a la comunicación y difusión de las políticas de seguridad informática al personal resalta la falta de consistencia en esta práctica. En términos generales se refleja que la mayoría de los encuestados (62,0%) experimenta una falta de comunicación efectiva en cuanto a estas políticas. La ausencia o falta de comunicación y difusión adecuada de las políticas de seguridad informática puede tener implicaciones negativas en la adhesión a estas políticas y en la comprensión de su importancia. La falta de conocimiento sobre las políticas de seguridad podría llevar a prácticas inseguras o incorrectas en el manejo de la información y sistemas.

Pregunta 5. ¿Se capacita a los empleados sobre las políticas y procedimientos de seguridad informática en las Unidades Administrativas?

Tabla 6

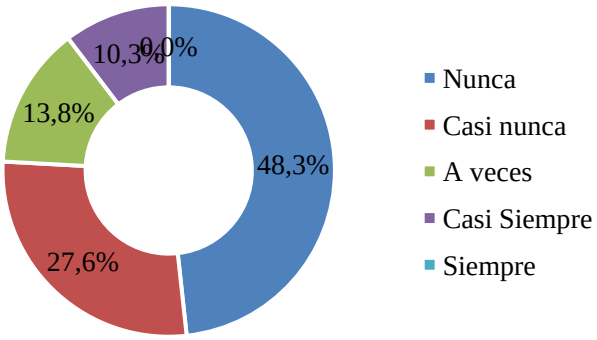
Capacitación sobre políticas de seguridad en Unidades Administrativas

Categoría	Frecuencia	Porcentaje
Nunca	14	48,3%
Casi nunca	8	27,6%
A veces	4	13,8%
Casi Siempre	3	10,3%
Siempre	0	0,0%
Total	29	100%

Nota. Elaboración propia a partir de los datos de la encuesta

Figura 16

Capacitación sobre políticas de seguridad en Unidades Administrativas



Nota. Elaboración propia a partir de los datos de la encuesta

Interpretación:

Los resultados de la encuesta señalan que el 48,3% respondió que Nunca se capacita al personal sobre estas políticas, mientras que un 27,6% indicó que esto se hace Casi nunca. Otro 13,8% manifestó que la capacitación ocurre A veces, y el 10,3% respondió Casi siempre. Ningún encuestado respondió que el personal se capacita Siempre sobre las políticas y procedimientos de seguridad informática. El resultado global en relación a la capacitación del personal sobre las políticas de seguridad informática muestra que más de tres cuartos de los encuestados (76,6%) indicaron que esta actividad no es llevada a cabo de manera constante. Este alto porcentaje que indicó que la capacitación es rara o nula sugiere una falta de conciencia y preparación en términos de seguridad informática. La falta de capacitación constante del personal sobre las políticas y procedimientos de seguridad informática podría tener implicaciones significativas en la seguridad de la información y los sistemas en las Unidades Administrativas.

Dimensión B: Protección física

Pregunta 6. ¿Los equipos informáticos de las Unidades Administrativas de la Dirección Distrital 05D01 Latacunga – Educación se resguardan en lugares seguros?

Tabla 7

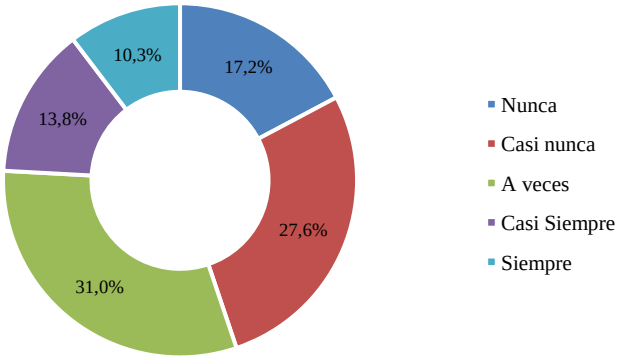
Resguardo seguro de equipos informáticos en Unidades Administrativas

Categoría	Frecuencia	Porcentaje
Nunca	5	17,2%
Casi nunca	8	27,6%
A veces	9	31,0%
Casi Siempre	4	13,8%
Siempre	3	10,3%
Total	29	100%

Nota. Elaboración propia a partir de los datos de la encuesta

Figura 17

Resguardo seguro de equipos informáticos en Unidades Administrativas



Nota. Elaboración propia a partir de los datos de la encuesta

Interpretación:

Se evidenció que el 17,2% de los encuestados respondió que Nunca se resguardan en lugares seguros los equipos informáticos, mientras que un 27,6% indicó que esto se hace Casi nunca. Otro 31,0% manifestó que los equipos se resguardan A veces, y el 13,8% respondió Casi siempre. Un 10,3% de los encuestados afirmó que los equipos se resguardan Siempre. El resultado general sugiere que existe una variabilidad significativa en la práctica de resguardo seguro de los equipos informáticos en las Unidades Administrativas. La falta de un resguardo seguro constante podría tener implicaciones en la protección de los equipos y la información que tienen.

Pregunta 7. ¿Se controla el acceso a las áreas donde están ubicados los equipos informáticos?

Tabla 8

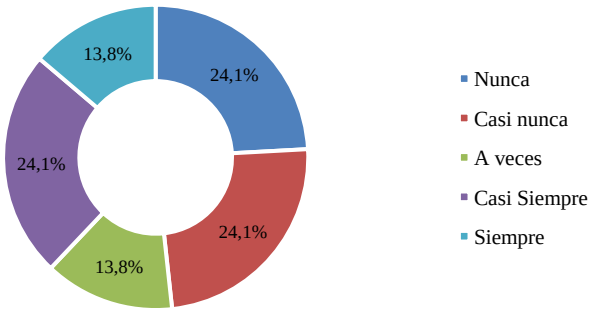
Control de acceso a áreas con equipos informáticos

Categoría	Frecuencia	Porcentaje
Nunca	7	24,1%
Casi nunca	7	24,1%
A veces	4	13,8%
Casi Siempre	7	24,1%
Siempre	4	13,8%
Total	29	100%

Nota. Elaboración propia a partir de los datos de la encuesta

Figura 18

Control de acceso a áreas con equipos informáticos



Nota. Elaboración propia a partir de los datos de la encuesta

Interpretación:

Las respuestas de los encuestados señalan que el 24,1% respondió que Nunca se controla el acceso a estas áreas, mientras que otro 24,1% indicó que esto se hace Casi nunca. Un 13,8% manifestó que se controla el acceso A veces, y el mismo porcentaje del 13,8% respondió que se controla Casi siempre. Otro 13,8% de los encuestados afirmó que el acceso a estas áreas se controla Siempre. Aunque un porcentaje pequeño indicó que esta práctica ocurre Siempre, más de un tercio de los encuestados parece experimentar una falta de consistencia en este aspecto. La falta de un control de acceso constante podría tener implicaciones en la seguridad de los equipos y la información que contienen. Una mayor consistencia en esta actividad puede contribuir a la protección efectiva de los activos tecnológicos y la información, reduciendo los riesgos de pérdida o acceso no autorizado a los equipos y los datos.

Pregunta 8. ¿Se registra la identificación de los usuarios que manipulan los equipos de la Dirección Distrital 05D01 Latacunga – Educación?

Tabla 9

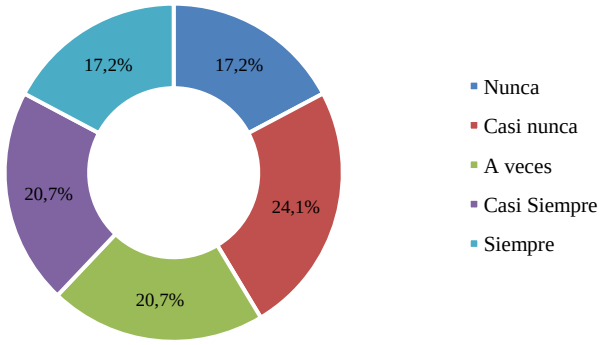
Registro de usuarios que manipulan equipos en Dirección Distrital 05D01

Categoría	Frecuencia	Porcentaje
Nunca	5	17,2%
Casi nunca	7	24,1%
A veces	6	20,7%
Casi Siempre	6	20,7%
Siempre	5	17,2%
Total	29	100%

Nota. Elaboración propia a partir de los datos de la encuesta

Figura 19

Registro de usuarios que manipulan equipos en Dirección Distrital 05D01



Nota. Elaboración propia a partir de los datos de la encuesta

Interpretación:

Con el 17,2% los encuestados respondieron que Nunca se registra la identificación de los usuarios que manipulan los equipos, mientras que otro 24,1% indicó que esto se hace Casi nunca. Un 20,7% manifestó que se registra A veces, y el mismo porcentaje del 20,7% respondió que se registra Casi siempre. Otro 17,2% de los encuestados afirmó que se registra la identificación de los usuarios Siempre. Además, un porcentaje pequeño indicó que esta práctica ocurre Siempre, un porcentaje igualmente pequeño (17,2%) indicó que esta práctica nunca se lleva a cabo. La implementación de políticas claras y la sensibilización del personal sobre la importancia de registrar la identificación de los usuarios podrían contribuir a una mayor seguridad. Una mayor consistencia en esta actividad puede contribuir a una mayor responsabilidad y control en el acceso y uso de los equipos, reduciendo los riesgos de acciones no autorizadas o no rastreables.

Pregunta 9. ¿Cuenta con áreas seguras específicas para los equipos informáticos?

Tabla 10

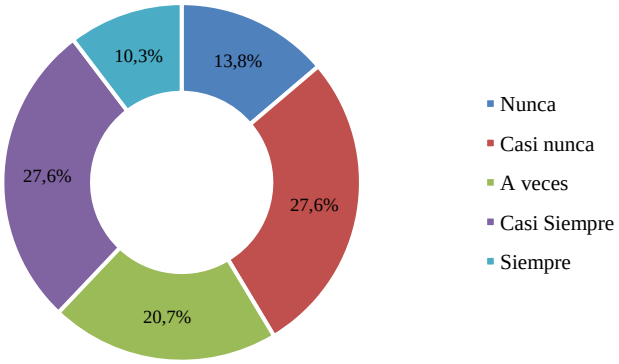
Áreas seguras específicas para equipos informáticos

Categoría	Frecuencia	Porcentaje
Nunca	4	13,8%
Casi nunca	8	27,6%
A veces	6	20,7%
Casi Siempre	8	27,6%
Siempre	3	10,3%
Total	29	100%

Nota. Elaboración propia a partir de los datos de la encuesta

Figura 20

Áreas seguras específicas para equipos informáticos



Nota. Elaboración propia a partir de los datos de la encuesta

Interpretación:

Los resultados de la encuesta en relación a la disponibilidad de áreas seguras específicas para los equipos informáticos denotan que el 13,8% respondió que Nunca se cuentan con áreas seguras específicas para los equipos informáticos, mientras que otro 27,6% indicó que esto se hace Casi nunca. Un 20,7% manifestó que se cuentan con estas áreas A veces, y el mismo porcentaje del 20,7% respondió que se cuentan con áreas seguras Casi siempre. Un 10,3% de los encuestados afirmó que siempre se cuentan con áreas seguras específicas. Los resultados de la encuesta resaltan el requerimiento de ir mejorando la consistencia en la disponibilidad de áreas seguras específicas para los equipos informáticos.

Pregunta 10. ¿Realizan mantenimientos periódicos de los equipos informáticos?

Tabla 11

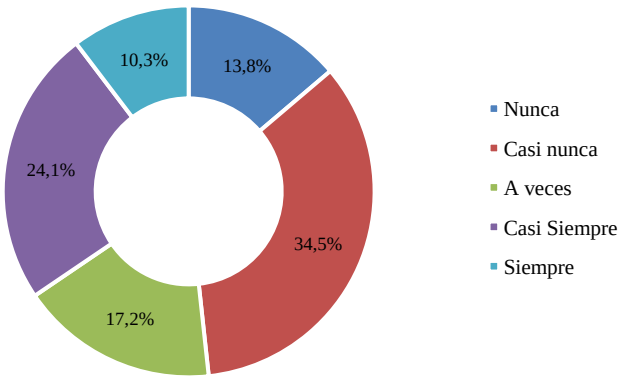
Mantenimientos periódicos de equipos informáticos

Categoría	Frecuencia	Porcentaje
Nunca	4	13,8%
Casi nunca	10	34,5%
A veces	5	17,2%
Casi Siempre	7	24,1%
Siempre	3	10,3%
Total	29	100%

Nota. Elaboración propia a partir de los datos de la encuesta

Figura 21

Mantenimientos periódicos de equipos informáticos



Nota. Elaboración propia a partir de los datos de la encuesta

Interpretación:

El resultado de la encuesta permitió observar que el 13,8% de los encuestados respondió que Nunca se realizan mantenimientos periódicos en los equipos informáticos, por otro lado, el 34,5% indicó que esto se hace "Casi nunca". Un 17,2% manifestó que se realizan mantenimientos A veces, y el mismo porcentaje del 17,2% respondió que se realizan mantenimientos Casi siempre. Un 10,3% de los encuestados afirmó que siempre se realizan mantenimientos periódicos. La falta de realización constante de mantenimientos podría tener implicaciones en el funcionamiento y la durabilidad de los equipos informáticos. La ejecución de un programa de mantenimiento regular y la sensibilización del personal sobre la importancia de los mantenimientos pueden contribuir a una mayor protección de los activos tecnológicos y la prevención de fallas.

Dimensión C: Respaldo y continuidad del negocio

Pregunta 11. ¿Existe un responsable del área de informática en las Unidades Administrativas de la Dirección Distrital 05D01 Latacunga – Educación?

Tabla 12

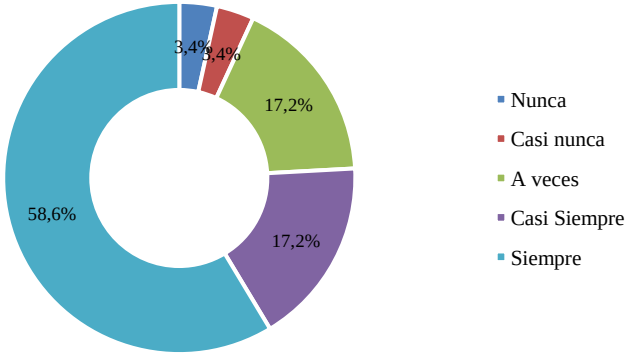
Responsable de informática en Unidades Administrativas de la Dirección Distrital

Categoría	Frecuencia	Porcentaje
Nunca	1	3,4%
Casi nunca	1	3,4%
A veces	5	17,2%
Casi Siempre	5	17,2%
Siempre	17	58,6%
Total	29	100%

Nota. Elaboración propia a partir de los datos de la encuesta

Figura 22

Responsable de informática en Unidades Administrativas de la Dirección Distrital



Nota. Elaboración propia a partir de los datos de la encuesta

Interpretación:

Los resultados indican que del total de encuestados que respondieron a esta pregunta, el 58.6% afirmó que Siempre se tiene un responsable encargado del área de informática en las Unidades Administrativas. Además, el 17.2% respondió Casi Siempre y otro 17.2% respondió A veces. Las respuestas de menor frecuencia son Nunca y Casi nunca, cada una con un 3.4%. Esto sugiere que la mayoría de las Unidades Administrativas tienen asignado un individuo para manejar asuntos relacionados con la informática. En general, aunque el resultado es mayoritariamente positivo, es fundamental que la Dirección Distrital continúe evaluando y fortaleciendo las estrategias para garantizar la presencia y la eficacia de un responsable del área de informática en todas las Unidades Administrativas, lo que contribuirá a una mejor gestión de la tecnología de la información y a conservar la continuidad de las operaciones.

Pregunta 12. ¿Se realizan copias de seguridad informática periódicas?

Tabla 13

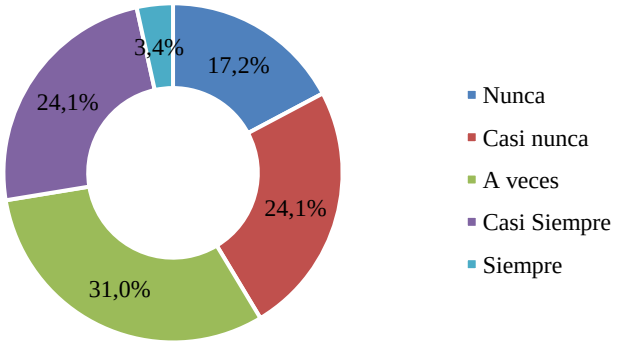
Copias de seguridad informática periódicas

Categoría	Frecuencia	Porcentaje
Nunca	5	17,2%
Casi nunca	7	24,1%
A veces	9	31,0%
Casi Siempre	7	24,1%
Siempre	1	3,4%
Total	29	100%

Nota. Elaboración propia a partir de los datos de la encuesta

Figura 23

Copias de seguridad informática periódicas



Nota. Elaboración propia a partir de los datos de la encuesta

Interpretación:

Los resultados revelan que el 17.2% indicó que las copias de seguridad Nunca se realizan. Un porcentaje ligeramente mayor, el 24.1%, respondió Casi nunca y otro 24.1% respondió Casi Siempre. Las respuestas que indican que las copias de seguridad se realizan A veces constituyeron el 31.0%, y solo un 3.4% afirmó que se realizan Siempre. Los resultados sugieren que las prácticas de realizar copias de seguridad informática periódicas no son muy consistentes en la Dirección Distrital 05D01 Latacunga – Educación lo cual evidencia que existe una situación que puede ser considerada preocupante. Para abordar esta situación, sería necesario tomar medidas para promover la importancia de las copias de seguridad informática periódicas. Esto podría incluir campañas de concienciación, capacitaciones y la implementación de procedimientos claros y automatizados para garantizar que las copias de seguridad se realicen de manera regular. Esto no solo resguardaría los datos y sistemas de la organización, sino que también contribuiría a la permanencia del negocio en caso de fallas o incidentes tecnológicos.

Pregunta 13. ¿Se dispone de un servidor para el resguardo de la información?

Tabla 14

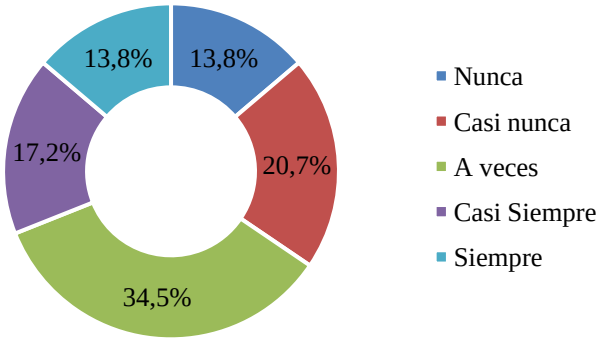
Resguardo de información en servidor.

Categoría	Frecuencia	Porcentaje
Nunca	4	13,8%
Casi nunca	6	20,7%
A veces	10	34,5%
Casi Siempre	5	17,2%
Siempre	4	13,8%
Total	29	100%

Nota. Elaboración propia a partir de los datos de la encuesta

Figura 24

Resguardo de información en servidor.



Nota. Elaboración propia a partir de los datos de la encuesta

Interpretación:

Un 34.5% de los participantes que respondieron que se dispone de un servidor para el resguardo de la información A veces. Un 20.7% respondió Casi nunca, mientras que un porcentaje similar (17.2%) indicó que esto ocurre Casi Siempre. El 13.8% de las respuestas corresponden a tanto Nunca como Siempre, mientras que otro 13.8% responde Siempre. En términos generales, los resultados indican que la disponibilidad de un servidor para el resguardo de la información no es consistente en la Dirección Distrital 05D01 Latacunga – Educación. Esto podría indicar que la infraestructura o los recursos necesarios para un servidor dedicado no están completamente establecidos en todas las áreas. Para mejorar esta situación, sería importante considerar una evaluación exhaustiva de los requerimientos en el almacenamiento y respaldo de datos en toda la Dirección Distrital. Esto podría llevar a la implementación de soluciones de servidores de respaldo eficientes y a la promoción de otras prácticas para garantizar la disponibilidad y seguridad de la información en todas las áreas.

Pregunta 14. ¿Cuenta con sistemas de alimentación eléctrica ininterrumpida (UPS) instalados en los equipos informáticos?

Tabla 15

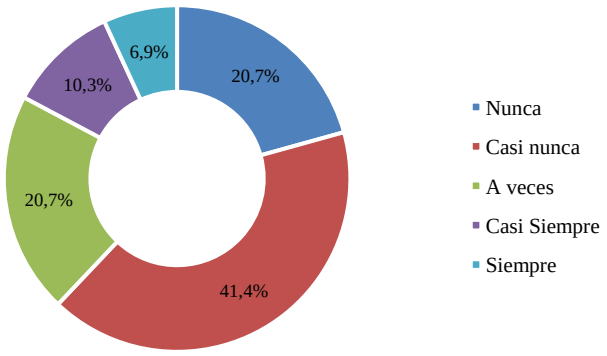
Sistemas de alimentación eléctrica ininterrumpida (UPS) en equipos

Categoría	Frecuencia	Porcentaje
Nunca	6	20,7%
Casi nunca	12	41,4%
A veces	6	20,7%
Casi Siempre	3	10,3%
Siempre	2	6,9%
Total	29	100%

Nota. Elaboración propia a partir de los datos de la encuesta

Figura 25

Sistemas de alimentación eléctrica ininterrumpida (UPS) en equipos



Nota. Elaboración propia a partir de los datos de la encuesta

Interpretación:

Con el 41.4% de las respuestas, los encuestados indicaron que los sistemas de alimentación eléctrica ininterrumpida (UPS) están instalados Casi nunca. Un 20.7% respondió Nunca, mientras que otro 20.7% respondió A veces. El 10.3% de las respuestas corresponden a Casi Siempre y el 6.9% a Siempre. Estos hallazgos sugieren que la presencia de sistemas de alimentación eléctrica ininterrumpida (UPS) en los equipos informáticos no es una práctica común en la Dirección Distrital por lo cual sería importante brindar capacitación a los empleados sobre la importancia de estos sistemas y cómo utilizarlos adecuadamente para asegurar la permanencia de las operaciones y la protección de la información. Para mejorar esta situación, la Dirección Distrital podría considerar la implementación de políticas y directrices que promuevan la instalación de sistemas de alimentación eléctrica ininterrumpida (UPS) en todos los equipos informáticos.

Pregunta 15. ¿Se ha establecido un plan de continuidad del negocio en caso de interrupciones del sistema?

Tabla 16

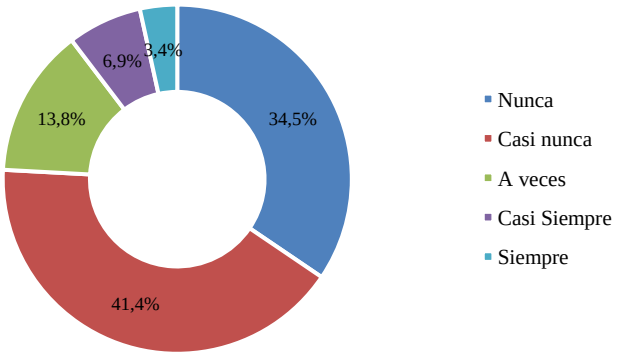
Plan de continuidad del negocio ante interrupciones

Categoría	Frecuencia	Porcentaje
Nunca	10	34,5%
Casi nunca	12	41,4%
A veces	4	13,8%
Casi Siempre	2	6,9%
Siempre	1	3,4%
Total	29	100%

Nota. Elaboración propia a partir de los datos de la encuesta

Figura 26

Plan de continuidad del negocio ante interrupciones



Nota. Elaboración propia a partir de los datos de la encuesta

Interpretación:

Los resultados muestran que un 41.4% indicó que un plan de continuidad del negocio nunca se ha establecido. Un 34.5% respondió "Casi nunca", mientras que el 13.8% de las respuestas corresponden A veces. Las respuestas que indican que se ha establecido un plan Casi Siempre y Siempre constituyen el 10.3% y el 3.4% respectivamente. El resultado indica que la existencia de un plan de continuidad del negocio en caso de interrupciones del sistema no está muy arraigada en la Dirección Distrital.Para mejorar esta situación, la Dirección Distrital podría considerar la importancia de desarrollar y promover la ejecución de planes de continuidad del negocio. Esto podría incluir la capacitación de los empleados, la asignación de recursos y la creación de procesos para garantizar que la organización esté preparada para enfrentar interrupciones en los sistemas y mantener la continuidad de las operaciones críticas.

Dimensión D: Gestión de accesos

Pregunta 16. ¿Se han realizado simulacros frente a la caída de los sistemas de información y de comunicación en las Unidades Administrativas de la Dirección Distrital 05D01 Latacunga – Educación?

Tabla 17

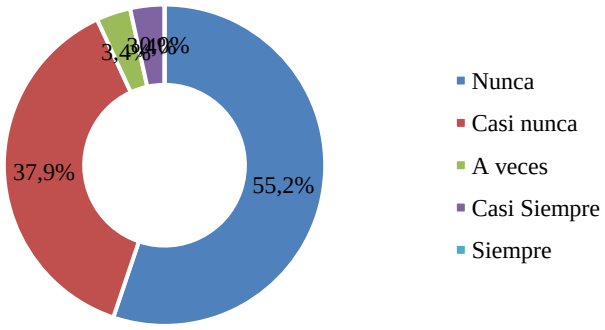
Simulacros ante caída de sistemas en Unidades Administrativas

Categoría	Frecuencia	Porcentaje
Nunca	16	55,2%
Casi nunca	11	37,9%
A veces	1	3,4%
Casi Siempre	1	3,4%
Siempre	0	0,0%
Total	29	100%

Nota. Elaboración propia a partir de los datos de la encuesta

Figura 27

Simulacros ante caída de sistemas en Unidades Administrativas



Nota. Elaboración propia a partir de los datos de la encuesta

Interpretación:

En base a los resultados el 55.2% de los encuestados respondió que nunca se han realizado simulacros frente a la caída de los sistemas de información y de comunicación. Además, un 37.9% respondió “Casi nunca”, mientras que el 3.4% de las respuestas corresponden a “A veces”. Las respuestas que indican que se han realizado simulacros “Casi Siempre” y “Siempre” constituyen el 3.4% y el 0.0% respectivamente. Estos resultados sugieren que la realización de simulacros frente a la caída de los sistemas de información y de comunicación. Para mejorar esta situación, la Dirección Distrital podría considerar la importancia de

desarrollar y promover la realización de simulacros para garantizar que la organización esté preparada para enfrentar interrupciones en los sistemas y mantener la continuidad de las operaciones críticas.

Pregunta 17. ¿Manejan personalmente las claves por cada usuario en las Unidades Administrativas?

Tabla 18

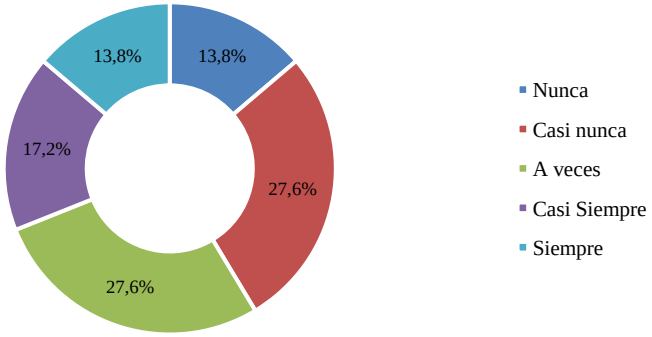
Uso personal de claves en Unidades Administrativas

Categoría	Frecuencia	Porcentaje
Nunca	4	13,8%
Casi nunca	8	27,6%
A veces	8	27,6%
Casi Siempre	5	17,2%
Siempre	4	13,8%
Total	29	100%

Nota. Elaboración propia a partir de los datos de la encuesta

Figura 28

Uso personal de claves en Unidades Administrativas



Nota. Elaboración propia a partir de los datos de la encuesta

Interpretación:

Conforme al resultado de los encuestados el 41.4% respondió que nunca o casi nunca manejan personalmente las claves por cada usuario en las Unidades Administrativas. Además, el 27.6% de las respuestas corresponden a “A veces” y “Casi siempre” respectivamente. Las respuestas que indican que se manejan personalmente las claves “Siempre” y “Nunca” constituyen el 13.8% respectivamente. En general, estos resultados sugieren que el manejo personal de las claves por cada usuario en las Unidades Administrativas no es una práctica común. La alta proporción de respuestas en las categorías “Nunca” y “Casi nunca” sugiere que el manejo personal de las claves no ha sido una prioridad en la organización. Para mejorar esta situación,

la Dirección Distrital podría considerar la importancia de desarrollar y promover el manejo personal de las claves por cada usuario en las Unidades Administrativas. Esto podría incluir la capacitación de los empleados, la asignación de recursos y la creación de procesos para garantizar que la organización esté preparada para enfrentar interrupciones en los sistemas y mantener la continuidad de las operaciones críticas.

Pregunta 18. ¿Aplican políticas de grupo para el acceso a la información en las Unidades Administrativas?

Tabla 19

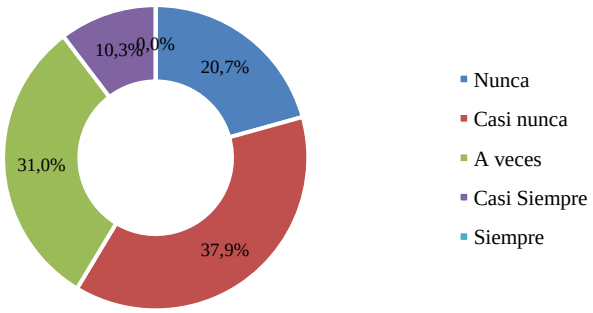
Políticas de grupo para acceso a información en Unidades Administrativas

Categoría	Frecuencia	Porcentaje
Nunca	6	20,7%
Casi nunca	11	37,9%
A veces	9	31,0%
Casi Siempre	3	10,3%
Siempre	0	0,0%
Total	29	100%

Nota. Elaboración propia a partir de los datos de la encuesta

Figura 29

Políticas de grupo para acceso a información en Unidades Administrativas



Nota. Elaboración propia a partir de los datos de la encuesta

Interpretación:

Los resultados nos indican que el 58.6% de los encuestados replico que las políticas de grupo para el ingreso a la información en las Unidades Administrativas se aplican “Nunca” o “Casi nunca”. Además, el 31.0% de las respuestas corresponden a “A veces”. Las respuestas que indican que se aplican políticas de grupo “Casi Siempre” y “Siempre” constituyen el 10.3% y

el 0.0% respectivamente. En general, estos resultados sugieren que la aplicación de políticas de grupo para el acceso a la información en las Unidades Administrativas no es una práctica común. La alta proporción de respuestas en las categorías “Nunca” y “Casi nunca” sugiere que la aplicación de políticas de grupo no ha sido una prioridad en la organización.

Para mejorar esta situación, la Dirección Distrital podría considerar la importancia de desarrollar y promover la aplicación de políticas de grupo para el acceso a la información en las Unidades Administrativas. Esto podría incluir la capacitación del personal, la asignación de recursos y la creación de procesos para garantizar que la organización esté preparada para enfrentar interrupciones en los sistemas y mantener la continuidad de las operaciones críticas.

Pregunta 19. ¿Cuenta con un procedimiento de identificación y autenticación de las personas que manipulan los equipos de cómputo?

Tabla 20

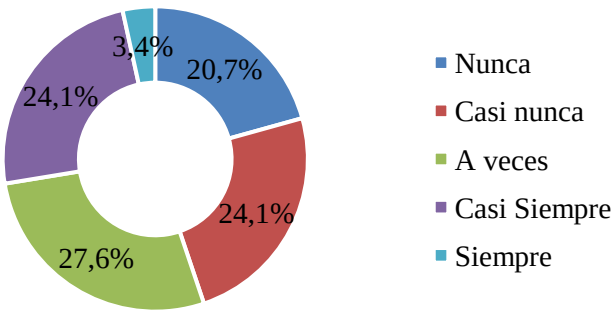
Procedimiento de identificación y autenticación en equipos

Categoría	Frecuencia	Porcentaje
Nunca	6	20,7%
Casi nunca	7	24,1%
A veces	8	27,6%
Casi Siempre	7	24,1%
Siempre	1	3,4%
Total	29	100%

Nota. Elaboración propia a partir de los datos de la encuesta

Figura 30

Procedimiento de identificación y autenticación en equipos



Nota. Elaboración propia a partir de los datos de la encuesta

Interpretación:

En la Tabla 20, nos indica que el 20.7% de los encuestados indicó que nunca cuentan con un procedimiento de identificación y autenticación de las personas que manipulan los equipos de cómputo. Además, el 24.1% de las respuestas corresponden a “Casi nunca” y “Casi siempre” respectivamente. Las respuestas que indican que se cuenta con un procedimiento “A veces” constituyen el 27.6%. Las respuestas que indican que se cuenta con un procedimiento “Siempre” y “Nunca” constituyen el 3.4% y el 24.1% respectivamente. En general, estos resultados sugieren que la existencia de un procedimiento de identificación y autenticación de las personas que manipulan los equipos de cómputo no es una práctica común. La alta proporción de respuestas en las categorías “Nunca” y “Casi nunca” sugiere que la implementación de un procedimiento de identificación y autenticación no ha sido una prioridad en la organización.

Para mejorar esta situación, la Dirección Distrital podría considerar la importancia de desarrollar y promover la implementación de un procedimiento de identificación y autenticación de las personas que manipulan los equipos de cómputo. Esto podría incluir la capacitación del personal, la asignación de recursos y la creación de procesos para garantizar que la organización esté preparada para enfrentar interrupciones en los sistemas y conseevar la permanencia de las operaciones críticas.

Pregunta 20. ¿Se revisan y actualizan periódicamente los privilegios de acceso al sistema?

Tabla 21

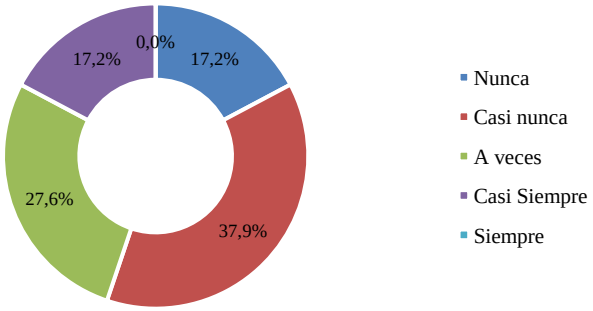
Revisión y actualización de privilegios de acceso

Categoría	Frecuencia	Porcentaje
Nunca	5	17,2%
Casi nunca	11	37,9%
A veces	8	27,6%
Casi Siempre	5	17,2%
Siempre	0	0,0%
Total	29	100%

Nota. Elaboración propia a partir de los datos de la encuesta

Figura 31

Revisión y actualización de privilegios de acceso



Nota. Elaboración propia a partir de los datos de la encuesta

Interpretación:

En la Tabla 21, nos indica que el 17.2% de los encuestados indicó que los privilegios de acceso al sistema nunca se revisan y actualizan periódicamente. Además, el 37.9% de las respuestas corresponden a "Casi nunca". Las respuestas que indican que los privilegios de acceso al sistema se revisan y actualizan "A veces" y "Casi siempre" constituyen el 27.6% y el 17.2% respectivamente. Al no existir revisión y actualización periódica de los privilegios de acceso al sistema puede aumentar el riesgo de ingreso no autorizado a la información y los sistemas. Para mejorar esta situación, la Dirección Distrital podría considerar la importancia de desarrollar y promover la revisión y actualización periódica de los privilegios de acceso al sistema. Esto podría incluir la capacitación de los empleados, la asignación de recursos y la creación de procesos para garantizar que la organización esté preparada para enfrentar interrupciones en los sistemas y mantener la continuidad de las operaciones críticas.

Dimensión E: Gestión de riesgos

Pregunta 21. ¿Se realizan evaluaciones periódicas de riesgos de seguridad informática en las Unidades Administrativas de la Dirección Distrital 05D01 Latacunga – Educación?

Tabla 22

Evaluaciones periódicas de riesgos en seguridad informática

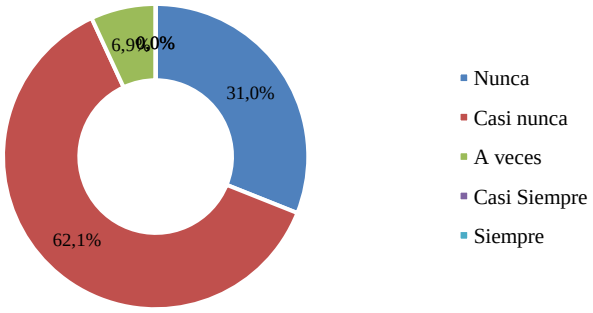
Categoría	Frecuencia	Porcentaje
Nunca	9	31,0%
Casi nunca	18	62,1%
A veces	2	6,9%
Casi Siempre	0	0,0%

Categoría	Frecuencia	Porcentaje
Siempre	0	0,0%
Total	29	100%

Nota. Elaboración propia a partir de los datos de la encuesta

Figura 32

Evaluaciones periódicas de riesgos en seguridad informática



Nota. Elaboración propia a partir de los datos de la encuesta

Interpretación:

En la Tabla 22, se muestra que el 31.0% de los encuestados indicó que nunca se realizan evaluaciones periódicas de riesgos de seguridad informática en las Unidades Administrativas de la Dirección Distrital 05D01 Latacunga – Educación. Además, el 62.1% de las respuestas corresponden a "Casi nunca". Las respuestas que indican que se realizan evaluaciones periódicas de riesgos "A veces" constituyen el 6.9%. En general, estos resultados sugieren que la realización de evaluaciones periódicas de riesgos de seguridad informática no es una práctica común en la Dirección Distrital. La alta proporción de respuestas en la categoría "Casi nunca" sugiere que la realización de evaluaciones periódicas de riesgos no ha sido una prioridad en la organización.

Por lo tanto, se debe considerar la importancia de desarrollar y promover la realización de evaluaciones periódicas de riesgos de seguridad informática. Esto podría incluir la capacitación del personal, la asignación de recursos y la creación de procesos para garantizar que la organización esté preparada para enfrentar interrupciones en los sistemas y conservar la continuidad de las operaciones críticas.

Pregunta 22. ¿Se asignan recursos para mitigar los riesgos identificados?

Tabla 23

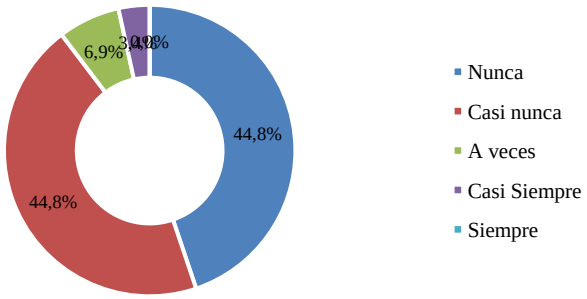
Evaluaciones periódicas de riesgos en seguridad informática

Categoría	Frecuencia	Porcentaje
Nunca	13	44,8%
Casi nunca	13	44,8%
A veces	2	6,9%
Casi Siempre	1	3,4%
Siempre	0	0,0%
Total	29	100%

Nota. Elaboración propia a partir de los datos de la encuesta

Figura 33

Evaluaciones periódicas de riesgos en seguridad informática



Nota. Elaboración propia a partir de los datos de la encuesta

Interpretación:

En la Tabla 23, se puede observar que el 44.8% de los encuestados indicó que nunca o casi nunca se asignan recursos para mitigar los riesgos identificados. Además, el 6.9% de las respuestas corresponden a "A veces". Las respuestas que indican que se asignan recursos "Casi Siempre" y "Siempre" constituyen el 3.4% y el 0.0% respectivamente. En general, estos resultados sugieren que la asignación de recursos para mitigar los riesgos identificados no es una práctica común en la Dirección Distrital. La alta proporción de respuestas en las categorías "Nunca" y "Casi nunca" sugiere que la asignación de recursos para mitigar los riesgos identificados no ha sido una prioridad en la organización. Es así, que se debe considerar la importancia de desarrollar y promover la asignación de recursos para mitigar los riesgos identificados. Esto podría contemplar la capacitación de los empleados, la creación de procesos y la asignación de presupuesto para garantizar que la organización esté preparada para enfrentar

interrupciones en los sistemas y mantener la continuidad de las operaciones críticas.

Pregunta 23. ¿Realizan auditorías internas de seguridad informática para evaluar la eficacia de los controles?

Tabla 24

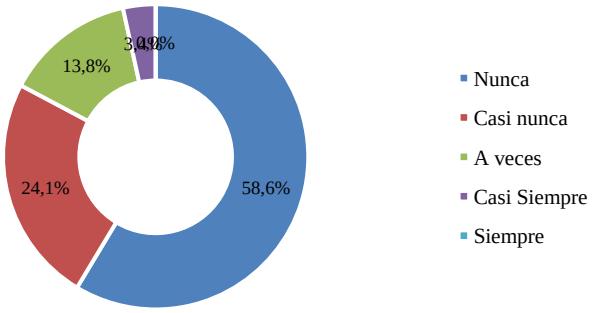
Auditorías internas de seguridad informática

Categoría	Frecuencia	Porcentaje
Nunca	17	58,6%
Casi nunca	7	24,1%
A veces	4	13,8%
Casi Siempre	1	3,4%
Siempre	0	0,0%
Total	29	100%

Nota. Elaboración propia a partir de los datos de la encuesta

Figura 34

Auditorías internas de seguridad informática



Nota. Elaboración propia a partir de los datos de la encuesta

Interpretación:

En la Tabla 24, se observa que el 58.6% de los encuestados indicó que nunca se realizan auditorías internas de seguridad informática para examinar la eficacia de los controles. Además, el 24.1% de las respuestas corresponden a “Casi nunca”. Las respuestas que indican que se realizan auditorías internas “A veces” y “Casi siempre” constituyen el 13.8% y el 3.4% respectivamente.

La falta de auditorías internas de seguridad informática puede aumentar el riesgo de ingreso no autorizado a la información y los sistemas. Para mejorar esta situación, la Dirección Distrital podría considerar la importancia de desarrollar y promover la ejecución de auditorías internas

de seguridad informática para examinar la eficacia de los controles. Esto podría incluir la capacitación del personal, la creación de procesos y la asignación de presupuesto para garantizar que la organización esté preparada para enfrentar interrupciones en los sistemas y mantener la continuidad de las operaciones críticas.

Pregunta 24. ¿Documentan adecuadamente los incidentes de seguridad informática y las acciones tomadas para resolverlos?

Tabla 25

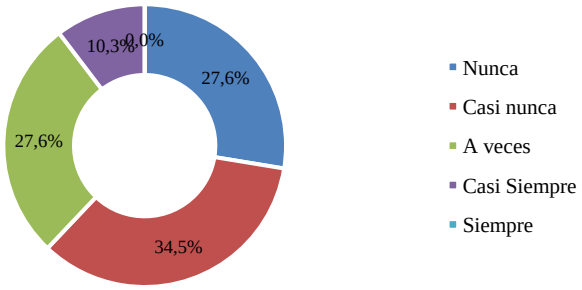
Documentación de incidentes y acciones de seguridad

Categoría	Frecuencia	Porcentaje
Nunca	8	27,6%
Casi nunca	10	34,5%
A veces	8	27,6%
Casi Siempre	3	10,3%
Siempre	0	0,0%
Total	29	100%

Nota. Elaboración propia a partir de los datos de la encuesta

Figura 35

Documentación de incidentes y acciones de seguridad



Nota. Elaboración propia a partir de los datos de la encuesta

Interpretación:

Los datos muestras que el 27.6% de los encuestados indicó que nunca se documentan adecuadamente los incidentes de seguridad informática y las acciones tomadas para resolverlos. Además, el 34.5% de las respuestas corresponden a “Casi nunca”. Las respuestas que indican que se documentan adecuadamente los incidentes “A veces” y “Casi siempre” constituyen el 27.6% y el 10.3% respectivamente.

La falta de documentación adecuada de los incidentes de seguridad informática y las acciones tomadas para resolverlos puede aumentar el riesgo de ingreso no autorizado a la información y los sistemas. Para mejorar esta situación, la Dirección Distrital podría considerar la importancia de desarrollar y promover la documentación adecuada de los incidentes de seguridad informática y las medidas que se toman para resolverlos. Esto podría incluir la capacitación del personal, la creación de procesos y la asignación de presupuesto para garantizar que la organización esté preparada para enfrentar interrupciones en los sistemas y conservar la continuidad de las operaciones críticas.

Pregunta 25. ¿Se evalúan y actualizan regularmente los planes de seguridad en función de los cambios en las amenazas y tecnologías?

Tabla 26

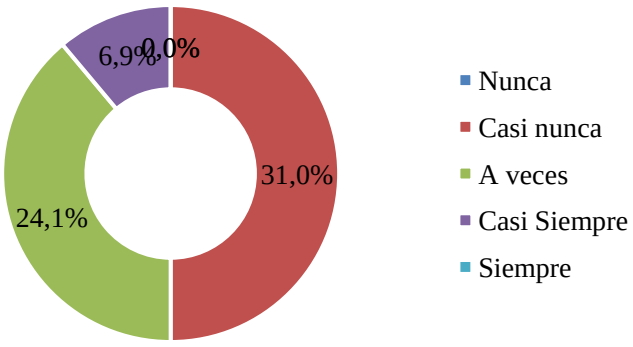
Evaluación y actualización de planes de seguridad regulares

Categoría	Frecuencia	Porcentaje
Nunca	11	37,9%
Casi nunca	9	31,0%
A veces	7	24,1%
Casi Siempre	2	6,9%
Siempre	0	0,0%
Total	29	100%

Nota. Elaboración propia a partir de los datos de la encuesta

Figura 36

Evaluación y actualización de planes de seguridad regulares



Nota. Elaboración propia a partir de los datos de la encuesta

Interpretación:

La información muestra que el 37.9% de los encuestados indicó que nunca se evalúan y actualizan regularmente los planes de seguridad en función de los cambios en las amenazas y tecnologías. Además, el 31.0% de las respuestas corresponden a “Casi nunca”. Las respuestas que indican que se evalúan y actualizan regularmente los planes “A veces” y “Casi siempre” constituyen el 24.1% y el 6.9% respectivamente.

La falta de evaluación y actualización regular de los planes de seguridad en función de los cambios en las amenazas y tecnologías puede aumentar el riesgo de acceso no autorizado a la información y los sistemas. Para mejorar esta situación, la Dirección Distrital podría considerar la importancia de desarrollar y promover la evaluación y actualización regular de los planes de seguridad en función de los cambios en las amenazas y tecnologías. Dentro de esto estará inclyuido la capacitación del personal, la creación de procesos y la asignación de presupuesto para garantizar que la organización esté preparada para enfrentar interrupciones en los sistemas y mantener la continuidad de las operaciones críticas.

CAPÍTULO V: PRESENTACIÓN DE LA PROPUESTA

Análisis de vulnerabilidades de la seguridad informática utilizando ISO 27001 caso de estudios unidades administrativas de la dirección Distrital 05D01 Latacunga – Educación

Con el propósito de instaurar un protocolo conforme a políticas de seguridad en línea con estándares internacionales, sustentado en el mantenimiento y mejora constante de un Sistema de Gestión de la Seguridad de la Información, se busca resguardar la confidencialidad, integridad y disponibilidad de la información. Este enfoque brinda un marco para la seguridad de la información que asiste a la Dirección Distrital 05D01 Latacunga – Educación en la identificación y gestión efectiva de sus riesgos de seguridad de la información, a través de la aplicación de la norma ISO 27001.

La evaluación detallada de las respuestas revela diversos desafíos en la puesta en marcha de medidas de seguridad informática en la Dirección Distrital 05D01 Latacunga – Educación. En primer lugar, se destaca la disponibilidad intermedia de políticas de seguridad informática, evidenciando una inconsistencia en su aplicación que podría implicar riesgos para la integridad de los sistemas y la protección de la información. Para abordar este desafío, se recomienda fortalecer los esfuerzos de capacitación y comunicación, mejorando así el conocimiento y la comprensión del personal respecto a estas políticas.

Asimismo, se identifica un notable desconocimiento y falta de comprensión de las políticas de seguridad informática entre más de la mitad de los encuestados en las Unidades Administrativas. Este hallazgo subraya la relevancia de mejorar la comunicación y la capacitación, con el objetivo de aumentar la conciencia y garantizar prácticas más seguras en el manejo de la información. La escasez de conocimiento sobre las políticas podría conducir a prácticas inseguras o incorrectas, destacando la necesidad de una intervención efectiva.

Además, se evidencia una carencia de consistencia en la actualización y revisión de las políticas de seguridad informática, ya que casi la mitad de los encuestados no realiza estas actividades de manera constante. Este aspecto plantea la posibilidad de lagunas de seguridad y vulnerabilidades no identificadas, subrayando la necesidad de mejorar continuamente los procesos y la cultura organizacional en torno a la seguridad informática. Estrategias más efectivas podrían ser necesarias para promover y establecer prácticas regulares de actualización y revisión de políticas, asegurando así una protección más robusta de los sistemas y la información.

5.1. Identificación de riesgos que pueden afectar a los activos de la información de las unidades administrativas de la dirección Distrital 05D01 Latacunga – Educación"

La evaluación detallada de la seguridad informática en las unidades administrativas de la Dirección Distrital 05D01 Latacunga – Educación ha revelado varios desafíos que podrían resultar en riesgos significativos para los activos de información. Estos desafíos incluyen inconsistencias en la aplicación de políticas, falta de conocimiento y comprensión de políticas de seguridad, variabilidad en la práctica de resguardo seguro de equipos, entre otros.

A continuación, se presenta una tabla que resume los riesgos identificados y su nivel de impacto potencial:

Tabla 27
Identificación de riesgos

N	Área Crítica	Tipo de Riesgo	Riesgo Identificado	Impacto Potencial
1	Disponibilidad Intermedia de Políticas	Conciencia	Inconsistencia en la aplicación de políticas de seguridad	Pérdida de integridad y disponibilidad.
2	Conocimiento y Comprensión de Políticas	Integridad	Falta de conocimiento sobre políticas de seguridad.	Riesgos de seguridad por prácticas erróneas.
3	Actualización y Revisión de Políticas	Consistencia	Falta de actualizaciones periódicas en políticas.	Posibles lagunas de seguridad.
4	Comunicación y Difusión de Políticas	Consistencia	Falta de comunicación efectiva sobre políticas de seguridad.	Desconocimiento de pautas de seguridad.
5	Capacitación del Personal	Integridad	Baja frecuencia de capacitación en seguridad informática.	Vulnerabilidad ante amenazas.
6	Resguardo Seguro de Equipos Informáticos	Integridad	Variabilidad en prácticas de resguardo seguro de equipos.	Riesgo de pérdida o daño a los equipos.
7	Control de Acceso a Áreas con Equipos	Disponibilidad	Falta de consistencia en el control de acceso a áreas.	Posible acceso no autorizado.
8	Registro de Identificación de Usuarios	Consistencia	Baja frecuencia en el registro de identificación de usuarios.	Riesgo de acceso no rastreable.
9	Disponibilidad de Áreas Seguras para Equipos	Disponibilidad	Inconsistencia en la disponibilidad de áreas seguras.	Riesgo de pérdida o daño a los equipos.
10	Mantenimientos Periódicos en Equipos	Disponibilidad	Falta de realización constante de mantenimientos periódicos.	Posible deterioro y fallos en equipos.

Nota. Elaboración propia

Esta evaluación destaca la necesidad de implementar medidas correctivas y preventivas para mitigar estos riesgos y fortalecer la seguridad de la información en las unidades administrativas.

5.2. Desarrollo de las políticas de seguridad de la información para la Dirección Distrital 05D01 Latacunga – Educación mediante normas ISO 27001

En el contexto presente, caracterizado por un aumento en la dependencia de la tecnología y un panorama de amenazas en constante evolución, la Dirección Distrital 05D01 Latacunga – Educación se enfrenta al desafío imperativo de proteger su información crítica. La adopción de las políticas de seguridad de la información, guiadas por las normativas de la ISO 27001, representa un paso fundamental hacia la salvaguarda de la integridad, confidencialidad y disponibilidad de los datos

---

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA DIRECCIÓN DISTRITAL 05D01 LATACUNGA – EDUCACIÓN MEDIANTE NORMAS ISO 27001

Alcance

Abarcar todos los aspectos críticos de la gestión de datos dentro de la Dirección Distrital 05D01 Latacunga – Educación. Esto incluye, pero no se limita a, la infraestructura tecnológica, los sistemas de información, el personal docente y administrativo, los estudiantes, así como los procesos operativos y de gestión. Las políticas están diseñadas para ser aplicables en todas las unidades administrativas, abarcando diversos tipos de datos, incluyendo datos personales, financieros, académicos y de investigación.

Marco Normativo

Las políticas se fundamentan en un marco normativo robusto, que incluye la norma ISO 27001 como pilar central. Además, se consideran las leyes locales y nacionales sobre resguardo de datos y privacidad, así como las regulaciones específicas del sector educativo. Este marco normativo proporciona las bases para un enfoque sistemático y coherente hacia la gestión de la seguridad de la información, asegurando el cumplimiento de estándares internacionales y regulaciones locales.

Cumplimiento de Regulaciones Sectoriales

Considerando que la Dirección Distrital opera en el sector educativo, las políticas también se

---

alinean con cualquier regulación o directriz específica del sector que afecte la gestión de la información y la seguridad de los datos.

Principios de Privacidad y Protección de Datos

Las políticas se adhieren a los principios fundamentales de la privacidad y protección de datos, asegurando que la información personal y sensible se maneje de manera confidencial y segura, y que su tratamiento cumpla con los derechos de ingreso, rectificación, cancelación y oposición

Desarrollo

En el panorama actual, donde la información ejecuta un papel crucial en el ámbito educativo, la Dirección Distrital 05D01 Latacunga reconoce la imperativa necesidad de adquirir Políticas de Seguridad de la Información robustas y eficaces. Estas políticas, diseñadas según los estándares internacionales de la norma ISO 27001, se erigen como el marco estratégico que guiará la salvaguarda de activos digitales y la protección de la integridad, confidencialidad y disponibilidad de la información crítica. Con un enfoque integral, estas políticas abordan aspectos fundamentales como el control de ingreso, gestión de activos, seguridad en el desarrollo de sistemas, y respuesta a incidentes, entre otros.

1. Política de acceso y control de usuarios

Asegura que el acceso a los sistemas de información esté autorizado y controlado.

-Directrices

- Los usuarios recibirán acceso basado en sus roles y responsabilidades.
- Se implementarán mecanismos de autenticación multifactor para fortalecer la seguridad de las cuentas de usuario.

2. Política de gestión de activos

Salvaguardar la información y los recursos tecnológicos de la Dirección Distrital 05D01.

-Directrices

- Se identificarán y clasificarán todos los activos de información críticos.
- Existirá un inventario actualizado de los activos, incluyendo su ubicación y propietarios.

3. Política de seguridad en desarrollo y mantenimiento de sistemas

Asegurar que la seguridad esté integrada en todas las fases del desarrollo y mantenimiento de sistemas.

-Directrices

- Se seguirán mejores prácticas de seguridad en el desarrollo de software.
- Las actualizaciones y parches de seguridad se implementarán de manera regular.

4. Política de gestión de incidentes de seguridad

Determinar un marco para responder de manera efectiva a incidentes de seguridad.

-Directrices

- Se mantendrá un plan de respuesta a incidentes que se revisará y probará regularmente.
- Se notificarán y documentarán todos los incidentes de seguridad.

5. Política de protección contra malware

Prevenir, detectar y responder a amenazas de malware.

-Directrices

- Se implementarán soluciones de seguridad actualizadas para la detección y prevención de malware.
- Se realizarán capacitaciones regulares para concienciar sobre las amenazas de malware.

6. Política de seguridad física

Proteger los recursos físicos y la infraestructura crítica.

- Directrices

- Se designarán áreas restringidas y sensibles.
- Se instalarán sistemas de seguridad física, como pueden ser cámaras de vigilancia y controles de acceso.

7. Política de respaldo y recuperación de datos

Garantizar la disponibilidad y la integridad de la información crítica.

-Directrices

- Se realizarán copias de seguridad regulares y se almacenarán en ubicaciones seguras.
- Se llevarán a cabo pruebas periódicas de recuperación para comprobar la eficacia de

los procesos.

8. Política de cumplimiento y conformidad con la legislación

Asegurar el cumplimiento de las leyes y regulaciones aplicables.

-Directrices

- Se mantendrá un registro de las leyes y regulaciones relevantes.
- Se realizarán revisiones regulares para asegurar el cumplimiento.

9. Política de concientización y formación en seguridad

Fomentar la conciencia y la comprensión de la seguridad de la información.

- Directrices

- Se llevarán a cabo programas de formación y concientización de manera regular.
- Se promoverá una cultura de seguridad informática en toda la organización.

10. Política de auditoría y monitoreo continuo

Evaluar y mejorar continuamente la efectividad de los controles de seguridad.

-Directrices

- Se implementará un sistema de monitoreo continuo para detectar y responder a eventos de seguridad.
- Se realizarán auditorías internas periódicamente con el fin de evaluar el cumplimiento y la eficacia de los controles.

Revisión de las Políticas

Las políticas serán sometidas a un proceso de revisión exhaustiva por parte de un comité compuesto por expertos en seguridad de la información y representantes legales. Este comité se encargará de verificar la precisión, relevancia y el cumplimiento normativo de las políticas propuestas.

Aprobación de la Dirección

Las políticas revisadas serán presentadas ante la alta dirección para su aprobación final. Este paso es crucial para asegurar el respaldo y compromiso organizacional con las políticas establecidas.

Comunicar las Políticas

Las políticas aprobadas serán comunicadas a todas las partes interesadas por medio de canales adecuados, tales como reuniones, correo electrónico y plataformas internas. Es fundamental asegurar que las políticas sean comprensibles y accesibles para todos los miembros de la organización.

Programas de Capacitación

Se desarrollarán e implementarán programas de capacitación destinados a educar al personal de la importancia de las políticas de seguridad de la información y su aplicación práctica. Estos programas incluirán sesiones interactivas, materiales de formación y evaluaciones periódicas.

Monitoreo y Revisión Continua

- **Monitoreo y Auditoría**: Se establecerán procesos de monitoreo y auditoría regulares para garantizar el cumplimiento continuo y evaluar la efectividad de las políticas implementadas.
- **Revisión y Actualización**: Las políticas serán revisadas y actualizadas periódicamente para representar los cambios en el entorno tecnológico, normativo y de riesgos.

Desarrollo de la Guía de Procedimientos

- **Guía de Procedimientos**: Basándose en las políticas aprobadas, se elaborará una guía detallada que describirá los procedimientos específicos para su implementación. Esta guía servirá como un documento de referencia para el manejo cotidiano de la seguridad de la información.

Retroalimentación y Mejora Continua

- **Recolección de Retroalimentación**: Se implementará un mecanismo para recoger la retroalimentación de los usuarios sobre la aplicabilidad y efectividad de las políticas y procedimientos.
- **Proceso de Mejora Continua**: La retroalimentación recogida será utilizada para

realizar ajustes y mejoras continuas en las políticas y procedimientos.

5.3. Elaboración de la guía actualizada de procedimientos para la seguridad informática enfocados a las unidades administrativas de la dirección distrital 05D01 Latacunga – educación.

La implementación de medidas de seguridad informática es crucial para mitigar las amenazas identificadas y reducir la fuga de información confidencial en las unidades administrativas de la Dirección Distrital 05D01 Latacunga – Educación. Esta guía se fundamenta en los principios de la norma ISO 27001 y proporciona procedimientos detallados para fortalecer la seguridad de la información.

Además, en el entorno digital actual, la seguridad informática se ha transformado en un elemento crucial para salvaguardar la integridad, confidencialidad y disponibilidad de la información en las unidades administrativas de la Dirección Distrital 05D01 de Latacunga en el ámbito educativo.

La creciente interconexión de sistemas y la gestión constante de datos sensibles exigen la implementación de medidas efectivas, asegurando el cumplimiento de estándares internacionales como la norma ISO 27001. Esta guía de procedimientos se presenta como una herramienta esencial para orientar a la comunidad educativa en la adopción de buenas prácticas en seguridad informática, fortaleciendo la protección de activos digitales y mejorando la resiliencia frente a amenazas cibernéticas.

La guía responde a la urgente necesidad de establecer un marco normativo y operativo para garantizar la seguridad informática en las unidades administrativas de la Dirección Distrital 05D01 en Latacunga. La información educativa, desde datos estudiantiles hasta material didáctico, representa un activo invaluable que debe gestionarse de manera segura y eficiente.

El cumplimiento de la normativa ISO 27001 ofrece un enfoque global y estructurado para abordar los riesgos de seguridad informática, fomentando la confianza tanto interna como externamente en la comunidad educativa. La guía, al alinearse con los principios de la ISO 27001, busca establecer procedimientos claros y efectivos que no solo mitiguen las amenazas actuales, sino que también preparen a las unidades administrativas para los desafíos digitales futuros, asegurando la continuidad y calidad de los servicios educativos proporcionados.

Actividades propuestas para la elaboración de la Guía

Las actividades que se propone a continuación simbolizan varios de pasos que se deben seguir, para Implementar políticas de seguridad de la información en la Dirección Distrital 05D01 Latacunga – Educación, alineadas con las Normas ISO 27001.

Tabla 28
Actividades para la implementar políticas de seguridad de la información

Categoría	Actividad	Resultados Esperados
C1	Identificar los activos de información críticos	• Lista de activos de información críticos identificados. • Evaluación de la importancia de cada activo de información crítico.
C2	Implementar controles de seguridad de la información	• Controles de seguridad de la información implementados para resguardar los activos de información críticos identificados en la actividad 1. • Cumplimiento de las políticas de seguridad de la información desarrolladas en la actividad 1.
	Realizar pruebas de seguridad de la información	• Pruebas de seguridad de la información realizadas para evaluar la efectividad de los controles de seguridad de la información implementados en la actividad 2. • Informe de resultados de las pruebas de seguridad de la información.
	Establecer un programa de capacitación en seguridad de la información.	• Programa de capacitación en seguridad de la información desarrollado y documentado. • Personal de la dirección Distrital 05D01 Latacunga - educación capacitado en seguridad de la información.
C3	Realizar auditorías internas de seguridad de la información	• Auditorías internas de seguridad de la información realizadas para evaluar el cumplimiento de las políticas de seguridad de la información y los controles de seguridad de la información implementados. • Informe de resultados de las auditorías internas de seguridad de la información.

Nota. Elaboración propia

1. Propósito

La presente guía tiene como propósito principal establecer un conjunto de procedimientos estandarizados para garantizar la seguridad de la información en las Unidades Administrativas de la Dirección Distrital 05D01 Latacunga - Educación. Este documento busca ser un recurso integral para la prevención, detección y respuesta efectiva ante cualquier amenaza que pueda comprometer la integridad, confidencialidad y disponibilidad de la información crítica manejada por la institución.

2. Alcance

El alcance de esta guía abarca todas las operaciones y actividades que tengan relación con la gestión de información dentro de las Unidades Administrativas de la Dirección Distrital. Esto incluye, pero no se limita a, el procesamiento, almacenamiento y transmisión de datos, tanto en formatos digitales como físicos. Se aplica a todo el personal, incluyendo empleados, contratistas y cualquier otra parte que interactúe con los sistemas de información de la Dirección.

3. Importancia de la Seguridad Informática

En la actualidad era digital, la información se ha transformado en uno de los activos con mayor valor para cualquier organización. La seguridad informática es crucial para proteger este activo contra una variedad de amenazas que pueden resultar en pérdidas financieras, daños a la reputación, interrupciones operativas y violaciones legales. En el contexto educativo, donde se manejan datos sensibles de estudiantes, personal y otros stakeholders, garantizar la confidencialidad y la integridad de la información es de suma importancia.

4. Cumplimiento Normativo

Esta guía se ha desarrollado teniendo en cuenta los estándares internacionales de seguridad de la información, en particular la norma ISO 27001. Asimismo, se alinea con las regulaciones y

políticas locales e institucionales vigentes, asegurando un cumplimiento normativo integral en varias las actividades relacionadas con la seguridad de la información.

5. Compromiso de la Dirección

La alta dirección de la Dirección Distrital 05D01 Latacunga - Educación está comprometida con la implementación efectiva de esta guía. Este compromiso se extiende a suministrar los recursos que se necesitan, tanto humanos como materiales, para garantizar que los procedimientos aquí establecidos se lleven a cabo de forma eficiente y efectiva.

6. Uso de la Guía

Esta guía se la debe utilizar como un documento de referencia obligatorio para todas las acciones que se relacionan con la seguridad de la información dentro de las Unidades Administrativas. Se anhela que todos los miembros del personal se familiaricen con su contenido y apliquen sus directrices en el desempeño de sus funciones.

Con la implementación de esta guía, la Dirección Distrital 05D01 Latacunga - Educación reforzará su compromiso con la protección de su capital informativo, asegurando un entorno seguro para la gestión eficiente de sus operaciones educativas y administrativas.

7. Marco Normativo

7.1. Fundamentación en la Norma ISO 27001

Esta guía se fundamenta en la norma ISO 27001, un estándar internacional que proporciona el marco para un sistema de gestión de seguridad de la información (SGSI). Esta norma establece los requisitos necesarios para proteger la información de manera efectiva, a través de la implementación de controles de seguridad adecuados y la gestión continua de riesgos. La ISO 27001 no solo se enfoca en los aspectos tecnológicos, sino que también considera la gestión organizativa y la mitigación de riesgos, lo cual es fundamental para una protección integral de la información.

7.2. Legislación y Regulaciones Locales

Además del cumplimiento con la ISO 27001, esta guía se alinea con las leyes, regulaciones y normativas locales e institucionales relacionadas con la seguridad de la información y la protección de datos personales. Esto incluye, pero no se limita a, leyes de protección de datos,

regulaciones de seguridad cibernética y políticas gubernamentales específicas para el sector educativo. La adhesión a estas regulaciones es crucial para garantizar la legalidad y la ética en el manejo de la información.

7.3. Políticas Institucionales

La guía también está en consonancia con las políticas internas de la Dirección Distrital 05D01 Latacunga - Educación. Esto incluye la adopción de las mejores prácticas y estándares establecidos por la institución en materia de seguridad de la información, privacidad de datos y uso responsable de recursos tecnológicos. Las políticas institucionales sirven como un marco para la implementación de los procedimientos descritos en esta guía y aseguran una coherencia en todas las operaciones y actividades relacionadas con la información.

7.4. Responsabilidad y Cumplimiento

Es responsabilidad de cada miembro del personal, incluyendo la alta dirección, los empleados, y los contratistas, cumplir con los estándares, políticas y procedimientos establecidos en esta guía. El incumplimiento de estas normativas puede resultar en riesgos significativos para la seguridad de la información y posibles sanciones legales o disciplinarias.

7.5. Revisión y Actualización

Esta guía deberá ser revisada y actualizada regularmente para asegurar su alineación continua con los cambios en las normas ISO, legislaciones locales y políticas institucionales. Esta revisión continuada es esencial para abordar los nuevos desafíos y amenazas en el ámbito de la seguridad de la información, y para garantizar la relevancia y efectividad de los procedimientos establecidos.

8. Activos de Información

Para la efectiva implementación del Sistema de Gestión de Seguridad de la Información en la Dirección Distrital 05D01 Latacunga - Educación, es primordial mantener un inventario actual de los activos de información. Este inventario debe reflejar los activos significativos para la institución, detallando la siguiente información:

8.1. Identificación

- **Código Ordenado**: Cada activo de información debe tener un código único que facilite su identificación y seguimiento dentro del inventario.

8.2. Tipo de Activos

- **Datos**: Incluye todos los datos generados, recogidos, gestionados, transmitidos y destruidos en la organización, en cualquier formato. Esto abarca registros académicos, información personal de estudiantes y personal, documentos administrativos, entre otros.

- **Aplicaciones**: Refiere al software utilizado para la gestión de la información. Esto incluye sistemas de gestión académica, plataformas de aprendizaje en línea, bases de datos administrativas, etc.

- **Personal**: Comprende la plantilla de empleados de la organización, personal subcontratado, estudiantes, usuarios y todas aquellas personas que acceden de alguna manera a los activos de información de la organización.

- **Servicios**: Incluye servicios internos como la gestión administrativa, y servicios externos como los ofrecidos a estudiantes y familias (por ejemplo, servicios de orientación educativa o actividades extracurriculares).

- **Tecnología**: Abarca los equipos que se utilizan para gestionar la información y las comunicaciones, como servidores, computadoras personales, teléfonos, impresoras, routers y cableado.

- **Instalaciones**: Se refiere a los lugares donde se alojan los sistemas de información, incluyendo oficinas, edificios, aulas, vehículos, entre otros.

- **Equipamiento Auxiliar**: Comprende activos que dan soporte a los sistemas de información y que no entran en las categorías anteriores, como equipos de destrucción de datos, sistemas de climatización, sistemas de alimentación ininterrumpida (UPS), entre otros.

8.3. Proceso de Identificación

a) **Creación de un Equipo de Trabajo**: Conformación de un equipo responsable de la identificación y clasificación de los activos de información, incluyendo personal de TI, administración y representantes de diferentes áreas funcionales.

b) **Recopilación y Clasificación**: Recopilación de información sobre cada activo, clasificación según los tipos descritos y asignación de un código de identificación.

c) **Evaluación de Importancia**: Determinación de la importancia de cada activo para la operación de la Dirección Distrital, considerando criterios como confidencialidad, integridad y disponibilidad.

d) **Registro y Mantenimiento**: Mantener un registro actualizado de todos los activos de información, revisándolo y actualizándolo periódicamente para reflejar cambios en la infraestructura, tecnología o necesidades organizativas.

Finalmente, para la realización de la identificación de los activos también se establece una ficha para la recolectar la información, la cual se pude visualizar en el Anexo 2.

9. Controles de confidencialidad, integridad y disponibilidad de información

Es prioritario establecer un marco de controles efectivos para asegurar la confidencialidad, integridad y disponibilidad de la información dentro de la Dirección Distrital 05D01 Latacunga - Educación. Estos controles son fundamentales para proteger los datos contra accesos no autorizados, garantizar su exactitud y confiabilidad, y asegurar su disponibilidad para cuando sean requeridos.

a) Confidencialidad de la Información

- **Control de Acceso:** Implementación de políticas de acceso basadas en roles para asegurar que solo el personal autorizado tenga acceso a la información confidencial. Esto incluye la autenticación de usuarios mediante contraseñas, tokens de seguridad o biometría.

- **Encriptación de Datos:** Uso de encriptación tanto en el almacenamiento como en la transmisión de datos para proteger la información confidencial de accesos no autorizados.

- **Gestión de Medios de Almacenamiento:** Procedimientos para el manejo seguro de medios de almacenamiento físico y digital, incluyendo la destrucción segura de datos cuando ya no sean necesarios.

- **Acuerdos de Confidencialidad:** Firma de acuerdos de confidencialidad por parte de los empleados y terceros que manejen información confidencial.

b) Integridad de la Información

- **Control de Modificaciones:** Restricciones sobre quién puede modificar la información y bajo qué circunstancias, incluyendo mecanismos de aprobación y revisión.

- **Protección contra Malware:** Implementación de soluciones antivirus y antimalware para proteger la información de alteraciones no autorizadas o maliciosas.

- **Auditorías y Registros de Actividad:** Mantenimiento de registros detallados de todas las actividades que afectan a la integridad de la información, permitiendo la trazabilidad y la detección de cualquier alteración indebida.

- **Integridad en el Desarrollo de Software:** Asegurar la integridad de las aplicaciones desarrolladas internamente mediante pruebas de software y revisiones de código.

c) Disponibilidad de la Información

- **Respaldo y Recuperación de Datos:** Establecimiento de procedimientos regulares de respaldo para asegurar la recuperación de la información en caso de pérdida o daño. Esto incluye la realización de pruebas periódicas de restauración.

- **Redundancia de Sistemas:** Implementación de soluciones de redundancia y balanceo de carga para asegurar la disponibilidad continua de los sistemas críticos.

- **Planes de Continuidad del Negocio:** Desarrollo de planes de continuidad operativa para garantizar que la información es accesible y utilizable incluso en situaciones de emergencia o desastre.

- **Gestión de la Capacidad:** Monitoreo constante y ajuste de los recursos de TI para asegurar que puedan soportar el acceso y uso continuo de la información.

Estos controles en un principio deben ser asignados al personal especializado, mediante el uso de una ficha para la designación del responsable de la gestión de control la cual se puede visualizar en el Anexo 3. De igual forma los elementos clave de cada control deberán ser registrados mediante una ficha de control la cual se puede observar en el Anexo 4.

10. Evaluación de Riesgos de seguridad

Este proceso implica la identificación sistemática y el análisis de los riesgos que podrían comprometer la confidencialidad, integridad y disponibilidad de los activos de información en las Unidades Administrativas de la Dirección Distrital 05D01 Latacunga - Educación. La finalidad es determinar la probabilidad de ocurrencia de eventos adversos y su potencial impacto, con el objetivo de implementar medidas adecuadas para mitigar o eliminar dichos riesgos. Esta evaluación se alinea con los principios establecidos en la norma ISO 27001, asegurando una gestión de riesgos coherente, integral y adaptada a las necesidades específicas de la organización.

a) Identificación de Riesgos

- **Identificación de Activos**: Enumerar y clasificar los activos de información relevantes en las Unidades Administrativas.
- **Identificación de Amenazas**: Determinar las potenciales amenazas que podrían dañar a cada activo identificado.
- **Identificación de Vulnerabilidades**: Reconocer las debilidades en los sistemas y procesos que podrían ser explotadas por las amenazas.

b) Análisis de Riesgos

- **Análisis de la Probabilidad**: Estimar la frecuencia con la que cada amenaza podría materializarse en cada activo.
- **Análisis del Impacto**: Evaluar las consecuencias que tendría la materialización de cada amenaza sobre los activos.

c) Evaluación de Riesgos

- **Determinación del Nivel de Riesgo**: Clasificar los riesgos en función de su

probabilidad e impacto, utilizando una matriz de riesgo.

- **Priorización de Riesgos**: Establecer un orden de prioridad para el tratamiento de los riesgos en función de su nivel.

d) Tratamiento de Riesgos

- **Selección de Medidas de Control**: Decidir sobre las medidas de seguridad adecuadas para mitigar, transferir, aceptar o evitar los riesgos.
- **Implementación de Controles**: Aplicar las medidas de seguridad seleccionadas.

e) Monitoreo y Revisión de Riesgos

- **Revisión Periódica**: Revisar regularmente la evaluación de riesgos para identificar cambios en el entorno o en los activos de información.
- **Actualización Continua**: Ajustar las estrategias de tratamiento y los controles de seguridad según sea necesario.

La realización de una evaluación de riesgos eficaz y detallada es esencial para asegurar que la Dirección Distrital 05D01 Latacunga - Educación posea un entendimiento claro de sus vulnerabilidades y esté en capacidad de implementar medidas efectivas de seguridad de la información. Este proceso se complementa con el uso de una ficha de valuación la cual se puede visualizar en el Anexo 5.

11. Control de acceso

El control de acceso constituye un pilar fundamental en la gestión de la seguridad de la información dentro de cualquier organización. Por lo cual, se aborda las políticas y procedimientos diseñados para regular el ingreso a los recursos de información, asegurando que solo las personas autorizadas puedan acceder a datos y sistemas críticos. Este literal detalla las estrategias y mecanismos, como la autenticación de múltiples factores, la gestión de permisos y la monitorización de accesos, esenciales para una gestión de riesgos efectiva en las Unidades Administrativas de la Dirección Distrital 05D01 Latacunga - Educación.

PROCEDIMIENTO PARA LA EJECUCIÓN DE CONTROLES DE ACCESO

FÍSICOS Y LÓGICOS

Objetivo: Garantizar la seguridad de la información y la integridad de los activos digitales y físicos mediante la implementación de controles de acceso físicos y lógicos en la Dirección Distrital 05D01 de Latacunga – Educación, en conformidad con los requisitos de la norma ISO 27001.

1. Evaluación de riesgos

- Realizar una evaluación de riesgos para identificar activos críticos y determinar los niveles de acceso necesarios.
- Establecer un equipo de evaluación que incluya representantes de seguridad, tecnología de la información y personal administrativo clave.

2. Identificación de usuarios y roles

- Crear una lista detallada de usuarios y sus roles específicos en la dirección distrital.
- Asignar niveles de acceso basados en las responsabilidades y funciones de cada usuario.

3. Implementación de controles de acceso físicos

- Designar áreas restringidas y sensibles que alberguen equipos y sistemas críticos.
- Instalar sistemas de cerraduras electrónicas y tarjetas de acceso para restringir el acceso físico a áreas sensibles.
- Implementar cámaras de vigilancia y sistemas de monitoreo para registrar y auditar actividades en áreas críticas.

4. Capacitación del personal

- Proporcionar formación regular sobre la importancia de los controles de acceso y las mejores prácticas de seguridad.
- Educar a los usuarios sobre lo importante de proteger sus credenciales de ingreso

y la información confidencial.

5. ***Monitoreo continuo***

- Establecer un sistema de monitoreo continuo para detectar y responder a eventos de seguridad en tiempo real.
- Configurar alertas para notificar anomalías en los patrones de acceso, tanto físicos como lógicos.

6. Auditorías periódicas

- Realizar auditorías periódicas de los controles de acceso para evaluar su eficacia.
- Documentar y abordar cualquier hallazgo o vulnerabilidad identificada durante las auditorías.

7. Registro y documentación

- Mantener registros detallados de cambios en los niveles de acceso, eventos de seguridad y auditorías.
- Documentar los procedimientos de implementación y mantenimiento de controles de acceso.

8. Evaluación y Revisión

- Realizar evaluaciones periódicas del cumplimiento con los controles de acceso.
- Revisar y actualizar este procedimiento según sea necesario para adaptarse a cambios en la infraestructura y las amenazas emergentes.

---

12. Concientización y capacitación

La concienciación y capacitación en seguridad de la información son aspectos cruciales para fortalecer la defensa contra incidentes de seguridad informática. Este literal se centra en la importancia de educar y sensibilizar al personal de la Dirección Distrital 05D01 Latacunga - Educación sobre los riesgos y las prácticas adecuadas en seguridad de la información.

PLAN DE CONCIENTIZACIÓN Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN PARA LA DIRECCIÓN DISTRITAL 05D01 LATACUNGA – EDUCACIÓN

Objetivo general

Fortalecer la conciencia y capacitación en seguridad de la información en todas las unidades administrativas de la Dirección Distrital 05D01 Latacunga – Educación, con el fin de reducir los riesgos asociados con la gestión de datos sensibles y promover un entorno seguro.

Objetivos específicos

- Sensibilizar al personal sobre las amenazas comunes de seguridad de la información y los riesgos asociados con la negligencia en prácticas seguras.
- Educar a los empleados sobre las mejores prácticas en el uso seguro de dispositivos, contraseñas, acceso a redes y la prevención de ingeniería social.
- Proporcionar pautas claras sobre la clasificación y manejo de datos sensibles, destacando la importancia de la confidencialidad e integridad de la información.
- Capacitar al personal en los procedimientos de respuesta a incidentes, asegurando una acción rápida y eficiente en caso de violaciones de seguridad.
- Informar sobre las regulaciones y normativas de seguridad de la información relevantes, asegurando que el personal esté al tanto de las obligaciones legales y organizativas.

Metodología

- Programar sesiones presenciales y/o virtuales de capacitación con expertos en seguridad de la información.
- Desarrollar material educativo, como folletos, carteles y documentos informativos, para reforzar los conceptos de seguridad.
- Realizar simulacros y ejercicios prácticos para que los empleados apliquen los conocimientos adquiridos en situaciones realistas.
- Implementar una plataforma de aprendizaje en línea para facilitar el acceso continuo a recursos educativos.

Evaluación

- Realizar evaluaciones periódicas para medir la eficacia del programa y realizar ajustes según sea necesario.

5.4. Formulación del cronograma de implementación mediante normas ISO 27001 para la dirección distrital 05D01 Latacunga - educación.

Tabla 29

cronograma de implementación mediante normas ISO 27001 para la dirección distrital 05D01 Latacunga - educación.

Actividad	Trimestre 1 (Semana)	Trimestre 2 (Semana)	Trimestre 3 (Semana)	Trimestre 4 (Semana)
Definición del alcance del SGSI	1-4	-	-	-
Conformación del equipo de evaluación de riesgos	5-8	-	-	-
Realización de la evaluación de riesgos	9-13	-	-	-
Desarrollo de la política de seguridad de la información	-	1-4	-	-
Identificación y selección de controles de seguridad	-	5-8	-	-
Implementación de los controles de seguridad seleccionados	-	-	1-4	-
Realización de la auditoría interna	-	-	5-8	-
Preparación para la auditoría externa	-	-	-	1-4
Realización de la auditoría externa	-	-	-	5-8
Obtención de la certificación ISO 27001	-	-	-	9-13

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- La evaluación de respuestas destaca desafíos claves en la implementación de medidas de seguridad informática en la Dirección Distrital 05D01 Latacunga – Educación. La disponibilidad intermitente de políticas de seguridad revela inconsistencias en su aplicación, planteando riesgos para la integridad de los sistemas e información. Se concluye que el fortalecimiento en las capacitaciones y la comunicación oportuna mejorara la comprensión y la aplicación de las políticas. Además, más del 50% de los encuestados en Unidades Administrativas muestra desconocimiento de las políticas, subrayando la necesidad de mejorar la comunicación y la capacitación para fomentar prácticas seguras. La falta de consistencia en la actualización de políticas, evidente en casi la mitad de los encuestados, señala posibles lagunas de seguridad y destaca la necesidad de mejorar los procesos y la cultura organizacional en torno a la seguridad informática. Estrategias efectivas son esenciales para promover prácticas regulares de actualización y revisión de políticas, asegurando una protección más robusta de sistemas e información.

- Por lo tanto, la identificación de los riesgos en las Unidades Administrativas de la Dirección Distrital 05D01 Latacunga – Educación ha proporcionado una comprensión profunda de las amenazas potenciales para los activos de información. Este análisis integral establece las bases para la implementación de medidas preventivas y correctivas, fortaleciendo así el sistema de seguridad de la información. La diversidad de riesgos identificados, que incluyen posibles brechas de seguridad y amenazas internas, destaca la necesidad urgente de una estrategia de seguridad proactiva.

- Por lo tanto, la creación de una guía actualizada de procedimientos para la seguridad informática en las Unidades Administrativas de la Dirección Distrital 05D01 Latacunga – Educación representara un avance significativo para resguardar la información confidencial. Esta guía ofrece directrices precisas para prevenir la fuga de datos, elevando la conciencia y capacidad de respuesta del personal. La focalización en reducir la fuga de información destaca el compromiso de la Dirección Distrital 05D01 con la integridad y confidencialidad de los datos. La guía, al abordar no solo aspectos tecnológicos sino también la importancia de la capacitación y la cultura de seguridad se rige como una defensa esencial contra las amenazas internas.

- En conclusión, el cronograma para la implementación de políticas de seguridad informática, alineado con las normas ISO 27001, ofrece una estructura temporal clara para la Dirección Distrital 05D01. Este enfoque metódico asegura una implementación gradual y efectiva, evitando interrupciones significativas en las operaciones diarias. La formulación del cronograma refleja el compromiso a largo plazo de la Dirección Distrital 05D01 con la mejora continua de la seguridad informática. Al adoptar estándares reconocidos internacionalmente, demuestra su disposición para mantenerse actualizada y ajustarse a las mejores prácticas en seguridad de la información.

Recomendaciones

- Se recomienda desarrollar programas de formación específicos para el personal de la Dirección Distrital 05D01 Latacunga - Educación, mejorando así su conocimiento y comprensión de las políticas de seguridad. Además, establecer canales de comunicación efectivos para mantener al personal informado sobre las actualizaciones y expectativas en materia de seguridad, la cual contribuirá a garantizar una aplicación más uniforme y efectiva de las políticas.

- Se sugiere implementar iniciativas intensivas de capacitación y concientización sobre las políticas de seguridad informática. Estas iniciativas deben destacar la importancia de prácticas seguras en el manejo de la información. Además, el desarrollo de material educativo claro y accesible contribuirá a mejorar la comprensión y fomentar prácticas más seguras, reduciendo así el riesgo asociado con el desconocimiento de las políticas.

- Poner en marcha las estrategias efectivas para fomentar prácticas regulares en este sentido. Esto incluiría establecer procedimientos claros para la revisión periódica de políticas, así como incentivos y recordatorios para garantizar su cumplimiento. La creación de una cultura organizacional que valore y priorice la seguridad informática promoverá la conciencia de la importancia de mantener las políticas actualizadas, reduciendo así posibles lagunas de seguridad y vulnerabilidades no identificadas.

REFERENCIAS

Aguiar, M. d. (s.f.). *Técnicas e Instrumentos de Recolección de Datos*. https://sabermetodologia.wordpress.com/2016/02/15/tecnicas-e-instrumentos-de-recoleccion-de-datos/

Aguilar, L. (2023). *Qué es Linux: el sistema operativo de código abierto*. https://www.adslzone.net/reportajes/software/que-es-linux/

Alvarado, C. (2023). *Sistema de gestión de seguridad de la información: qué es y sus etapas*. https://gestion.pensemos.com/sistema-de-gestion-de-seguridad-de-la-informacion-que-es-etapas#:~:text=Un%20SGSI%20consiste%20en%20el,sus%20activos%20de%20informaci%C3%B3n%20esenciales.

Avast Software. (2022). *¿Qué es el malware? La guía definitiva sobre el malware*. https://www.avg.com/es/signal/what-is-malware#topic-3

Avast Software. (2023). *¿Qué es el malware y cómo protegerse de los ataques?* https://www.avast.com/es-es/c-malware

Bazante Veloz, D., Barona López, I., Valdivieso, L., y Hernández Álvarez, B. (2019). Indicadores para la detección de ataques ransomware. *RISTI, Revista Ibérica de Sistemas e Tecnologias de Informação*(19), 493-506. https://www.proquest.com/openview/841aa93ba3c3df451268e843ef187b70/1?pq-origsite=gscholar&cbl=1006393

Bojacá Garavito, E. (2021). *Diseño de un Sistema de Gestión de Seguridad Informática basado en la norma ISO/IEC 27001-27002 para el área administrativa y de historias clínicas del Hospital San Francisco de Gachetá.* Universidad Nacional Abierta y a Distancia.

Catuto Pilay, R. M. (2021). *Análisis de amenazas y vulnerabilidades informáticas basado en la Norma ISO 27002,*. Universidad Estatal Península de Santa Elena. https://repositorio.upse.edu.ec/xmlui/bitstream/handle/46000/5754/UPSE-TTI-2021-0007.pdf?sequence=1&isAllowed=y

CEPAL. (2020). *Gestión de datos de investigación*. https://biblioguias.cepal.org/c.php?g=495473&p=4398069

Chávarry Bonilla, S. (2021). *Implementación de ISO 27001 y 27002 adaptadas para gestión de seguridad de información en secretaría ejecutiva de policía nacional del Perú.* Universidad César Vallejo. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/79133/Ch%c3%a1varry

_BSNF-SD.pdf?sequence=1&isAllowed=y

Cumbicus Pineda, M., Ludeña Preciado, V., y Neyra Romero, A. (2022). Técnicas de machine Learning para la detección de Ransomware: Revisión sistemática de Literatura. *Journal of Science and Research, 7*(3), 32-60. https://revistas.utb.edu.ec/index.php/sr/article/view/2684

DocuSign, Inc. (2021). *¿Cuáles son los pilares de la seguridad de la información?* https://www.docusign.mx/blog/seguridad-de-la-informacion

Editorial Etecé. (2023). *Seguridad*. https://concepto.de/seguridad/

Educación, M. d. (2023). *Misión / Visión / Valores*. https://educacion.gob.ec/valores-mision-vision/

EMERGE AVEZALIA, S.L. (2020). *Diferencias entre el software libre y el software propietario*. https://www.avezalia.es/software-libre-software-propietario/

Escuela Europea de Excelencia. (s.f.). *ISO 27001: ¿Qué son las vulnerabilidades y amenazas?* Sistemas de gestión ISO . https://doi.org/https://www.europeanquality.es/iso-27001-que-son-las-vulnerabilidades-y-amenazas/

ESGinnova, G. (2021). *¿Qué es la ISO 27001?* https://www.isotools.us/normas/riesgos-y-seguridad/iso-27001/

Figueroa Suárez, J., Rodríguez Andrade, R., Bone Obando, C., y Saltos Gómez, J. (2018). La seguridad informática y la seguridad de la información. *Revista Polo del Conocimiento, 2*(12), 145-155. https://doi.org/10.23857/pc.v2i12.420

Gómez Torres, E. R. (2018). *Implementación de un sistema de gestión de seguridad de información basado en la Norma ISO 27001:2013 para el control físico y digital de documentos aplicado a la empresa LOCKERS S.A.* Universidad de las Fuerzas Armadas ESPE. http://repositorio.espe.edu.ec/handle/21000/14397

Grupo ESGINNOVA. (2022). *ISO 27001*. ISO Tools: https://www.isotools.us/normas/riesgos-y-seguridad/iso-27001/

Guaña Moya, J., Sánchez Zumba, A., Chérrez Vintimilla, P., y Chulde Obando, L. (2022). Ataques informáticos más comunes en el mundo digitalizado. *RISTI, Revista Ibérica de Sistemas e Tecnologias de Informação*(54), 87-100. https://www.proquest.com/openview/02492b51bc001f7bf3254a198698d1d7/1?pq-origsite=gscholar&cbl=1006393

Hernández, K. (19 de abril de 2023). *¿Qué es la seguridad informática?* https://www.servnet.mx/blog/que-es-la-seguridad-informatica-y-como-implementarla#:~:text=Mecanismos%20preventivos%20de%20seguridad%20inform

%C3%A1tica,y%20procesos%20de%20la%20compa%C3%B1%C3%ADa.

IBM. (20 de 04 de 2021). *Identificación y autenticación*. https://www.ibm.com/docs/es/ibm-mq/7.5?topic=ssfksj-7-5-0-com-ibm-mq-sec-doc-q009740--htm

Imagar. (2021). *Ventajas y desventajas de Windows Server*. https://www.imagar.com/blog-desarrollo-web/ventajas-y-desventajas-de-windows-server/

Instituto para una Cultura de seguridad Industrial. (2018). *¿Qué es la cultura de seguridad?* https://www.icsi-eu.org/es/revista/cultura-seguridad-definicion

Intedya. (2018). *Riesgos y Seguridad: ¿qué es la Norma ISO 27001?* https://www.intedya.com/internacional/466/noticia-riesgos-y-seguridad-que-es-la-norma-iso-27001.html

IONOS. (2020). *¿Qué es un backup y cuál es la mejor manera de proteger los datos?* https://www.ionos.es/digitalguide/servidores/seguridad/que-es-un-backup/

ISO 27001. (2017). *¿Seguridad informática o seguridad de la información?* https://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/

ISO 27001. (2022). *Cuestiones básicas de la norma ISO 27001*. https://co.isotools.us/cuestiones-basicas-de-la-norma-iso-27001/

ISOTools. (26 de 01 de 2017). *Seguridad de la Información*. https://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/

Ixiam. (15 de 11 de 2022). *Software libre: características y ventajas de su uso*. https://www.ixiam.com/es/blog/software-libre-caracteristicas-y-ventajas-de-su-uso/

Jacha Rojas, J. P. (2019). *Propuesta de un sistema de gestión de seguridad de información para la protección de activos de información basado en la norma ISO 27001 en el área de informática de la municipalidad provincial de Huánuco.* Universidad de Huánaco. http://repositorio.udh.edu.pe/bitstream/handle/123456789/2084/ARG%c3%9cEZO%20RAMIREZ%2c%20EDUARDO%20DANIEL.pdf?sequence=3&isAllowed=y

KeepCoding. (2022). *Los 5 pilares básicos de la ciberseguridad*. https://keepcoding.io/blog/pilares-basicos-de-la-ciberseguridad/

Kiuwan. (2023). *¿Cual es objetivo de la seguridad informática?* https://www.apuntateuna.es/nuevo/cual-es-el-objetivo-de-la-seguridad-informatica.html

López, E. R., y Francisco, J. (01 de noviembre de 2020). *Investigación de campo*. https://economipedia.com/definiciones/investigacion-de-campo.html

MINTEL. (SN). *Ecuador ocupa sexto lugar en la región, según Índice de Ciberseguridad*. https://www.telecomunicaciones.gob.ec/ecuador-ocupa-sexto-lugar-en-la-region-

segun-indice-de-ciberseguridad/

Montalvo Cisneros, O. A. (2021). *Efectos de la implementación de una auditoría informática a las empresas de seguros a través de la ISO 27001 :2013 ubicadas en el Norte del DMQ*. Universidad Politécnica Salesiana. https://dspace.ups.edu.ec/bitstream/123456789/19918/1/UPS-TTQ245.pdf

Moreno, J., Rodriguez, C., y Leguias, I. (2020). Revisión sobre propagación de ransomware en sistemas operativos Windows. *I+D Tecnológico, 16*(1), 39-45. https://doi.org/https://doi.org/10.33412/idt.v16.1.2438

Netec. (2023). *¿Qué es seguridad informática?* https://www.netec.com/que-es-seguridad-informatica

Norton. (08 de 08 de 2018). *¿Qué es un virus informático?* https://mx.norton.com/blog/malware/what-is-a-computer-virus

Nueva ISO 9001. (2017). *Principios de gestión de la calidad.* Grupo ESGinnova. https://doi.org/https://www.nueva-iso-9001-2015.com/2017/07/principios-de-gestion-de-la-calidad/

Ortiz, A. E. (2018). *¿Qué es CentOs? ¿Que significa y que hace? ¿Es Linux? ¿RedHat? ¿Open Source?* https://www.hostdime.la/blog/que-es-centos-que-significa-y-que-hace-es-linux-redhat-open-source/

Postigo Palacios, A. (2020). *Seguridad informática.* Paraninfo. https://books.google.es/books?hl=es&lr=&id=UCjnDwAAQBAJ&oi=fnd&pg=PR5&dq=La+seguridad+inform%C3%A1tica&ots=-H01nj5Rf1&sig=jgGYL6BOCI7nNiTeEhZtqh-o2Y4#v=onepage&q=La%20seguridad%20inform%C3%A1tica&f=false

Precitool. (2021). *Windows Server*. https://precitool.com/windows-server/

Quispe, A. (2020). *sistemas operativos libres y licenciados.* https://es.slideshare.net/yonathanalexisquispe/sistemas-operativos-libres-y-licenciados

Riveros, A. (2020). *Qué es la norma ISO 27001 y para qué sirve*. EALDE: https://www.ealde.es/iso-27001-para-que-sirve

Romero Castro, M. I., Figueroa Moràn, G. L., Vera Navarrete, D. S., y Álava Cruzatty, J. E. (10 de 2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades.* Universidad Estatal del Sur de Manabí. https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Saeckel, A. (2023). *Gestión de la vulnerabilidad en el contexto de la norma ISO 27001*. dqs. https://doi.org/https://www.dqsglobal.com/es-co/aprenda/blog/gestion-de-la-

vulnerabilidad-en-el-contexto-de-la-norma-iso-27001

SISSA Monitoring Integral. (2023). *La importancia de la Cultura de seguridad en organizaciones*. https://www.linkedin.com/pulse/la-importancia-de-cultura-seguridad-en-organizaciones-sissamx/?originalSubdomain=es

Sontay, R. (2020). *Sistemas Operativos Propietario o Licenciados.* https://es.scribd.com/document/274135995/SISTEMAS-OPERATIVOS-PROPIETARIO-O-LICENCIADOS-docx

Toledo, R. (2022). *Tipos de copias de seguridad: ¿Cuál es la mejor?* https://doi.org/https://www.grupocibernos.com/blog/tipos-de-copias-de-seguridad-cual-es-la-mejor

UNIR. (12 de 11 de 2019). *¿Qué es la certificación ISO 27001 y para qué sirve?* https://www.unir.net/ingenieria/revista/iso-27001/#:~:text=La%20ISO%2027001%20es%20una,y%20aplicaciones%20que%20la%20tratan.

UNIR. (15 de 06 de 2021). *¿Qué es la seguridad informática y cuáles son sus tipos?* https://ecuador.unir.net/actualidad-unir/que-es-seguridad-informatica/

Valdeviezo Troya, J. L., y Rodriguez Poveda, R. J. (2015). *Informe de evaluación de seguridad en la información basada en la norma ISO 27001 en el Departamento de TI de una Empresa de Lácteos.* Universidad Politécnica Salesiana. https://dspace.ups.edu.ec/bitstream/123456789/10307/1/UPS-GT001204.pdf

Vazquez Reyna, J. E. (2018). *Qué Es Seguridad Informática.* https://es.scribd.com/document/458444037/Que-es-seguridad-informatica-docx#

ANEXOS

Anexo 1.

Encuesta dirigida al personal administrativo

Pontificia Universidad Católica del Ecuador
FACULTAD DE INGENIERÍA
COORDINACIÓN DE POSGRADO

PUCE

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

Analizar las vulnerabilidades de la seguridad informática utilizando ISO 27001 caso de estudios Unidades Administrativas de la Dirección Distrital 05d01 Latacunga - Educación

Objetivo: Estimado/a Sr. /a el presente cuestionario tiene como objetivo identificar los riesgos que pueden afectar a los activos de la información de las Unidades Administrativas de la Dirección Distrital 05D01 Latacunga – Educación, por favor responda con toda sinceridad pues de ello dependerá que los resultados de esta investigación sean objetivos.

Instrucciones: Marcar con una (X) de acuerdo a la valoración que usted lo asigna considerando la siguiente leyenda: 5. Siempre 4. Casi Siempre 3. A veces 2. Casi nunca 1. Nunca

N°	Pregunta	Escala				
		1	2	3	4	5
A	**Políticas y procedimientos de seguridad informática**					
1	¿Se dispone de políticas de seguridad informática en las Unidades Administrativas de la Dirección Distrital 05D01 Latacunga – Educación?					
2	¿Conoce y comprende las políticas de seguridad informática en las Unidades Administrativas?					
3	¿Actualizan y revisan las políticas de seguridad informática en las					

	Unidades Administrativas?
4	¿Comunican y difunden las políticas de seguridad informática al personal de las Unidades Administrativas?
5	¿Se capacita al personal sobre las políticas y procedimientos de seguridad informática en las Unidades Administrativas?
B	**Protección física**
6	¿Los equipos informáticos de las Unidades Administrativas de la Dirección Distrital 05D01 Latacunga – Educación se resguardan en lugares seguros?
7	¿Se controla el acceso a las áreas donde se encuentran los equipos informáticos?
8	¿Se registra la identificación de los usuarios que manipulan los equipos de la Dirección Distrital 05D01 Latacunga – Educación?
9	¿Cuenta con áreas seguras específicas para los equipos informáticos?
10	¿Realizan mantenimientos periódicos de los equipos informáticos?
C	**Respaldo y continuidad del negocio**
11	¿Existe un responsable del área de informática en las Unidades Administrativas de la Dirección Distrital 05D01 Latacunga – Educación?
12	¿Se realizan copias de seguridad informática periódicas?
13	¿Se dispone de un servidor para el resguardo de la información?
14	¿Cuenta con sistemas de alimentación eléctrica ininterrumpida (UPS) instalados en los equipos informáticos?
15	¿Se ha establecido un plan de continuidad del negocio en caso de interrupciones del sistema?
D	**Gestión de accesos**
16	¿Se han realizado simulacros frente a la caída de los sistemas de información y de comunicación en las Unidades Administrativas de la Dirección Distrital 05D01 Latacunga – Educación?
17	¿Manejan personalmente las claves por cada usuario en las Unidades Administrativas?
18	¿Aplican políticas de grupo para el acceso a la información en las Unidades Administrativas?

19	¿Cuenta con un procedimiento de identificación y autenticación de las personas que manipulan los equipos de cómputo?
20	¿Se revisan y actualizan periódicamente los privilegios de acceso al sistema?
B	**Gestión de riesgos**
21	¿Se realizan evaluaciones periódicas de riesgos de seguridad informática en las Unidades Administrativas de la Dirección Distrital 05D01 Latacunga – Educación?
22	¿Se asignan recursos para mitigar los riesgos identificados?
23	¿Realizan auditorías internas de seguridad informática para evaluar la eficacia de los controles?
24	¿Documentan adecuadamente los incidentes de seguridad informática y las acciones tomadas para resolverlos?
25	¿Se evalúan y actualizan regularmente los planes de seguridad en función de los cambios en las amenazas y tecnologías?

Anexo 2

Formato para identificación y documentación de activos de información.

IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN

Fecha: _____

Responsable de la Identificación**:** _____

1. Descripción del Activo

- Nombre del Activo: _____

- Ubicación: _____

- Propietario: _____

- Valor del Activo: _____

- **Categoría del Activo**

Hardware	
Software	
Datos	
Recursos Humanos	
Instalaciones	

- **Valor del Activo**

Crítico	
Importante	
No crítico	

- **Clasificación de la Información**

Pública	
Interna	
Confidencial	
Altamente confidencial	

- **Documentación Asociada**

Políticas relacionadas	
Procedimientos	
Planes de contingencia	

_____

Firma del responsable

Anexo 3

Formato para designar responsable de la gestión de control

DESIGNACIÓN DEL RESPONSABLE DE GESTIÓN DE CONTROL

Fecha: _____

Responsable de Designación: _____

1. Identificación del Responsable

- Nombre: _____

- Cargo: _____

- Departamento: _____

2. Responsabilidades:

- Descripción detallada de responsabilidades

3. Formación y Concienciación:

- Plan de formación

- Actividades de concienciación

_____

Firma del Responsable

……

Anexo 4

Formato para la identificación de controles

IDENTIFICACIÓN DE CONTROLES DE SEGURIDAD

Fecha: _____
Responsable: _____

Item	Descripción
	Información General
Nombre del Control	(Descripción breve del control)
Categoría del Control	(Confidencialidad / Integridad / Disponibilidad)
Fecha de Implementación	(DD/MM/AAAA)
Ubicación del Control	(Especificar la ubicación física o lógica)
	Descripción del Control
Detalle del Control	(Descripción detallada del control)
Activos Protegidos	(Activos de información específicos protegidos)
	Evaluación del Riesgo
Amenazas Mitigadas	(Amenazas específicas que el control busca mitigar)
Vulnerabilidades Abordadas	(Vulnerabilidades que se reducen o eliminan)
	Efectividad del Control
Indicadores de Efectividad	(Métricas o KPIs para medir la efectividad)
Resultados de Evaluaciones Previas	(Resumen de evaluaciones anteriores)
Fecha de Última Revisión	(DD/MM/AAAA)
	Acciones Correctivas y Preventivas
Recomendaciones de Mejora	(Sugerencias para mejorar el control)
Plan de Acción	(Pasos para implementar mejoras)
Fecha de Seguimiento	(DD/MM/AAAA para próxima revisión)
	Documentación Adicional
Referencias	(Documentos, políticas o procedimientos relacionados)
Comentarios Adicionales	(Notas o consideraciones extras)

_____

Firma del Responsable

Anexo 5

Ficha de evaluación de riesgos de seguridad

EVALUACIÓN DE RIESGOS DE SEGURIDAD

Fecha: _____

Responsable de la Evaluación: _____

1. **Identificación de Amenazas**

Acceso no autorizado	
Pérdida o robo de dispositivos	
Ataques de malware	
Fallos en la seguridad física	
Vulnerabilidades en software no parcheadas	
Ataques de ingeniería social	
Interrupciones del servicio	
Fallos en la gestión de contraseñas	
Fugas de información	
Ataques de denegación de servicio (DDoS)	

Vulnerabilidades Asociadas

Falta de actualizaciones de seguridad	
Configuraciones incorrectas de sistemas	
Insuficientes medidas de cifrado	
Débiles políticas de gestión de contraseñas	
Falta de control de acceso adecuado	
Deficiencias en la protección física	
Errores en el desarrollo de software	
Falta de capacitación en seguridad para el personal	
Inadecuado monitoreo y registro de eventos	
Deficiencias en la gestión de parches de software	

3. Análisis de Impacto

- Impacto en la confidencialidad: Evalúa las repercusiones resultantes de la divulgación no autorizada de información confidencial, como secretos comerciales, datos personales o información estratégica. Las consecuencias pueden ser significativas para la reputación y la seguridad de la organización.

- Impacto en la integridad: Se enfoca en los efectos potenciales de la alteración no

autorizada o accidental de la información. La integridad se ve comprometida si los datos son modificados de manera inapropiada, lo que podría conducir a decisiones erróneas, pérdida de confianza en los sistemas o riesgos legales, según la naturaleza de la información afectada.

- Impacto en la disponibilidad: Evalúa las consecuencias de la pérdida o reducción del acceso a información o servicios críticos. Un impacto en la disponibilidad podría resultar en la interrupción de operaciones comerciales, pérdida de productividad o, en situaciones críticas, amenazar la seguridad física o la salud pública, dependiendo del contexto de la información afectada.

2. Niveles de Riesgo

- **Bajo:** Riesgos que tienen un impacto limitado en la confidencialidad, integridad o disponibilidad de la información. Pueden manejarse con medidas de seguridad existentes y no representan una amenaza significativa para la organización. Las consecuencias son manejables y las pérdidas potenciales son mínimas.

- **Moderado:** Riesgos que podrían tener un impacto significativo en la confidencialidad, integridad o disponibilidad, pero que pueden ser mitigados mediante la implementación de controles adicionales. Requieren atención y supervisión, y las consecuencias pueden ser gestionables con la aplicación adecuada de medidas de seguridad.

- **Alto:** Riesgos que presentan una amenaza significativa para la confidencialidad, integridad o disponibilidad de la información. Pueden tener consecuencias graves para la organización y podrían requerir medidas inmediatas de mitigación. La falta de acción podría resultar en pérdidas significativas, daño a la reputación y posibles repercusiones legales o regulatorias. Se necesita una atención urgente y la implementación de medidas de control robustas.

3. Decisiones y Acciones

Decisiones

- Implementar un sistema de parcheo regular para abordar vulnerabilidades de seguridad en software.

- Establecer controles de acceso más estrictos para limitar la posibilidad de accesos no autorizados.

- Mejorar la concienciación en seguridad mediante programas de formación para el personal.

Acciones a seguir

- Establecer un calendario de parcheo regular y automatizado para garantizar

actualizaciones oportunas.

- Revisar y ajustar las políticas de acceso, implementando la autenticación multifactorial donde sea necesario.

- Desarrollar e implementar programas de formación en seguridad, incluyendo simulacros de phishing y buenas prácticas de seguridad de la información.

Firma del Responsable

……