Análisis de la seguridad de la información en los procesos administrativos en las oficinas del Colegio Técnico Profesional San Isidro

Informe de la tesis presentado en
Universidad Nacional de Costa Rica
Facultad de Ciencias Sociales
Escuela de Secretariado Profesional

Para optar por el grado académico de grado de Licenciatura en
Administración de Oficinas

Ericka Yuliana Acuña Durán
Yirlany Benavides Solís
Yilda Vanessa Varela González

Mayo, 2025

Análisis de la seguridad de la información en los procesos administrativos en las oficinas del Colegio Técnico Profesional San Isidro

Informe de la tesis presentado en
Universidad Nacional de Costa Rica
Facultad de Ciencias Sociales
Escuela de Secretariado Profesional

Para optar por el grado académico de grado de Licenciatura en
Administración de Oficinas

Ericka Yuliana Acuña Durán
Yirlany Benavides Solís
Yilda Vanessa Varela González

Mayo, 2025

Análisis de la seguridad de la información en los procesos administrativos en las oficinas del Colegio Técnico Profesional San Isidro

Ericka Yuliana Acuña Durán
Yirlany Benavides Solís
Yilda Vanessa Varela González

APROBADO POR:

Director (a) del TFG_____
MSc. Digna Valverde Fallas

Asesor (a)_____
MBA. Leonella Naranjo Jiménez

Asesor (a)_____
M.Sc. Ariel Hidalgo Brenes

Decano _____
Dr. Elvis Rojas Ramírez

Director Académico_____
MBA. Erick Madrigal Villanueva

Dedicatoria

En primer lugar, dedico este trabajo a Dios por darme la fortaleza, sabiduría y la guía necesaria para enfrentar cada obstáculo durante todo mi proceso, a mi familia por su apoyo incondicional especialmente a mi madre, padre, hermanos y sobrino, por motivarme constantemente y por su amor. A mis compañeras de trabajo final de graduación, que más que eso son mis amigas, gracias por la paciencia, el amor y la comprensión en cada momento de este proceso. Y a la Universidad Nacional por darme la oportunidad de ser lo que hoy soy.

Yirlany Benavides Solís

Esta tesis está especialmente dedicada a Dios por ser quien me ha guiado durante este proceso, quien me ha dado sabiduría para seguir adelante y no desistir en ningún momento, así como a mi familia principalmente a mi madre, padre y hermana, quienes han sido mi apoyo primordial durante todos estos años de estudio y sacrificios, de igual forma dedico este trabajo a mis compañeras y amigas de trabajo final de graduación, por la constante dedicación y apoyo y, para finalizar, a la Universidad Nacional junto con los docentes que han sido parte de mi formación profesional.

Ericka Acuña Durán

Este trabajo lo dedico a Dios, por guiar cada uno de mis pasos, cuidarme, darme salud y fortaleza para lograr mis objetivos y concluir con retos que me he propuesto. A mi familia principalmente a Lidia Calvo, por apoyarme en cada decisión, por estar presentes en cada triunfo o caída que se ha presentado en mi vida, por enseñarme y fomentarme valores esenciales en la vida. A mis compañeras y amigas de proyecto, por su dedicación, paciencia y amor hacia este trabajo. Y a la Universidad Nacional y el Colegio Científico de Pérez Zeledón, por ser parte de mi formación Profesional.

Vanessa Varela González

Agradecimientos

En primer lugar, le agradecemos a Dios por su guía y fiel compañía durante todo este tiempo realizando el trabajo final de graduación. Agradecemos a nuestras familias por siempre estar con nosotras y por toda la motivación en momentos de crisis. A todas esos amigos, conocidos o personas que se cruzaron en nuestras vidas durante esta etapa muchas gracias por cada enseñanza.

También agradecemos infinitamente a cada profesor que ha sido parte de este proceso, pero esencialmente le agradecemos a la profesora Digna Valverde Fallas por cada consejo, apoyo incondicional y compañía durante todo el trayecto de trabajo final.

Finalmente, agradecemos a la Universidad Nacional por permitirnos estudiar en esta institución tan privilegiada. Agradecidas de poder decir que somos sello UNA.

Resumen

La presente investigación tiene como objetivo principal analizar oportunidades de mejora en la protección de la información en el Colegio Técnico Profesional San Isidro, mediante la identificación de los protocolos de seguridad en los procesos administrativos. Se aborda la necesidad de asegurar la privacidad, integridad y accesibilidad de los datos ante amenazas tanto internas como externas, en un entorno educativo cada vez más digitalizado. Mediante una metodología cualitativa, descriptiva y explicativa, se recopilan datos a través de entrevistas y listas de cotejo aplicadas al personal administrativo, con el objetivo de evaluar la situación presente de la seguridad de la información. Se reconocen varias debilidades, tales como la ausencia de políticas formales, carencia en la capacitación del personal y en la implementación de técnicas efectivas, como la autenticación múltiple o el respaldo de datos. El estudio propone una variedad de acciones de optimización como lo es la creación de políticas institucionales de seguridad de la información, digitalización segura de los documentos, fortalecimiento de los controles de acceso, el respaldo periódico de los archivos digitales y físicos y capacitaciones constantes para el personal administrativo. Asimismo, se recomienda crear un comité institucional que supervise y de seguimiento a la seguridad de la información. Se concluye que la seguridad de la información en las instituciones educativas es fundamental no solo para salvaguardar la información, sino también para asegurar la eficacia en las operaciones y procesos administrativos. Este trabajo ofrece recomendaciones prácticas para potenciar y fortalecer la gestión administrativa, ajustándose a las exigencias del entorno tecnológico actual.

Tabla de contenido

Índice de tablas

Índice de figuras

Índice de Apéndices

Lista de abreviaturas

MEP: Ministerio de Educación Pública

DRE: Dirección Regional de Educación

DREPZ: Dirección Regional de Educación de Pérez Zeledón

SGSI: Sistema de Gestión de Seguridad de la Información

CTPSI: Colegio Técnico Profesional San Isidro

CAIPAD: Centros de Atención Integral para Adultos con Discapacidad

CINDEA: Centros Integrados de Educación de Adultos

CAPÍTULO I

Pregunta de investigación

¿Cuáles son los protocolos de seguridad de la información en los procesos administrativos en las oficinas del Colegio Técnico Profesional San Isidro?

Objetivos

Objetivo General:

Analizar oportunidades de mejora en la protección de la información del Colegio Profesional San Isidro mediante la identificación de los protocolos de seguridad de la información en los procesos administrativos.

Objetivos Específicos:

1. Identificar el tipo de seguridad de la información utilizada en los procesos administrativos en las oficinas para el análisis de la eficacia de las medidas de seguridad existentes.
2. Evaluar el nivel de concientización y capacitación en seguridad de la información del personal administrativo con el fin de obtener información sobre el grado de conocimiento y comprensión sobre las políticas y prácticas de seguridad de la información.
3. Proponer medidas de protección de la información para el fortalecimiento de la seguridad en los procesos administrativos del Colegio Técnico Profesional San Isidro.

Introducción

El presente trabajo corresponde al informe de trabajo final de graduación titulado: Análisis de la seguridad de la información en los procesos administrativos en las oficinas del Colegio Técnico Profesional San Isidro. Esta investigación se desarrolla mediante la modalidad de proyecto en dos semestres.

La seguridad de la información tema de relevancia en la actualidad, se refleja como un conjunto de actividades o estrategias que se utilizan para mitigar riesgos o pérdidas de información, la ISO/IEC (2016), afirmo lo siguiente:

> Se podría definir como aquellos procesos, buenas prácticas y metodologías que busquen proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizada. Es necesario mantener la seguridad en los datos en un entorno digital cada vez más sensible.

El análisis de la seguridad de la información en los procesos administrativos se convierte en el motivo indagatorio debido al incremento de amenazas externas e internas que se reciben en los procesos administrativos donde se trabaja constantemente con datos e informaciones digitales.

Por otro lado, la presente investigación presenta diversos apartados, en los cuales se abarca información relevante y necesaria para cumplir con el objetivo planteado.

El primer apartado corresponde al Capítulo I, en el cual se encuentra información como la introducción, el planteamiento del problema, la pregunta de investigación, el objetivo general y específicos, así como la justificación, el contexto de la investigación y los antecedentes, tanto históricos, así como teóricos y metodológicos, donde se refleja la información principal del trabajo y base para poder darle continuidad.

El segundo apartado corresponde al Capítulo II, compuesto por el marco teórico que sustenta conceptualmente la investigación. Se examinan las teorías, modelos y conceptos

importantes que dan el fundamento necesario para comprender el problema de estudio y formular hipótesis. Se exploran las investigaciones previas y la literatura existente en el área temática, identificando los principales pensamientos y enfoques teóricos que surgen en el desarrollo del campo de estudio.

El tercer apartado corresponde al Capítulo III, compuesto por el marco metodológico que guía el proceso de investigación. En este se describe el enfoque general que se utiliza para abordar el problema de estudio, así como el tipo de investigación se aplica. Además, se describen las técnicas de control que se emplea para garantizar la validez y confiabilidad de los resultados, junto con el instrumento que se utilizan para recopilar la información necesaria.

Planteamiento del problema

En un mundo globalizado, en el ámbito de los procesos administrativos la información digital, enfrenta problemas como los robos o pérdida de información, por falta de seguridad. El tema de la seguridad de la información es crucial, especialmente en un mundo digitalizado, es fundamental promover el conocimiento del tema. En las oficinas de las instituciones, la información y los datos digitales son confidenciales dentro de las organizaciones.

En la actualidad, se presentan múltiples problemas como la falta de capacitación, ausencia de ciberseguridad, accesos no autorizados y deficiencia en las políticas de seguridad. Como consecuencia, las instituciones enfrentan amenazas, como la divulgación, la pérdida, y el robo de información que puede causar grandes problemas para las instituciones, como daños en la reputación o pérdida de credibilidad en la sociedad.

Generalmente no se presta la atención necesaria a la ciberseguridad y a las políticas de seguridad, por esto se crean problemas con el manejo de la información debido a que, en la mayoría de los casos, dicha información no se encuentra respaldada, ni en otro dispositivo tal

como en una computadora, laptop o tableta electrónica, ni en mecanismos de almacenamiento como llave maya, disco duro o demás dispositivos, dando así como resultado la pérdida de información que puede resultar importante para cualquier entidad.

Además, existe información como los expedientes de los funcionarios que pueden ser eliminados, no archivados adecuadamente o que no tiene respaldo lo cual genera un impacto negativo, porque se pierden datos importantes, como por ejemplo la documentación de los funcionarios que se jubilan, personal que se trasladan del centro educativo, cuando se incapacitan o en casos extremos cuando fallecen, existe desconocimiento acerca de cómo proteger esa documentación; siendo datos importantes es relevante resguardarlos y reforzar los procesos que se utilizan.

Por lo mencionado, esta investigación es relevante en el campo empresarial, se tiene como finalidad identificar la problemática que enfrentan las oficinas, al momento de incorporar la seguridad a la información que se maneja digitalmente, además, es importante resaltar que toda empresa debe salvaguardar la información, otro aspecto relevante es que en el momento de implementar las medidas de seguridad lo ideal es realizar estos procesos con precaución, manteniendo así siempre la información a salvo.

Antecedentes:

Los antecedentes de la investigación se desarrollan en 3 enfoques, históricos, teóricos y metodológicos, relacionados con la seguridad de la información en los procesos administrativos de la oficina, donde en cada uno de los aspectos se menciona información relevante para el entendimiento al tema expuesto.

Antecedentes históricos

En este apartado se detallan antecedentes históricos, para conocer sobre la historia del Colegio Técnico Profesional San Isidro, así como del Ministerio de Educación Pública (MEP) y la Dirección Regional de Educación (DRE), se consulta en las páginas la siguiente información:

Como parte integral de la calidad en la educación, el MEP, creado el 10 de agosto de 1949, se encarga de la infraestructura educativa a nivel nacional. Ante el desarrollo de procesos cambiantes del sistema educativo, son significativos ante las necesidades de dotar espacios educativos, así como el mobiliario requerido según la modalidad educativa, brindando una mejor calidad, pero con la clara consigna de la maximización de los recursos económicos disponibles anualmente en el presupuesto nacional.

Dirección Regional de Educación. Las Direcciones Regionales de Educación (DRE), se establecen para organizar geográficamente la prestación de servicios de educación y facilitar la atención de las comunidades educativas. Por lo anterior, se han conformado un total de 27 DRE, distribuidas en las diferentes provincias del país.

Circuitos de Dirección Regional de Educación de Pérez Zeledón. La DREPZ, se divide en circuitos escolares, con un total de 10 circuitos que están conformados por diferentes centros educativos, como se detallan:

Tabla 1

Cantidad de instituciones que se encuentran en los circuitos de la DREPZ

N° Circuito	Cantidad de instituciones
01	28
02	37
03	21
04	33
05	29
06	23

07	26
08	30
09	23
10	17

Asimismo, se centra en el Circuito 03 que está conformado por 21 instituciones, estas son: Escuela Lourdes, Los Ángeles, Escuela IDA Jorón, Escuela Las Lagunas, Escuela Las Juntas de Pacuar, Escuela Villa Ligia, Escuela La Aurora de Pérez Zeledón, Escuela Laboratorio Daniel Flores, Escuela San Francisco de Asís, Escuela Daniel Flores Zavaleta, Escuela La Repunta, Escuela El Peje de Pérez Zeledón, Escuela Quebrada Honda, Escuela Hernán Rodríguez, Unidad Pedagógica José Breinderhoff, Colegio Nocturno de Palmares, Liceo Fernando Volio, Centros de Atención Integral para Adultos con Discapacidad (CAIPAD), Bilingual Multidisciplinary School (BMS), Cindea San Francisco- Cocori y por último Colegio Técnico Profesional San Isidro donde llevará cabo el proyecto.

Colegio Técnico Profesional San Isidro. El Colegio Técnico Profesional San Isidro fue fundado en 1974, durante la administración de José Figueres Ferrer, cuando era Ministro de Educación el señor Uladislao Gámez. Nace como Liceo de Tercer Ciclo en el año 1974, bajo la dirección del Profesor Carlos Francisco Vega Soto, con secciones de sétimo únicamente y una matrícula de 189 estudiantes, ocupaba las instalaciones de la Escuela Pedro Pérez Zeledón.

Para el año 1975 se contemplan los niveles de III Ciclo, con una matrícula de 364 alumnos. En 1976, después de varias gestiones realizadas por su director Profesor Marco Tulio Arias Álvarez, el ministro de Educación Pública transforma el Liceo en un Colegio Técnico, de modalidad industrial con tres especialidades: Secretariado-Comercial, Contabilidad y Electromecánica.

Hasta noveno año se cumple el Plan de Estudios y a partir de décimo nivel se escoge la especialidad respectiva.

El Colegio Técnico Profesional de San Isidro pertenece al Circuito 03. Actualmente, se encuentran aprobadas las siguientes especialidades: Contabilidad, Contabilidad y Finanzas, Diseño Gráfico, Electromecánica, Informática en Desarrollo de Software, Mecánica de Precisión, Secretariado Ejecutivo, Gerencia y Producción de Cocina, Operación de Empresas de Alojamiento y Desarrollo de Aplicaciones Móviles

Antecedentes teóricos

En un artículo original elaborado por Vega (2008) que tiene por título Políticas y Seguridad de la Información explica que seguridad significa disponer de medios que permitan reducir lo más que se pueda, la vulnerabilidad de la información y de los recursos; aunque no se puede alcanzar el 100% de seguridad, la tendencia debe ser llegar a ese valor extremo.

En el mismo artículo original, por Vega (2008) menciona que:

> Las facilidades para conectarse a las redes han aumentado; además, las aplicaciones y el software son cada vez más amigables y accesibles, de esto modo todos tienden a conectarse en una red para compartir los recursos, pero esa facilidad de conexión también representa un aumento en los riesgos de que la información y los recursos de una organización puedan ser vulnerados.

Por otra parte, en una investigación, que lleva por título Asistente Virtual en el Sistema de Gestión Seguridad de la Información para Gestor de Base de Datos ORACLE realizada por Alvarado, et. al. (2019) Indagan que las organizaciones cada día dependen más de los sistemas informáticos, la mayoría de las empresas dependen de sistemas de información que gestionan los datos, es decir, la información más valiosa que tiene la compañía. Resguardar dicha información aumenta el espectro de riesgos a la que se ve expuesta: atacantes informáticos, robo, destrucción, filtración o extorsión por información confidencial son algunos ejemplos de los riesgos a los que se expone la información.

Antecedentes metodológicos

Metodológicamente se cuenta con una investigación enfocada en la Seguridad de la Información, del autor Vega (2021), en este libro se abordan temas muy relevantes, como conocer qué es la seguridad de la información, aspectos como la importancia de la confidencialidad, integridad y la disponibilidad, el control, la autenticidad y utilidad, los tipos de amenazas, ataques, aquellas vulnerabilidades, los riesgos, entre otros, la metodología se basa en recopilar información de fuentes secundarias. Sin embargo, por otro lado, se asegura que otra de las formas eficientes de recolectar información es por medio de fuentes primarias, es decir, mediante la aplicación de encuestas y entrevistas.

Una forma eficiente de obtener información verídica es por medio de fuentes primarias, que brindan que seguridad que la información es real y actualizada, lo que otorga credibilidad a lo investigado, con el respaldo de fuentes secundarias para desarrollar y cumplir con todos los objetivos planteados. Se cuenta con una investigación que se titula Propuesta de un Sistema de Gestión de la Seguridad de la Información para organizaciones en Costa Rica, por el autor Roldán, et. al. (S.f) y señala que Costa Rica existen organizaciones que no cuentan con sistemas de seguridad para sus dispositivos, arriesgando la información, carecen de indicaciones claras de cómo proteger la información, la cual queda dispersa y vulnerable.

De igual forma por Roldán, et. al. (S.f) en este mismo artículo menciona que la implementación de una política de seguridad de la información puede controlar la seguridad de las terminales y sistemas, porque todo se encuentra correctamente asegurado y respaldado. Para reducir los riesgos, toda empresa u organización debe contar con un Sistema de Gestión de Seguridad de la Información (SGSI) basado en alguna norma técnica.

Justificación

El propósito del estudio es analizar los protocolos de seguridad de la información en los procesos administrativos en las oficinas del Colegio Técnico Profesional San Isidro, periodo 2024.

La investigación se realiza porque la seguridad de la información juega un papel vital en los procesos administrativos en las oficinas de las empresas, la información constituye uno de los recursos importantes de las instituciones. Actualmente, las instituciones carecen de seguridad en sus datos e informaciones digitales, por esta razón la necesidad de conocer el tema, para aprender y capacitarse, y así evitar consecuencias a futuro, que puedan perjudicar a las empresas a corto o largo plazo, dependiendo del nivel de confiabilidad de la información que se mantiene digitalmente en los diferentes dispositivos electrónicos.

Con el avance de la tecnología, la implementación de dispositivos electrónicos y su conexión a redes plantea el riesgo de robo de datos o información, debido a esto nace la sed en la segunda mitad del siglo XX, para proteger datos e informaciones, y evitar ataques digitales, por lo que Ospina y Sanabria (2020) mencionan que:

> La Ciberseguridad se enfoca entonces en la protección de la infraestructura computacional y de la información circulante en las redes informáticas. La implementación de la ciberseguridad en las organizaciones ayudará a proteger estos datos, mitigando posibles riesgos de ataques o robos a la información.

La seguridad de la información ha transformado el ámbito de las instituciones, fomentando a que se integren técnicas o procedimientos que contribuyan a garantizar la seguridad y confiabilidad de los datos en los sistemas de información, para evitar robos o perdidas que perjudiquen la información digital que se manejan en los procesos administrativos en las oficinas de las instituciones.

Se requiere conocer la seguridad que mantiene la institución para resguardar sus datos, tema crucial para garantizar que la información sensible esté protegida de accesos no autorizados, que permitan a la empresa mantener confiabilidad en sus informaciones.

La importancia social de la investigación radica principalmente en que, más allá de las instituciones y empresas, la sociedad en general debe comprender que, como individuos, su información o datos también están expuestos al robo a través de dispositivos electrónicos como laptops, teléfonos celulares o tabletas. El conocimiento de que es posible implementar estrategias para mitigar el robo de información personal resulta relevante para la protección de la privacidad en la vida cotidiana.

Las instituciones se benefician de este estudio porque les permite visibilizar la importancia de mantener seguridad en la información, fomentando la confiabilidad, integridad, y estrategias para proteger la información contra amenazas externas e internas, para mitigar riesgos, minimizar pérdida de datos o daños a la organización. Además, con la implementación de medidas de seguridad efectivas se fortalece la eficiencia operativa, para aumentar la confianza del personal, funcionarios y demás representantes pertenecientes a la institución, dando como resultado el cumplimiento con las regulaciones y estándares de seguridad que cada vez son más estrictos.

Contexto de la investigación

La institución donde se desarrolla la investigación es el Colegio Técnico Profesional San Isidro donde se tiene como objetivo principal analizar la seguridad de la información en los procesos administrativos, además la importancia de realizar este estudio radica en la necesidad de garantizar confidencialidad, integridad y la disponibilidad de toda la información que se maneja en las oficinas de esta institución educativa.

Se busca analizar los protocolos de seguridad de la información implementados en sus procesos administrativos. Este enfoque se origina en la necesidad de salvaguardar la

integridad, confidencialidad y disponibilidad de los datos manejados en las oficinas de la institución, en un entorno cada vez más digitalizado y vulnerable a amenazas cibernéticas.

Uno de los aspectos más importantes es que cuando se hace referencia a la seguridad de la información, se debe tomar en cuenta la creciente amenaza que existe en ciberataques, robos o pérdida de información y por lo que nace una la necesidad de proteger los datos sensibles de la institución. A través de este análisis, se busca identificar posibles vulnerabilidades en los procesos administrativos y con ello proponer medidas de seguridad efectivas para mitigar los riesgos y proteger la información del Colegio Técnico Profesional San Isidro.

Este estudio se justifica por la importancia de proteger la información sensible del colegio, evitar posibles riesgos y garantizar la confiabilidad de los datos. La investigación no solo beneficia a la institución en términos de seguridad y eficiencia operativa, sino que también contribuye al desarrollo de un entorno seguro y consciente en el ámbito educativo.

Viabilidad de la investigación

La investigación se enfoca en el análisis de la seguridad de la información en los procesos administrativos. Dicho proyecto es viable puesto que se cuenta con la aprobación de la administración del del Colegio Técnico Profesional San Isidro, ubicado en San Isidro de El General, la cual acepta brindar la información necesaria para alcanzar los objetivos planteados.

Por otro lado, al ser un tema de relevancia existe información documental acerca de este, la cual también podrá que puede ser utilizada para generar bases sólidas acerca del análisis de la seguridad de la información, siendo así aspectos claves para el entendimiento del tema y su correcto desarrollo durante el proceso de investigación.

Se realiza un proceso formal con el propósito de garantizar la aceptación institucional por parte del Colegio Técnico Profesional San Isidro, asegurando que el apoyo brindado por

dicha entidad quede debidamente documentado y formalizado. La información fue recopilada por medio de diferentes métodos, como las fuentes primarias utiliza instrumentos como encuestas aplicadas a funcionarios de la institución. También se utiliza fuentes secundarias, como libros, artículos, revistas y documentos propios de la institución.

CAPÍTULO II

Marco teórico

El marco teórico brinda la posibilidad de presentar y demostrar información relevante para la investigación y el problema de estudio. Asimismo, su relevancia radica en informar sobre conceptos que contribuyan al conocimiento durante la investigación.

Contexto Organizacional

El contexto organizacional se refiere a la identificación de las organizaciones involucradas en la investigación, proporcionando información sobre ellas, tales como su historia, principales actividades y los departamentos con los que cuenta. Conocer estos datos es fundamental, ya que ofrece una perspectiva amplia sobre las instituciones.

El contexto organizacional permite conocer el entorno en que una institución opera, reconociendo muchos factores, como lo es la cultura, su estructura organizativa. Según Navarro (2020, p. 4). “El contexto de la organización es una combinación de cuestiones internas y externas que pueden tener un efecto en el enfoque de la organización para el desarrollo y logro de sus objetivos”.

A continuación, se proporcionan reseñas históricas e información relevante sobre las instituciones: Ministerio de Educación Pública, Dirección Regional y el Colegio Técnico Profesional San Isidro, con el objetivo de ubicar al lector dentro del contexto pertinente.

Ministerio de Educación Pública

Como parte integral de la calidad de la educación, el Ministerio de Educación Pública (MEP), creado el 10 de agosto de 1949, es responsable de la infraestructura educativa en todo el país. Con el desarrollo de los procesos cambiantes del sistema educativo, los principales problemas relacionados con las necesidades de garantizar los espacios educativos, así como el mobiliario necesario de acuerdo con el método educativo, con la finalidad de mejorar la calidad educativa, pero procurando optimizar el uso de los recursos económicos anuales disponibles en el presupuesto nacional.

Actualmente, el MEP tiene un sistema educativo que ofrece diferentes modalidades entre ellas se encuentra la Primera Infancia, I y II ciclo, III Ciclo y Educación Diversificada, Educación Técnica, Educación Intercultural, Educación Religiosa, Personas Jóvenes y Adultas, Colegio Marco Tulio Salazar, Bachillerato por Madurez, Colegios Científicos y Colegios Humanísticos.

Además, el Ministerio de Educación Pública se conforma por diferentes Direcciones Regionales, divididas en las siete provincias del país.

Dirección Regional de Educación

Las Direcciones Regionales de Educación (DRE), se establecen para organizar geográficamente la prestación de servicios de educación y facilitar la atención de las comunidades educativas. En el país existen 27 direcciones regionales de educación.

Tienen como principio orientador, el reconocimiento de la educación como derecho fundamental de todos los habitantes del país, a cuya satisfacción asisten el Estado, la familia y la comunidad para la obtención de los fines establecidos en la Ley Fundamental de Educación.

Dirección Regional de Pérez Zeledón (DREPZ)

Fue creada un 23 de enero de 1980, cuando sale publicado el decreto de creación y tiene la responsabilidad de toda la Zona Sur. Sin embargo, por el crecimiento, con los años, se crean dos regionales más en la Región Brunca y está incluye el cantón de Pérez Zeledón.

Se encarga de coordinar, supervisar y apoyar el desarrollo del sistema educativo en los centros educativos ubicados en el cantón de Pérez Zeledón y sus alrededores. Su labor se enfoca en garantizar la correcta implementación de las políticas educativas nacionales, brindar acompañamiento técnico y administrativo a las instituciones, y promover procesos de mejora continua en la calidad de la educación. Además, impulsa la formación profesional del

personal docente y administrativo, y vela por el cumplimiento de los objetivos educativos establecidos por el (MEP) en la región.

Circuitos de Dirección Regional de Educación de Pérez Zeledón

Un circuito se constituye como la unidad básica de supervisión integrada dentro de un área geográfica y es una estrategia organizacional de la gestión escolar.

En cada circuito hay un supervisor el cual se encarga de atender consultas y denuncias realizadas por las comunidades educativas del circuito, asimismo, colaborar y respaldar las visitar colegiadas, orientar a los directores en la adecuada comprensión de la política educativa, planes, presupuesto, programas y las normativas emitidas, también debe de supervisar las visitas a los centros educativos y realizar reuniones mensuales de coordinación con los directores que se encuentran a su cargo y asegurar que se mantenga un registro de actas que incluya la agenda, asistencia, temas abordados y los acuerdos alcanzados, entre otros. Además, el supervisor cuenta con un asistente algunas de las funciones principales de este son: colaborar en las tareas de asesoría y supervisión, también, participa en la creación de estadísticas relacionadas con la matricula, promoción, deserción escolar, asimismo se encarga de divulgar los resultados obtenidos en el estudio. Otras de sus funciones es elaborar informes, circulares, cartas, memorandos y otros documentos relacionados

La DREPZ se divide en 10 circuitos escolares, conformados por centros educativos, además como se menciona en el Ministerio de Educación Pública (S.f, párr. 3). “Los circuitos, cumplen con la función de mejorar la organización, administración y supervisión de la Política Educativa vigente, con el fin de mejorar la calidad del sistema educativo costarricense”

Se centra especialmente en el Circuito 03, conformado por 21 instituciones dentro de las cuales se encuentra el Colegio Técnico Profesional San Isidro. En cada circuito se

encuentran centros educativos como; escuelas, secundarias, liceos rurales, Ambientalistas, CINDEA y Técnicos Profesionales.

Colegio Técnico Profesional San Isidro. El Colegio Técnico Profesional San Isidro (CTPSI) pertenece al Circuito 03, fue funda en 1974, durante la administración de José Figueres Ferrer, cuando era Ministro de Educación el señor Uladislao Gámez. Nace como Liceo de Tercer Ciclo en el año 1974, bajo la dirección del Profesor Carlos Francisco Vega Soto, con secciones de sétimo únicamente y una matrícula de ciento ochenta y nueve alumnos. Ocupaba las instalaciones de la Escuela Pedro Pérez Zeledón.

En 1975, se completan los tres niveles de tercer ciclo con una matrícula de trescientos sesenta y cuatro alumnos. En esta época funge como director el profesor Marco Tulio Arias Álvarez.

En 1976, el Ministerio de Educación Pública, transforma el Liceo de Tercer Ciclo en un Colegio Técnico Profesional de modalidad Industrial con tres especialidades: Secretariado Comercial, Contabilidad y Electromecánica. Hasta noveno año, el plan de estudios es académico y a partir de décimo año el estudiante tiene la posibilidad de elegir una especialidad técnica.

En 1977 la matrícula aumenta a novecientos siete alumnos, lo que genera la necesidad de conseguir un terreno apropiado para construir un nuevo edificio.

Después de varias gestiones, don Jorge Halder Lacher por medio de la Asociación Shuraben, dona un terreno de tres manzanas, el cual se ubica en Villa Ligia a tres kilómetros de la ciudad de San Isidro de El General. Mismo que se utiliza para construir la planta física del centro educativo. La construcción inicia en el año1979 y culmina en 1980, la compañía Ingesur es la responsable de la construcción de la planta física.

El Colegio Técnico Profesional San Isidro cuenta con una población de 1325 estudiantes y el personal lo conforman 158 personas divididos en administrativos, profesores,

cocineras, guardas, personal de limpieza y mantenimiento, entre otros. Como se muestra en las siguientes tablas.

Tabla 2

Población estudiantil del CTP San Isidro.

Grado Académico	Hombres	Mujeres	Total
7º	104	102	206
8º	102	101	203
9º	87	87	174
10º	89	100	189
11º	71	72	143
12º	71	60	131
Total	666	686	1325

La Tabla 2 muestra la distribución del estudiantado del colegio según grado académico y género, con un total de 1325 alumnos, donde se observa una mayor representación femenina. Este desglose no solo permite analizar la composición demográfica de la población estudiantil, resulta útil para la planificación institucional en aspectos como asignación de recursos, diseño de políticas inclusivas y estrategias de comunicación. Conocer el perfil de los estudiantes ayuda a dimensionar el volumen y tipo de información que se gestiona, reforzando la importancia de implementar medidas efectivas para proteger los datos personales y académicos en los sistemas administrativos del colegio.

Tabla 3

Cantidad de secciones que hay en el CTP San Isidro.

Grado Académico	Cantidad de secciones
7º	6
8º	6
9º	5
10º	6
11º	6
12º	4
Total	33

La Tabla 3 refleja el número de secciones por nivel académico en el colegio, abarcando desde sétimo hasta duodécimo año, con un total de 33 secciones. Esta información no solo permite comprender la estructura académica de la institución, sino que también resulta clave para dimensionar la infraestructura necesaria para atender esa población estudiantil. Aulas, laboratorios, recursos tecnológicos y administrativos deben responder a esta distribución, lo cual tiene una relación directa con el volumen de información que se maneja. Por tanto, su inclusión en el estudio es fundamental para evidenciar la magnitud del flujo de datos y la necesidad de contar con sistemas seguros que garanticen una gestión eficiente de la información en los procesos académicos y administrativos.

Tabla 4

Matrícula inicial en técnica diurna según modalidad y especialidad en el CTP San Isidro.

Modalidad y especialidad	Total
Comercial y de Servicios	
Contabilidad	71
Contabilidad y Finanzas	64
Desarrollo de aplicaciones móviles	20
Gerencia y Producción en cocina	20
Informática en Desarrollo de Software	16
Mercadeo	13
Operaciones de Empresas de Alojamiento	55
Secretariado Ejecutivo	84
Turismo en Alimentos y Bebidas	32
Industrial	
Diseño Gráfico	30
Electromecánica	30
Mecánica de Precisión	28
Total	463

La Tabla 4 muestra la inscripción inicial en las distintas modalidades y especialidades técnicas diurnas del colegio, con un total de 463 alumnos. Este desglose permite identificar las áreas de mayor demanda estudiantil y facilita una planificación más eficiente de los recursos académicos. Además, evidencia la gran cantidad de datos que se gestionan desde el inicio del curso lectivo, lo que resalta la importancia de contar con sistemas adecuados para el manejo, protección y resguardo de la información estudiantil.

Tabla 5

Cantidad de personal Administrativo en el CTP San Isidro.

Puesto	Cantidad de personal administrativo
Director	1
Subdirectora	1
Asistente de Dirección	1
Oficinista	3
Bibliotecaria	1
Auxiliares Administrativas	3
Coordinadores	6
Guardas de seguridad	6
Mantenimiento	5
Orientación	4
Personal de limpieza	7
Total	98

La Tabla 5 presenta el desglose del personal administrativo del colegio, que suma un total de 98 colaboradores distribuidos en diferentes puestos. Es esencial para observar la capacidad operativa del colegio, su funcionamiento y distribución del personal administrativo.

Tabla 6

Cantidad de docentes que hay en cada una de las asignaciones.

Asignatura	Cantidad de docentes
Ciencias	8
Diseño gráfico	5
Educación especial	17
Educación física	5
Educación musical	2
Educación Religiosa	2
Electromecánica	3
Español	4
Estudios Sociales y Cívica	7
Francés	3
Informática	5
Inglés	14
Matemática	6
Mecánica de Precisión	2
Psicología	1
Secretariado	6
Turismo	8
Total	98

La Tabla 6 presenta la distribución del personal docente en el colegio, con un total de 98 profesores asignados a distintas áreas académicas y técnicas. Más allá de identificar las asignaturas que se imparten, esta información evidencia el amplio flujo de datos que se maneja dentro de la institución. Esta dinámica resalta la importancia de implementar medidas

adecuadas para proteger la información, garantizando su confidencialidad, integridad y disponibilidad en todo momento.

Fundamentación Teórica

En esta sección, se establece el fundamento de la teoría cuya finalidad es adquirir información relevante sobre el tema para expandir el conocimiento y orientar el proceso de estudio.

> El marco teórico es uno de los elementos más relevantes en la investigación, menciona que el marco teórico del estudio, proyecto y/o tesis que se esté llevando a cabo detalla los modelos teóricos, conceptos, argumentos e ideas, investigaciones y antecedentes, en general, que se han desarrollado en relación con el tema de que se trate. (Rivero, 2021, p. 7).

Procesos Administrativos

Estos procesos son actividades coordinadas en las oficinas de las instituciones, cuya finalidad es alcanzar los objetivos, son fundamentales para el funcionamiento eficaz dentro de la organización.

Se trata de un conjunto de etapas con una secuencia determinada, a partir de ellas se logra una adecuada administración, lo que permite un desempeño eficiente, así como el mantenimiento del orden, la seguridad y el control dentro de las organizaciones.

El proceso administrativo es fundamental en cualquier organización, busca alcanzar los objetivos de manera eficiente, y de la manera óptima posible, según, Cano (2017, p. 24). “El proceso administrativo busca armonizar estos elementos; planeando acciones, organizando las cosas, integrando recursos, ejecutando tareas, ordenando y controlando resultados, proceso y fundamentalmente generando mecanismos de comunicación para dar a conocer sus ideas”

Estos procesos proponen una estructura coherente dentro de las organizaciones, fomentan las decisiones informadas y al mismo tiempo reconocer necesidades de cambio empresariales.

Con los procesos administrativos, se busca que las organizaciones entiendan la importancia del éxito empresarial, a largo plazo, frente al mercado, también para Cano (2017), “las organizaciones deben prepararse para la adaptación rápida y eficiente a los avances tecnológicos, preferencias del cliente, exigencias del mercado, la competencia, las variaciones macro y microeconómicas. Esto implica disposición al cambio” (p. 25).

> También, se obtiene como resultado, los diferentes momentos del proceso administrativo deben ser dependientes, armónicos, coherentes, equilibrados y complementarios entre sí, que garanticen logros, mejoramientos, cambios y desarrollo. Por esos se llaman etapas, pero secuenciales, para que no se corra el riesgo de desarticularlas (Cano, 2027, p. 26).

Por lo tanto, el proceso administrativo busca facilitar el logro de objetivos, impulsar mejoras continuas y promover un desarrollo eficiente, al mismo tiempo que minimiza los riesgos asociados a su ejecución.

Seguridad de la información

La seguridad de la información juega un papel de suma relevancia frente a las administraciones de las empresas en las oficinas encargadas de los procesos administrativos, ya que están presentes buscando la protección de los datos e informaciones que se manejan, frente a amenazas, o accesos no autorizados.

> Rocha (2011) menciona que “en una definición más amplia, un programa de seguridad de la información es un plan para mitigar los riesgos asociados con el procesamiento de la información y el uso de los recursos que lo soportan” (p. 29).

Siendo la seguridad un elemento esencial en los procesos administrativos de las oficinas para mantener salvaguardada la información, con menos probabilidades de sufrir robos o pérdidas que jueguen con la integridad y confiabilidad de los datos de la organización.

La información es un elemento importante en las organizaciones independientemente del tamaño o sector, porque en las oficinas se maneja información confidencial, de clientes, estudiantes, empleados, proveedores, esto dependiendo de la organización, por lo que Rodríguez (2010) expresa que "la seguridad de la información tiene una significativa relevancia corporativa porque tiene como objetivo proteger un activo extremadamente importante y porque existe una amplia regulación que obliga a las compañías a proveer seguridad de la información" (p. 7).

La seguridad de la información es un concepto que cada vez se involucra más con los aspectos de una sociedad hiperconectada, como lo expresa Vega (2021).

> Es gran parte como resultado de la adopción casi ubicua de la tecnología de información y comunicación, la seguridad de la información se vuelve parte de la vida cotidiana de las personas, puesto que, una de las principales herramientas son las computadoras, laptops, celulares y demás, en los cuales se almacena información relevante y aunque la tecnología permite ser más productivos y acceder a una gran cantidad de información con solo un clic, también conlleva una gran cantidad de problemas de seguridad. (p. 9).

Con problemas de seguridad lo ideal es realizar la búsqueda de herramientas o técnicas que ayuden a proteger los datos y recursos de infraestructura tecnológica de aquellos quiénes intentarían hacer un mal uso de estos, o en otros casos únicamente puede presentarse la pérdida de dicha información, según Flores y Caiza (2017).

> Mantener la seguridad de la información y proteger los activos de datos sigue siendo una preocupación principal para las organizaciones, muchas violaciones de datos continúan siendo accidentales, intencionales o maliciosos. Factores humanos, que conducen a pérdidas financieras o de reputación. (p. 4).

Pese a los esfuerzos en seguridad, las organizaciones siguen siendo vulnerables a incidentes provocados principalmente por errores o conductas humanas. Esto subraya la necesidad de fortalecer la capacitación del personal y aplicar medidas preventivas para reducir riesgos financieros y reputacionales.

Importancia de la seguridad de la información

Las empresas dependen cada vez más de la tecnología para procesar información, porque constantemente se manejan gran cantidad de datos sensibles y que requieren seguridad, con el fin que no sean robados o expuesto por personas maliciosas, razón por la que es importante que la información tenga seguridad, para evitar que sea comprometida, alterada o robada. Rodríguez (2010), afirmó lo siguiente:

> La información es valiosa debido a que, en primer lugar, cierta información representa intrínsecamente dinero, por ejemplo, la propiedad intelectual. En segundo término, la información es la materia prima para tomar decisiones, un activador de negocios sin el cual muchas organizaciones simplemente no podrían funcionar. (p. 8).

La seguridad de la información debe ser un tema prioritario, ya que la información en las organizaciones constituye un activo esencial. Por ello, es necesario asegurar su protección para evitar consecuencias negativas, garantizar un alto nivel de resguardo y preservar la integridad de los datos sensibles. En un mundo altamente digitalizado, la seguridad se convierte en un componente clave para la estabilidad y confianza institucional.

Principios fundamentales de la seguridad de la información

Actualmente la seguridad de la información cuenta con principios fundamentales para asegurar el cuidado y la protección de información sensible, estos principios trabajan en conjunto para garantizar que la seguridad de la información esté protegida de amenazas y riesgos que la rodean constantemente.

Como lo menciona Vega (2021), “tres de los conceptos principales en seguridad de la información son precisamente la confidencialidad, integridad y disponibilidad, comúnmente conocida como la tríada de la seguridad de la información” (p. 12).

Existiendo tres elementos o principios básicos que la concretan:

Integridad. La integridad en los datos permite reconocer que la información presente sea verídica y no haya sido alterada, lo cual permite mantener la precisión, como lo menciona Rocha (2011) “este principio asegura que la información sea exacta, completa, sin alteraciones o modificaciones en su contenido, efectuada por usuarios o procesos no autorizados. Una información podrá cambiar tanto en su sentido como en el ambiente que lo soporta” (p. 29).

Con la integridad presente se puede evitar la falsificación de documentos, o la alteración de estos, la integridad de la información se logra con medidas que ayudan a reconocer la integridad del documento o de la información, como la validación de la firma digital. En ocasiones ayuda a verificar la validez de esa información. Vega (2021), dice que “con el fin de prevenir cambios no autorizados, tales sistemas a menudo implementan permisos que restringen las acciones que un usuario no autorizado puede realizar en un archivo determinado” (p. 13).

La integridad también es la condición que garantiza que la información sólo puede ser modificada, incluyendo su creación y borrado, por el personal autorizado. Garantiza que la información sea exacta y completa y que el sistema no modifique o corrompa

la información o permita que alguien no autorizado lo haga. (García y Vidal, 2016, p. 51).

Confidencialidad. La confidencialidad, permite que los encargados de la documentación mantengan los datos con protección, garantizando que personas ajenas no accedan a ellos, ya que se trabaja con información sensible que no pueden ser expuestas o manipulada por terceras personas.

Rocha (2011), explica que tiene como propósito prevenir el uso no autorizado de la información, por personas no facultadas para tal efecto. Eso significa que estos datos deben ser conocidos sólo por un individuo o grupo controlado de personas, definidos por el responsable de la información. La privacidad es un tema estrechamente relacionado con este elemento, consiguiéndose últimamente un mejor entendimiento sobre su aplicación (p. 29).

La confidencialidad en las organizaciones garantiza la privacidad de los datos e informaciones personales que maneja dicha empresa, y del mismo modo cumplir con las regulaciones de privacidad, mostrando confianza a sus clientes o a la población en general que la constituye.

Disponibilidad. La disponibilidad garantiza el acceso y empleo de los recursos informáticos en cualquier momento cuando las personas lo requieran y con la respectiva autorización, un sistema debe permanecer seguro y mantener la información disponible para los usuarios, como lo menciona García y Vidal (2016) la disponibilidad significa que “el sistema, tanto hardware como en software, funciona de forma eficiente y es capaz de recuperarse rápidamente en caso de fallo” (p. 51).

Entonces, la disponibilidad permite que las organizaciones tengan acceso a la información que se maneje, es decir, que la información se mantenga disponible y funcional en todo momento cuando sea requerida. Se busca garantizar que no sea objeto de ataques que comprometan su accesibilidad o interfieran con su uso adecuado, por lo que Rocha (2011)

también menciona que “este principio asegura que los usuarios tengan acceso oportuno y fiable a sus recursos de información, permitiendo de esta forma la continuidad del negocio” (p. 29).

Con la disponibilidad presente, se espera que las organizaciones eviten los accesos no autorizados, que puedan afectar la productividad y hasta consecuencias como el robo de información.

> El entendimiento de estos tres principios básicos es fundamental en el desarrollo e implementación de toda política de seguridad, a la vez que confluyen en la idea de proteger la información como un recurso del negocio y otorgarle el posicionamiento estratégico que se merece” (Rocha, 2011, p. 29).

Además, dichos elementos básicos pueden ser reforzados con otra tríada, como lo expone Vega (2021) compuesta por el control, la autenticidad y la utilidad, ayudando así a obtener bases sólidas que concreten la seguridad de la información.

Control. El control de disponibilidad de la información tiene como objetivo asegurar que los datos se mantengan accesibles y protegidos ante cualquier eventualidad.

Este se enfoca en la disposición física de los medios en los que se almacenan los datos, por lo que el control permite que haya diferentes dispositivos donde se puedan encontrar los mismos datos, es decir que, no debe de existir temor en perder información relevante, puesto que esta se encuentra respaldada en otro dispositivo (p. 14).

Son aquellas medidas que se implementan para garantizar la correcta seguridad de información de una organización, este tipo de control o controles está especialmente diseñado para proteger la confidencialidad, integridad y disponibilidad de la información y activos. En algunos casos como lo expresa Sisti (2019), se pueden utilizar controles como:

Contraseñas: Ya que en su mayoría permiten distinguir entre los usuarios autorizados y los no autorizados para ingresar al sistema (p. 52).

Pista de auditoría: Consiste en un rastro o registro generado por el sistema informático que muestra el historial de las operaciones, por lo que permite su reconstrucción y llegar al documento de origen siguiendo el camino hacia atrás de los procesamientos. (p. 53).

Backup y recuperación: Cuando se poseen archivos cuyos datos se desean preservar o salvaguardar se realiza una copia de seguridad denominada backup. Esta copia se hace en un medio de almacenamiento distinto al que contiene los datos copiados. (p. 53).

Criptografía: consiste en ocultar lógicamente la información a través de técnicas matemáticas que utilizan algoritmos para transformarla en secuencias de bits ininteligibles para los usuarios no autorizados. (p. 53).

En resumen, el control trata de salvaguardar la información, protegerla, mitigar todos los riesgos posibles, evitar aquellas amenazas potenciales hacia una organización, con la implementación de medidas que faciliten el proceso.

Autenticidad. La autenticidad es la coherencia personal que tienen las personas y se enfoca en lo que se hace se dice o se siente, de acuerdo con Vega (2021) la autenticidad esta "relacionada con la atribución adecuada en cuanto a lo que es el propietario o el creador de los datos o la información"

Es decir, la autenticidad es la garantía que la información o la identidad de un usuario sea genuina y verídica, implica que de donde proviene la información sean una fuente confiable lo que ayuda a que la integridad exista en los procesos administrativos. Como también lo menciona Rodríguez (2010) quien indica:

> La falta de confianza en la autenticidad de la información crea una gran incertidumbre, por lo tanto, las organizaciones que no pueden confiar en sus sistemas de información y comunicaciones dudarán en usar las nuevas tecnologías o métodos que aseguren la confidencialidad de la información (p. 8).

Utilidad. La utilidad de la información tiene como propósito ofrecer valor y facilitar su acceso de manera eficiente, permitiendo que los usuarios puedan emplearla de forma práctica y oportuna en sus actividades, como lo expresa Vega (2021).

> La utilidad se refiere al uso que se les dan a los datos, es decir por qué y para qué está esa información allí, para qué sirve y qué tipo de manejo se le puede dar, además, depende del tipo de seguridad con la que esta cuente, ya que en caso de que se pierda información se deriva la utilidad de esta para los externos (p. 15).

La utilidad se refiere a la capacidad que tienen los sistemas de información para alcanzar sus objetivos, los cuales, en la mayoría de los casos, incluyen la protección y resguardo. En síntesis, implica que los controles implementados no deben limitar el acceso ni el uso adecuado por parte de los usuarios autorizados.

Existiendo una cadena entre el control, la autenticidad y la utilidad, ya que se necesita de los tres para mantener a salvo la información, al alcance de las personas autorizadas y por último que el manejo de la información sea para procesos propios de la organización.

Tipos de seguridad de la información

Toda empresa, institución u organización tiene la responsabilidad de proteger su información, ya que esta representa un recurso estratégico que incluye el conocimiento del personal, los sistemas especializados y los resultados de la interacción con el entorno. Estos elementos, junto con los datos sensibles que se generan, conforman un sistema de información estructurado que debe resguardarse adecuadamente para garantizar su correcto funcionamiento y toma de decisiones.

Salvaguardar la información importante, ya que previene consecuencias negativas, como el robo, pérdida, el mal uso y otros, como lo menciona Roldán et al. (2022).

> Una empresa o institución debe confrontar los avances innovadores y los cambios constantes de la tecnología, por lo que debe trazar un plan de políticas de seguridad de

> la información, las cuales se deben de mantener actualizadas, así como su infraestructura; para lograr estar a la vanguardia de la operación. (p. 3).

No abordar las vulnerabilidades en una organización representa un riesgo, ya que la información puede ser interceptada por ciberdelincuentes que buscan esquivar estas protecciones, con el fin de sustraer o modificar la información.

> La seguridad de la información es fundamental en la era digital en la que vivimos. Cada vez son más los ataques cibernéticos y las amenazas a la privacidad de nuestros datos. Por eso, es imprescindible conocer y aplicar los protocolos de seguridad más importantes. (LOPD,2023, párr. 7).

En la era digital, la seguridad de la información se convierte en un elemento esencial para enfrentar las crecientes amenazas cibernéticas y proteger los datos críticos de las organizaciones. Para cumplir con este propósito, se implementan diversos protocolos y herramientas de seguridad que permiten establecer controles, prevenir accesos no autorizados y garantizar la integridad, confidencialidad y disponibilidad de la información en todos los niveles operativos, mencionando los siguientes:

1. Firewall: Es una barrera de protección que controla el tráfico de red y filtra las conexiones no autorizadas. Actúa como un escudo entre la red interna y externa, bloqueando accesos no deseados.
2. Encriptación: Consiste en convertir la información en un código ilegible para que las personas que no tienen la clave de descifrado. Esto garantiza que en caso de interceptación los datos no puedan ser utilizados.
3. Autenticación de dos factores: Es un método de verificación que requiere dos elementos para acceder a una cuenta o sistema. Se combinan dos pasos el usuario conoce (cómo una contraseña) y algo que posee (como un código generado en su smartphone) el objetivo es aumentar la seguridad.

4. Actualización de software: Los desarrolladores de software lanzan actualizaciones periódicas para corregir errores y vulnerabilidades. Mantener el software actualizado es esencial para la protección de posibles ataques.

5. Copias de seguridad: Realizar copias de seguridad de forma regular permite recuperar la información en caso de pérdida, robo o daño. Es importante almacenar las copias en un lugar seguro y separado del sistema principal.

Existen tipos de seguridad que ayudan a mitigar los problemas que enfrentan la información en una sociedad vulnerable y digitalizada, es importante tomarlas en cuenta para proteger las instituciones de ataques cibernéticos que expongan información sensible de la institución, y provoque consecuencias como la sustracción no autorizada de datos y el deterioro de la imagen institucional ante la opinión pública.

Medidas de seguridad

Las medidas de seguridad son esenciales, en cualquier ámbito organizacional, en el que se necesite seguridad con el fin que los activos o la información valiosa sea resguardada, se puede decir de manera general según lo menciona Infoem (2023) que las medidas de seguridad son“ los medios físicos y técnicos necesarios para garantizar la integridad, confidencialidad y disponibilidad de los datos personales en posesión de los sujetos obligados, a efecto de evitar su daño, alteración, pérdida, destrucción o el uso y transmisión no autorizado” (párr. 1).

Las medidas de seguridad en las organizaciones son fundamentales, especialmente en las oficinas, donde a diario se maneja información sensible que no debe ser expuesta. Estas medidas permiten proteger los datos, prevenir su pérdida y resguardarlos frente a amenazas tanto internas como externas. Por ello, su implementación resulta esencial para asegurar la integridad y confidencialidad de la información dentro de los procesos administrativos.

Con base en los componentes de la seguridad de la información, la integridad, disponibilidad y confidencialidad se determinan recomendaciones para la protección de datos, información y documentos importantes, entre ellas:

- Contraseñas seguras
- Antivirus
- Copias de seguridad con frecuencia
- Controlar acceso a la información

Políticas y prácticas de la seguridad de la información

Las políticas de seguridad representan un componente esencial en la gestión de los sistemas informáticos dentro de una organización. Estas orientan el uso adecuado de las tecnologías de información y comunicación, y establecen directrices claras para garantizar su eficiencia y resguardo.

Las políticas de seguridad determinan según García y Vidal (2016, p. 56). “De qué manera se emplean las tecnologías de información y comunicación para aprovecharlas con la mayor eficiencia y seguridad posible, las políticas establecen las normas generales que debe cumplir el personal que participa en el sistema informático”

Es decir, las políticas constituyen la estrategia general con que cuenta la organización, se definen como un conjunto de reglas, procedimientos y acciones diseñadas para proteger la información sensible de una organización, empresa o institución contra amenazas como el acceso no autorizado, el robo, la pérdida o la manipulación. Una política de seguridad se puede implementar a través de procedimientos que indiquen cómo manejar, almacenar, compartir y proteger los datos relevantes de una organización.

Las políticas y procedimientos de seguridad de la información se encargan de asegurar el cumplimiento mediante herramientas de seguridad, donde sea pertinente las responsabilidades de todas las personas que tienen acceso a los sistemas y servicios.

Para Vega (2021, p.11). “Definir cuándo tenemos un ambiente inseguro es una tarea mucho más sencilla y podemos enumerar rápidamente una serie de elementos que nos pondrían en este estado”

- No actualizar sistemas operativos y aplicaciones.
- Usar contraseñas débiles como “contraseña” o “1234”.
- Descarga de programas de internet de fuentes no seguras.
- Abrir archivos adjuntos de correo electrónico de remitentes desconocidos.
- Usar y desplegar redes inalámbricas sin cifrado.

Estas son algunas de las prácticas que se realizan frente a la información digital que se custodia, es importante no realizar estos elementos o prácticas frente a los procesos administrativos.

Concientización

Es importante que en las áreas de trabajo se tome conciencia de los procesos que se lleva a cabo, con el fin de brindar y asegurar hábitos, dado que la seguridad constituye una responsabilidad esencial en el uso de la información.

> La tarea de concientización no solo debe esforzarse en capacitar al usuario en los nuevos temas, sino que también debe trabajar en erradicar las malas costumbres adquiridas durante mucho tiempo con respecto a la seguridad de la información. Hay que crear conciencia para formar hábitos y cultura. La seguridad es responsabilidad de todos, Como lo menciona (Flores y Caiza 2017, p. 6).

La concientización debe estar alineada con las políticas de la organización para aumentar la comprensión y la sensibilidad dentro de la empresa.

Promover la concientización sobre seguridad de la información ayuda a mitigar estos riesgos al prevenir la ocurrencia de brechas de seguridad, y a esto los autores Flores y Caiza (2017, p. 6) dicen que:

> Cuando se habla de estrategias de concientización, se expone un conjunto de técnicas tales como selección de controles, entrenamiento de seguridad, educación y desarrollo. Cualquier estrategia debe proporcionar los elementos de juicio para que el personal esté consciente de sus responsabilidades como parte de sus labores.

La promoción de la conciencia en los espacios de trabajo contribuye significativamente a la protección de la información sensible. No solo permite prevenir incidentes relacionados con la seguridad, sino que proporciona al personal estrategias claras para fomentar un entorno laboral seguro. Al seguir las recomendaciones y aplicar las medidas establecidas, el personal fortalece la cultura de seguridad dentro de la institución y ayuda a reducir los riesgos asociados al manejo inadecuado de la información.

Capacitación

Con la implementación de la capacitación se espera que las personas adquieran conocimientos y habilidades que les permitan desempeñarse de manera eficiente en sus áreas de trabajo. Este proceso contribuye al fortalecimiento de las competencias individuales y colectivas, mejorando la productividad, la toma de decisiones y la correcta aplicación de medidas relacionadas con la seguridad de la información.

> La capacitación como elemento cultural, es un proceso continuo y sistemático, y debe concebirse para todos los colaboradores de la Institución, como un apoyo indispensable para lograr un mejoramiento constante de los resultados, así como un proceso facilitador del desarrollo y el crecimiento. (Arias, 2021, párr. 2)

La capacitación es un proceso de suma importancia porque facilita a los colaboradores desarrollar y mejorar las habilidades y así mismo el rendimiento del área en el que se especializan, como lo expresa Flores y Caiza (2017)

> La mejor forma de protegerse de estas amenazas es desplegar sistemas de autenticación múltiple, pero sobre todo capacitar al personal sobre los hábitos de crear

> contraseñas seguras y renovarlas periódicamente. Elaborar políticas de seguridad de la información y capacitar a los empleados sobre el riesgo, es una acción muy utilizada para hacer frente a esta problemática. (p.6).

Por otro lado, como lo menciona Obando (2020):

> Se puede decir que "la capacitación se debe realizar de acuerdo con las necesidades que presentan cada uno de los trabajadores de la organización, partiendo como punto principal dar a conocer a cada trabajador los objetivos y metas de la organización, lo que ella espera de su desempeño y esfuerzo y cómo debe ser el uso de cada instrumento y herramienta de trabajo para que de este modo se pueda obtener un mejor desempeño laboral. (párr. 30).

Es decir, la capacitación es parte del talento humano de una organización, la cual va a permitir que todos los empleados logren desenvolverse de manera eficiente en la organización, cumplir con las tareas asignadas de forma adecuada, lo que permite un correcto ambiente organizacional.

Conocimiento

Cuando se hace referencia al concepto conocimiento se refiere a las experiencias aprendidas o adquiridas a través del tiempo o en cierta ciencia a través del estudio o investigaciones. Se puede adquirir o demostrar por medio de habilidades, es decir, puede expresarse de forma escrita, como en los libros o verbal por la forma en la que las personas se expresan.

Esparza y Rubio (2016) definen el conocimiento como:

> Una cierta certeza que confiere sobre lo que es el mundo, y dicha certeza, permite actuar, dar el siguiente paso en el transitar que es la vida, que, de lo contrario, se estaría hundidos en un ámbito de incertidumbre, y la incertidumbre genera angustia, y

ésta a su vez, paraliza, inmoviliza. Es pues, el conocimiento una suerte de luz que ilumina el sendero de la existencia. (párr. 40).

Es todo aquello que una persona sabe, o aprende en el transcurso del tiempo, ya sea por medio de la lectura, escucha, observación o experimentación, es todo el conocimiento aprendido desde aspectos sencillos hasta los complejos.

Comprensión

Es la capacidad que tienen las personas por captar el significado de algo, según Lorenzon y Romero (2019, p. 4). También se puede definir como "una situación de entendimiento intersubjetiva, en la que una persona se coloca en lugar de la otra, logrando saldar la distancia entre sentimientos, agravios, entendimientos, dando por resultado un vínculo de solidaridad"

La comprensión se encamina en dos principales vías, una relacionada con el solidarismo, es decir más personal, entender a los demás por sus acciones y sentimientos. También se relaciona con la interpretación de información, comprensión de textos, vídeos, investigaciones o documentos relevantes. De tal forma, se puede definir la comprensión como la capacidad de entendimiento, que trata de comprender, interpretar y manejar todo aquello que se conoce o se pretende conocer.

CAPÍTULO III

Marco metodológico

En este capítulo, se presenta el marco metodológico que se aplicó en la investigación, en esta sección se especifica todo lo relacionado al marco metodológico, para Azuero (2018, p. 111). “Es el conjunto de acciones destinadas a describir y analizar el fondo del problema planteado, a través de procedimientos específicos que incluye las técnicas de observación y recolección de datos, determinando el “cómo” se realizará el estudio”

En el presente apartado se desarrollan, el paradigma de la investigación, enfoque metodológico, tipo de investigación, sujetos y fuentes de información, sistema de variables, técnicas y descripción de los instrumentos. Esto permite definir cómo se desarrolló la investigación, asegurando la validez y confiabilidad de los resultados, permitiendo recolectar y analizar los datos necesarios para responder al problema planteado y alcanzar los objetivos propuestos.

Paradigma de investigación

La investigación se desarrolló bajo el paradigma hermenéutico, lo cual permitió realizar un estudio y análisis de la seguridad de la información del personal administrativo del Colegio Técnico Profesional San Isidro, de acuerdo con Ballina (s.f) “el paradigma hermenéutico, también llamado paradigma cualitativo, fenomenológico, humanista o etnográfico indica que “no interesa llegar a un conocimiento objetivo”, sino alcanzar un “conocimiento consensuado” lo que importa es ponerse de acuerdo en la interpretación, de lo que se está estudiando”.

Enfoque metodológico

A partir de un análisis detallado se determinó que el enfoque metodológico adecuado para desarrollar el estudio es cualitativo, dadas las características de este.

El enfoque de la investigación fue cualitativo, ya que se fundamentó en antecedentes teóricos existentes y se buscó comprender a los fenómenos a través de sus percepciones y

experiencias del tema, se usaron instrumentos como la entrevista o el cuestionario, para la recolección de los datos. Según Ferrer y Senovia (2023), la investigación cualitativa “aborda los significados, las acciones de los individuos y la manera en que estos se vinculan con otras conductas propias de la comunidad; además, conlleva a explicar los hechos sociales, buscando la manera de comprenderlos. De la misma manera, analiza, interpreta y comprende la realidad estudiada tal como aparece, esto es, tal como es y se da, situación que la hace caracterizar como una metodología fenomenológica”. (Párr. 7).

Por tanto, la recopilación de información se llevó a cabo mediante instrumentos cualitativos con preguntas abiertas y cerradas, que facilitaron la obtención de datos descriptivos y contextuales. Este método permitió a las investigadoras explorar el tema en profundidad y analizar las opiniones de la población estudiada. Como resultado, se identificaron oportunidades para mejorar la protección de la información en el Colegio Técnico Profesional San Isidro, especialmente en evaluación y fortalecimiento de los protocolos de seguridad en los procesos administrativos.

Tipo de investigación

Considerando las características y el enfoque de esta investigación, se identificó en relación con el tema propuesto que el tipo de investigación es descriptiva y explicativa, Corona Martínez, et al. (2023), mencionan que “Los estudios descriptivos, como el término indica, pretenden la determinación de características y atributos del fenómeno en estudio, y se utilizan para resolver problemas mejor precisados. Por su relativa “sencillez” metodológica, es precisamente este tipo de estudio el que más abunda entre las propuestas investigativas.” (Párr. 8).

La investigación descriptiva permitió un análisis de la seguridad de la información en los procesos administrativos que caracteriza el objeto de estudio, a partir de hipótesis que

identificaron tipos de seguridad, niveles de concientización y capacitación de la información en la institución seleccionada para la investigación.

Del mismo modo, el tipo explicativo busca entender las causas y efectos de la situación, de acuerdo con Guevara Alban et al. (2020). “La investigación explicativa es aquella que tiene relación causal, no sólo persigue describir o acercarse a un problema, sino que intenta precisar las causas del mismo”. (Pág. 165).

Por lo tanto, este enfoque permitió identificar las causas que afectan los procesos administrativos de la institución debido a la falta de seguridad en el manejo de los datos. La metodología explicativa resultó fundamental, ya que ofrece una comprensión profunda del problema y facilita la implementación de soluciones viables y efectivas. De esta manera, se pudieron detectar oportunidades para mejorar la protección de los datos en el Colegio Técnico Profesional San Isidro, a través de la evaluación de los protocolos de seguridad aplicados en los procesos administrativos.

Sujetos y fuentes de información

Población

La población corresponde a los individuos que cumplían con los criterios o características al problema de la investigación, para ser el objeto de estudio, según Pacheco (2024) “la población involucra a la totalidad de elementos que coinciden con ciertos aspectos o características de interés para el estudio” (párr. 3).

La población bajo estudio abarcó a todos los funcionarios administrativos del Colegio Técnico Profesional San Isidro, Sección Diurna, periodo 2024, la cual consistió en un total de 13 colaboradores.

Muestra

Se puede describir la muestra como un pequeño conjunto de personas, individuos o elementos extraídos de una población para realizar un estudio y de esta forma generalizar los

resultados, como lo menciona Otzen y Manterola (2017) la muestra es “la representatividad, que permite extrapolar y por ende generalizar los resultados observados en ésta, a la población accesible; y a partir de ésta, a la población blanco” (párr. 1).

Sin embargo, para efectos del presente trabajó con una muestra, sino que se realizó el estudio con la población total, con el fin de evitar el sesgo y detallar los resultados de forma completa.

Fuentes de información

Fuentes primarias

Las fuentes utilizadas en la investigación fueron principalmente primarias, de acuerdo con Cruz (2019, pág. 28). Las fuentes primarias “contienen información original que ha sido publicada por primera vez y que no ha sido filtrada, interpretada o evaluada por nadie más”

Se utilizaron libros relacionados con la seguridad de la información de los cuales extraen datos relevantes que ayudaron a dar forma y contexto al tema propuesto. Se obtuvo información de primera mano por medio de la aplicación de entrevistas y lista de cotejo.

Fuentes secundarias

Otro de los métodos tomados en cuenta fueron las fuentes secundarias como lo menciona Cruz (2019, pág. 28). Las fuentes secundarias “están diseñadas para facilitar y maximizar el acceso a las fuentes o a sus contenidos, como enciclopedias, antologías, reseñas de películas, artículos, etc” (p. 28).

Es decir que, las fuentes secundarias interpretan información primaria, así dando oportunidad de obtener un mejor acceso y extensibilidad, algunos de los principales documentos a utilizar son revistas, páginas de internet, artículos, libros, con el fin de obtener mayor interpretación.

En el trabajo se utilizaron tanto las fuentes primarias como las secundarias, con el uso de ambas se logró la recolección de información necesaria para alcanzar los objetivos propuestos.

Sistemas de variables

Una variable es un rasgo, cualidad o característica de los individuos, objetos o fenómenos que se analizan y que tiene la capacidad de cambiar de valores. Las variables son esenciales en el análisis estadístico, puesto que posibilitan la recopilación y el examen de información para sacar conclusiones sobre una población o fenómeno.

Hernández Sampieri et al. (2014), menciona que una variable es una propiedad que puede fluctuar y cuya variación es susceptible de medirse u observarse. El concepto de variable se aplica a personas u otros seres vivos, objetos, hechos y fenómenos, los cuales adquieren diversos valores respecto de la variable referida. En todos los casos se producen variaciones. Las variables adquieren valor para la investigación científica cuando llegan a relacionarse con otras variables, es decir, si forman parte de una hipótesis o una teoría. En este caso, se les suele denominar constructos o construcciones hipotéticas. (p.105)

Variable 1: Tipos de seguridad. A continuación, se proporciona una definición conceptual, instrumental y operacional de tipos de seguridad.

Definición conceptual. Para, LOPD (2023, (párr. 7). “La seguridad de la información es fundamental en la era digital en la que vivimos. Cada vez son más los ataques cibernéticos y las amenazas a la privacidad de nuestros datos.

Definición Instrumental. Para responder a la variable, se aplicó una entrevista dirigida a los funcionarios administrativos del Colegio Técnico Profesional San Isidro, Sección Diurna. Las preguntas número: 1,5,6,7,9,12 son enfocadas a dicha variable. También se aplicó una lista de cotejo para obtener la información requerida con las siguientes preguntas:1,6,8, 11.

Definición operacional. Hace referencia a las acciones y normas puestas en práctica para resguardar la información en documentos (tanto físicos como digitales) de accesos no autorizados, pérdidas, robos, cambios o daños. Si el 70% de los funcionarios explican el concepto y su importancia correctamente significa que si tienen una idea clara sore la seguridad de la información. Si el 80% de los funcionarios eligen todas o la mayoría de las opciones significa que cuentan con buenos tipos de seguridad. Si el 80% de los colaboradores responden que muy efectivos, se considera que los tipos de seguridad si han sido efectivos. Si el 80% de los colaboradores mencionan las distintas medidas de protección significa que conocen de esta y además las han aplicado. Si el 80% de los funcionarios eligen todas o la mayoría de las opciones, significa que gestionan correctamente los datos sensibles. Si el 70% de los colaboradores seleccionan todas o la mayoría de las opciones, quiere decir que las medidas de seguridad tienen un impacto en la eficiencia y operatividad. Si el 85% de los funcionarios responden que sí, se considera que existen políticas de seguridad. Si el 80% de los funcionarios responden que sí, significa que saben cómo funciona la autenticación multifactor. Si el 80% de los funcionarios responden que sí, se considera que las herramientas de seguridad están configuradas y actualizadas correctamente. Si el 85% de los funcionarios dicen que sí, se considera que ambiente de trabajo es seguro.

Variable 2: Concientización. La concientización se define a continuación:

Definición conceptual. Es el proceso en el que las personas aumenten su comprensión o conciencia sobre un tema concreto, con el objetivo de modificar actitudes, comportamientos o percepciones. Como lo menciona Flores y Caiza (2017, p. 6). “La tarea de concientización no solo debe esforzarse en capacitar al usuario en los nuevos temas, sino que también debe trabajar en erradicar las malas costumbres adquiridas durante mucho tiempo con respecto a la seguridad de la información.

Definición Instrumental. Para responder a la variable, se aplicó una entrevista dirigida a los funcionarios administrativos del Colegio Técnico Profesional San Isidro, Sección Diurna, las preguntas número 8,10,11,13 son enfocadas a dicha variable. También se aplicó una lista de cotejo para obtener la información requerida con las siguientes preguntas:2,5,9,10,11

Definición operacional. La concientización se puede definir como aquella capacidad que tienen la personas de adquirir mayor comprensión, sensibilidad o toma de conciencia sobre un tema específico, como es en la seguridad de la información. Si un 65% de los funcionarios indican no utilizar ningún método de seguridad significa que la organización no implementa ninguna de las medidas mencionadas para gestionar los datos sensibles. Si el 80% de los funcionarios eligen todas o la mayoría de las opciones significa que tienen la capacidad de asegurar un acceso continuo y oportuno a los datos esenciales. Si el 75% de los funcionarios seleccionan la mayoría significa que existe mucha debilidad en los procesos administrativos. Si el 80% de los funcionarios seleccionan cuatro o más opciones significa que hay significativos problemas de seguridad. Si un 85% de los funcionarios responden que sí, significa que existen mecanismos oficiales, formales y estructurados de supervisión. Si el 85% de los funcionarios responde que sí, significa que el personal tiene el conocimiento y las directrices necesarias para manejar información sensible. Si el 80% de los funcionarios contestan que sí, es porque existen procesos establecidos para documentar, analizar y aprender de los incidentes de seguridad. Si el 75% de los funcionarios responde que sí, significa que en la institución existen procedimientos claros ante esas situaciones. Si el 80% de los funcionarios responden que sí, significa que estos perciben la existencia de suficientes medidas de seguridad.

Variable 3: Capacitación. A continuación, se proporciona una definición conceptual, instrumental y operacional de la concientización.

Definición conceptual. Como señala Arias (2021, párr. 2). “La capacitación como elemento cultural, es un proceso continuo y sistemático, y debe concebirse para todos los colaboradores de la Institución, como un apoyo indispensable para lograr un mejoramiento constante de los resultados, así como un proceso facilitador del desarrollo y el crecimiento”

Definición Instrumental. Para responder a la variable, se aplicó una entrevista dirigida a los funcionarios administrativos del Colegio Técnico Profesional San Isidro, sección diurna, las preguntas numero 2,3,4. También se aplicó una lista de cotejo aplicada para obtener la información requerida ítems:3,4,7.

Definición operacional. Es el procedimiento mediante el cual se enseña a las personas los conocimientos, capacidades y destrezas que necesitan para mejorar su rendimiento en un campo concreto. Si el 75% de los funcionarios responden que tienen un nivel de conocimiento alto sobre las políticas de seguridad, esto indica que tienen un conocimiento estas políticas. Si el 80% de los funcionarios responden que sí, significa que si han recibido alguna capacitación en la seguridad de la información. Si el 85% de los funcionarios responden varias opciones, esto quiere decir que el personal administrativo se capacita utilizando diferentes medios. Si el 75% de los funcionarios responden que sí, significa que si realizan capacitaciones de seguridad de la información constantemente. Si el 80% de los funcionarios contesta que sí, significa que si tienen accesos a documentos con respecto a la seguridad de la información. Si el 85% de los funcionarios contesta que sí, significa que si saben cómo clasificar manejar la información.

Tabla 7

Cuadro de variables.

Objetivo especifico	Variable	Subvariable	Definición Instrumental
Identificar el tipo de seguridad de la información utilizada en los procesos administrativos en las oficinas para el análisis de la eficacia de las medidas de seguridad existentes.	Tipos de seguridad	Eficiencia Medidas de seguridad	Entrevista a los administrativos y lista de cotejo
Evaluar el nivel de concientización y capacitación en seguridad de la información del personal administrativo con el fin de obtener información sobre el grado de conocimiento y comprensión sobre las políticas y prácticas de seguridad de la información.	Concientización	Comprensión de las políticas	Entrevista a los administrativos y lista de cotejo
Evaluar el nivel de concientización y capacitación en seguridad de la información del personal administrativo con el fin de obtener información sobre el grado de conocimiento y comprensión sobre las políticas y prácticas de seguridad de la información.	Capacitación	Conocimiento	Entrevista a los administrativos y lista de cotejo

La Tabla 7 muestra el cuatro de variables donde se buscó identificar y evaluar aspectos clave relacionados con la seguridad de la información en los procesos administrativos. Se examinan los tipos de seguridad implementados, evaluando su eficiencia

y las medidas existentes mediante una entrevista y lista de cotejo. También, se analizó el nivel de concientización del personal administrativo, enfocándose en su comprensión de las políticas de seguridad. Finalmente, se evalúo la capacidad del personal, sobre su conocimiento sobre prácticas y protocolos de seguridad. Para ambas variables se utilizaron los mismos instrumentos.

Técnicas y descripción de los instrumentos

De acuerdo con el tipo de investigación seleccionada, se realizó la recolección de datos por medio de una entrevista, según Piza et al (2019, párr. 16) la entrevista es "más íntima, manejable y abierta, además es donde el entrevistador se desempeña sobre la base de preguntas especificas contenidas en una guía previamente elaborada y se supedita a ésta". Esta técnica se realizó de manera presencial a la muestra seleccionada para obtener los datos requeridos, además, nos permitió recabar datos detallados, específicos y tener una interacción humana directa, en la cual se obtuvo información detallada. Además, según Peña (2017, pág. 75) "como técnica cualitativa, la entrevista se entiende como un acto comunicativo, bien sea verbal o escrito, que tiene como objetivo obtener cierta información u opinión respecto a un tema o personalidad en especial. Tiene como característica enfocar la realidad desde un método inductivo."

Por otra parte, se utilizó la lista de cotejo como segundo instrumento para la recolección de datos, desde un punto de vista general, esta herramienta de evaluación se utilizó para verificar una serie de criterios. Para la UNED (2017, pág.10). "Es un instrumento de evaluación que contiene una lista de criterios o desempeños de evaluación, previamente establecidos, en la cual únicamente se califica la presencia o ausencia de estos mediante una escala dicotómica, por ejemplo: si–no, 1–0".

Con este instrumento, se buscó identificar el desempeño y el cumplimento de la seguridad de la información en los procesos administrativos. En esta investigación, la lista de

cotejo fue fundamental para evaluar de manera imparcial y sistemática el cumplimiento de los requisitos de seguridad en el manejo de la información en los procesos administrativos. Al utilizar esta herramienta, se obtuvo datos de los puntos fuertes y débiles en la gestión de la seguridad de la información, permitiendo identificar áreas de mejora y tomar decisiones basadas en datos. Esto garantizó la flexibilidad de los procedimientos administrativos para una mayor protección y confidencialidad de la información sensible de la institución.

Análisis de datos

El análisis de datos es el proceso de examinar datos con el objetivo de descubrir información útil y llegar a conclusiones. Según Peña (2017, pág. 30). “El análisis de datos integra distintas operaciones en la que el investigador o analista somete ciertos datos, bien sea de orden cuantitativo o cualitativo, a una serie de análisis, lecturas e interpretaciones, según sea el enfoque de su investigación o requerimiento informativo.”

Para el análisis de datos se necesita diversas técnicas y herramientas que permitieron la interpretación de los mismos, utilizaron tablas y gráficos los cuales detallan la información recolectada.

Consideraciones éticas

Al realizar un trabajo de investigación es fundamental tener en cuenta varias consideraciones éticas que van a asegurar la integridad, validez y sobre todo autenticidad de la investigación, como lo menciona Alvarez (2018, pág.9) “las consideraciones éticas son especialmente importantes en estudio de investigación que requieren la participación de seres humanos”, esto es porque los investigadores deben de aplicar los principios morales al mundo real.

Es decir que, a medida que se realiza el trabajo de investigación de deben cumplir principios morales, donde se evidencia que lo investigado es único y auténtico. Existen una serie de consideraciones éticas que son base para la investigación tales como:

- Transparencia
- Honestidad
- Respeto a la propiedad intelectual
- Beneficencia

Propuesta

En el marco de la investigación sobre el "Análisis de la seguridad de la información en los procesos administrativos en las oficinas del Colegio Técnico Profesional San Isidro", con el objetivo de brindar medidas que permitan proteger y resguardar la información. Se propuso un plan para:

Fortalecer la seguridad de la información en los procesos administrativos, asegurando la confidencialidad, integridad y disponibilidad de los datos.

CAPÍTULO IV

Análisis e interpretación de resultados

En este capítulo se muestra el análisis e interpretación de los datos obtenidos por medio de los diferentes instrumentos aplicados, entre ellos: entrevista y lista de cotejo. Este análisis hace uso de tablas y gráficos que logran presentar de manera visual los resultados principales de la investigación.

Tipos de seguridad

En cuanto al concepto de seguridad de la información y la importancia en el trabajo, el personal administrativo indica que la seguridad de la información hace referencia al conjunto de prácticas, técnicas y metodologías enfocadas en la protección y resguardo de información sensible, ya sea en formato digital o físico. Su objetivo principal es asegurar la privacidad, integridad y accesibilidad de la información, previniendo accesos no permitidos, pérdidas o aprovechamientos no autorizados.

Además, es un factor esencial para proteger la privacidad, la integridad y la disponibilidad de los datos que administra una oficina de gestión. Asegura que los procedimientos administrativos y educativos se lleven a cabo de forma eficaz, responsable y profesional.

Tabla 8

Principales tipos de seguridad implementados en los procesos administrativos

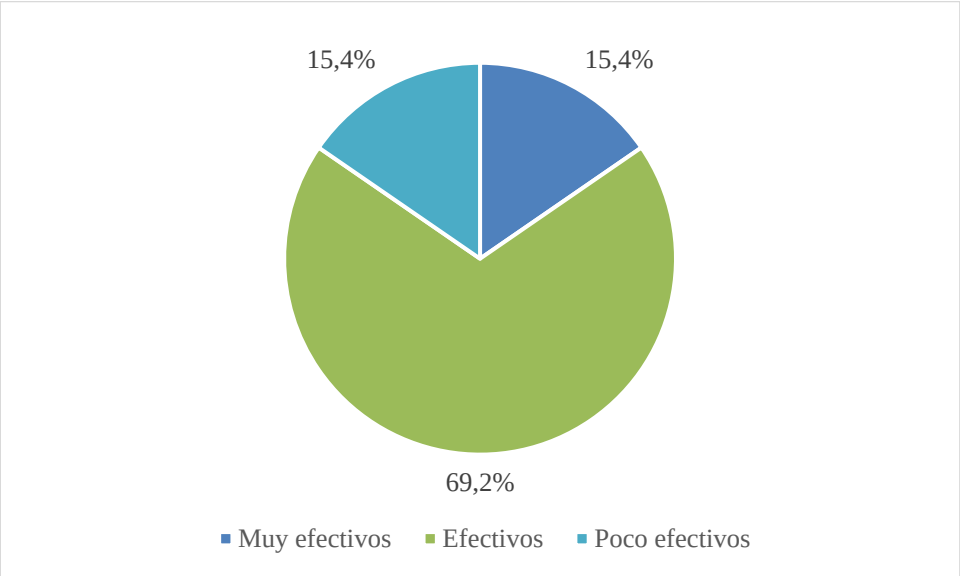
Criterios	Valor absoluto	Valor relativo
Copia de seguridad	10	76,9%
Actualización de software	6	46,2%
Antivirus	11	84,6%
Contraseñas seguras	9	69,2%
Verificación en dos pasos	3	23,1%
Información física bajo llave	2	15,4%
Disco duro	1	7,7%

Con la Tabla 8, se muestra que un total de 11 personas indican que implementan antivirus como su principal medida de protección, mientras que 10 señalan la copia de seguridad como una práctica habitual. Asimismo, 9 personas afirman utilizar contraseñas seguras, lo que refleja una inclinación hacia la protección digital. Por otro lado, solo 3 personas reportan usar verificación en dos pasos, y un porcentaje aún menor indica que emplea métodos de seguridad física como guardar documentos bajo llave 2 personas, y disco duro externo 1 persona.

Asimismo, aunque las medidas digitales dominan la preferencia de los entrevistados y estos son seguros, es importante fortalecer las prácticas de seguridad complementarias, especialmente aquellas relacionadas con la protección física y la implementación de procesos adicionales de seguridad como la autenticación en dos pasos.

Figura 1

Los tipos de seguridad implementados han sido efectivos en los procesos administrativos



Con la Figura 1, se observa que la mayoría de las personas encuestadas consideran que las medidas de seguridad de la información implementadas en los procesos administrativos lo que equivale a un 69%. Por otro lado, un 15,4% de los encuestados opina que estas medidas son efectivas, esto indica que, aunque representan un porcentaje menor, existe un grupo que percibe un alto nivel de confianza en las herramientas de seguridad utilizadas. Sin embargo, un 15,4% señalan que las medidas son poco efectivas.

A pesar que el grado de satisfacción general es alto, con la mayoría de los entrevistados valorando las medidas como efectivas o muy efectivas, es importante determinar las causas de las percepciones negativas para mejorar los procesos y lograr un nivel alto de seguridad en la información administrativa.

Tabla 9

Impacto que tienen las medidas de seguridad en la eficiencia y operatividad

Criterios	Valor absoluto	Valor Relativo
Reducción de riesgos y mayor confianza en los procesos	11	84,6%
Mejora en la protección de datos y cumplimiento normativo	11	84,6%
Mayor conciencia y responsabilidad del personal	11	84,6%
Mayor carga en los procesos administrativos	4	30,8%

Con base a la Tabla 9, se observa que las medidas de seguridad implementadas tienen un impacto positivo significativo en la eficiencia y operatividad de los procesos administrativos. De los encuestados, 11 personas indican que estas medidas contribuyen a la reducción de riesgos, generan confianza en los procesos, así como en la mejora para la protección de datos y el cumplimiento normativo. Además, fomentan conciencia y responsabilidad en el personal. En cambio, 4 personas señalan que estas medidas incrementan la carga en los procedimientos administrativos, indicando que su implementación demanda tiempo y recursos extra.

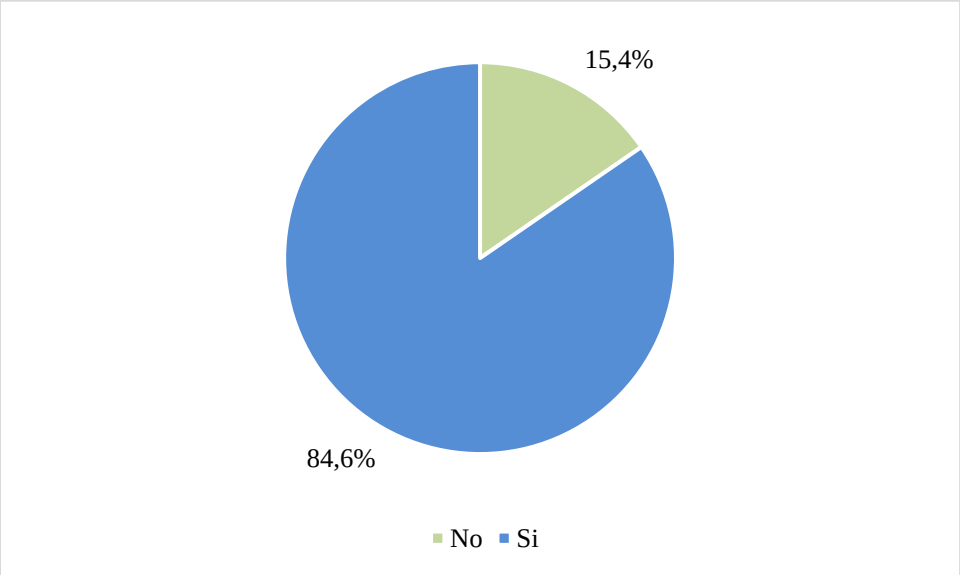
Considerando lo anterior, a pesar que los beneficios son reconocidos, resulta crucial tratar las inquietudes asociadas a la carga administrativa. La implementación de capacitación y procedimientos eficaces pueden disminuir esta percepción negativa y asegurar que las acciones de seguridad protegen la información y favorecen la eficiencia del personal administrativo.

Sobre el conocimiento de cómo funciona la autenticación multifactor, las 13 personas encuestadas desconocen el uso, esto explica que los administrativos no están familiarizados con el funcionamiento de la autenticación. Lo que puede provocar debilidades en el acceso a datos confidenciales y en la protección de información sensible. Además, el desconocimiento de estos procedimientos puede limitar el cumplimiento de las normativas de seguridad,

perjudicando la confianza tanto interna como externa en las acciones de protección de la información del colegio, y poniendo en riesgo la integridad de los datos académicos y administrativos.

Figura 2

Percepción de ambiente de trabajo como seguro en términos de seguridad de la información



Como se muestra en la Figura 2, el 84,6% de los encuestados perciben su ambiente laboral como seguro en cuanto a la protección de la información de la información, mientras que un 15,4% no percibe lo mismo.

Este estudio indica una mayoría del personal que confía en las estrategias de seguridad establecidas para proteger los datos y sistemas dentro de sus espacios laborales. Sin embargo, las personas que no perciben la seguridad de la información como adecuada puede estar relacionado con la falta de comunicación o con la sensación de que las medidas no son lo suficientemente efectivas.

Concientización

Tabla 10

Gestión de los datos sensibles

Criterios	Valor absoluto	Valor relativo
Con monitoreo y controles de acceso	3	23,1%
Capacitación y concientización del personal	1	7,7%
Uso de software y gestión de documentos seguros	1	7,7%
Políticas de seguridad de la información	3	23,1%
Copias de seguridad seguras	9	69,2%
Contratos de confidencialidad	2	15,4%
Ninguno	1	15,4%

De acuerdo con la gestión de datos sensibles, 9 personas del personal administrativo del colegio indican que el uso frecuente para cuidar y resguardar los datos sensibles es con el uso de las copias de seguridad, lo cual significa que utilizan los métodos conocidos, mientras que, una parte conformada por 3 personas dicen usar monitoreos, control de acceso y políticas de seguridad de la información, lo cual puede reflejar que una parte del personal administrativo realmente aplican diversos métodos para gestionar los datos sensibles buscando asegurar a su máximo nivel la información sensible.

Dicho esto, se puede afirmar que, aunque se utilicen algunos métodos para proteger la información, es necesario reforzar las medidas de seguridad para garantizar que la información sensible esté debidamente resguardada.

Tabla 11

Aseguramiento de la disponibilidad de la información ante amenazas

Criterios	Valor absoluto	Valor relativo
Videos	0	0%
Copias de seguridad periódicas	6	46,2%
Servicios en la nube	8	61,5%
Amenazas de recuperación ante desastres	0	0%
Controles de acceso y autenticación segura	3	23,1%
Otra	1	7,7%

En referencia a la Tabla 11, acerca del aseguramiento de la disponibilidad de la información ante las amenazas 8 personas aseguran utilizar especialmente los servicios en la nube, Las copias de seguridad periódicas, conformado por un total de 6 personas, lo cual refleja que una parte del personal utiliza los mismos métodos para asegurar la disponibilidad de la información ante posibles amenazas, mientras que solo 3 personas utilizan controles de acceso y autenticación segura, esto sucede porque trabajan con información de cuidado y por esto implementan medidas preventivas efectivas.

Tabla 12

Vulnerabilidades de seguridad en los procesos administrativos

Criterios	Valor absoluto	Valor relativo
Accesos no autorizados	7	53,8%
Contraseñas débiles	6	46,2%
Errores humanos	10	76,9%
Falta de capacitación y concientización	10	76.9,8%
Almacenamiento inseguro de documentos digitales	4	30,8%
Uso inseguro de correos electrónicos	4	30,8%
Falta de respaldo	6	42,2%
Redes inseguras	6	42,2%
Otra	0	0%

Acerca de las vulnerabilidades de seguridad en los procesos administrativos una parte del personal indica que los principales factores son tanto el error humano, así como la falta de capacitación y concientización, de igual forma 7 personas mencionan que otra vulnerabilidad presente son los accesos no autorizados, la falta de respaldo y redes inseguras, así como 4 personas indican que el uso inseguro de correos electrónicos son otro de los factores que afectan la vulnerabilidad en los procesos administrativos.

Esas son las principales debilidades presentes en los procesos administrativos del colegio, lo cual evidencia que existen riesgos y lo ideal es que la institución brinde capacitaciones para mitigar los problemas ante estas situaciones, con ello se logra obtener un personal capacitado, que no se deje llevar por falsos trucos de atacantes cibernéticos y así dar protección al colegio.

Tabla 13

Experiencia negativa con la gestión de información.

Criterios	Valor absoluto	Valor relativo
Pérdida de información sensible	3	23,1%
Robo de información	0	0%
Accesos no autorizados	4	30,8%
Daños a la reputación	0	0%
Interrupciones en los procesos	2	15,4%
Información desorganizada	5	38,5%
Robo de equipo	0	0%
Ninguna de las anteriores	3	23,1%
Otra: Problemas con Internet	1	7,7%

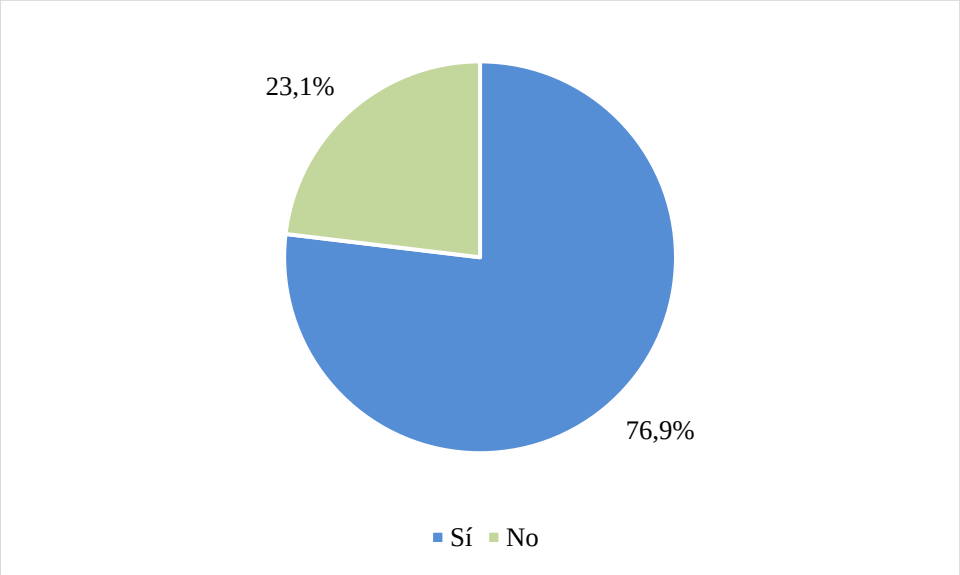
Acerca de la experiencia negativa con la gestión de información por parte de los funcionarios del colegio, un total de 5 personas afirman que un factor frecuente es la información desorganizada, así como los accesos no autorizados. Una pequeña parte conformada por 1 persona indica que los problemas con el internet también traen repercusiones negativas con la gestión de la información, también 2 personas aseguran que las en los procesos generan repercusiones negativas y por supuesto la pérdida de información sensible.

Por tanto, se deduce que los aspectos que traen experiencias negativas en realidad se pueden cambiar y evitar, ya que al tener información desorganizada o el acceso a la información de personas sin autorización tiene repercusiones negativas para la institución en general, sin embargo, con capacitación y explicaciones amplias eso se puede cambiar y fortalecer la seguridad de los procesos administrativos de la institución y también reforzar el conocimiento del personal ante estos procesos.

Capacitación

Figura 3

Sistemas de supervisión, seguimiento y auditoría.

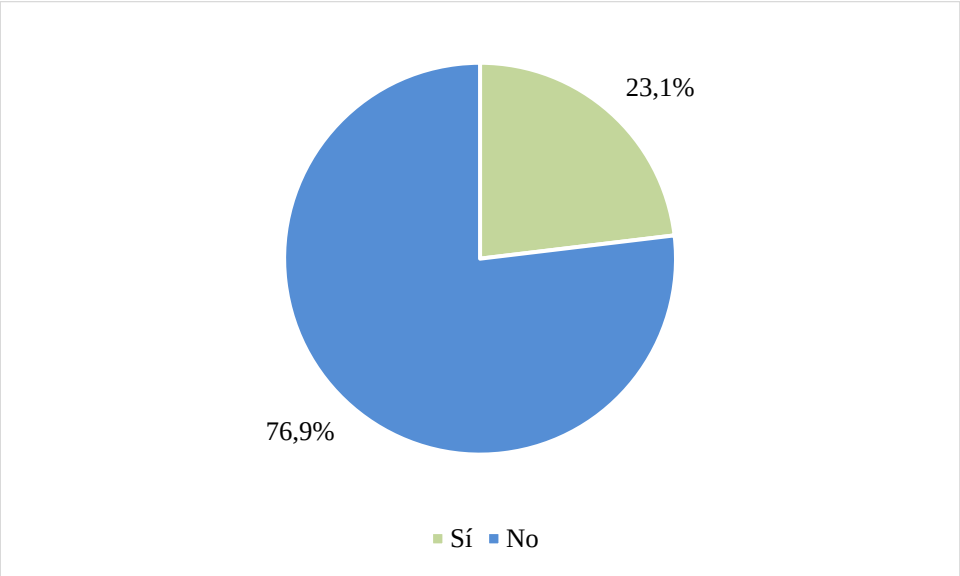


De acuerdo con la Figura 3, un 76,9% de la población mencionan que sí existen sistemas de supervisión, seguimiento y auditoría de parte del Ministerio Educación Pública hacia la institución, mientras que tan solo un 23,1% de los entrevistados dicen que no hay seguimiento alguno por parte del Ministerio de Educación Pública.

Se deduce que el Ministerio de Educación si realiza seguimientos y una adecuada supervisión, sin embargo, una parte de la población no lo percibe de esa forma y lo cree insuficiente, lo cual genera un impacto negativo ante la institución puesto que, aunque sea una minoría quienes perciben que no existe un seguimiento, significa que estas visitas no son tan constantes.

Figura 4

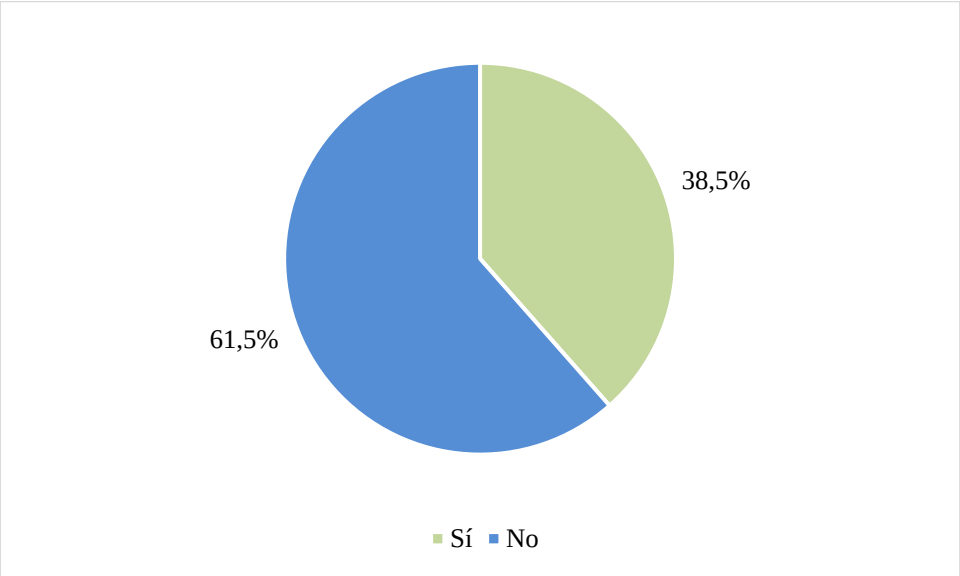
Conocimiento sobre clasificación y manejo de información sensible.



En cuanto al conocimiento sobre la clasificación y manejo de la información sensible, se demuestra que, un 76,9% del personal administrativo dice desconocer cómo se realizan estos procesos y tan solo un 23,1% si saben cómo clasificar y manejar información sensible. Se deduce que estos resultados pueden provocar un impacto negativo en la institución, el hecho de no conocer como clasificar o manejar información sensible crea grandes vulnerabilidades, lo ideal es que la mayor parte del personal administrativo sepa cómo lidiar con información clasificada y tenga a mano un manual o una guía a seguir en casos de utilizar información sensible.

Figura 5

Medidas disciplinarias en caso de incumplimiento de las políticas de seguridad.

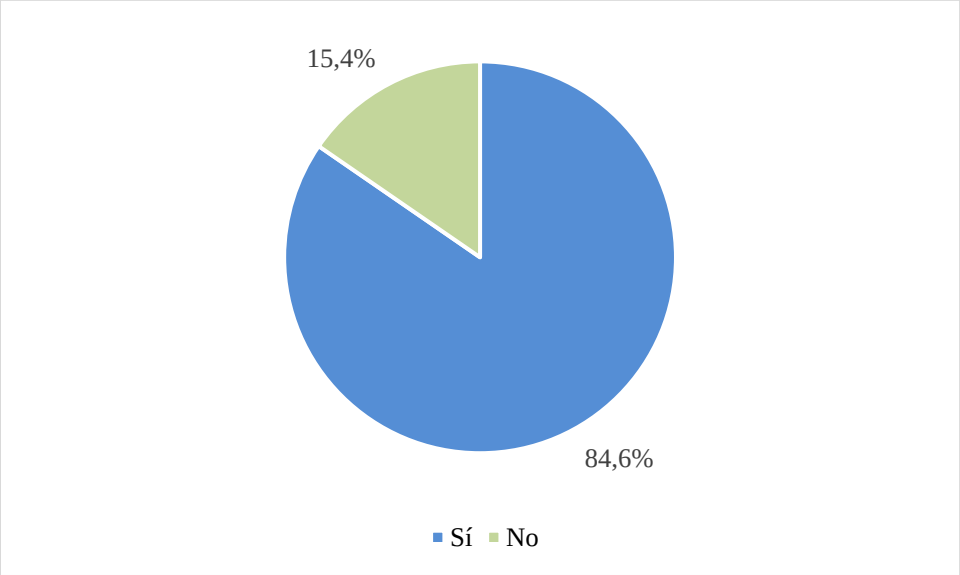


Según la Figura 5, el 61,5% de los encuestados afirma que en el colegio no se aplican sanciones ni medidas disciplinarias en caso de incumplimiento de las políticas de seguridad, mientras que el 38,5% señala que sí existen estas medidas disciplinarias. La ausencia de un sistema disciplinario claro se convierte en un factor negativo para la institución, ya que, al no existir consecuencias ante los errores, estos pueden repetirse sin control, afectando la seguridad y el adecuado manejo de la información.

Implementar un reglamento que detalle sanciones específicas ayuda a prevenir reincidencias y fomenta una cultura de responsabilidad y compromiso entre los miembros de la comunidad educativa. De esta manera, se incentiva un uso cuidadoso de la información, que garantice un entorno seguro y estructurado dentro del colegio.

Figura 6

Ambiente de trabajo seguro en seguridad de la información.



Según la Figura 6, solo un 15,4% de los encuestados considera que este no es positivo. Este grupo minoritario puede haber tenido experiencias negativas o incidentes que hayan afectado su confianza en la seguridad del entorno laboral, lo cual evidencia la importancia de atender cualquier situación que pueda comprometer dicha percepción.

Una parte significativa, representada por el 84,6% de la población, afirma sentirse en un ambiente de trabajo confiable en términos de seguridad de la información. Este resultado sugiere que los espacios de trabajo, así como los equipos que se utilizan, favorecen el control y la protección de la información sensible.

Además, se agrega el hecho que las oficinas de trabajo cuentan con acceso restringido y limitado solo al personal autorizado. Esto contribuye de forma directa al fortalecimiento de las prácticas de seguridad, lo que protege los datos administrativos, y crea un entorno de confianza que promueve una cultura organizacional responsable; así como colaboradores respaldados y comprometidos con el resguardo de la información institucional.

Tabla 14

Nivel de conocimiento sobre las políticas de seguridad de la información

Criterios	Valor absoluto
Alto	1
Medio	11
Bajo	1
Total	13

Según la Tabla 14, 11 personas indican tener un nivel medio y una personas nivel bajo, mientras que solo una de ellas menciona que el nivel de conocimiento es alto, por lo tanto, se puede afirmar que el nivel de conocimiento se encuentra en un término medio, si bien no es alarmante, refleja la falta de capacitación o actualización en las políticas de seguridad, y de este modo vulnerabilidades que amenacen a la institución en temas de la protección de la información.

El nivel medio de conocimiento demuestra ser efectivo puesto que los empleados realizan tareas diarias y mantienen seguridad básica en sus informaciones como contraseñas en sus datos, pero con este nivel sería incapaz poder identificar o gestionar avanzadas o complejas, es necesario que en los procesos administrativos se mantenga un nivel alto, sobre todas o la mayoría de las políticas de seguridad de la información, para asegurar que la información este siempre protegida, y mantener un espacio de trabajo seguro donde se fortalezca la seguridad organizacional de manera integral y asegurar que se esté bien preparado para manejar la información sensible.

Tabla 15

Capacitación en seguridad de la información

Criterios	Valor absoluto
Sí	4
No	9
Total	13

Según la Tabla 15, acerca de si el personal administrativo ha recibido o no capacitaciones se refleja que la mayoría con 9 votos, no han recibido capacitaciones sobre seguridad de la información, donde únicamente 4 personas si han recibido y no precisamente brindadas por la institución a la que trabajan, lo cual puede provocar un impacto negativo ya que lo ideal es que todas las personas que manejan información sensible o confidencial tenga conocimiento de cómo llevar a cabo estos procesos y para ello son necesarias las capacitaciones, la falta de capacitación en seguridad de la información representa una vulnerabilidad significativa. Es fundamental que el personal administrativo encargado de gestionar información sensible y confidencial esté preparado para identificar y gestionar posibles amenazas o incidentes asociados con la seguridad de los datos.

Tabla 16

Capacitación en políticas y procedimientos de seguridad de la información

Criterios	Valor absoluto	Valor relativo
Manuales	2	15,4%
Videos	8	61,5%
Cursos en línea	5	38,5%
Talleres y charlas presenciales	2	15,4%
Ninguno	2	15,4%

En referencia a la Tabla 16, la mayoría del personal administrativo recibió capacitación por medio de videos y cursos en línea, lo cual indica que hay preferencia o accesibilidad a estos métodos, mientras que solo una parte recibió capacitación por medio de manuales, talleres y charlas presenciales, mientras que 2 de ellas no han recibido ningún tipo de capacitación por estos medios. Se demuestra que la institución debe de disponer videos a disposición del personal administrativo, que refuercen el tema de seguridad de la información, las capacitaciones por medio de estos son fundamentales para proteger los datos sensibles y garantizar un entorno de trabajo seguro, la falta de capacitación expone a la organización a una serie de riesgos, incluyendo filtraciones de datos o errores humanos.

Una posibilidad es cursos en línea para potenciar el conocimiento sobre las políticas y procedimientos de seguridad de la información y lograr un ambiente seguro, a la vez mitiga posibles amenazas puesto que existen dos personas que no han recibido ningún tipo de capacitación por estos medios y es necesario para reforzar la seguridad de la información de la institución.

Tabla 17

Capacitaciones constantes en seguridad de la información

Criterios	Valor absoluto
Sí	1
No	12
Total	13

De acuerdo con la Tabla 17, con la capacitación constante en seguridad de la información por parte del colegio 12 personas indican que no se realizan capacitaciones constantes en seguridad de la información mientras que 1 de ellas indica que sí se realizan capacitaciones constantes sobre este aspecto, dicho esto se afirma que el colegio no capacita al personal administrativo en temas de seguridad de la información.

Debido a la falta de capacitaciones constantes la institución se expone a posibles consecuencias, por ejemplo, perdida de información sensible, ciberataques, o accesos no autorizados, lo que puede afectar las labores diarias del colegio por falta de conocimiento en el tema, en un mundo globalizado los ciberataques y las técnicas para robar o exponer información sensible avanza vertiginosamente. Siendo una necesidad las capacitaciones constantes que ayuden al personal a reforzar el tema y mantener un espacio seguro, una capacitación regular ayuda a los empleados no solo a aprender a detectar y prevenir los riesgos, sino también a adoptar una mentalidad de responsabilidad compartida para proteger la información.

Tabla 18

Acceso a documentos de seguridad de la información

Criterios	Valor absoluto
Sí	3
No	10
Total	13

De acuerdo con la Tabla 18, 10 de los participantes mencionan que no tienen acceso a documentos de seguridad de la información, mientras que 3 de ellos mencionan que, si tienen acceso a documentos sobre el tema, la mayoría de estas no cuentan con accesibilidad a estos documentos lo que puede ser una desventaja para la institución y la seguridad de la información que se manejen.

Por lo anterior, es necesario poner a disposición del personal administrativo diversos documentos relacionados con la seguridad de la información, de manera que puedan acceder a ellos para su estudio y capacitación continua. Esto garantiza que el personal cuente con los conocimientos necesarios para mantener un entorno laboral seguro en materia de protección de datos. No solo se debe facilitar el acceso a estos documentos, sino también brindar

capacitaciones periódicas sobre su contenido y aplicación. El acceso a esta información permitirá al personal no solo identificar y prevenir riesgos, sino también adoptar una cultura de responsabilidad compartida en la protección de la información, contribuyendo así al bienestar y seguridad de la institución.

CAPÍTULO V

Conclusiones

De acuerdo con los resultados obtenidos y los objetivos de seguridad de la información, se concluye que la falta de acceso a documentos de seguridad de la información es una brecha significativa en la protección de datos dentro de la institución. Las acciones que se aplican en la actualidad son parciales, informales o implementadas de manera aislada por algunos administrativos. No se cuenta con una política institucional que controle de forma sistemática el acceso, almacenamiento, respaldo y eliminación de la información.

Asimismo, el Colegio no dispone de herramientas avanzadas de protección digital, como sistemas de cifrado de archivos, controles de acceso diferenciados por roles o autenticación basada en múltiples factores. Además, no se llevan a cabo copias de seguridad periódicas automatizadas, ni auditorias regulares del estado de la información digital o física. Todo esto amenaza la privacidad, confidencialidad, integridad y disponibilidad de la información sensible, tales como registros institucionales de importancia, expedientes de estudiantes, datos personales de los estudiantes y personal docente y administrativo entre otros.

La falta de una estrategia institucional para enfrentar amenazas como el acceso no autorizado, pérdida de información, muestra una debilidad estructural que compromete la eficiencia de los procesos administrativos, la confianza institucional ante incidentes informáticos.

Además, el análisis realizado sobre los procesos administrativos en las oficinas del Colegio Técnico Profesional San Isidro, se evidencia la necesidad de fortalecer la concientización del personal respecto a la seguridad de la información. Se identifican deficiencias significativas en el conocimiento y manejo de datos sensibles, lo que incrementa las vulnerabilidades frente a amenazas internas y externas. La falta de conciencia sobre

prácticas seguras compromete no solo la integridad de los procesos, sino también la imagen institucional.

Los funcionarios desconocen los protocolos para proteger la información, lo que genera prácticas riesgosas, como el uso de contraseñas débiles y sensibles, abrir correos o links sospechosos o el manejo incorrecto de información digital o física.

Asimismo, no hay campañas internas, ni materiales de apoyo informativo, ni lineamientos que mantenga el tema en el trabajo diario. La institución no promueve activamente una mentalidad preventiva en materia de la seguridad de la información, lo que limita al personal detectar riegos o amenazas, actuar con precaución e informar a tiempo. Esta falta de sensibilización aumenta considerablemente la vulnerabilidad del colegio ante posibles vulneraciones, ya que los fallos humanos son una de las principales razones de incidentes de seguridad en entidades.

Se concluye que el nivel de conocimiento del personal administrativo sobre las políticas de seguridad de la información está claramente por debajo de lo ideal, pone en peligro la protección de los datos dentro de la organización. Es necesario tomar medidas inmediatas para elevar este nivel de conocimiento y asegurar que todos los empleados estén bien preparados para manejar la información de manera segura. Esto no solo mitiga las amenazas internas, sino que también fortalece la seguridad organizacional de manera integral.

En un entorno donde la utilización de plataformas digitales electrónicas, el intercambio de información en línea y la gestión digital de documentos se ha vuelto cotidiano, la capacitación se convierte en un componente indispensable para la resiliencia institucional. Su omisión coloca al personal en una posición de vulnerabilidad en las operaciones y expone los recursos informáticos del colegio en riesgos evitables.

Recomendaciones

Desarrollar e implementar políticas de seguridad de la información institucional, con especificaciones de roles, tareas, protocolos de acceso, niveles de seguridad y disciplina para las medidas disciplinarias ante posibles incumplimientos.

Incorporar herramientas de protección de tecnología, como software para actualizaciones, sistemas de codificación de documentos, Autenticación de Factores Múltiples (MFA) y plataforma de administración de documentos con control de versiones. Establecer mecanismos de operación de datos automáticos, tanto en dispositivos físicos como en la nube, con una o dos semanas y realizando pruebas de recuperación para garantizar la pérdida de información. Clasificar la información de acuerdo con los niveles de sensibilidad, determinando diferentes datos secretos, reservas o procedimientos de datos públicos. Este proceso permite determinar qué documento requiere protección especial.

Asimismo, realizar periódicamente un análisis de auditoría interna y riesgos informáticos para identificar vulnerabilidad, considerar el cumplimiento político y evaluar la efectividad de los factores de gestión de la realidad.

Del mismo modo, se recomienda que el colegio implemente un programa integral de concientización en seguridad de la información dirigido en especial al personal administrativo. Este programa debe incluir campañas informativas, talleres prácticos y simulaciones de escenarios de riesgo que promuevan una cultura de prevención y responsabilidad. Además, es ideal complementar esto con capacitaciones periódicas, enfocadas en el desarrollo de una actitud hacia la protección de datos. La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) puede servir como marco para estructurar estas iniciativas y asegurar así que la concientización se mantenga como un proceso continuo. Esto permite que todos los colaboradores comprendan su papel en la seguridad institucional y actúen en consecuencia ante los desafíos digitales actuales.

Establecer sistemas de comunicación ágil y anónimo para incidentes vinculados a la seguridad de la información, de manera que los responsables adviertan sobre anomalías sin miedo a represalias. Incorporar la seguridad de la información como asunto transversal en las reuniones, con el objetivo de mantener el asunto visible y potenciar su relevancia en la cultura de la organización. Promover buenas prácticas a través de reconocimientos o incentivos, como un componente de una estrategia para fomentar la mejora continua en el uso responsable de la tecnología.

Por lo tanto, se recomienda que la institución implemente un plan de formación continua que incluya sesiones periódicas, ya sea trimestrales o semestrales, sobre temas relacionados con la seguridad de la información. La capacitación debe ser un proceso constante, integrado en la cultura organizacional que prioriza la seguridad.

También, es beneficioso crear manuales, guías rápidas y recursos accesibles que los empleados consulten en cualquier momento. Esto resulta útil para aquellos con niveles de conocimiento intermedios o bajos, ya que les proporciona herramientas para recordar y aplicar adecuadamente las políticas de seguridad. En suma, implementar evaluaciones diagnósticas periódicas para determinar los niveles de conocimiento del personal y adaptar la formación a sus necesidades reales. Capacitar a los eliminar funcionarios desde su ingreso, integrando contenidos sobre seguridad digital en el proceso de inducción institucional.

Para mejorar la seguridad, es necesario proporcionar acceso adecuado a los documentos, mantenerlos actualizados y ofrecer capacitación continua que ayude a mantener a los administrativos actualizados sobre los riegos de la información sensible. Los objetivos de seguridad de la información en una institución, generalmente, se centran en garantizar que los datos sensibles sean protegidos de accesos no autorizados y que todos los empleados comprendan las políticas y procedimientos necesarios para asegurar dicha protección.

Se recomiendan medidas de protección de la información para el fortalecimiento de la seguridad en los procesos administrativos que garanticen la integridad, confidencialidad y disponibilidad de los datos, entre ellas:

Ejecutar actualizaciones periódicas de los protocolos existentes de la seguridad de la información al menos una vez al año, ya que las amenazas informáticas son frecuentes.

También realizar procedimientos específicos según el tipo de incidente, asignar responsables y tiempo de respuesta, asimismo, generar informes y planes de mejora para evitar recurrencias.

Crear un comité de seguridad de la información conformado por personal administrativo, docente de informática y representante de dirección, con la finalidad de que supervisen la implementación de las políticas y la evaluación continua de los riegos.

En medidas técnicas de seguridad, es importante que se implementen sistemas de autenticación confiables como usar contraseñas complejas, autenticación de factores múltiples y control de sesiones de usuarios para los sistemas utilizados por los administrativos y académicos.

Asimismo, mantener todos los sistemas utilizados en la institución en constante actualización de software y sistemas operativos para protegerlos contra vulnerabilidad. Establecer niveles de acceso según las funciones de cada administrativo o académico para así evitar que usuarios sin autorización accedan a información sensible. Toda información confidencial, como expedientes de estudiantes, datos financieros o documentos legales deben almacenarse utilizando algoritmos de cifrado.

Realizar copias de seguridad periódicas en medios físicos y en la nube, con pruebas de recuperación programadas para garantizar la recuperación ante incidentes.

También, actualizaciones de software continuas y sistemas operativos: para todos los sistemas utilizados en la organización para protegerlos.

En el mejoramiento de la gestión documental se recomienda implementar sistemas que registren los cambios realizados en documentos administrativos y este permita identificar el responsable de cada modificación.

También, utilizar escáneres, impresoras y software que garanticen la integridad y legibilidad de los documentos. Y almacenar estos documentos en espacios seguros, con acceso restringido y sistemas de inventario controlado.

Es importante realizar capacitaciones periódicas sobre la seguridad de la información abarcado temas como, reconocimientos de correos electrónicos, utilización de factores múltiples, manejo adecuado de las contraseñas, manipulación segura de la información física y digital, actualización de software y sistemas operativos, navegación segura en internet, entre otros, que ayuden a la concientización del personal.

Asimismo, implementar simulacros de respuesta ante incidentes de seguridad que permitan medir la capacidad de respuesta del personal ante posibles violaciones de seguridad.

Elaborar material informativo que permita mantener presente la importancia de la seguridad de la información.

Referencias

Alvarado J. et al. (2019). Asistente Virtual en el Sistema de Gestión Seguridad de la Información para Gestor de Base de Datos ORACLE. https://repositorio.una.ac.cr/bitstream/handle/11056/17263/Asistente%20Virtual%20en%20el%20Sistema%20de%20Gestión%20Seguridad%20de%20la%20Información%20para%20Gestor%20de%20Base%20de%20Datos%20ORACLE.pdf?sequence=1&isAllowed=y

Álvarez, P. (2018). Ética e investigación. file:///C:/Users/user/Downloads/Dialnet-EticaEInvestigacion-6312423.pdf

Arias, W. (2021). La Unidad de Capacitación y Desarrollo, es una de las cuatro unidades que conforman el Área de Desarrollo Humano, siendo las otras tres: Gestión del Desempeño, Calidad de Vida Laboral y Reclutamiento y Selección. Unidad de Capacitación y Desarrollo – Oficina de Recursos Humanos (ucr.ac.cr)

Azuero Á. (2018). Significatividad del marco metodológico en el desarrollo de proyectos de investigación. Revista Arbitrada Interdisciplinaria Koinonía, 4(8), 110-127. Significatividad del marco metodológico en el desarrollo de proyectos de investigación (redalyc.org)

Ballina, F. (s.f). Paradigmas y perspectivas teórico-metodológicas en el estudio de la administración. https://www.uv.mx/iiesca/files/2013/01/paradigmas2004-2.pdf

Cano, C. (2017). La administración y el proceso administrativo. Proceso-Administrativo.pdf (ccie.com.mx)

Colegio Técnico Profesional San Isidro. (S.f). Historia. Colegio Técnico Profesional San Isidro (edupage.org)

Corona Martínez, Luis A., y Fonseca Hernández, Mercedes. (2023). Las hipótesis en el proyecto de investigación: ¿cuándo si, cuándo no?. *Medir*, *21*(1), 269-273

http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1727-897X2023000100269&lng=es&tlng=es

Cruz García, M. (2019). Fuentes de información. Boletín Científico de las Ciencias Económico Administrativas del ICEA, 8(15), 57-58. https://doi.org/10.29057/icea.v8i15.4864

Esparza, R y Rubio, J. (2016). La pregunta por el conocimiento. Saber, 28(4), 813-818. http://ve.scielo.org/scielo.php?script=sci_arttext&pid=S1315-01622016000400016&lng=es&tlng=es

Ferrer, P. y Senovia, L. (2023). El enfoque cualitativo: Una alternativa compleja dentro del mundo de la investigación. *Revista Arbitrada Interdisciplinaria Koinonía*, *8*(15), 1-3. https://doi.org/10.35381/r.k.v8i15.2440

Flores, C. y Caiza, E. (2017). La concientización como factor crítico para la gestión de la seguridad de lainformación. https://www.researchgate.net/publication/322882278_La_concientizacion_como_factor_critico_para_la_gestion_de_la_seguridad_de_la_informacion

García, G y Vidal, M. (2016). La informática y la seguridad. Un tema de importancia para el directivo. Infodir, 12(22), 47-58. https://www.medigraphic.com/pdfs/infodir/ifd-2016/ifd1622g.pdf

Guevara, G; Verdesoto A y Castro N. (2020). Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción). RECIMUNDO, 163-173.file:///C:/Users/user/Downloads/Dialnet-MetodologiasDeInvestigacionEducativaDescriptivasEx-7591592.pdf

Hernández Sampieri, R., Fernández Collado, C., y Baptista Lucio, M. (2014). Metodología de la investigación (sexta ed.). McGraw-Hill Education. https://apiperiodico.jalisco.gob.mx/api/sites/periodicooficial.jalisco.gob.mx/files/metodologia_de_la_investigacion_-_roberto_hernandez_sampieri.pdf

Hernández Sampieri, R., Fernández Collado, C., y Baptista Lucio, M. (2014). Metodología de la investigación (sexta ed.). https://www.esup.edu.pe/wp-content/uploads/2020/12/2.%20Hernandez,%20Fernandez%20y%20Baptista-Metodolog%C3%ADa%20Investigacion%20Cientifica%206ta%20ed.pdf

Infoem. (2023). Medidas de seguridad. https://www.infoem.org.mx/es/contenido/datos-personales/medidas-de-seguridad

LOPD. (2023).Tipos de seguridad de la información: una guía completa. Tipos de seguridad de la información: una guía completa - LOPD y Más (lopddirecta.es)

Lorenzon, A y Romero, M. (2019). Educación para la comprensión humana: desarrollo de la intersubjetividad desde la complejidad. Revista Educação em Questão, 57(53), 1-18. https://www.redalyc.org/articulo.oa?id=563965384002

Ministerio de Educación Pública. (S.f). Circuitos Educativos / Supervisores de centros educativos. https://juntas.mep.go.cr/circuitos-educativos-supervisores-de-centros-educativos/#:~:text=Los%20Circuitos%2C%20cumplen%20con%20la,calidad%20del%20sistema%20educativo%20costarricense.

Ministerio de Educación Pública. (S.f). Reseña histórica. Reseña histórica | Dirección de Infraestructura Educativa (mep.go.cr)

Ministerio de Educación Pública. (S.f.). Oferta educativa https://www.mep.go.cr/oferta-educativa

Navarro, B. (2020). ANÁLISIS DEL CONTEXTO Y PLANIFICACIÓN ESTRATÉGICA. http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1061_VilcaSM.pdf

Obando, M. (2020). Capacitación del talento humano y productividad: Una revisión literaria. ECA Sinergia, vol. 11, núm. 2, pp. 166-173. https://www.redalyc.org/journal/5885/588563773012/html/

Ospina, M., y Sanabria, P. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Reviste Criminalidad,* 62(2), 199-217. https://repositorio.una.ac.cr/bitstream/handle/11056/17263/Asistente%20Virtual%20en%20el%20Sistema%20de%20Gestión%20Seguridad%20de%20la%20Información%20para%20Gestor%20de%20Base%20de%20Datos%20ORACLE.pdf?sequence=1&isAllowed=y

Otzen, T y Manterola, C. (2017). Técnicas de Muestreo sobre una Población a Estudio. http://dx.doi.org/10.4067/S0717-95022017000100037

Pacheco, V. (2024). Población y muestra. *International journal of interdisciplinary dentistry*, *17*(2), 66. https://dx.doi.org/10.4067/s2452-55882024000200066

Piza, N., Amaiquema, F., y Beltrán, G. (2019). Métodos y técnicas en la investigación cualitativa. Algunas precisiones necesarias. *Conrado, 15*(70), 455-459. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1990-86442019000500455&lng=es&tlng=es

Rivero, M. (2021). Cómo elaborar el Marco teórico de tu tesis o proyecto de investigación. (PDF) Cómo elaborar el Marco teórico de tu tesis o proyecto de investigación (researchgate.net) (PDF)

Rocha C. (2011). La Seguridad Informática. Revista Ciencia Unemi, 4(5), 26-33. https://www.redalyc.org/articulo.oa?id=582663867004

Rodríguez F. (2010). Seguridad de la información: estrategia para fortalecer el gobierno corporativo. Revista de Derecho Privado, (43), 3-24. SEGURIDAD DE LA INFORMACIÓN: ESTRATEGIA PARA FORTALECER EL GOBIERNO CORPORATIVO (redalyc.org)

Roldán, G. et. al. (2015). *Propuesta de un Sistema de Gestión de la Seguridad de la Información para organizaciones en Costa Rica.* https://hdl.handle.net/20.500.14230/5244

Sisti, M. (2019).Seguridad informática: La protección de la información de una empresa vitivinícola de Mendoza, 2019. https://bdigital.uncu.edu.ar/objetos_digitales/15749/sistimariaagustina.pdf

Vega W. (2008). POLITICAS Y SEGURIDAD DE LA INFORMACION. *Fides et Ratio - Revista de Difusión cultural y científica de la Universidad La Salle en Bolivia*, *2*(2), 63-69. http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2008000100008&lng=es&tlng=es

Vega, E. (2021). *Seguridad de la Información.* https://3ciencias.com/wp-content/uploads/2021/03/LIBRO-SEGURIDAD-INFORMACIO%CC%81N.pdf

APÉNDICES

Apéndice 1. Carta de tutor

19 de abril de 2024
San Isidro de El General, Pérez Zeledón

Señores
Comisión Trabajos Finales de Graduación
Universidad Nacional
Sede Regional Brunca
Campus Pérez Zeledón

Estimados señores:

Acepto colaborar como Tutora del Trabajo Final de Graduación denominado "Análisis de la seguridad de la información en los procesos administrativos en las oficinas del Colegio Técnico Profesional San Isidro, Periodo 2024", en atención a la solicitud realizada por las personas estudiantes, quienes optan por el grado de Licenciatura en Administración de Oficinas:

Nombre	Cédula
Ericka Acuña Durán	1-1852-0705
Yirlany Benavides Solís	1-1850-0700
Vanessa Varela González	1-1782-0480

Es importante señalar que en este I Ciclo 2024, imparto a los estudiantes el curso Metodología de Investigación para Administración de Oficinas I.

Sin otro particular,

DIGNA MARIA DEL CARMEN VALVERDE FALLAS (FIRMA)
PERSONA FISICA, CPF-01-0729-0109.
Fecha declarada: 19/04/2024 06:17:06 PM
Esta es una representación gráfica únicamente,
verifique la validez de la firma.

MSc Digna Valverde Fallas
Cédula: 107290109

Apéndice 2. Cartas de asesores

19 de abril de 2024
San Isidro de El General, Pérez Zeledón

Señores
Comisión Trabajos Finales de Graduación
Universidad Nacional
Sede Regional Brunca
Campus Pérez Zeledón

Estimados señores:

Acepto colaborar como asesora del Trabajo Final de Graduación denominado "Análisis de la seguridad de la información en los procesos administrativos en las oficinas del Colegio Técnico Profesional San Isidro, Periodo 2024", en atención a la solicitud realizada por las personas estudiantes, quienes optan por el grado de Licenciatura en Administración de Oficinas:

Nombre	Cédula
Ericka Acuña Durán	1-1852-0705
Yirlany Benavides Solís	1-1850-0700
Vanessa Varela González	1-1782-0480

Sin otro particular,

LEONELLA NARANJO JIMENEZ (FIRMA)

Firmado digitalmente por LEONELLA NARANJO JIMENEZ (FIRMA)
Fecha: 2024.04.22 21:19:31 -06'00'

Leonella Naranjo Jiménez
Cédula: 304090958

17 de abril de 2024
San Isidro de El General, Pérez Zeledón

Señores
Comisión Trabajos Finales de Graduación
Universidad Nacional
Sede Regional Brunca
Campus Pérez Zeledón

Estimados señores:

Acepto colaborar como asesor del Trabajo Final de Graduación denominado "Análisis de la seguridad de la información en los procesos administrativos en las oficinas del Colegio Técnico Profesional San Isidro, Periodo 2024", en atención a la solicitud realizada por las personas estudiantes, quienes optan por el grado de Licenciatura en Administración de Oficinas:

Nombre	Cédula
Ericka Acuña Durán	1-1852-0705
Yirlany Benavides Solís	1-1850-0700
Vanessa Varela González	1-1782-0480

Sin otro particular,

ARIEL ALFREDO HIDALGO BRENES (FIRMA)
Firmado digitalmente por ARIEL ALFREDO HIDALGO BRENES (FIRMA)
Fecha: 2024.04.22 13:35:14 -06'00'

Ariel Hidalgo Brenes
Cédula: 115120732

Apéndice 3. Transcripción de acuerdo

Sede Regional Brunca
Comisión de Trabajos Finales de Graduación

TRANSCRIPCIÓN DE ACUERDO
UNA-CTFG-SRB-ACUE-011-2024
31 de mayo de 2024

PARA: Ericka Acuña Durán
Yirlany Benavides Solís
Vanessa Varela González
Licenciatura en Administración de Oficinas

DE: Comisión de Trabajos Finales de Graduación
Sede Regional Brunca

Para su información y efectos consiguientes, me permito transcribir el acuerdo tomado por la Comisión de Trabajos finales de Graduación de la Sede Regional Brunca, Universidad Nacional, en la Sesión Extraordinaria N°001-2024, del treinta de mayo de dos mil veinticuatro, que dice:

CONSIDERANDO:

1. Correo suscrito por Digna Valverde Fallas, con fecha del 30 de abril, donde adjunta los documentos requeridos para la revisión del anteproyecto y aprobación del comité asesor.

2. Carta con fecha del 19 de abril de 2024, suscrita por la académica Leonella Naranjo Jiménez, donde acepta colaborar como asesora en el proyecto.

3. Carta con fecha del 17 de abril de 2024, suscrita por el académico Ariel Hidalgo Brenes, donde acepta colaborar como asesor en el proyecto.

4. Carta con fecha del 30 de abril, de la académica Digna Valverde Fallas, donde acepta ser la Directora del Proyecto.

5. Documento del Anteproyecto titulado: "Análisis de la seguridad de la información en los procesos administrativos en las oficinas del Colegio Técnico Profesional San Isidro, Periodo 2024."

POR TANTO, SE ACUERDA:

5. APROBAR EL ANTEPROYECTO CON OBSERVACIONES EN MODALIDAD PROYECTO TÍTULADO "ANÁLISIS DE LA SEGURIDAD DE LA INFORMACIÓN EN LOS PROCESOS

UNA-CTFG-SRB-ACUE-011-2024
31 de mayo de 2024
Pág. -2-

ADMINISTRATIVOS EN LAS OFICINAS DEL COLEGIO TÉCNICO PROFESIONAL SAN ISIDRO, PERIODO 2024"

Enlace a las observaciones:
https://drive.google.com/file/d/1qXpUo1B0lxn_1DWeofg7NMmLuYbsTmtG/view?usp=sharing

6. APROBAR EL COMITÉ ASESOR CONFORMADO POR:

- **DIGNA VALVERDE FALLAS. DIRECTORA DEL TFG**
- **LEONELLA NARANJO JIMÉNEZ. ASESORA**
- **ARIEL HIDALGO BRENES. ASESOR**

Cordialmente,

JOSUE ALEJANDRO NARANJO CORDERO (FIRMA)
PERSONA FISICA, CPF-01-1398-0764.
Fecha declarada: 31/05/2024 03:07:01 PM

MSc. Josué Naranjo Cordero
Presidente
Comisión Trabajos Finales de Graduación

C.
Digna Valverde Fallas. Directora del TFG
Leonella Naranjo Jiménez. Asesora
Ariel Hidalgo Brenes. Asesor

Apéndice 4. Carta de solicitud de aplicación de instrumentos

Universidad Nacional
Sede Regional Brunca
Campus Pérez Zeledón

San Isidro de El General
31 de octubre de 2024

Máster Agnes Makré Mora
Directora Institucional
Colegio Técnico Profesional San Isidro

Estimada Directora

Las estudiantes de la carrera de Administración de Oficinas de la Universidad Nacional: Ericka Acuña Durán, cédula 1-1852-0705, Yirlany Benavides Solís, cédula 1-1850-0700 y Vanessa Varela González, cédula 1-1782-0480; están interesadas en realizar el Trabajo Final de Graduación de la Licenciatura en Administración de Oficinas en el Colegio Técnico Profesional San Isidro.

El tema planteado es **"Análisis de la seguridad de la información en los procesos administrativos en las oficinas del Colegio Técnico Profesional San Isidro"**. La investigación se realizará desde el mes de marzo hasta finales de diciembre aproximadamente y se requiere obtener datos de la seguridad de la información utilizada en los procesos administrativos del colegio. Por tanto, es necesario visitar las instalaciones del colegio para obtener datos que respalden la investigación.

El objetivo es realizar un trabajo de excelencia que favorezca tanto a las estudiantes como al colegio, brindándoles alguna propuesta beneficiosa como parte del proyecto. Por lo anterior, le ruego analice la posibilidad de brindar el permiso para trabajar en el colegio a la brevedad posible.

Quedo atenta a su respuesta para iniciar la coordinación con ustedes de ser afirmativa su resolución.

MSc. Digna Valverde Fallas
Académica, Universidad Nacional
digna.valverde.fallas@una.ac.cr
Tel. 8810-9648

COLEGIO TÉCNICO PROFESIONAL SAN ISIDRO, P.Z. DIRECCIÓN

Apéndice 5. Carta de aprobación de aplicación de instrumentos

MINISTERIO DE EDUCACIÓN PÚBLICA | GOBIERNO DE COSTA RICA

Dirección Regional de Educación de Pérez Zeledón
Circuito 03
Colegio Técnico Profesional San Isidro

San Isidro, Pérez Zeledón
31 de octubre de 2024

MSc. Digna Valverde Fallas
Académica, Universidad Nacional
Sede Regional Brunca
Campus Pérez Zeledón

Cordial saludo:

Como directora institucional del Colegio Técnico Profesional San Isidro, apruebo que las estudiantes de la carrera de Administración de Oficinas de la Universidad Nacional: Ericka Acuña Durán, cédula 1-1852-0705, Yirlany Benavides Solís, cédula 1-1850-0700 y Vanessa Varela González, cédula 1-1782-0480; realicen la tesis de la Licenciatura en Administración de Oficinas, en este centro educativo.

Por este motivo, se aprueba el ingreso de las estudiantes antes mencionadas, a las instalaciones la institución; así mismo se autoriza la obtención de información y aplicación de instrumentos al personal, esto en el periodo de marzo a diciembre de 2024.

A sus órdenes para lo que corresponda, atentamente.

Máster Agnes Makré Mora
Directora Institucional
CTP San Isidro

COLEGIO TÉCNICO PROFESIONAL TECNOLOGÍA A LA MEDIDA DEL FUTURO SAN ISIDRO, P.Z. DIRECCIÓN

C/c: Archivo

Apéndice 6. Validación de asesores del instrumento entrevista

Estudiantes: Ericka Acuña Durán, Yirlany Benavides Solís y Yilda Vanessa Varela González

Tema TFG: Análisis de la seguridad de la información en los procesos administrativos en las oficinas del Colegio Técnico Profesional San Isidro

Instrumento: Entrevista

ÍTEM	CRITERIOS A EVALUAR CADA INSTRUMENTO										Observaciones (si debe eliminarse o modificarse un ítem por favor indique)
	Claridad en la redacción		Coherencia interna		Inducción a la respuesta (Sesgo)		Lenguaje adecuado con el nivel del informante		Mide lo que pretende		
	Sí	No	Sí	No	Sí	No	Sí	No	Sí	No	
1	X		X		X		X		X		
2	X		X		X		X		X		
3	X		X		X		X		X		
4	X		X		X		X		X		
5	X		X		X		X		X		

Aspectos Generales	Sí	No	
El instrumento contiene instrucciones claras y precisas para responder el cuestionario	x		
Los ítems permiten el logro del objetivo de la investigación	x		
Los ítems están distribuidos en forma lógica y secuencial	x		
El número de ítems es suficiente para recoger la información. En caso de ser negativa su respuesta, sugiera los ítems a añadir	x		

VALIDEZ			
APLICABLE	x	NO APLICABLE	
APLICABLE ATENDIENDO A LAS OBSERVACIONES			

Validado por: Ariel Hidalgo Brenes		Fecha: 16/10/2024

Firma: ARIEL ALFREDO HIDALGO BRENES (FIRMA) — Firmado digitalmente por ARIEL ALFREDO HIDALGO BRENES (FIRMA) Fecha: 2024.10.16 13:01:30 -06'00'	Teléfono: 86457100	
Correo: ariel.hidalgo.brenes@una.cr		
Observaciones:		

Estudiantes: Ericka Acuña Durán , Yirlany Benavides Solís y Yilda Vanessa Varela González

Tema TFG: Análisis de la seguridad de la información en los procesos administrativos en las oficinas del Colegio Técnico Profesional San Isidro

Instrumento: Entrevista

ÍTEM	CRITERIOS A EVALUAR CADA INSTRUMENTO										Observaciones (si debe eliminarse o modificarse un ítem por favor indique)
	Claridad en la redacción		Coherencia interna		Inducción a la respuesta (Sesgo)		Lenguaje adecuado con el nivel del informante		Mide lo que pretende		
	Sí	No	Sí	No	Sí	No	Sí	No	Sí	No	
1	x		x			x	x		x		Sin observaciones
2	x		x			x	x		x		Sin observaciones
3	x		x			x	x		x		Sin observaciones
4	x		x			x	x		x		Sin observaciones
5	x		x			x	x		x		Sin observaciones
6	x		x			x	x		x		Sin observaciones
7	x		x			x	x		x		Sin observaciones
8	x		x			x	x		x		Sin observaciones
9	x		x			x	x		x		Sin observaciones
10	x		x			x	x		x		Sin observaciones
11	x		x			x	x		x		Sin observaciones
12	x		x			x	x		x		Sin observaciones
13	x		x			x	x		x		Sin observaciones

Aspectos Generales	Sí	No	
El instrumento contiene instrucciones claras y precisas para responder el cuestionario	x		
Los ítems permiten el logro del objetivo de la investigación	x		
Los ítems están distribuidos en forma lógica y secuencial	x		
El número de ítems es suficiente para recoger la información. En caso de ser negativa su respuesta, sugiera los ítems a añadir	x		

VALIDEZ			
APLICABLE	x	NO APLICABLE	
APLICABLE ATENDIENDO A LAS OBSERVACIONES			

Validado por: M.B.A María Leonella Naranjo Jiménez		Fecha:
Firma: LEONELLA NARANJO JIMENEZ (FIRMA) Firmado digitalmente por LEONELLA NARANJO JIMENEZ (FIRMA) Fecha: 2024.10.09 11:08:21 -06'00'	Teléfono:8309-6684	9-10-2024
Correo: : maria.naranjo.jimenez@una.cr		
Observaciones:		

Apéndice 7. Validación de asesores del instrumento lista de cotejo

Estudiantes: Ericka Acuña Durán, Yirlany Benavides Solís y Yilda Vanessa Varela González

Tema TFG: Análisis de la seguridad de la información en los procesos administrativos en las oficinas del Colegio Técnico Profesional San Isidro

Instrumento: Lista de cotejo

ÍTEM	CRITERIOS A EVALUAR CADA INSTRUMENTO										Observaciones (si debe eliminarse o modificarse un ítem por favor indique)
	Claridad en la redacción		Coherencia interna		Inducción a la respuesta (Sesgo)		Lenguaje adecuado con el nivel del informante		Mide lo que pretende		
	Sí	No	Sí	No	Sí	No	Sí	No	Sí	No	
1	X		X		X		X		X		
2	X		X		X		X		X		
3	X		X		X		X		X		
4	X		X		X		X		X		
5	X		X		X		X		X		

Aspectos Generales	Sí	No	
El instrumento contiene instrucciones claras y precisas para responder el cuestionario	x		
Los ítems permiten el logro del objetivo de la investigación	x		
Los ítems están distribuidos en forma lógica y secuencial	x		
El número de ítems es suficiente para recoger la información. En caso de ser negativa su respuesta, sugiera los ítems a añadir	x		

VALIDEZ			
APLICABLE	x	NO APLICABLE	
APLICABLE ATENDIENDO A LAS OBSERVACIONES			

Validado por: Ariel Hidalgo Brenes		Fecha: 16/10/2024

Firma: ARIEL ALFREDO HIDALGO BRENES (FIRMA) — Firmado digitalmente por ARIEL ALFREDO HIDALGO BRENES (FIRMA) Fecha: 2024.10.16 13:02:02 -06'00'	Teléfono: 86457100	
Correo: ariel.hidalgo.brenes@una.cr		
Observaciones:		

Estudiantes: Ericka Acuña Durán , Yirlany Benavides Solís y Yilda Vanessa Varela González

Tema TFG: Análisis de la seguridad de la información en los procesos administrativos en las oficinas del Colegio Técnico Profesional San Isidro

Instrumento: Lista de cotejo

ÍTEM	CRITERIOS A EVALUAR CADA INSTRUMENTO										Observaciones (si debe eliminarse o modificarse un ítem por favor indique)
	Claridad en la redacción		Coherencia interna		Inducción a la respuesta (Sesgo)		Lenguaje adecuado con el nivel del informante		Mide lo que pretende		
	Sí	No	Sí	No	Sí	No	Sí	No	Sí	No	
1	x		x			x	x		x		Sin observaciones
2	x		x			x	x		x		Sin observaciones
3	x		x			x	x		x		Sin observaciones
4	x		x			x	x		x		Sin observaciones
5	x		x			x	x		x		Sin observaciones
6	x		x			x	x		x		Sin observaciones
7	x		x			x	x		x		Sin observaciones
8	x		x			x	x		x		Sin observaciones
9	x		x			x	x		x		Sin observaciones
10	x		x			x	x		x		Sin observaciones
11	x		x			x	x		x		Sin observaciones

Aspectos Generales	Sí	No	
El instrumento contiene instrucciones claras y precisas para responder el cuestionario	x		
Los ítems permiten el logro del objetivo de la investigación	x		
Los ítems están distribuidos en forma lógica y secuencial	x		
El número de ítems es suficiente para recoger la información. En caso de ser negativa su respuesta, sugiera los ítems a añadir	x		

VALIDEZ			
APLICABLE	x	NO APLICABLE	
APLICABLE ATENDIENDO A LAS OBSERVACIONES			

Validado por: M.B.A María Leonella Naranjo Jiménez		Fecha:
Firma: LEONELLA NARANJO JIMENEZ (FIRMA) Firmado digitalmente por LEONELLA NARANJO JIMENEZ (FIRMA) Fecha: 2024.10.09 11:07:04 -06'00'	Teléfono: 8309-6684	9 -10-2024
Correo: maria.naranjo.jimenez@una.cr		
Observaciones:		

Apéndice 8. Entrevista

Trabajo final de graduación denominado “Análisis de la seguridad de la información en los procesos administrativos en las oficinas del Colegio Técnico Profesional San Isidro”, realizado por estudiantes de la Universidad Nacional de la carrera Administración de Oficinas.

Objetivo para investigar: Analizar oportunidades de mejora en la protección de la información del Colegio Profesional San Isidro mediante identificación de los protocolos de seguridad de la información en los procesos administrativos.

Importante: La información se utilizará para fines académicos y es de carácter confidencial.

Instrucciones:

Responda de forma clara y concisa, ampliar su respuesta cuando corresponda.

1. ¿Cómo explicaría el concepto de seguridad de la información y la importancia en su trabajo?

2. ¿Cómo clasificaría su nivel de conocimiento sobre las políticas de seguridad de la información del centro educativo?

☐ Bajo
☐ Medio
☐ Alto

3. ¿Ha recibido alguna capacitación en seguridad de la información?

☐ Si
☐ No

4. El personal administrativo se capacita sobre las políticas y procedimientos de seguridad de la información por medio de:

☐ Manuales

- [ ] Videos
- [ ] Cursos en línea
- [ ] Talleres y charlas presenciales
- [ ] Ninguno

5. Elija los principales tipos de seguridad de la información implementados en los procesos administrativos de su oficina.

- [ ] Copias de seguridad
- [ ] Actualización de software
- [ ] Antivirus
- [ ] Contraseñas seguras
- [ ] Verificación en dos pasos (dos formas de identificación)
- [ ] Otra:

6. ¿Considera que los tipos de seguridad de la información implementados han sido efectivos en los procesos administrativos?

- [ ] Muy efectivos
- [ ] Efectivos
- [ ] Poco efectivos
- [ ] Nada efectivos

7. ¿Qué medidas de protección de la información se han implementado hasta ahora en los procesos administrativos?

8. ¿Cómo gestionan los datos sensibles dentro de los procesos administrativos?

- [ ] Con monitoreo y controles de acceso
- [ ] Capacitación y Concienciación del Personal
- [ ] Uso de Software de Gestión de Documentos Seguros
- [ ] Políticas de Seguridad de la Información
- [ ] Copias de seguridad seguras
- [ ] Uso de Contratos de Confidencialidad
- [ ] Ninguna

9. ¿De las siguientes acciones cuáles realiza para proteger la información sensible con la que trabaja?

- ☐ Contraseñas fuertes y únicas para cada cuenta y sistema
- ☐ Cambio las contraseñas regularmente
- ☐ Los documentos y archivos sensibles se protegen antes de ser almacenados o enviados
- ☐ Actualización del equipo tecnológico, mantengo el equipo tecnológico actualizado
- ☐ Copias de seguridad periódicas
- ☐ No se comparte información sensible por correo electrónico o plataformas no seguras
- ☐ Uso software y antivirus de seguridad
- ☐ Control al acceso de la información sensible a través de permisos
- ☐ Otra:

10. ¿Cómo se asegura la disponibilidad de la información en los procesos administrativos ante posibles amenazas?

- ☐ Videos
- ☐ Copias de seguridad periódicas
- ☐ Servicios en la nube
- ☐ Sistemas de recuperación ante desastres
- ☐ Controles de acceso y autenticación segura
- ☐ Otra:

11. ¿Qué vulnerabilidades de seguridad existen en los procesos administrativos actuales?

- ☐ Accesos no autorizados
- ☐ Contraseñas débiles
- ☐ Errores humanos
- ☐ Falta de capacitación y concientización
- ☐ Almacenamiento inseguro de documentos digitales
- ☐ Uso inseguro de correos electrónicos
- ☐ Falta de respaldo
- ☐ Redes inseguras
- ☐ Otra:

12. ¿Qué impacto tienen las medidas de seguridad en la eficiencia y operatividad de los procesos administrativos?

- ☐ Reducción de riesgos y mayor confianza en los procesos
- ☐ Mejora en la protección de datos y cumplimiento normativo
- ☐ Mayor conciencia y responsabilidad del personal
- ☐ Mayor carga en los procesos administrativos
- ☐ Otro:

13. ¿Ha tenido alguna experiencia negativa relacionada con la gestión de información en su lugar de trabajo? De la siguiente lista cuales ha tenido que enfrentar en su puesto de trabajo.

- ☐ Perdida de información sensible
- ☐ Robo de información
- ☐ Accesos no autorizados
- ☐ Daños a la reputación
- ☐ Interrupciones en los procesos
- ☐ Información desorganizada
- ☐ Robo de equipo
- ☐ Otra:

Apéndice 9. Lista de Cotejo

Objetivo: La lista de cotejo tiene como objetivo analizar oportunidades de mejora en la protección de la información del Colegio Profesional San Isidro mediante identificación de los protocolos de seguridad de la información en los procesos administrativos. La información se utilizará para fines académicos, y es de carácter confidencial por las estudiantes de la Universidad Nacional de la carrera de Administración de Oficinas.

Nombre Completo: _____

Puesto: _____ Fecha: _____

Criterios	Si	No	Observación
1. ¿Existen políticas de seguridad de la información en el centro educativo?			
2. ¿Existen sistemas de supervisión, seguimiento y auditoría de parte del Ministerio Educación?			
3. ¿El colegio realiza capacitaciones sobre seguridad de la información constantemente?			
4. ¿Tienen acceso a documentos que ayuden a mantener un trabajo seguro respecto a la seguridad de la información?			
5. ¿El personal tiene claro cómo clasificar y manejar la información más sensible?			
6. ¿Saben cómo funciona la autenticación multifactor?			
7. ¿Las herramientas de seguridad están configuradas y actualizadas?			
8. ¿Se documentan y revisan los incidentes de seguridad para prevenir futuros riesgos?			
9. ¿Se aplican sanciones o medidas disciplinarias en caso de incumplimiento de las políticas de seguridad?			
10. ¿Perciben el ambiente de trabajo como seguro en términos de seguridad de la información?			