Universidad Nacional de Loja

Facultad de la Energía, las Industrias y los Recursos Naturales no Renovables

Maestría en Telecomunicaciones

Análisis y propuesta de gestión de riesgo en infraestructura TI en la Unidad Educativa Quevedo

Trabajo de Titulación previa a la obtención del título de Magíster en Telecomunicaciones

AUTOR:

Ing. Carlos Alberto Bermeo Zamora

DIRECTOR:

Ing. Kleber Rolando Morillo Aguilar, Mg. Sc.

LOJA – ECUADOR

2023

Certificación

Loja, 22 de mayo de 2023

Ing. Kleber Rolando Morillo Aguilar Mg. Sc.

DIRECTOR DE TRABAJO DE TITULACIÓN

CERTIFICO:

Que he revisado y orientado todo proceso de la elaboración del Trabajo de Titulación denominado: **Análisis y propuesta de gestión de riesgo en infraestructura TI en la Unidad Educativa Quevedo**, previo a la obtención del título **de Magíster en Telecomunicaciones,** de autoría del estudiante **Carlos Alberto Bermeo Zamora,** con **cédula de identidad No. 1105761124,** una vez que el trabajo cumple con todos los requisitos exigidos por la Universidad Nacional de Loja para el efecto, autorizo la presentación para la respectiva sustentación y defensa.

Firmado electrónicamente por:
KLEBER ROLANDO MORILLO AGUILAR

Ing. Kleber Rolando Morillo Aguilar Mg. Sc.
DIRECTOR DE TRABAJO DE TITULACIÓN

Autoría

Yo, Carlos Alberto Bermeo Zamora, declaro ser autor del presente Trabajo de Titulación y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos y acciones legales, por el contenido del mismo. Adicionalmente acepto y autorizo a la Universidad Nacional de Loja la publicación del Trabajo de Titulación en el Repositorio Digital Institucional – Biblioteca Virtual.

Firmado electrónicamente por:
CARLOS ALBERTO
BERMEO ZAMORA

Firma:

Cédula de Identidad: 1105761124

Fecha: 24-05-2023

Correo electrónico: carlos.a.bermeo@unl.edu.ec

Teléfono: 0967860770

Carta de autorización por parte del autor, para consulta, reproducción parcial o total y/o publicación electrónica de texto completo, del Trabajo de Titulación.

Yo, **Carlos Alberto Bermeo Zamora**, declaro ser autor del Trabajo de Titulación denominado: **Análisis y propuesta de gestión de riesgo en infraestructura TI en la Unidad Educativa Quevedo**, como requisito para optar el título de **Magíster Telecomunicaciones**, autorizo al sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos muestre la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el Repositorio Institucional, en las redes de información del país y del exterior con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia del Trabajo de Titulación que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los veinticuatro días del mes de mayo de dos mil veintitrés.

Firmado electrónicamente por:
CARLOS ALBERTO BERMEO ZAMORA

Firma:

Autor: Ing. Carlos Alberto Bermeo Zamora

Cédula: 1105761124

Dirección: Quevedo, Los Ríos

Correo Electrónico: carlos.a.bermeo@unl.edu.ec

Teléfono: 0967860770

DATOS COMPLEMENTARIOS:

DIRECTOR DE TRABAJO DE TITULACIÓN: Ing. Kleber Rolando Morillo Aguilar Mg. Sc.

Dedicatoria

Este Trabajo de Titulación va dedicado primeramente a Dios, a mi familia ya que a ustedes les debo todo lo que soy, les debo mi vida entera, sin ustedes no hubiera llegado hasta acá y no hubiera logrado mi sueño.

Le agradezco a Dios porque me permitió conocer a personas tan maravillosas con las cuales pude compartir muchas anécdotas y me sigue permitiendo realizar mis sueños. Este trabajo representa la culminación de uno de mis más grandes sueños.

Este Trabajo de Titulación también se la dedico a mis hijos y puedan ver que es mucho más que un simple trabajo académico para mí. Es una prueba tangible de que con esfuerzo y dedicación se pueden lograr grandes cosas en la vida.

Carlos Alberto Bermeo Zamora

Agradecimiento

En primer lugar, quisiera agradecer a mi supervisor del Trabajo de Titulación por su orientación y su dedicación a lo largo de todo el proceso, por ende, extender el agradecimiento a la Universidad Nacional de Loja por permitir llevar a cabo este paso en mi vida profesional.

Agradezco a mi familia por su amor, paciencia y apoyo incondicional. Sus palabras de aliento y su confianza en mí han sido mi mayor motivación.

Este es un logro que comparto con todos ustedes y espero seguir contando con su apoyo en mis futuros proyectos. ¡Gracias de todo corazón!

Carlos Alberto Bermeo Zamora

Índice de Contenidos:

Índice de Figuras:

Índice de Tablas:

Índice de Anexos:

1. Título

Análisis y propuesta de gestión de riesgo en infraestructura ti en la unidad educativa Quevedo

2. Resumen

A medida que la tecnología se vuelve más omnipresente, la información que se transmite utiliza diferentes métodos de almacenamiento, desde los escaneos de las escritura en papel hasta el almacenamiento en la nube; sin embargo, esta forma de proteger la información se ha visto expuesta por los diferentes tipos de filtraciones de información, dado que algunas instituciones tanto públicas y privadas no suelen tener políticas y reglamentos de seguridad para proteger la información y han sido víctima de amenazas y robo de información.

Es por ello que, a través de este trabajo, se plantea desarrollar una propuesta de un modelo de gestión de seguridad de la información basado en la norma ISO 27001 que se implementara a futuro, para los docentes de la Unidad Educativa Quevedo, inicialmente se basara en los diagnósticos que se obtengan mediante la evaluación del control y gestión de las políticas de seguridad en el sector de las TIC´S.

La propuesta se basa en una serie de lineamientos relacionados con el manejo y clasificación de la información, control de acceso, manejo de contraseñas, manejo de incidentes y sanciones para quienes no apliquen estas políticas, encaminadas a mejorar la seguridad de la información.

Palabras Clave: *Norma ISO 27001; Seguridad de la Información; Sistemas de Gestión de la Información (SGSI).*

2.1. Abstract

As technology becomes more ubiquitous, the information that is transmitted uses different storage methods, from paper writing to scanning to cloud storage; however, this method of protecting information has been exposed by different types of information leaks, since some institutions both public and private do not usually have security policies and regulations to protect information and have been victims of threats and information theft.

This is why a proposal for an information security management model based on the ISO 27001 standard has been developed through this work, initially based on the results of an evaluation of the control and management of security policies in the ICT sector, which will be implemented in the future for the teachers of the Quevedo Educational Unit.

The proposal is based on a series of guidelines related to the management and classification of information. For improving information security, these guidelines include access control, password management, incident management, and sanctions for non-compliance.

Keywords: ISO 27001; Information Security; Information Management Systems (ISMS).

3. Introducción

Hoy en día, la tecnología de la información (TI) es una parte esencial de la mayoría de las organizaciones, incluidas las instituciones educativas. La Unidad Educativa Quevedo no es la excepción, ya que depende en gran medida de su infraestructura de TI para llevar a cabo sus actividades diarias y brindar una educación de calidad a sus estudiantes. Sin embargo, esta dependencia también trae riesgos, como la posible pérdida de datos, la interrupción del servicio y la violación de la privacidad de la información.

La investigación que se pretende abordar con este tema, con la gestión de riesgos como elemento clave para abordar esta situación, se basa en la serie ISO de Normas Internacionales 27000, 27001 y 27002, las cuales contienen datos o información diseñada para ayudar a las diferentes organizaciones para mejorar el procesamiento institucional en la administración informática de los datos (Ladino, Villa, & López, 2019).

De estos estándares, ISO 27001: 2013 es el más utilizado, ya que se ha demostrado que brinda a los usuarios confianza en la seguridad de su información, ya que emplea una técnica de proceso para hacer frente a sus amenazas siguiendo el estándar, los pilares fundamentales de este estándar son la Confidencialidad, Integridad y Disponibilidad, independientemente de su formato, previenen cualquier amenaza y garantizan la continuidad de las actividades de la empresa, entidad corporativa o educativa que lo aplica (Flores, 2021).

En base a la investigación de (Camacho Reyes & Patiño Maisanche, 2022) donde se manifiesta que, A nivel local, en la ciudad de Quevedo, las diversas instituciones de educación presentan una problemática similar a la que muchas empresas u organizaciones se han enfrentado, acerca de la seguridad de la información en las diferentes áreas y departamentos, pues esta también ha sido vulnerada.

En base a ello, el propósito de este trabajo investigativo es diseñar e implementar a través de la propuesta de una política de seguridad basada en la norma ISO 27001:2013, un modelo de protección y seguridad para el uso y manejo de la información que manejan los docentes de la institución, a través de la cual se espera lograr verse expuesta a la vulnerabilidad de información a la que solo tienen acceso los docentes y funcionarios de la institución.

Para resolver el problema de la falta de seguridad en la U.E. Quevedo, se prevé proponer un sistema de gestión de infraestructuras de TI partiendo del análisis de los activos críticos de la Unidad Educativa Quevedo. Para cumplir esto, se plantea desarrollar la propuesta en tres objetivos específicos, realizar el levantamiento de activos e infraestructuras críticas en la Unidad Educativa Quevedo, Identificar acciones de corto, medio y largo plazo en la gestión de riesgos a ser aplicado en la Unidad Educativa Quevedo y proponer un plan de gestión de riesgos en infraestructuras TI para la seguridad de datos.

Por lo tanto, la gestión de riesgos de la infraestructura de TI es un enfoque importante para la Unidad Educativa Quevedo, y es necesario contar con un plan de gestión de riesgos efectivo para minimizar estos riesgos, con esta investigación, también se pretende proporcionar una guía útil para otras organizaciones educativas que enfrentan desafíos similares en la gestión de sus recursos de TI.

4. Marco Teórico

Actualmente, las organizaciones poseen diferentes tipos de información, lo que las hace cada vez más vulnerables a posibles amenazas que ponen en riesgo todos los datos que manejan los diferentes departamentos. Por ello, es necesario implementar un sistema que asegure y garantice su protección.

Siguiendo ese mismo punto, (Aguilera López, 2017) establece que los sistemas de información al no tener un control y seguridad se ven expuestos a amenazas y vulnerabilidades por la falta de normas y políticas de seguridad; lo que compromete a las empresas e instituciones a implementar mecanismos seguros para la manipulación de los datos.

Por su parte, (Freddo & Flores, 2012) manifiestan que tanto la seguridad informática como la seguridad de la información, contemplan un papel fundamental a la hora de resguardar los datos que son manipulados por las empresas en sus diferentes áreas. Pero cada una de ellas abarca situaciones y características que son importantes de conocer, por eso es importante distinguirlas, tal como muestra en los siguientes subapartados.

4.1. Norma ISO

Para desarrollar el presente trabajo se usará la norma ISO 27000. La serie ISO 27000 contempla un conjunto de estándares desarrollados por ISO (*Internacional Standard Organization*) e IEC (*International Electrotechnical Commission*), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización.

ISO 27000: Que contendrá términos y definiciones que se emplean en toda la serie, hace referencia Sistemas de Gestión de Seguridad de la Información, Generalidades y vocabulario; esta recoge los términos y conceptos relacionados con la seguridad de la información, dando una visión general de la familia de estándares de esta área, una introducción a los SGSI y una descripción del ciclo de mejora continua. Fue publicada en mayo de 2009, revisada para su segunda edición en diciembre de 2012, llegando a su tercera edición en enero de 2014 (López Neira, 2023).

ISO 27001: Es la norma principal que contiene los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI), fue publicada en el 2005, revisada para septiembre de 2013, se origina en la BS7799-2:2002 (López Neira, 2023).

ISO 27001:2013 es un estándar internacional que proporciona un marco para un Sistema de Gestión de Seguridad de la Información (SGSI) para garantizar la confidencialidad, integridad y disponibilidad continua de los datos, así como el cumplimiento legal, la implementación de ISO 27001 es una respuesta ideal a los requisitos legislativos y del cliente, incluidas otras amenazas potenciales, como ciberdelincuencia y filtraciones de datos (Becerra, Betancourt, & Serrato, 2022).

La estructura de ISO 27001 es compatible con otros estándares de sistemas de gestión como ISO 9001 y es neutral en cuanto a tecnología y proveedor, lo que significa que es completamente independiente de la plataforma de TI. Por lo tanto, es imperativo que todos los miembros de una organización comprendan qué significa el estándar y cómo se aplica en la organización (Becerra, Betancourt, & Serrato, 2022).

ISO 27002: Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información, fue publicada en el 2007, es el nuevo nombre ISO 17799:205. No es certificable. Contiene 39 objetivos de control y 133 controles agrupados en 11 dominios (López Neira, 2023).

ISO 27003: Consiste en la guía de implementación de SGSI e información del modelo PDCA, y los requerimientos de sus diferentes fases. Publicada en el 2010, tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación (López Neira, 2023).

ISO 27004: Estándar para la medición de la efectividad de la implantación de un SGSI y de los controles relacionados (López Neira, 2023).

ISO 27005:2008 Diseñada para establecer las directrices para la gestión de riesgos de seguridad, publicada en el año 2008. Esta norma al pertenecer a la familia de las Normas 27000, se ajusta a las necesidades de las organizaciones que pretende realizar su análisis de riesgos en este ámbito y cumplir con los requisitos de la Norma ISO 27001 (López Neira, 2023)..

ISO 27007: Guía de auditoría de un SGSI, como complemento lo específico en ISO 19011.

ISO/IEC 27011: Contiene las directrices para la seguridad de la información en organizaciones de telecomunicaciones utilizado en el Norma ISO/IEC 27002, facilitando el

cumplimiento de la Norma ISO27001 para la consecución de un nivel de seguridad aceptable (ISO/IEC27001:2005, 2013) (López Neira, 2023).

Un eje central de la planificación del SGSI incluye la identificación de los riesgos de la información, que se relacionan con posibles amenazas y vulnerabilidades a la confiabilidad, seguridad y disponibilidad de la información de una organización (Torres, 2020).

En base a la identificación, análisis y evaluación de estos riesgos, se determinará un plan de control o tratamiento de riesgos. También incluye la documentación y aplicación de los procedimientos requeridos para aplicar dichos controles, así como la capacitación y concientización de los empleados sobre la seguridad de la información y los controles a aplicar (Torres, 2020).

La validación incluye la medición del desempeño del SGSI, la evaluación de riesgos y la efectividad de los controles implementados, la realización de auditorías internas del sistema y la resolución de su gestión (Torres, 2020).

La obtención de la certificación ISO 27001 demuestra el compromiso de la empresa o institución de seguir las mejores prácticas de seguridad de la información. Además, la certificación ISO 27001 proporciona una evaluación experta de si la información de su empresa o institución está correctamente segura (Torres, 2020).

4.2. Seguridad de la Información

La seguridad de la información se define como todas las medidas preventivas y reactivas tomadas por individuos, organizaciones y tecnologías para proteger la información; buscan preservar esta confidencialidad, autenticidad e integridad, debe quedar claro que los términos seguridad de la información y seguridad informática son diferentes. La segunda trata únicamente de la seguridad en el entorno informático, mientras que el primero es para cualquier tipo de información, digital o impresa (Universidad Libre, 2015).

La seguridad de la información es muchas cosas, pero toda gira en torno a la información. por ejemplo, disponibilidad, comunicación, identificación de problemas, análisis de riesgos, integridad, confidencialidad, recuperación de riesgos.

Para implementar la seguridad de la información dentro de una organización se debe considerar tres elementos clave: personas, procesos y tecnología (Universidad Libre, 2015).

- Personas: realizan la gestión y tratamiento de la información. Pueden ser empleados, gerentes, autoridades, clientes, proveedores, contratistas y prestadores de servicios.
- Procesos: son actividades que se realizan para lograr un objetivo establecido, la mayoría de los cuales contienen información o dependen de la información, por lo que son frágiles.
- Tecnología: está relacionada con los servicios e infraestructura de la empresa, es la maestra del manejo y desarrollo de la información, además, brinda la oportunidad de almacenar, restaurar, difundir y mantener los valiosos datos disponibles.

Fundamentalmente la seguridad de la información se encarga de la protección de confidencialidad, integridad y disponibilidad de la información, así como de los sistemas integrados en su tratamiento de información dentro de una entidad (Garcia, 2016).

Para proteger la información, utilizamos precauciones, incluida la seguridad de la información de activos, para que la información esté protegida dentro de la organización. La seguridad de la información es un concepto asociado a la certeza, sin riesgo ni azar. Se entiende por seguridad un estado de cualquier sistema o tipo de información (informática o no informática) que indica que el sistema o la información está libre de peligro, daño o riesgo. Se entiende por peligro o daño todo aquello que pueda afectar a su funcionamiento inmediato a los resultados obtenidos.

Áreas o Dominios de Seguridad de la ISO/IEC 27001 (ISOTools, 2017):

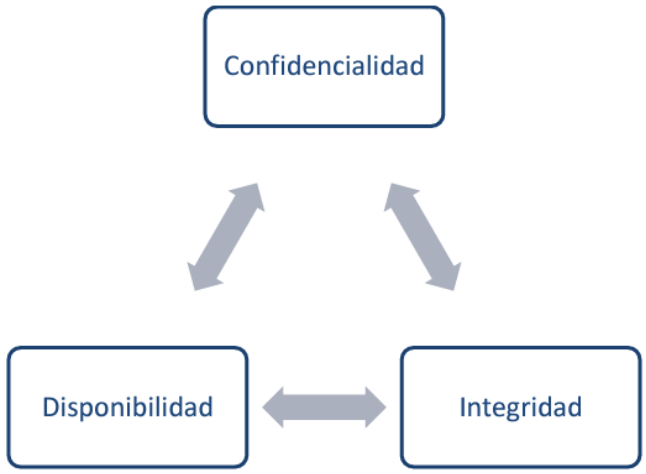
- A 5: Políticas de seguridad de la Información.
- A 6: Organización de la seguridad de la información.
- A 7: Seguridad de los Recursos Humanos.
- A 8: Gestión de recursos.
- A 9: Control de Acceso.
- A 10: Criptografía.
- A 11: Seguridad física y ambiental.

- A 12: Seguridad Operacional.
- A 13: Seguridad de las Comunicaciones.
- A 14: Adquisición, desarrollo y mantenimiento de Sistemas.
- A 15: Relaciones con los proveedores.
- A 16: Gestión de Incidentes en Seguridad de la Información.
- A 17: Aspectos de Seguridad de la Información para la gestión de la continuidad del negocio.
- A 18: Cumplimiento

La información es el valor del dato, algo que proporciona conocimiento. Los manuales de programas, profesores, personal de servicio y los estudiantes son datos estructurados de tal manera que se convierten en información que agrega valor a la institución.

La seguridad de la información se basa en la necesidad de que todos deben tener acceso a la información, su importancia, integridad y disponibilidad para poder aprovecharla al máximo con el mínimo (Romero, y otros, 2018).

Figura 1 *Objetivos de la seguridad de la información*



Nota: en la Figura 1 se visualiza las 3 etapas de la seguridad de la información. Tomada de elaboración propia.

Confidencialidad: La confidencialidad incluye asegurar que solo el personal autorizado tenga acceso a la información que le corresponde, de modo que cada sistema automatizado o

individuo solo tenga acceso a los recursos que necesita para realizar sus tareas. Para garantizar la confidencialidad, se utilizan tres recursos principales (Romero, y otros, 2018):

- **Autenticación de Usuario**: Se utiliza para identificar quién accede a la información y es quien dice ser.
- **Gestión de autoridades:** Para los usuarios que acceden al sistema, solo se puede utilizar la información autorizada para operar, y solo de forma autorizada, como la gestión basada en usuarios de permisos de lectura y escritura.
- **Cifrado de información:** El cifrado evita que personas no autorizadas accedan a ella, para esto, la información se convierte de una forma inteligible a una forma ilegible, se aplica tanto a la información autorizada como a la que no esté autorizada. La información solo se puede extraer de forma inteligible a través de la criptografía. y se aplica tanto a la información que se transmite como a la que se almacena.

El principio de confidencialidad se aplica no solo a la protección de la información, sino también a la protección de todos los datos e información de los que es responsable. Esta información puede ser confidencial no solo porque es de alto valor para la organización, sino también, por ejemplo, porque puede estar protegida por la legislación de protección de datos personales. Un ejemplo de violación de la confidencialidad es la divulgación de información al público por parte de entidades bancarias, grandes corporaciones y gobiernos exponiendo algunas de sus actividades (Romero, y otros, 2018).

La integridad: Se trata de asegurarse de que la información no se pierda o se filtre, ya sea intencional o accidentalmente, usar la información incorrecta puede ser tan dañino para una empresa como perderla, de hecho, si la manipulación de la información es lo suficientemente sutil, puede conducir a una cascada de los errores acumulativos que se arrastran hacia abajo, hechos en sucesión, toman la decisión equivocada. Para garantizar la integridad de la información se debe considerar lo siguiente (Romero, y otros, 2018):

- Supervise el tráfico de la red en busca de posibles intrusiones.
- El sistema de auditoría hace cumplir las políticas de auditoría, registrando información sobre quién hizo qué y cuándo.

- Implementar un sistema de control de cambios es tan simple como verificar un resumen de los archivos de información almacenados en el sistema para ver si han cambiado.
- Como otro recurso, existen copias de seguridad que protegen la información de manipulación o pérdida en caso de falla, o permiten restaurarla a un estado anterior.

Disponibilidad: Para poder considerar la seguridad mínima de la información, existe la disponibilidad, de nada sirve si el usuario accede a la información y es indestructible, si acceder es tedioso o imposible, la información debe ser útil y estar disponible para ser utilizada por quienes lo necesitan, se deben implementar las medidas necesarias para que tanto la información como los servicios estén disponibles, por ejemplo, los ataques de denegación de servicio distribuido o DDoS pueden inutilizar una red. Los clientes acceden y pueden comprar. Otro ejemplo de pérdida de usabilidad es cuando las direcciones de correo electrónico se utilizan para lanzar campañas de spam y como resultado, se agregan a listas negras, lo que impide que los destinatarios de correos electrónicos legítimos las reciban. Para ello, estrategias de control como (Romero, y otros, 2018):

- Acuerdo de Nivel de Servicio o (SLA).
- Los balanceadores de carga de tráfico minimizan el impacto de DDoS.
- Copias de seguridad para restaurar la información perdida.
- Existen recursos alternativos al recurso principal.

La información y los sistemas son seguros si solo aquellos que deberían tener acceso a la información y los recursos, si se puede detectar y recuperar la manipulación voluntaria o accidental de la información, y si se pueden garantizar niveles aceptables de servicio y requisitos de acceso a la información (Romero, y otros, 2018).

Indica que el uso de los sistemas de información implica el establecimiento de normas y procedimientos aplicables al uso de los sistemas de información y ante posibles amenazas, tales como (Romero, y otros, 2018):

- Desarrollar diversas normas y procedimientos.
- Definir acciones para que las personas tomen.
- Definición del perímetro afectado.

4.3. Sistemas de Gestión de la Información (SGSI)

El propósito central de un SGSI es proporcionar protección a la información sensible o de valor. La información sensible incluye información sobre los empleados, clientes y proveedores. La información de valor incluye propiedad intelectual, datos financieros, registros legales datos comerciales y datos operativos (Russell, 2022). Los riesgos de seguridad de la información generalmente resultan de amenazas a los activos que procesan, almacenan, mantienen, protegen o controlan el acceso a la información, lo que resulta en incidentes (Russell, 2022).

Los activos en este caso suelen ser personas, equipos, sistemas o infraestructura. La información son conjuntos de datos que las organizaciones desean proteger, como registros de empleados, registros de clientes, datos financieros, datos de diseño, datos de prueba, entre otros(Russell, 2022).

Un incidente es un evento no deseado que resulta en una pérdida de confidencialidad (violación de datos), integridad (corrupción de datos) o disponibilidad (falla del sistema) (Russell, 2022).

Una amenaza es la causa de un incidente, que puede ser malintencionado (como un robo), accidental (como un error tipográfico) o un desastre natural (como una inundación) (Russell, 2022).

Vulnerabilidades como una ventana abierta, errores de código fuente o la ubicación de un río aumentan la probabilidad de que una amenaza provoque un evento inesperado y costoso (Russell, 2022).

En la seguridad de la información, el riesgo se gestiona mediante el diseño, la implementación y el mantenimiento de controles, como ventanas bloqueadas, pruebas de software o la ubicación de dispositivos vulnerables por encima del nivel del suelo (Russell, 2022).

Un SGSI que cumple con la norma ISO 27001 tiene un conjunto de procesos de mejores prácticas interrelacionados que facilitan y respaldan el diseño, la implementación y el mantenimiento de los controles (Russell, 2022).

Los procesos que forman parte de un SGSI suelen ser procesos empresariales centrales existentes (ej., contratación, incorporación, formación, adquisición, diseño de productos,

mantenimiento de equipos, prestación de servicios) y procesos específicos para mantener y mejorar la seguridad de la información (p. ej., gestión de cambios, copia de seguridad de la información, acceso control, gestión de eventos, clasificación de la información) (Russell, 2022).

El SGSI es el eje central sobre el que se desarrolla la ISO 27001, donde la gestión de la seguridad de la información busca la protección de la información bajo las tres dimensiones de confiabilidad, integridad y disponibilidad. Esta gestión debe realizarse mediante un proceso sistemático, documento y conocido por toda la organización. Para garantizar que la seguridad de la información es gestionada adecuadamente se debe identificar los aspectos relevantes adoptados para garantizar las tres dimensiones. El SGSI se fundamenta en las cuatro fases del ciclo de mejora continua de Edwards Deming que son: planificar, hacer, verificar, actuar (PHVA) (Russell, 2022).

4.4. Ciclo PHVA

ISO 27001 se basa en el ciclo PHVA, también conocido como ciclo Deming. El ciclo PHVA se puede aplicar no solo a los sistemas de gestión. También proporciona un enfoque para la mejora continua de cada elemento individual (Russell, 2022).

Figura 2 *Modelo PHVA para ISO 27001*

Nota: La Figura 2 muestra el ciclo de los sistemas de gestión de seguridad de la información. Tomado de Russell, J. (2022). ISO 27001:2013 Guía de Implementación para la seguridad de la información. Madrid: Nqa.

- Planificar (Russell, 2022)

En la primera fase, se planifican las tareas a realizar de acuerdo a la asignación de roles y responsabilidades de cada funcionario, a partir de los cuales se pueden identificar los riesgos que pueden enfrentar. Información manipulada por los usuarios.

Con tareas y asignaciones claras, el alcance y los objetivos que se planifican se pueden medir y complementar con información sobre los recursos y el equipo necesarios para lograr el establecimiento de objetivos.

- Hacer (Russell, 2022)

Al planificar las actividades a realizar, según sean docentes, administrativos o estudiantes, luego de realizar el trabajo anterior, las políticas de seguridad, esto tiene relación con las herramientas de seguridad que serán parametrizadas y configuradas de acuerdo a los recursos disponibles analizados durante la planificación. fase.

- Verificar (Russell, 2022)

Para verificar que los objetivos propuestos y programados se estén cumpliendo adecuadamente, es necesario realizar un seguimiento que permita medir y revisar cada objetivo de seguridad y operativo planteado en las fases de planificación y ejecución.

Los resultados obtenidos deben reforzarse con revisiones periódicas con el fin de verificar los requisitos especificados en la norma ISO 27001, que forma parte del sistema de gestión de seguridad de la información.

Cabe señalar que las auditorías deben reforzarse con auditorías periódicas en función del estado actual de los procesos y dependencias a auditar.

- Actuar (Russell, 2022)

Con los resultados obtenidos de las fases anteriores se hace necesario recopilar y analizar los datos para determinar el estado de la gestión de seguridad que se está desarrollando, posterior a identificar los problemas de seguridad encontrados se planifican e implementan las mejoras que permiten actuar sobre los puntos encontrados que requieran sean controlados o minimizados.

4.5. Criterio de evaluación de riesgo

La evaluación del riesgo es el proceso de determinar el alcance de la posible pérdida o daño y la probabilidad de que dicho daño o pérdida ocurra u ocurra, este concepto se tiene presente en todas las actividades de una organización que, de concretarse, afectará el producto y/o los servicios que ofrece.

La evaluación e identificación de riesgos en el campo de la información, se cuenta con la norma ISO 27001, la cual cuenta 14 dominios, 35 objetivos de control y 114 controles, las cuales son seleccionadas luego de identificar los riesgos que existen en la organización, con el fin de enfrentarlos en línea con los riesgos de eliminar, mitigar o transferirlos.

4.6. Evaluación de riesgo

A partir de las amenazas identificadas en los criterios de evaluación de riesgos y criterios descritos en este proyecto, ajustarlos a las condiciones del área de TIC'S de la Unidad Educativa Quevedo para determinar el nivel de riesgo, teniendo en cuenta la frecuencia y el impacto.

En la encuesta se utilizó una matriz de riesgos, herramienta que nos permite identificar los riesgos más importantes inherentes al área de estudio, para ello la variable es la frecuencia de ocurrencia, que representan la amenaza de ejecución, la severidad del impacto que se producirá.

4.7. Matriz de evaluación del riesgo institucional

Según (Fiscalia General del Estado, 2016) en la resolución 019 FGE-2016 donde dice que el objetivo principal de la matriz es el de sistematizar la identificación, el análisis y la respuesta o tratamiento de riesgo institucionales por procesos.

- **Identificación del riesgo**

En esta sección se describe los riesgos relacionados a un proceso o área determinada. Para el efecto cuenta con 5 columnas, cada una de las cuales contempla aspectos característicos del riesgo descrito: Objetivos Operativos, Riesgos Identificados, Descripción de la Situación Riesgosa, Descripción de las Causas del Riesgo y Consecuencias Potenciales (Fiscalia General del Estado, 2016).

- **Análisis y valoración del riesgo**

En esta sección se realiza el análisis de riesgo considerando dos variables: probabilidad e impacto. En esta sección se encuentran las categorías cualitativas y cuantitativas definidas para cada una de las variables, así como una columna para anotar los resultados y categoría de riesgo que refleja la combinación de ambas variables. El análisis del riesgo se enfoca específicamente en cada una de las situaciones riesgosas y no en las causas, orígenes o consecuencias asociadas (Fiscalia General del Estado, 2016).

- **Respuesta del riesgo**

En esta sección se describen las acciones que deben de ser adoptadas para Eliminar, Evitar, Reducir, Compartir o Asumir el riesgo ante una eventual materialización. Además, es imprescindible la asignación de responsables y plazos para cada acción, con el objetivo de asegurar su ejecución (Fiscalia General del Estado, 2016).

Tabla 1 *Escala de Probabilidad*

NIVEL	DESCRIPCIÓN	FRECUENCIA	CALIFICACIÓN
FRECUENTE	Se espera que ocurra en la mayoría de las circunstancias.	Mas de 1 vez al año	5
ALTAMENTE PROBABLE	Probablemente ocurrirá en la mayoría de circunstancia.	1 vez en el último año	4
PROBABLE	Podría ocurrir en algún momento.	1 vez en los últimos 2 años	3
POCO PROBABLE	Podría ocurrir solo en circunstancias excepcionales.	1 vez en los últimos 5 años	2
IMPROBABLE	La eventualidad de ocurrencia es muy baja, casi nula.	No en la historia reciente	1

Nota: En la Tabla 1 tenemos la escala de la probabilidad en la cual está identificado desde el nivel más frecuente hasta el poco probable donde la calificación de 5 es para los casos que es muy frecuente y se espera que ocurra en la mayoría de casos o circunstancias y la calificación de 1 para la poco probable para aquellos casos que serían casi nulos que ocurran. Tomado de fiscalía general del Estado. (2016). Guía para la administración del riesgo institucional. Quito.

Tabla 2 *Escala de Impacto*

NIVEL	DESCRIPCIÓN (SI EL HECHO LLEGARA A PRESENTAR)	CALIFICACIÓN
CATASTRÓFICO	Tendría desastrosas o catastróficas consecuencias o efectos sobre la institución.	5
ALTO	Tendría altas consecuencias o efectos sobre la institución.	4
MODERADO	Tendría medianas consecuencias o efectos sobre la Institución.	3
LEVE	Tendría bajo impacto o efecto sobre la Institución.	2
INSIGNIFICANTE	Tendría consecuencias o efectos mínimos sobre la Institución.	1

Nota: En la Tabla 2 tenemos la escala de impacto donde se identifica las consecuencias sobre la Unidad Educativa. Tomado de fiscalía general del Estado. (2016). Guía para la administración del riesgo institucional. Quito.

Tabla 3 *Valoración del Riesgo por Categorías*

VALORACIÓN DEL RIESGO POR CATEGORIA			
CALIFICACIÓN DE	A	ZONA DE RIESGO	TRATAMIENTO
60%	100%	EXTREMA	Eliminar el riesgo, reducir, evitar, compartir o transferir.
30%	59%	ALTA	Reducir el riesgo, evitar, compartir o transferir.
16%	29%	MODERADA	Asumir el riesgo, reducir el riesgo.
1%	15%	BAJA	Asumir el riesgo.

Nota: En la Tabla 3 identificamos la valoración de riesgos por categorías y el tratamiento que se debe tomar acorde al riesgo que se tiene en la Unidad Educativa. Tomado de fiscalía general del Estado. (2016). Guía para la administración del riesgo institucional. Quito.

Tabla 4 *Mapa de Calor del Riesgo*

MAPA DE CALOR DEL RIESGO

PROBABILIDAD	**FRECUENTE**	**5**	20%	40%	60%	80%	100%
			MODERADO	ALTO	EXTREMO	EXTREMO	EXTREMO
	ALTAMENTE	**4**	16%	32%	48%	64%	80%
	PROBABLE		MODERADO	ALTO	ALTO	EXTREMO	EXTREMO
	PROBABLE	**3**	12%	24%	36%	48%	60%
			BAJO	MODERADO	ALTO	ALTO	EXTREMO
	POCO	**2**	8%	16%	24%	32%	40%
	PROBABLE		BAJO	MODERADO	MODERADO	ALTO	ALTO
	IMPROBABLE	**1**	4%	8%	12%	16%	20%
			BAJO	BAJO	BAJO	MODERADO	MODERADO
	IMPACTO		**1**	**2**	**3**	**4**	**5**
			INSIGNIFICANTE	**LEVE**	**MODERADO**	**ALTO**	**CATASTROFICO**

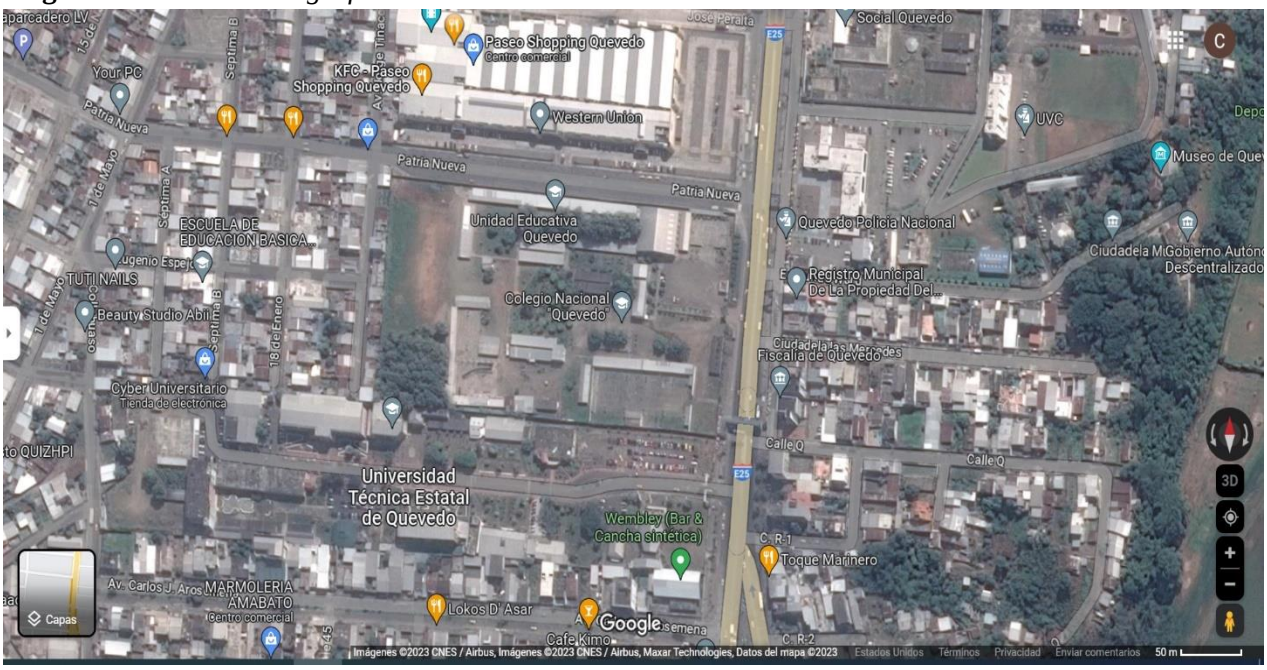
Nota: Porcentajes de probabilidades de ocurrencias de los diversos riesgos que puedan darse dentro de la institucion. Tomado de fiscalía general del Estado. (2016). Guía para la administración del riesgo institucional. Quito.

4.8. Descripción de la Unidad Educativa Quevedo

Figura 3 *Unidad Educativa Quevedo*

Nota: La Figura 3 es una parte de la repotenciación realizada en la institución. Tomado de elaboración propia.

Figura 4 *Ubicación Geográfica*



Nota: La Figura 4 es la ubicación geográfica de la institución. Tomada de elaboración propia.

La Unidad Educativa Quevedo, de la ciudad del mismo nombre, provincia de Los Ríos, fue creado mediante Decreto Ejecutivo Nro. 1007 de fecha 7 de agosto de 1968, con el nombre de "LUCILA SANTOS DE AROSEMENA", con las opciones prácticas de MANUALIDADES FEMENINAS ARTESANÍA, ARTÍSTICAS Y FOLKLÓRICAS, así como COMERCIO Y ADMINSTRACIÓN estableciendo su inicio a partir del periodo 1968 – 1969, en este último año, se percibiría los fondos asignados en el Presupuesto Nacional (UnidadEducativaQuevedo, 2023).

De esta manera se constituye el primer cuerpo docente que sin honorarios laboro en el periodo de 1968 y estos son Dr. Jorge García Jaime como rector y profesor de ciencia naturales, Sr. Carlos Peñafiel Arce en matemáticas, Lcdo. Francisco Carcache en castellano, Abogado Oswaldo Trávez Borja en historia, geografía y música, Dr. Miguel Ángel Carrión en inglés (UnidadEducativaQuevedo, 2023).

El ultimo local en el que el colegio funciono fue en la calle decima tercera y siete de octubre en propiedades del Sr. Miguel Mueckay. Hasta mediados de 1971 se autorizó el funcionamiento de cuarto curso de bachillerato, para entonces en el actual terreno del colegio se terminó la construcción de un largo pabellón de material mixto, inmediatamente trasladándose en donde se reiniciaría las clases. Al año siguiente del funcionamiento por predio propio el consejo provincial

termino la construcción de los pabellones de cemento armado, siendo estas aulas pedagógicas que hasta ahora existen (UnidadEducativaQuevedo, 2023).

Se otorgó por primera vez la inspección general a la Sr. Primitiva Murillo de Yánez en 1971 y así mismo al no existir profesores para las materias de especialización se logró la colaboración de excelentes maestros como economista Jorge Noriega, Lcda. Mariana Meneses, Lcda. Nisa Rodríguez, Lcda. Marilú Haon entre otros (UnidadEducativaQuevedo, 2023).

El 14 de agosto de 1972, mediante Acuerdo Ministerial Nro. 1991, se autoriza cambiar el nombre de Lucila Santos de Arosemena, por el de COLEGIO NACIONAL DE SEÑORITAS "QUEVEDO", en homenaje a nuestro cantón, gracias a las gestiones realizadas por la rectora de aquella época, la Lcda. Magdalena Serrano de Mueckay (UnidadEducativaQuevedo, 2023).

En el año 1973, desde el 21 de agosto se autorizó el funcionamiento del CICLO DIVERSIFICADO, con el primer curso diversificado del bachillerato en HUMANIDADES MODERNAS, modalidades en ciencias: FÍSICO - METAMÁTICO; QUIMICO – BIOLÓGICAS Y CIENCIAS SOCIALES, debiendo para el efecto, aplicarse el Plan de estudios expedido mediante resolución Ministerial No. 828 del 27 de marzo de 1968, los cursos: 2do y 3ero del ciclo que se autoriza, los organizarán progresivamente (UnidadEducativaQuevedo, 2023).

En 1982 - 1983 se autoriza el funcionamiento del TERCER CURSO de ciclo básico de la sección nocturna, mediante acuerdo ministerial Nro. 002536 de fecha 20 de septiembre de 1982. En el periodo lectivo 1993 – 1994, se alcanza la autorización para el funcionamiento del primer curso ciclo diversificado con Bachillerato en Comercio y Administración, especialización Contabilidad y el primer curso de igual ciclo, con bachillerato en Ciencias, especialización Informática, secciones diurna y nocturna (UnidadEducativaQuevedo, 2023).

De igual manera, mediante acuerdo ministerial Nro. 01411, se logra la autorización para el funcionamiento de primero, segundo y tercer curso del ciclo diversificado, con Bachillerato en Comercio y Administración, especialización informática, para las jornadas diurna y nocturna, en forma progresiva. Era el 30 de octubre del 2011 la dirección provincial de educación de Los Ríos con concordancia a la resolución ministerial del acuerdo N 364-11 del 21 de octubre del 2011 suscrito por la Dra. Sofía Vidal designa al colegio nacional de Srtas. Quevedo perteneciente al

cantón del mismo nombre, a Colegio Fiscal Quevedo en diciembre del 2012, luego el 21 de mayo del 2013 pasa a llamarse Unidad Educativa Quevedo (UnidadEducativaQuevedo, 2023).

La Unidad Educativa Quevedo tiene como: **Misión. -**Nuestra institución tiene el compromiso fundamental, de formar bachilleres bajo las condiciones establecidas por la Ley de Educación, cuyos principios inculcamos en nuestras estudiantes, para que puedan participar crítica, competente, responsable y exitosamente en la vida económica, política, social y cultural de nuestro cantón y el país (UnidadEducativaQuevedo, 2023).

Para el efecto contamos con los recursos económicos, académicos, científicos, pedagógicos, didácticos y por, sobre todo, el personal humano con capacidad para ofrecer una educación de calidad y con calidez, así, formamos bachilleres impolutos, pletóricas de entereza para enfrentar los retos que la sociedad ecuatoriana y el mundo actual nos imponen, trabajando, solidaria, comunitaria y patrióticamente por la paz, la justicia y equidad para las ecuatorianas y ecuatorianos (UnidadEducativaQuevedo, 2023).

Visión. -Mejoraremos los niveles de planificación estratégica integral de la institución en todas las fases del proceso de enseñanza- aprendizaje, los elementos organizacionales administrativos y de gestión institucional, para ubicarnos en los más altos estándares de calidad exigidos para la educación del país (UnidadEducativaQuevedo, 2023).

Contaremos para el efecto, con la implementación y aplicación del modelo pedagógico constructivista acordes con nuestra oferta educativa, desarrollando el perfeccionamiento docente e implementando cambios en planes, programas y proyectos que realizaremos para constituirnos en el primer plantel de la provincia de Los Ríos por prestigio, credibilidad, eficacia, efectividad y eficiencia (UnidadEducativaQuevedo, 2023).

La Institución posee una estructura organizacional conformada por El rector en un primer nivel, en segundo nivel los vicerrectores de las jornadas correspondientes, en tercer nivel el consejo ejecutivo, en cuarto los inspectores, en quinto lugar, secretaria, departamento de consejería estudiantil (Dece) y Tics.

4.9. Situación actual

Con referencia a lo anterior, la institución cuenta con lineamientos internos para el manejo de la tecnología de la información que deben ser aplicados para asegurar las operaciones en diversas áreas.

Un conjunto estructurado de disciplinas, responsabilidades, habilidades y competencias compartidas y asumidas dentro de una empresa por ejecutivos, gerentes, técnicos y usuarios de TI para controlar de manera efectiva los procesos, mantener la información segura, optimizar el uso de los recursos y brindar soporte para las decisiones, todo alineado. con la visión, misión y objetivos estratégicos de la institución.

El primer paso hacia este objetivo es el desarrollo de un SGSI (Sistema de Gestión de la Seguridad de la Información), cuyo objetivo es establecer un conjunto de controles de gestión de la seguridad de la información.

Conceptos, criterios y argumentos para facilitar la investigación y selección del área de Tic como área estratégica para la implementación de controles de seguridad, mediante el diseño de información que permita el cumplimiento de las políticas nacionales de gestión de seguridad jurídica en materia de gestión de la información.

5. Metodología

Se pueden utilizar diversas técnicas de investigación científica para recopilar y analizar datos relevantes. Algunas de las técnicas más comunes utilizadas en este tipo de investigación son:

Investigación documental: Esta técnica consiste en recopilar información de documentos, libros, revistas, informes y publicaciones relacionadas con el tema de la investigación. En este caso, se pueden utilizar documentos como políticas de seguridad de la información, manuales de usuario, informes de auditoría, entre otros (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2016).

Entrevistas: Las entrevistas son una técnica de recopilación de datos que implica hacer preguntas a personas con experiencia en el tema de la investigación. En este caso, se pueden entrevistar a profesionales de TI, administradores de la unidad educativa Quevedo, estudiantes y otros expertos relevantes para obtener información sobre la infraestructura TI y los riesgos asociados (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2016).

Observación: La observación consiste en observar el comportamiento y la interacción de los sujetos en un entorno específico. En este caso, se puede utilizar la observación para evaluar la infraestructura TI y detectar posibles vulnerabilidades y riesgos (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2016).

Análisis de datos: Esta técnica implica analizar los datos recopilados de las otras técnicas de investigación para identificar patrones y relaciones. En este caso, se puede utilizar el análisis de datos para identificar los riesgos más críticos y desarrollar una estrategia de gestión de riesgos efectiva (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2016).

En base a las técnicas de investigación citadas anteriormente la metodología de investigación para el análisis y recomendaciones de gestión de riesgos de infraestructura de TI en la Unidad Educativa Quevedo incluirá los siguientes pasos:

Identificación de problemas: Se realizará una revisión bibliográfica para identificar los problemas más comunes relacionados con la infraestructura de TI en la institución y cómo estos problemas afectan la seguridad y la gestión de riesgos.

Recopilación de datos: se entrevistará al personal responsable de la infraestructura de TI de la institución para recopilar información sobre problemas de seguridad y riesgos asociados con su infraestructura de TI.

Análisis de datos: la información recopilada de las entrevistas a las encargadas se analizará para identificar los problemas y riesgos de seguridad más comunes en la infraestructura de TI de la institución.

Diseño de la propuesta: Se diseñará una propuesta de gestión de riesgos para la infraestructura informática de la institución, basada en las mejores prácticas y estándares internacionales de seguridad informática.

Validación de la propuesta: La propuesta de gestión de riesgos se presentará para su validación y comentario a los directivos y responsable de la infraestructura de TI de la institución.

Ajustes de la propuesta: La propuesta de gestión de riesgos se ajustará de acuerdo a los comentarios y sugerencias del equipo responsable de la infraestructura informática de la institución.

Presentación de Propuesta: La propuesta final de gestión de riesgos se presentará a la Secretaría de Educación de Quevedo junto con un informe detallado que explique la metodología utilizada y los resultados que se obtendrían para su posterior ejecución.

En resumen, la metodología de investigación de la Unidad Educativa Quevedo para el análisis y las propuestas de gestión de riesgos de infraestructura de TI para la institución se centrará en el diseño de propuestas. Se realizarán la identificación de problemas, la selección de muestras, la recopilación de datos, el análisis de datos, el diseño de protocolos, la validación de protocolos, el ajuste de protocolos y la entrega de protocolos.

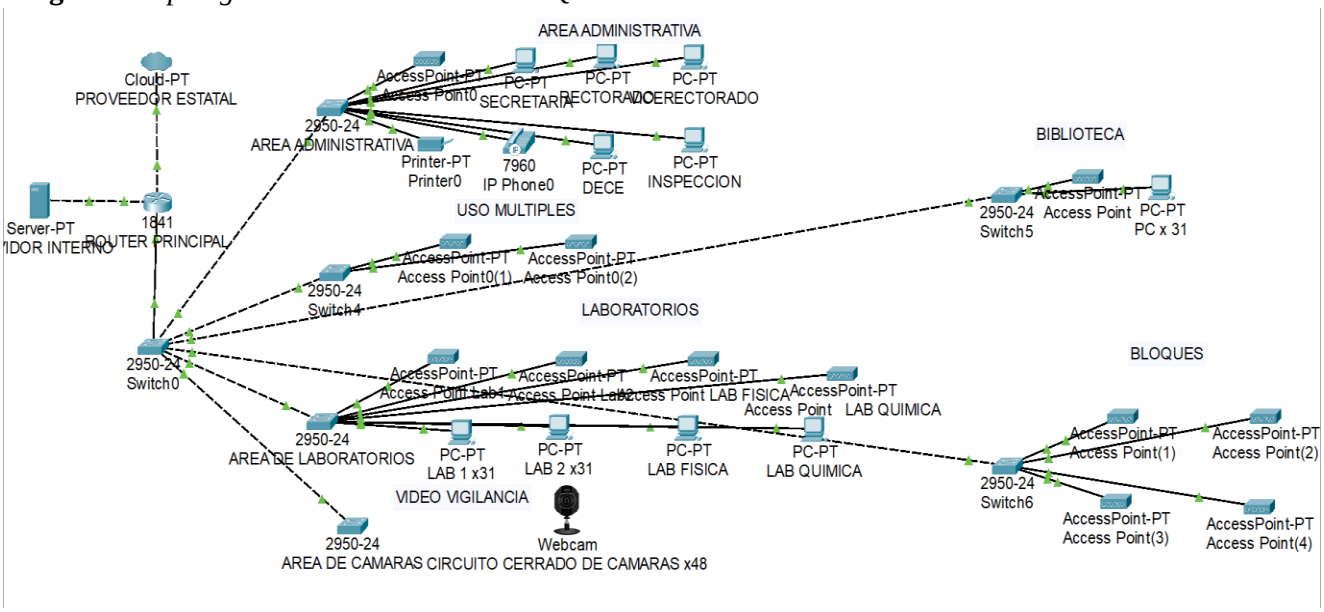
6. Resultados

En esta sección se podrá observar la situación Tecnológica de la institución, las diferentes áreas de funcionamiento de las TIC´S, la descripción de los equipos que utilizan y los diferentes protocolos a usarse dentro de la institución.

6.1. Situación Tecnológica de la Unidad Educativa Quevedo

- **Topología de Red**

Figura 5 *Topología de la Unidad Educativa Quevedo*



Nota: en la Figura 5 se muestra como está estructurada la red institucional. Tomado de la investigación propia realizada. Tomada de elaboración propia.

- **Área de TIC'S**

  - Área administrativa

    Rectorado

    Vice rectorado

    Secretaria

    Departamento de consejería estudiantil (DECE)

    Inspección

  - Laboratorios

    Laboratorio técnico

    Laboratorio físico y química

- Área de videovigilancia
- Bloques

  Bloque b1

  Bloque b2

  Bloque b3

  Bloque b4

- Biblioteca
- Usos múltiples

  Sala de profesores

  Auditorio

➢ **Personal del área**

El área está conformada por personal docente que labora dentro de la institución y están encargadas del departamento de las Tics:

Mg. Mariangy Gissela Mancero Ponce

Lic. Jessica Ximena Gómez Bastidas

➢ **Descripción de equipos**

Computadoras. -La Unidad Educativa Quevedo repartidas entre los diferentes laboratorios, área administrativa, biblioteca.

- Se cuenta con 182 equipos de marca DELL.
- 12th Gen Intel(R) Core (TM) i5-12500 3.00GHz.
- RAM 8GB
- Sistema operativo de Windows 11 Pro Education
- Disco SSD de 250 GB.

Figura 6 *Modelo de computadoras adquiridas por la Unidad Educativa Quevedo*

Nota: Referencia del equipo adquirido por la institución. Tomada de https://www.dell.com/es-es/shop/servidores-almacenamiento-y-redes/smart-selection-poweredge-r650-servidor-rack/spd/poweredge-r650/per6501a.

Servidor. -Equipo marca Dell R650.

- Xeon 4310 10 Core
- 32gb RAM 480 Gb
- SSD 2TB

Figura 7 *Modelo de servidor adquiridas por la Unidad Educativa Quevedo*

Nota: Referencia del equipo adquirido por la institución. Tomada de https://www.dell.com/es-es/shop/servidores-almacenamiento-y-redes/smart-selection-poweredge-r650-servidor-rack/spd/poweredge-r650/per6501a.

Access Point. -Punto de acceso Wifi 6 de doble banda para interiores que admite más de 300 clientes con su tasa de rendimiento total de 5,3 Gbps.

- Banda Wifi 6 (802.11ax) de doble banda de 5 GHz (4x4 MU-MIMO) con una velocidad de rendimiento de 4,8 Gbps Banda de 2,4 GHz (2x2 MIMO) con una velocidad de rendimiento de 573,5 Mbps.
- Funciona con MIMO 4x4 completo con ancho de banda de 160 MHz.
- Capacidad de más de 300 clientes simultáneos.
- Aislamiento del tráfico de invitados, que mejora la seguridad de la red inalámbrica y reduce la congestión del tráfico.

Figura 8 *Modelo de Access Point adquiridas por la Unidad Educativa Quevedo*

Nota: Referencia del equipo adquirido por la institución. Tomada de https://www.dell.com/es-es/shop/servidores-almacenamiento-y-redes/smart-selection-poweredge-r650-servidor-rack/spd/poweredge-r650/per6501a.

Switch. - 24 -Puerto 10/100/1000 + 2 x 1GE SFP

- SENCILLO: Plug-and-play sin necesidad de soporte o conocimientos de TI.
- ALIMENTACIÓN A TRAVÉS DE ETHERNET: 12 puertos PoE con un presupuesto de energía total de 100 W.
- RENDIMIENTO: Gigabit Ethernet e inteligencia de calidad de servicio (QoS) integrada optimizan los servicios sensibles a los retrasos y mejoran el rendimiento general de la red.
- DISEÑO INNOVADOR: Diseño elegante y compacto, ideal para la instalación fuera del armario de cableado, como tiendas minoristas, oficinas abiertas y aulas.

- EFICIENCIA ENERGÉTICA: optimiza el uso de energía para reducir los costos operativos. Cumple con IEEE802.3az Energy Efficient Ethernet. Fanless en todos los modelos.

Figura 9 *Modelo de switch adquiridas por la Unidad Educativa Quevedo*

Nota: Referencia del equipo adquirido por la institución. Tomada de https://www.zoostock.com/categoria/cisco-switches.

Router. CISCO1921/K9 w/ 2 GE.

- 2 EHWIC Slots
- 256MB int Flash
- 512MB DRAM Service Router

Figura 10 *Modelo de Router adquiridas por la Unidad Educativa Quevedo*

Nota: Referencia del equipo adquirido por la institución. Tomada de https://www.zoostock.com/categoria/cisco-switches.

- **Seguridad física**

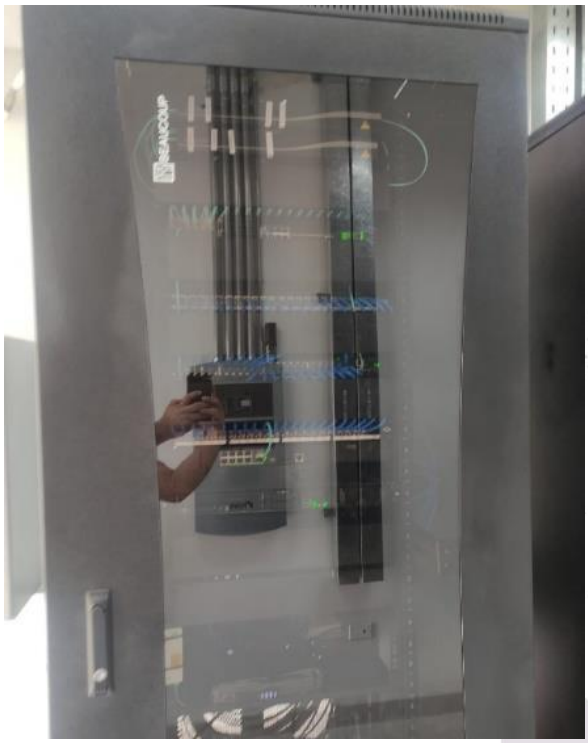
El centro de datos de la institución es de fácil acceso debido a que no posee ningún tipo de seguridad a más de las llaves de la puerta, cuenta con una refrigeración estable, posee un Power Bank para emergencias con una duración de hasta 2 horas.

Figura 11 *Power bank dentro de la central de datos.*

Nota: Instalaciones de la institución.

Tomada de elaboración propia.

Figura 12 *Gabinete de la central de datos*



Nota: Instalaciones de la institución.

Tomada de elaboración propia.

Figura 13 *Entrada de la central de datos*

Nota: Instalaciones de la institución. Tomada de elaboración propia.

El centro de datos no cuenta con ningún firewall, se puede realizar cualquier tipo de infiltración sin ninguna dificultad.

El cuarto de video vigilancia se encuentra dentro del bloque administrativo, pero no posee ningún tipo de seguridad ya que es de fácil acceso.

Figura 14 *Gabinetes de las camaras de la institución*

Nota: Instalaciones de la institución. Tomada de elaboración propia.

Figura 15 *Tv para monitorear toda la institución*

Nota: Instalaciones de la institución. Tomada de elaboración propia.

Las computadoras que se encuentran en las diferentes oficinas de la institución no cuentan con ningún tipo de seguridad y son de fácil acceso, también no cuentan con doble usuario, las computadoras que están en la biblioteca no tienen restricción alguna.

Figura 16 *Entrada a uno de los laboratorios sin seguridad*

Nota: Instalaciones de la institución. Tomada de elaboración propia.

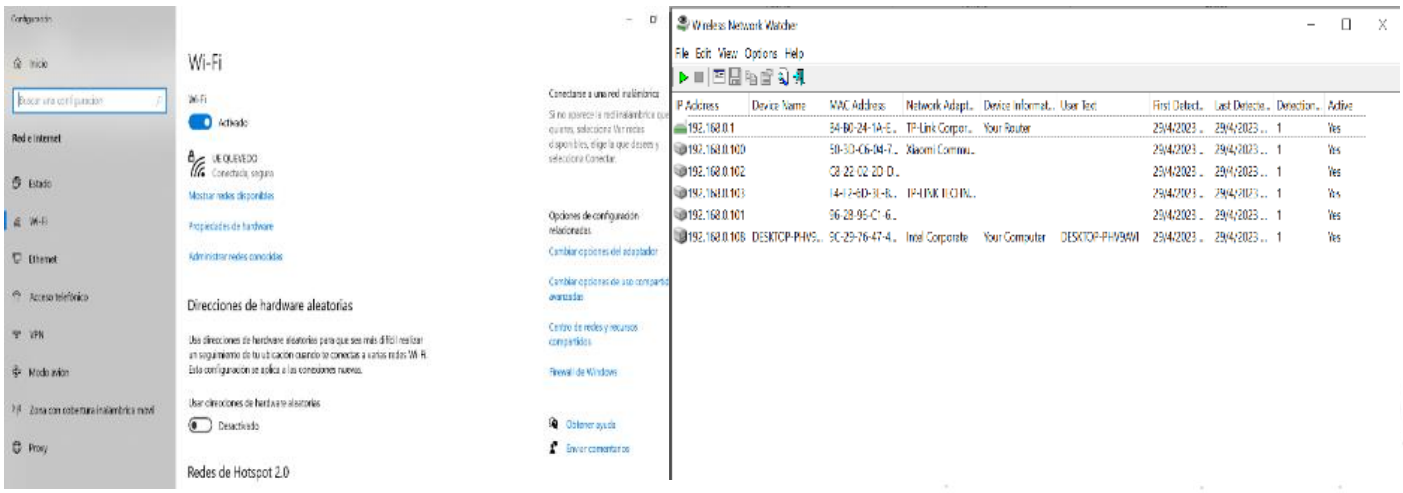
Figura 17 *Ventanas sin ninguna seguridad*

Nota: Instalaciones de la institución.

Tomada de elaboración propia.

El wifi que está en toda la institución no se encuentra segmentado, no cuenta con portal cautivo ni restricción alguna.

Figura 18 *Red sin segmentar dentro de la institución*



Nota: Instalaciones de la institución.

Tomada de elaboración propia.

Los puertos de red que se encuentran dentro de la institucion no poseen ningún tipo de seguridad y son de fácil acceso.

Figura 19 *Puertos de red de fácil acceso*

Nota: Instalaciones de la institución.

Tomada de elaboración propia.

6.2. Identificación de Activos

De acuerdo con una investigación de la Redalyc, los activos dentro de una unidad educativa en Ecuador pueden incluir, entre otros, la infraestructura, los recursos humanos, los materiales educativos, la tecnología, las actividades extracurriculares y la salud de los estudiantes. La investigación también señala que el buen sistema educativo es la mejor garantía para conseguir el bienestar de la población (Angulo Alegría & Aparicio Caicedo, 2017).

Lista de los activos dentro de la Unidad Educativa Quevedo:

- Infraestructura
- Equipos de Cómputo
- Vehículos
- Herramientas
- Sistemas de comunicación
- Paquetes Informáticos
- Bienes Artísticos y Culturales
- Archivos
- Personal

6.3. Identificación de Riesgos

A continuación, se detalla un resumen de los riesgos identificados dentro de la investigación realizada en la institución educativa.

Tabla 5 *Resumen de identificación de los riesgos*

EVENTOS/RIESGOS IDENTIFICADOS	DESCRIPCIÓN
Introducción de software dañino o perjudicial	Uso de equipos que poseen softwares propios de la institución.
Mal uso de recursos del sistema	Uso de equipos que poseen softwares propios de la institución.
Infiltración de las comunicaciones	Uso de equipos que permiten la comunicación dentro de la institución.
Fallo de la conexión	Toda red de datos tiene la probabilidad de que los servicios que se distribuyen a través de ella fallen.
Incrustación de códigos malicioso	Es una de las amenazas con mayor probabilidad de producirse debido al uso de correo electrónico y de descargas de páginas desconocidas.
Fallo de sistema	Malas configuraciones existentes en los equipos de capa 2 y 3.
Fallo de aplicaciones	Fallo con los servidores internos de la institución.
Error de usuario	Ejecuciones no mal intencionadas de procedimientos en los equipos.
Error de mantenimiento	Falta de mantenimientos a los diversos equipos interconectados a la red.
Escasez del personal	Falta de personal especializado en el monitoreo de la red.
Robo por internos	Personal que se sustrae equipamiento o hardware de la institución.
Robo por externos	Personas ajenas que se sustraen equipamiento o hardware de la institución.
Daño intencional por internos	Personal que no ayuda con el cuidado de la institución.
Daño intencional por externos	Personas ajenas que no ayudan con el cuidado de la institución.
Terrorismo	Amenaza que no se puede controlar.

Nota: En la Tabla 5 se puede observar el resumen de los diferentes eventos considerados que pueden ocurrir dentro de la Unidad Educativa Quevedo, se la puede visualizar completa en La Tabla 19 que se encuentra ubicada en el Anexo 1. Tomada de elaboración propia.

A continuación, se detalla el análisis y la valoración de los riesgos de la investigación realizada en la institución educativa.

Tabla 6 *Matriz de análisis y valoración de riesgos*

EVENTOS/RIESGOS IDENTIFICADOS	PROBABILIDAD (1 al 5)	IMPACTO (1 al 5)	VALORACIÓN DEL RIESGO (P * I)	CATEGORIA DEL RIESGO (P * I) / 25
Introducción de software dañino o perjudicial	5	3	15	60% EXTREMA Eliminar el riesgo, reducir, evitar, compartir o transferir.
Mal uso de recursos del sistema	5	5	25	1% BAJA Asumir el riesgo.
Infiltración de las comunicaciones	3	3	9	36% ALTA Reducir el riesgo, evitar, compartir o transferir.
Fallo de la conexión	4	4	16	64% EXTREMA Eliminar el riesgo, reducir, evitar, compartir o transferir.
Incrustación de códigos malicioso	2	5	10	40% ALTA Reducir el riesgo, evitar, compartir o transferir.
Fallo de software o sistema	4	5	20	80% EXTREMA Eliminar el riesgo, reducir, evitar, compartir o transferir.
Fallo de aplicaciones	4	5	20	80% EXTREMA Eliminar el riesgo, reducir, evitar, compartir o transferir.

				40% ALTA Reducir el riesgo, evitar, compartir o transferir.
Error de usuario	5	2	10	
Error de mantenimiento	5	2	10	40% ALTA Reducir el riesgo, evitar, compartir o transferir.
Escasez del personal	5	5	25	1% BAJA Asumir el riesgo.
Robo por internos	1	2	2	8% BAJA Asumir el riesgo.
Robo por externos	3	2	6	24% MODERADA Asumir el riesgo, reducir el riesgo.
Daño intencional por internos	1	3	3	12% BAJA Asumir el riesgo.
Daño intencional por externos	3	3	9	36% ALTA Reducir el riesgo, evitar, compartir o transferir.
Terrorismo	1	5	5	20% MODERADA Asumir el riesgo, reducir el riesgo.

Nota: En la Tabla 6 de análisis y valoraciones de los riesgos podemos identificar cada evento según su probabilidad e impacto y según la valoración que se ha obtenido se puede categorizar cada riesgo para poder tomar medidas en el asunto y poder minimizar el impacto o a su vez poder suprimir dicho impacto. Tomada de elaboración propia.

6.4. Tratamiento del riesgo

En base a la Tabla 6 podemos identificar los riesgos y el impacto que tiene cada uno de ellos, para el tratamiento de los mismos riesgos se ha optado en dar directrices a las personas responsables del departamento de TIC'S de la Unidad Educativa Quevedo.

Para el tratamiento de riesgos de nivel "extremo" y "alto", es necesario adoptar ciertas medidas de control y políticas de gestión obligatorias para reducir la posibilidad de ocurrencia de los riesgos identificados anteriormente. Finalmente, los criterios de tratamiento se aplicarán a los niveles de riesgo "moderado" y "bajo", en la medida en que se considere que la institución puede soportar los riesgos señalados sin afectar significativamente el normal funcionamiento de los servicios educativos.

Una vez que se haga una evaluación de riesgos dentro de la unidad educativa y se evalúe al personal docente responsable de las TIC´S a través de un formulario, si utilizan algún tipo de control de seguridad, se informará en el mismo.

Tras la evaluación de riesgos de los encargados del departamento TIC´S de la Unidad Educativa Quevedo, si se tenían controles de seguridad, determinación de políticas, organización, seguridad de la información, gestión de activos, control de acceso, criptografía, seguridad física y ambiental. aplicada, seguridad operativa, la comunicación, adquisición, desarrollo y mantenimiento de sistemas de información, los aspectos de seguridad de la información en curso de gestión de incidentes de seguridad de la información, gestión de seguridad y cumplimiento, sin los cuales está seguro.

Como resultados de la evaluación de riesgos se determinó, con base en métricas anteriores aborda las siguientes medidas de control.

- Gestión de Activos

La política de gestión de activos de la institución posee diversos equipos de comunicación dentro de la misma, también posee archivos de información pasada por lo que, mediante la creación, generación y control de un inventario de activos de información, se aplicarán procedimientos de protección, identificación, gestión documental, designación de equipos y personal encargado de gestionar dichos activos.

Pautas:

- Tener un inventario actualizado de los diferentes activos que posee la institución.
- Por cada proceso que se realice en el área TIC´S, habrá un responsable de dichos bienes, quien deberá documentar su estado para una mejor administración de los recursos de la institución.
- Cumplimiento de los acuerdos de confidencialidad de los activos otorgados por los responsables de las TIC´S.

➢ Dispositivos Móviles

La política de la institución en los dispositivos móviles es a través del ministerio de educación ya que tiene una aplicación a través de la cual se tiene la información de la misma.

Pautas:

- Se debe solicitar a los responsables de TIC´S que se les asigne una contraseña segura para la utilización de la plataforma.
- Se debería mantener un back up de la información que se posee en la plataforma.
- No mantener usuarios y contraseñas guardadas en los dispositivos móviles personales.
- No usar redes wifi de lugares públicos por la vulneración de seguridad que pueda existir.

➢ Control de Accesos

La política en los controles de acceso se espera que se controle el acceso a la información, los usuarios deberían autentificarse para poder hacer uso de los recursos técnicos que puede ofrecer la institución, los métodos de acceso a Internet, etc. se puedan lograr mediante la creación de roles y permisos adicionales necesarios para realizar actividades.

Pautas:

- Contar con un correo institucional para poder ingresar a la red institucional para el acceso libre al internet.
- Inhabilitar los puntos de red que se encuentre fuera de oficinas o en lugares que no estén bajo supervisión.

- Según el nivel de acceso que tengan las personas podrán acceder a los diferentes servicios de la red de la institución.

➢ Gestión de Contraseñas

La política de la gestión de contraseñas mejora el acceso a la plataforma ya que se controla de mejor manera de una manera más confiable.

Pauta:

- Usar contraseñas alfa numéricas que posean letras mayúsculas, minúsculas, números y símbolos.
- Cambiar la contraseña mínima cada tres meses.
- No usar contraseñas que ya hayan sido usado con anterioridad.
- Configurar límite de tiempo para la sesión en caso de suspensión o falta de uso de la misma.
- Configurar accesos en dos pasos para el ingreso de la plataforma.

➢ Clasificación de la Información

La política de clasificación de la información de la institución por los diversos tipos de procesos que se pueden generar y usarla de la manera más eficiente cuando se la necesite.

Pautas:

- Calificar como información confidencial a aquella información que contenga datos relevantes de convenios, donaciones, denuncias.
- Calcificar como información legal a aquella información que contenga datos de visitas técnicas dentro y fuera de la ciudad.
- Calificar como información interna a aquella información de la planta docente y estudiantes de la institución, subida de calificaciones.
- Calificar como información pública a aquella información que se pueda mostrar en la aplicación del ministerio de educación.

➢ Dispositivos de Escritorios

La política de dispositivos de escritorio se debe de dar en toda la institución, ya que todos los dispositivos están interconectados en los varios bloques de la misma red y puede ser riesgo de visualización y manipulación o perdida de datos.

Pautas:

- Configurar modo de suspensión con bloqueo de pantalla al reactivarse la sesión.
- Acceder a los dispositivos con los usuarios y contraseña establecidos por el departamento de TIC´S.
- No permitir el uso de los dispositivos fuera de horarios laborales.

➢ Protección contra los Códigos Maliciosos

La política de protección contra códigos maliciosos es la de defender los dispositivos de virus, de esta manera se pretende que las vulneraciones a los diferentes tipos de dispositivos disminuyan y los usuarios puedan usarlos sin riesgos.

Pautas:

- Prevenir la descarga indebida de archivos potencialmente peligrosos para los dispositivos.
- Instalar aplicaciones que congelen los dispositivos para prevenir la instalación de programas potencialmente dañinos.
- Evitar el uso de proxys para vulnerar los firewalls configurados en la red institucional.
- Planificar mantenimientos preventivos y revisiones periódicas de los dispositivos.

➢ Gestión de Incidentes

La política de gestión de incidentes es la de gestionar una respuesta inmediata y practica a cualquier novedad o situación que pueda presentarse dentro de la red institucional y al personal de la misma, siempre y cuando esté relacionado a la seguridad informática.

Pautas:

- Crear una bitácora donde se detalle el uso, ingreso a los diferentes lugares donde están los activos de la institución y que actividad va a realizar.

- Solucionar las novedades e incidentes que puedan presentarse en el menor tiempo posible.

6.5. Medidas a tomar

En esta sección se va a citar los diversos tipos de protocolos que se pueden usar dentro de la Unidad Educativa Quevedo, considerando sus activos y la eficacia del protocolo dentro de la misma.

A continuación, se detallan la aplicación de los diferentes de controles de la información y características dentro de la investigación realizada en la institución educativa.

Tabla 7 *Resumen de la aplicación del Control de Seguridad de la Información*

TIPOS Y MEDIDAS DE CONTROL		CARACTERÍSTICA	
SECCIÓN	**DOMINIO - CONTROL**	**RESPONSABLE**	**FECHA DE IMPLEMENTACIÓN**
A5	Políticas de seguridad.	DIRECTIVOS DE LA INSTITUCIÓN	Implementada
		DIRECTIVOS DE LA INSTITUCIÓN	Implementada
		INSPECTOR GENERAL	Implementada
A6	Aspectos organizativos de la seguridad de la información.	DEPARTAMENTO DE TIC´S	Abril - 2023
		DEPARTAMENTO DE TIC´S	Octubre - 2023
		DEPARTAMENTO DE TIC´S	Octubre - 2023
A7	Seguridad ligada a los recursos humanos.	INSPECTOR GENERAL	Octubre - 2023
		INSPECTOR GENERAL	En fase de prueba
		INSPECTOR GENERAL	En fase de prueba
A8	Gestión de activos.	COMUNIDAD EDUCATIVA	Implementada
		DEPARTAMENTO DE TIC´S	Abril - 2023
		COMUNIDAD EDUCATIVA	Implementada

		COMUNIDAD EDCUATIVA	Abril - 2023
		DEPARTAMENTO DE TIC´S	Abril - 2023
A9	Control de accesos.	COMUNIDAD EDCUATIVA	Abril - 2023
		DEPARTAMENTO DE TIC´S	Abril - 2023
A10	Cifrado.	DEPARTAMENTO DE TIC´S	Octubre - 2023
		COMUNIDAD EDCUATIVA	Abril - 2023
A11	Seguridad física y ambiental.	COMUNIDAD EDCUATIVA	Abril - 2023
		DEPARTAMENTO DE TIC´S	Abril - 2023
		DEPARTAMENTO DE TIC´S	Octubre - 2023
A12	Seguridad en la operativa.	DEPARTAMENTO DE TIC´S	Octubre - 2023
		DEPARTAMENTO DE TIC´S	Octubre - 2023
		DEPARTAMENTO DE TIC´S	Octubre - 2023
A13	Seguridad en las telecomunicaciones.	DEPARTAMENTO DE TIC´S	Octubre - 2023
		DEPARTAMENTO DE TIC´S	Octubre - 2023
A14	Adquisición, desarrollo y mantenimiento de los sistemas de información.	DEPARTAMENTO DE TIC´S	Octubre - 2023
		DEPARTAMENTO DE TIC´S	Octubre - 2023
A16	Gestión de incidentes en la seguridad de la información.	COMUNIDAD EDCUATIVA	Abril - 2023

Nota: En la Tabla 7 se puede observar el resumen de la situación actual y la aplicación del Control de Seguridad de la Información, se la puede visualizar completa en La Tabla 20 que se encuentra ubicada en el Anexo 2. Tomada de elaboración propia.

A continuación, se detallan las políticas de seguridad de la información adoptadas para la presente propuesta de investigación.

Tabla 8 *Medidas a tomar de las políticas de seguridad de la información*

A.5	**Políticas de seguridad de la información**	
A.5.1	**Directrices de gestión de la seguridad de la información**	
Objetivo: Proporcionar orientación y apoyo a la gestión de la seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normativa pertinentes.		
A.5.1.1	Políticas para la seguridad de la información	*Control* Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.
A.5.1.2	Revisión de las políticas para la seguridad de la información	*Control* Las políticas de seguridad de la información deben revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Nota: Dentro de la Tabla 7 podemos observar los controles que se propone usar dentro de la institución. Fuente: (López Neira, 2023).

Dentro de la institución debe existir normativas legales para la seguridad de la información de cada uno de las personas que conforman la comunidad educativa, estas políticas tienen que ser públicas y socializadas con todos los partícipes.

A continuación, se detallan las políticas de la organización de la seguridad de la información adoptadas para la presente propuesta de investigación.

Tabla 9 *Medidas a tomar de la organización de la seguridad de la información*

A.6	**Organización de la seguridad de la información**	
A.6.1	**Organización interna**	
Objetivo: Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.		
A.6.1.1	Roles y responsabilidades en seguridad de la información	*Control* Todas las responsabilidades en seguridad de la información deben ser definidas y asignadas.

A.6.1.2	Segregación de tareas	*Control* Se deberían segregar tareas y las áreas de responsabilidad ante posibles conflictos de interés con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de un mal uso de los activos de la organización.
A.6.1.3	Contacto con las autoridades	*Control* Deben mantenerse los contactos apropiados con las autoridades y asociaciones profesionales especializados en seguridad.
A.6.2 Dispositivos para movilidad y teletrabajo Objetivo: El objetivo es el de garantizar la seguridad de la información en el uso de recursos de informática móvil y teletrabajo.		
A.6.2.1	Política de uso de dispositivos para movilidad	*Control* Se debería establecer una política formal y se deberían adoptar las medidas de seguridad adecuadas para la protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones.
A.6.2.2	Teletrabajo	*Control* Se debería desarrollar e implantar una política y medidas de seguridad de apoyo para proteger a la información accedida, procesada o almacenada en ubicaciones destinadas al teletrabajo.

Nota: Dentro de la Tabla 9 podemos observar los controles que se propone usar dentro de la institución. Tomada de https://www.iso27000.es/.

Dentro de la institución debe existir roles de responsabilidad en cada uno de los departamentos en los cuales se segrega las diversas actividades, también debe existir un asertivo acercamiento hacia las autoridades para poder notificar situaciones irregulares, también se debe tener medidas sustitutivas en el caso del teletrabajo ya que al ser una institución pública se tiene estudiantes de varias clases económicas y por ende debe haber una política del uso de dispositivos móviles dentro de la institución.

A continuación, se detallan las políticas de la seguridad ligada a los recursos humanos adoptadas para la presente propuesta de investigación.

Tabla 10 *Medidas a tomar de la seguridad ligada a los recursos humanos*

A.7 Seguridad ligada a los recursos humanos		
A.7.2 Antes de la contratación		
Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección adecuadas.		
A.7.2.2	Concienciación, educación y capacitación en SI	*Control* Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.
A.7.2.3	Proceso disciplinario	*Control* Debería existir un proceso formal disciplinario comunicado a empleados que produzcan brechas en la seguridad.
A.7.3 Cese o cambio de puesto de trabajo		
Objetivo: El objetivo es el de proteger los intereses de la organización durante el proceso de cambio o finalización de empleo por parte de empleados y contratistas.		
A.7.3.1	Cese o cambio de puesto de trabajo	*Control* Las responsabilidades para ejecutar la finalización de un empleo o el cambio de éste deberían estar claramente definidas, comunicadas a empleado o contratista y asignadas efectivamente.

Nota: Dentro de la Tabla 10 podemos observar los controles que se propone usar dentro de la institución. Tomada de https://www.iso27000.es/.

Dentro de la institución debe de existir una normativa interna de la implementación de capacitaciones continuas para los docentes ya que no pueden estar desactualizados en temas de tecnologías de la información, debe de existir una normativa interna en la cual se pueda buscar la forma jurídica para sancionar a un docente que regularmente infrinja o viole la seguridad. Las contrataciones no son responsabilidad de la institución, pero debe de existir una base de datos de cada uno de los docentes que laboren o laboraron dentro de la misma en la cual deberían tener fichas médicas, fichas de estudios, entre otros.

A continuación, se detallan las políticas de la gestión de activos adoptadas para la presente propuesta de investigación.

Tabla 11 *Medidas a tomar de la gestión de activos*

A.8	**Gestión de Activos**	
A.8.1	**Responsabilidad sobre los activos**	
Objetivo: El objetivo es identificar los activos en la organización y definir las responsabilidades para una protección adecuada.		
A.8.1.1	Inventario de activos	*Control* Debe implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.
A.8.1.3	Uso aceptable de los activos	*Control* Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.
A.8.1.4	Devolución de activos	*Control* Todos los empleados y usuarios de terceras partes deberían devolver todos los activos de la organización que estén en su posesión/responsabilidad una vez finalizada el acuerdo, contrato de prestación de servicios o actividades relacionadas con su contrato de empleo.
A.8.2	**Clasificación de la información**	
Objetivo: El objetivo es el de asegurar que se aplica un nivel de protección adecuado a la información.		
A.8.2.1	Directrices de clasificación	*Control* La información debería clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización.
A.8.2.2	Etiquetado y manipulado de la información	*Control* Se debería desarrollar e implantar un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.2.3	Manipulación de activos	*Control* Se deberían desarrollar e implantar procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la organización.
A.8.3	**Manejo de los soportes de almacenamiento**	

Objetivo: El objetivo es evitar la divulgación, modificación, retirada o destrucción de activos no autorizada almacenada en soportes de almacenamiento.		
A.8.3.1	Gestión de soportes extraíbles	*Control* Se deberían establecer procedimientos para la gestión de los medios informáticos removibles acordes con el esquema de clasificación adoptado por la organización.
A.8.3.3	Soportes físicos en tránsito	*Control* Se deberían proteger los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización.

Nota: Dentro de la Tabla 11 podemos observar los controles que se propone usar dentro de la institución. Tomada de https://www.iso27000.es/.

Dentro de la institución debe de existir un inventario de los activos, también debe haber una comisión que supervise los activos que se poseen, en qué estado están, quien los manipula y en manos de quien reposan los activos o si han sido devueltos, debe de existir una normativa interna donde se regule el etiquetado de los activos, la clasificación de los mismos y la cadena de custodia de los mismos.

A continuación, se detallan las políticas del control de accesos adoptadas para la presente propuesta de investigación.

Tabla 12 *Medidas a tomar del control de accesos*

A.9 Control de accesos **A.9.1 Requisitos de negocio para el control de accesos** Objetivo: El objetivo es controlar los accesos a la información y las instalaciones utilizadas para su procesamiento.		
A.9.1.1	Política de control de accesos	*Control* Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la organización.
A.9.1.2		*Control*

	Control de acceso a las redes y servicios	Se debería proveer a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar.

A.9.2 Gestión de acceso de usuario

Objetivo: El objetivo es el de garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información y servicios.

A.9.2.1	Gestión de altas/bajas en el registro de usuarios	*Control* Debería existir un procedimiento formal de alta y baja de usuarios con objeto de habilitar la asignación de derechos de acceso.
A.9.2.2	Gestión de los derechos de acceso asignados a usuarios	*Control* Se debería de implantar un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios.

A.9.3 Responsabilidades del usuario

Objetivo: El objetivo es hacer que los usuarios sean responsables de la protección de la información para su identificación.

A.9.3.1	Uso de información confidencial para la autenticación	*Control* Se debería exigir a los usuarios el uso de las buenas prácticas de seguridad de la organización en el uso de información confidencial para la autenticación.

A.9.4 Control de acceso a sistemas y aplicaciones

Objetivo: El objetivo es impedir el acceso no autorizado a la información mantenida por los sistemas y aplicaciones.

A.9.4.1	Restricción del acceso a la información	*Control* Se debería restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.
A.9.4.2	Procedimientos seguros de inicio de sesión	Cuando sea requerido por la política de control de accesos se debería controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de log-on.

A.9.4.3	Gestión de contraseñas de usuario	Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar contraseñas de calidad.

Nota: Dentro de la Tabla 12 podemos observar los controles que se propone usar dentro de la institución. Tomada de https://www.iso27000.es/.

Dentro de la institución debe de existir una normativa interna en la cual debe estar especificado como manipular un control de acceso en la cual permita ingresar nuevos usuarios, eliminar, modificar usuarios existentes, la asignación de niveles de restricción a la información que posee la institución, el gestionamiento de contraseñas seguras, tiempo de duración y reseteo de las mismas, también debe de existir bitácoras para quien ingresa a la documentación de la institución.

A continuación, se detallan las políticas de cifrados adoptadas para la presente propuesta de investigación.

Tabla 13 *Medidas a tomar de cifrados*

A.10	**Cifrados**	
A.10.1	**Controles criptográficos**	
Objetivo: El objetivo es garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.		
A.10.1.2	Gestión de claves	*Control* Se debería desarrollar e implementar una política sobre el uso, la protección y el ciclo de vida de las claves criptográficas a través de todo su ciclo de vida.

Nota: Dentro de la Tabla 13 podemos observar los controles que se propone usar dentro de la institución. Tomada de https://www.iso27000.es/.

Dentro de la normativa interna del control de accesos debe de haber una extensión para poder gestionar las contraseñas de los usuarios que accedan a la información de la institución, no es necesario la creación de políticas de controles criptográficos ya que no existen muchos subniveles de seguridad dentro de la institución.

A continuación, se detallan las políticas de la seguridad física y ambiental adoptadas para la presente propuesta de investigación.

Tabla 14 *Medidas a tomar de Seguridad física y ambiental*

A.11	**Seguridad física y ambiental**	
A.11.1	**Áreas seguras**	
Objetivo: El objetivo es evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.		
A.11.1.1	Perímetro de seguridad física.	*Control* Se deberían definir y utilizar perímetros de seguridad para la protección de las áreas que contienen información y las instalaciones de procesamiento de información sensible o crítica.
A.11.1.2	Controles físicos de entrada.	*Control* Las áreas seguras deberían estar protegidas mediante controles de entrada adecuados para garantizar que solo el personal autorizado dispone de permiso de acceso.
A.11.1.3	Seguridad de oficinas, despachos y recursos.	*Control* Se debería diseñar y aplicar un sistema de seguridad física a las oficinas, salas e instalaciones de la organización.
A.11.1.4	Protección contra las amenazas externas y ambientales.	*Control* Se debería diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes.
A.11.2	**Seguridad de los equipos**	
Objetivo: El objetivo es evitar la pérdida, los daños, el robo o el compromiso de activos y la interrupción a las operaciones de la organización.		
A.11.2.1	Emplazamiento y protección de equipos	*Control* Los equipos se deberían emplazar y proteger para reducir los riesgos de las amenazas y peligros ambientales y de oportunidades de acceso no autorizado.
A.11.2.3	Seguridad del cableado	*Control* Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se deberían proteger contra la intercepción, interferencia o posibles daños.
A.11.2.4	Mantenimiento de los equipos	*Control* Los equipos deberían mantenerse adecuadamente con el objeto de garantizar su disponibilidad e integridad continuas.
A.11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	*Control* Se debería adoptar una política de puesto de trabajo despejado para documentación en

		papel y para medios de almacenamiento extraíbles y una política de monitores sin información para las instalaciones de procesamiento de información.

Nota: Dentro de la Tabla 14 podemos observar los controles que se propone usar dentro de la institución. Tomada de https://www.iso27000.es/.

Dentro de la institución debe existir debe haber una normativa interna donde se estipule las zonas de los bloques de la institución, de qué manera deben estar protegidas todas las áreas y los equipos, también como deberían estar protegidos los cables para que no se puedan manipular fácilmente, también debe de existir la política de que si uno abandona el área de trabajo el equipo que se esté manipulando entre en suspensión y al reactivarse solicite identificación.

A continuación, se detallan las políticas de la seguridad en la operativa adoptadas para la presente propuesta de investigación.

Tabla 15 *Medidas a tomar de Seguridad en la operativa*

A.12	**Seguridad en la operativa**	
A.12.1	**Responsabilidades y procedimientos de operación**	
Objetivo: El objetivo es evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.		
A.12.1.2	Gestión de cambios	*Control* Se deberían controlar los cambios que afectan a la seguridad de la información en la organización y procesos de negocio, las instalaciones y sistemas de procesamiento de información.
A.12.2	**Protección contra código malicioso**	
Objetivo: El objetivo es garantizar que la información y las instalaciones de procesamiento de información estén protegidas contra el malware.		
A.12.2.1	Controles contra el código malicioso	*Control* Se deberían implementar controles para la detección, prevención y recuperación ante afectaciones de malware en combinación con la concientización adecuada de los usuarios.
A.12.3	**Copias de seguridad**	
Objetivo: El objetivo es alcanzar un grado de protección deseado contra la pérdida de datos.		

A.12.3.1	Copias de seguridad de la información	*Control* Se deberían realizar y pruebas regulares de las copias de la información, del software y de las imágenes del sistema en relación a una política de respaldo (Backup) convenida.

A.12.4 Registro de actividad y supervisión

Objetivo: El objetivo es registrar los eventos relacionados con la seguridad de la información y generar evidencias.

A.12.4.1	Registro y gestión de eventos de actividad	*Control* Se deberían producir, mantener y revisar periódicamente los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información.
A.12.4.2	Protección de los registros de información	*Control* Se debería proteger contra posibles alteraciones y accesos no autorizados la información de los registros.

A.12.6 Gestión de la vulnerabilidad técnica

Objetivo: El objetivo es evitar la explotación de vulnerabilidades técnicas.

A.12.6.2	Restricciones en la instalación de software	*Control* Se deberían establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios.

Nota: Dentro de la Tabla 15 podemos observar los controles que se propone usar dentro de la institución. Tomada de https://www.iso27000.es/.

Dentro de la institucion debe de existir una normativa interna donde se haga referencia a las medidas de seguridad que se tienen dentro de la institución entre las cuales deben de existir bitácoras de cambios dentro la red, controles de códigos de fuentes desconocidas, back ups de respaldos de la diferentes informaciones que se puedan manejar, bitácoras de actividades que se realicen dentro de los usuarios que manipulan información delicada, también la restricción de programas no autorizados por la institución.

A continuación, se detallan las políticas de la seguridad en las telecomunicaciones adoptadas para la presente propuesta de investigación.

Tabla 16 *Medidas a tomar de Seguridad en las telecomunicaciones*

A.13	**Seguridad en las telecomunicaciones**	
A.13.1	**Gestión de la seguridad en las redes**	
Objetivo: El objetivo es evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.		
A.13.1.1	Controles de red	*Control* Se deberían administrar y controlar las redes para proteger la información en sistemas y aplicaciones.
A.13.1.3	Segregación de redes	*Control* Se deberían segregar las redes en función de los grupos de servicios, usuarios y sistemas de información.
A.13.2	**Intercambio de información con partes externas**	
Objetivo: El objetivo es mantener la seguridad de la información que transfiere una organización internamente o con entidades externas.		
A.13.2.1	Políticas y procedimientos de intercambio de información	*Control* Deberían existir políticas, procedimientos y controles formales de transferencia para proteger la información que viaja a través del uso de todo tipo de instalaciones de comunicación.
A.13.2.3	Mensajería electrónica	*Control* Se debería proteger adecuadamente la información referida en la mensajería electrónica.
A.13.2.4	Acuerdos de confidencialidad y secreto	*Control* Se deberían identificar, revisar y documentar de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la organización para la protección de información.

Nota: Dentro de la Tabla 16 podemos observar los controles que se propone usar dentro de la institución. Tomada de https://www.iso27000.es/.

Dentro de la institución debe de existir una normativa interna sobre la seguridad de las telecomunicaciones en las cuales tiene que detallarse los controles de redes que se deben de realizar, como se debería estar segmentada la red, correo institucional para cada docente, también

deben de estar los acuerdos de confidencialidad para la no divulgación de cierta documentación que sea delicada y sea de uso estricto de la institución.

A continuación, se detallan las políticas de la adquisición, desarrollo y mantenimiento de los sistemas de información adoptadas para la presente propuesta de investigación.

Tabla 17 *Medidas a tomar de Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información*

A.14	**Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información**	
A.14.1	**Requisitos de seguridad de los sistemas de información**	
Objetivo: El objetivo es garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo su ciclo de vida.		
A.14.1.1	Análisis y especificación de los requisitos de seguridad	*Control* Los requisitos relacionados con la seguridad de la información se deberían incluir en los requisitos para los nuevos sistemas o en las mejoras a los sistemas de información ya existentes.
A.14.2	**Seguridad en los procesos de desarrollo y soporte**	
Objetivo: El objetivo de este control es garantizar la seguridad de la información en los entornos de diseño e implementación dentro del ciclo de vida de desarrollo de los sistemas de información.		
A.14.2.2	Procedimientos de control de cambios en los sistemas	*Control* En el ciclo de vida de desarrollo se deberían hacer uso de procedimientos formales de control de cambios.

Nota: Dentro de la Tabla 17 podemos observar los controles que se propone usar dentro de la institución. Tomada de https://www.iso27000.es/.

Dentro de la institución debe de existir un informe técnico donde se detalle las características de cada uno de los equipos que se tiene dentro de la misma, también el soporte técnico de cada que tiempo se debe realizar los mantenimientos preventivos y en caso de haber mantenimientos correctivos.

A continuación, se detallan las políticas de la gestión de incidentes de la seguridad de la información adoptadas para la presente propuesta de investigación.

Tabla 18 *Medidas a tomar de Gestión de Incidentes de Seguridad de la Información*

A.16 Gestión de Incidentes de Seguridad de la Información		
A.16.1 Gestión de incidentes de seguridad de la información y mejoras		
Objetivo: El objetivo es de garantizar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de vulnerabilidades e incidentes de seguridad.		
A.16.1.1	Responsabilidades y procedimientos	*Control* Deben establecerse responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información

Nota: Dentro de la Tabla 18 podemos observar los controles que se propone usar dentro de la institución. Tomada de https://www.iso27000.es/.

Dentro de la institución debería haber una bitácora donde exista los incidentes que se puedan dar dentro de la misma, con qué frecuencia, que tipo de incidente y complejidad del mismo.

A continuación, se detallan las políticas de la organización de la seguridad de la información adoptadas para la presente propuesta de investigación.

6.6. Aceptación y comunicación del riesgo

Una vez realizado y socializado las recomendaciones con los encargados del departamento de las TIC´S se procede a realizar recomendaciones para el caso de que el personal se resista acatar las recomendaciones.

Las sanciones por incumplimiento de la política propuesta también se consideran importantes una vez que se identifiquen los lineamientos a considerar, ya que esto permitirá que los responsables de las TIC´S tengan mayor conocimiento de los lineamientos y evite inconvenientes en materia de seguridad de la información. En otras palabras, de esta forma se quiere prevenir cualquier operación que ponga en riesgo la confidencialidad, disponibilidad e integridad de la información.

Los responsables del departamento de las TIC´S podrán regular a cualquier persona que administre recursos tecnológicos dentro de la institución. Su vigencia estará sujeta a sanciones internas las cuales se harán efectivas a partir de la aplicación de la política de seguridad en la Unidad Educativa Quevedo.

7. Discusión

La gestión de riesgos en la infraestructura de tecnología de la información (TI) es un tema de gran importancia en la actualidad, ya que la tecnología se ha convertido en una herramienta crítica para las operaciones organizacionales y educativas. En este sentido, la Unidad Educativa Quevedo es una institución que también necesita implementar medidas de gestión de riesgos para garantizar la seguridad y el buen funcionamiento de su infraestructura informática.

Considerando que el uso de las tecnologías de la información y la comunicación se ha convertido en parte integral de la educación, el tema del análisis y asesoramiento en gestión de riesgos en la infraestructura TI del sector educativo de Quevedo cobra mucha relevancia en la actualidad. El asesoramiento en gestión de riesgos es un paso importante para garantizar el buen funcionamiento de los sistemas de información y la protección de los datos institucionales y de los estudiantes. Para ello se realiza una revisión bibliográfica del concepto de gestión de riesgos en TI y se aplica una metodología de evaluación de riesgos adecuada a las necesidades de la institución.

Las propuestas presentadas enfatizan la importancia de identificar riesgos y vulnerabilidades en la infraestructura de TI y establecer controles y mitigaciones para reducir la probabilidad y el impacto de los incidentes de seguridad. Incluye aspectos relacionados con la aplicación de políticas de seguridad, capacitación y concientización de usuarios, administración de accesos y privilegios, copias de respaldo y monitoreo del sistema.

Cabe mencionar que las recomendaciones presentadas son efectivas en la medida en que se implementen correctamente y su efectividad sea monitoreada y evaluada continuamente. Además, es imperativo involucrar a todos los empleados de la institución en el proceso de gestión de riesgos y promover una cultura de seguridad de la información.

En pocas palabras la gestión de riesgos para la infraestructura de TI de la Unidad Educativa Quevedo son un avance importante para garantizar la seguridad y protección de los sistemas de información y datos institucionales y estudiantiles. Es necesario seguir haciendo un buen trabajo en la implementación y evaluación continua para asegurar la efectividad a largo plazo.

8. Conclusiones

En base a los objetivos específicos planteados en la investigación sobre el análisis y propuesta de gestión de riesgo en infraestructura TI en la Unidad Educativa Quevedo, se pueden obtener las siguientes conclusiones:

- Con respecto del primer objetivo, el levantamiento de activos e infraestructura crítica se realizó y se evidencio la Tabla 5 identifica los sistemas y tecnologías de información más relevantes para la institución y proporciona una comprensión integral de los riesgos y vulnerabilidades dentro de la infraestructura de TI.
- Las acciones a corto, mediano y largo plazo sobre la gestión de riesgos, identificando los diversos controles y mitigaciones que se pueden implementar en la institución para reducir la probabilidad de un incidente de seguridad y minimizar su impacto si ocurre, se encuentran en el apartado 6.3.
- El plan de gestión de riesgos incluye los controles necesarios para minimizar los riesgos identificados y establece procesos continuos de seguimiento y evaluación para asegurar su eficacia a largo plazo.
- Las medidas propuestas en la presente tesis son las mínimas requeridas para la seguridad de la información en la Unidad Educativa Quevedo. Esto significa que se puede desarrollar muchas más medidas que deberían ser evaluadas por el jefe de seguridad informática dentro de la institución según su necesidad e infraestructura.
- Es fundamental fomentar una cultura de seguridad en la institución, en la que todos los usuarios estén conscientes de la importancia de proteger la información y los sistemas de información.

9. Recomendaciones

En base a los objetivos específicos planteados en la investigación sobre el análisis y propuesta de gestión de riesgo en infraestructura TI en la Unidad Educativa Quevedo, se pueden realizar las siguientes recomendaciones:

- Es importante que se realicen evaluaciones periódicas de los riesgos presentes en la infraestructura TI de la institución, de manera que se puedan identificar nuevas amenazas y vulnerabilidades y se puedan aplicar medidas de control y mitigación adecuadas.
- Se recomienda establecer políticas de seguridad claras y bien definidas, que incluyan aspectos como la gestión de accesos y privilegios, la realización de copias de seguridad, la monitorización de los sistemas y la formación y concienciación de los usuarios.
- Se sugiere la realización de pruebas de penetración en la infraestructura TI, con el fin de identificar posibles puntos débiles y vulnerabilidades que puedan ser explotados por atacantes externos o internos.
- Se recomienda establecer un plan de contingencia que contemple los procedimientos a seguir en caso de que ocurran incidentes de seguridad en la infraestructura TI de la institución.
- Se sugiere la realización de capacitaciones a los usuarios de la infraestructura TI, con el fin de que conozcan las políticas de seguridad y sepan cómo actuar en caso de incidentes de seguridad.

10. Bibliografía

Aguilera López, P. (2017). *Seguridad Informática.* Madrid: Editex.

Angulo Alegría, M., & Aparicio Caicedo, N. (2017). Mapa de activos de salud en una unidad educativa fiscal de Esmeraldas. Esmeraldas: Archivo Médico de Camagüey.

Becerra, Y., Betancourt, R., & Serrato, Y. (2022). *Propuesta para mejores prácticas en el proceso de gestión de infraestructura e interconexiones, alineado con la norma ISO 27001:2013, para la compañía sistemas satelitales de Colombia (SSC).* Bogota: Libertadores.

Camacho Reyes, R., & Patiño Maisanche, B. (2022). *Implementación de un Modelo de Gestión de la Seguridad de la Información basado en la Norma ISO 2700, para los docentes de la Universidad Técnica Estatal de Quevedo.* Logroño: Unir.

Dell. (01 de Febrero de 2022). *https://www.dell.com/*. Obtenido de https://www.dell.com/: https://www.dell.com/es-es/shop/servidores-almacenamiento-y-redes/smart-selection-poweredge-r650-servidor-rack/spd/poweredge-r650/per6501a

Fiscalia General del Estado. (2016). *Guía para la administración del riesgo institucional.* Quito.

Flores, D. (25 de Agosto de 2021). *OpenWebinars*. Obtenido de OpenWebinars: https://openwebinars.net/blog/triangulo-de-seguridad-informatica-que-es-y-sus-objetivos/#:~:text=Qu%C3%A9%20es%20el%20tri%C3%A1ngulo%20de,los%20datos%20que%20se%20manejan.

Freddo, J., & Flores, D. (18 de 05 de 2012). Seguridad de la información de archivo: el control de acceso. *Seguridad de la información de archivo: control de acceso en archivos públicos estatales*, págs. 158-178.

Garcia, R. (11 de Junio de 2016). *Escuela de Organización Industrial*. Obtenido de Escuela de Organización Industrial: https://www.eoi.es/blogs/ciberseguridad/2016/06/11/analisis-de-situacioniso27001-en-las-organizaciones-3/.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. (2016). Metodologia de la Investigación. En R. Hernández Sampieri, C. Fernández Collado, & M. d. Baptista Lucio, *Metodologia de la Investigación* (págs. 396-404). México: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V.

ISOTools. (20 de Abril de 2017). *ISOTools Excellence*. Obtenido de ISOTools Excellence: https://www.pmg-ssi.com/2017/04/dominios-iso-27001-2013/

Ladino, M., Villa, P., & López, A. (2019). *Fundamentos de ISO 27001 y su aplicación en las empresas.* Pereira: Scientia et Technica.

López Neira, A. (05 de Marzo de 2023). *ISO27000.es*. Obtenido de ISO27000.es: https://www.iso27000.es/

Puga Jácome, C. (2019). *Diseño de una política de gestión de seguridad de la información ara el área de imagenología del hospital general docente de calderón utilizando los estándares iso 27001 e iso 27799.* Quito: Institución Internacional SEK.

Romero, M., Figueroa, G., Vera, D., Álava, J., Parrales, G., Álava, C., . . . Castillo, M. (2018). *Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades.* Jipijapa: 3 Ciencias.

Russell, J. (2022). *ISO 27001:2013 Guía de Implementación para la seguridad de la información.* Madrid: Nqa.

Torres, C. (2020). *Plan de seguridad informática basado en la norma ISO 27001, para proteger la información y activos de la empresa privada MEGAPROFER S.A.* Ambato: Universidad Técnica de Ambato.

Unidad Educativa Quevedo. (01 de 05 de 2023). *https://sites.google.com/view/unidadeducativaquevedo-ueq/inicio?authuser=0*. Obtenido de https://sites.google.com/view/unidadeducativaquevedo-ueq/inicio?authuser=0: https://sites.google.com/view/unidadeducativaquevedo-ueq/inicio?authuser=0

Universidad Libre, C. (10 de Junio de 2015). *Universidad Libre Seccional Bogota*. Obtenido de Universidad Libre Seccional Bogota: https://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/152-seguridad-de-la-informacion

Zoostock. (01 de Febrero de 2022). *https://www.zoostock.com*. Obtenido de https://www.zoostock.com: https://www.zoostock.com/categoria/cisco-switches

11. Anexos

Anexo 1. Identificación de Riesgos

Tabla 19 *Identificación de Riesgos*

EVENTOS/RIESGOS IDENTIFICADOS	DESCRIPCIÓN	CAUSAS	CONSECUENCIAS POTENCIALES
Introducción de software dañino o perjudicial	Uso de equipos que poseen softwares propios de la institución.	Ingresar al sistema e instalar aplicaciones no autorizadas.	Evidencia la falta de protección de un antivirus o el mismo control de softwares en los equipos.
Mal uso de recursos del sistema	Uso de equipos que poseen softwares propios de la institución.	Ingresar al sistema y descargar información no autorizada.	Genera una degradación de las capacidades de procesamiento y almacenamiento del equipo.
Infiltración de las comunicaciones	Uso de equipos que permiten la comunicación dentro de la institución.	Libre uso de los puertos de red de la institución.	Interrumpir, modificar o adulterar la información de la institución.
Fallo de la conexión	Toda red de datos tiene la probabilidad de que los servicios que se distribuyen a través de ella fallen.	Instalaciones de red sin ningún tipo de seguridad y al alcance de todos.	Los fallos pueden generar accesos no deseados dejando la información disponible a ser extraída o alterada.
Incrustación de códigos malicioso	Es una de las amenazas con mayor probabilidad	Uso de softwares sin licencias.	Se infecta el software evidenciando la falta de antivirus o

	de producirse debido al uso de correo electrónico y de descargas de páginas desconocidas.		procedimientos de prevención de real de intrusiones.
Fallo de sistema	Malas configuraciones existentes en los equipos de capa 2 y 3.	Uso de software sin licencia.	Ataques de denegación de servicios.
Fallo de aplicaciones	Fallo con los servidores internos de la institución.	No se usa firewalls, ni programas de seguridad.	Fácil acceso a la información de los servidores.
Error de usuario	Ejecuciones no mal intencionadas de procedimientos en los equipos.	Mal uso de los equipos y baja supervisión de los equipos.	Probabilidad de filtración de información.
Error de mantenimiento	Falta de mantenimientos a los diversos equipos interconectados a la red.	Mantenimientos realizados por externos y personal propio.	Probabilidad de filtración de información.
Escasez del personal	Falta de personal especializado en el monitoreo de la red.	Bajo monitoreo de la red de la institución.	Probabilidad de pérdida o adulteramiento del hardware de la empresa.
Robo por internos	Personal que se sustrae	Falta de personal	Puede ir desde algún fallo en la red hasta

	equipamiento o hardware de la institución.	responsable del seguimiento de los equipos.	la perdida de información.
Robo por externos	Personas ajenas que se sustraen equipamiento o hardware de la institución.	Falta de personal responsable del seguimiento de los equipos.	Puede ir desde algún fallo en la red hasta la perdida de información.
Daño intencional por internos	Personal que no ayuda con el cuidado de la institución.	Falta de personal responsable del seguimiento de los equipos.	Rápido deterioro de la de la institución.
Daño intencional por externos	Personas ajenas que no ayudan con el cuidado de la institución.	Falta de personal responsable del seguimiento de los equipos.	Rápido deterioro de la de la institución.
Terrorismo	Amenaza que no se puede controlar.	No determinado.	Daños en la institución y daño en el entorno.

Nota: En la Tabla 19 podemos identificar los tipos de riesgos que tenemos dentro de la Unidad Educativa Quevedo, en la cual podemos identificar el evento, la descripción del evento, la causa del evento y las consecuencias que podemos tener dentro de la Unidad Educativa. Tomada de elaboración propia.

Anexo 2. Situación Actual y Aplicación del Control de Seguridad de la Información

Tabla 20 *Situación Actual y Aplicación del Control de Seguridad de la Información*

TIPOS Y MEDIDAS DE CONTROL				NIVEL DE ALERTA					CARACTERÍSTICA	
SECCIÓN	DOMINIO - CONTROL	MECANISMO DE CONTROL	CANTIDAD DE MEDIDAS	N_I	N_II	N_III	N_IV	N_V	RESPONSABLE	FECHA DE IMPLANTACIÓN
A5	Políticas de seguridad.	Se debería definir un conjunto de políticas para la seguridad de la información, aprobado por la dirección, publicado y comunicado a los docentes, así como a todas las partes externas relevantes.	2	1	2	3	4	5	DIRECTIVOS DE LA INSTITUCIÓN	Implementada
		Las políticas para la seguridad de la información se deberían planificar y revisar con regularidad o si ocurren cambios significativos para		1	2	3	4	5	DIRECTIVOS DE LA INSTITUCIÓN	Implementada

		garantizar su idoneidad, adecuación y efectividad.								
A6	Aspectos organizativos de la seguridad de la información.	Se deberían definir y asignar claramente todas las responsabilidades para la seguridad de la información.	4	1	2	3	4	5	INSPECTOR GENERAL	Implementada
		Se deberían mantener los contactos apropiados con las autoridades pertinentes.				3	4	5	DEPARTAMENTO DE TIC´S	Abril - 2023
		Se debería establecer una política formal y se deberían adoptar las medidas de seguridad adecuadas para la protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones.				3	4	5	DEPARTAMENTO DE TIC´S	Octubre - 2023

		Se debería desarrollar e implantar una política y medidas de seguridad de apoyo para proteger a la información accedida, procesada o almacenada en ubicaciones destinadas al teletrabajo.			3	4	5	DEPARTAMENTO DE TIC´S	Octubre - 2023
A7	Seguridad ligada a los recursos humanos.	Todos los docentes de la institución y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.	3			4	5	INSPECTOR GENERAL	Octubre - 2023
		Debería existir un proceso formal				4	5	INSPECTOR GENERAL	En fase de prueba

		disciplinario comunicado a empleados que produzcan brechas en la seguridad.					4	5		
		Las responsabilidades para ejecutar la finalización de un empleo o el cambio de éste deberían estar claramente definidas, comunicadas a empleado o contratista y asignadas efectivamente.					4	5	INSPECTOR GENERAL	En fase de prueba
A8	Gestión de activos.	Identificar los activos en la organización y definir las responsabilidades para una protección adecuada.	3	1	2	3	4	5	COMUNIDAD EDUCATIVA	Implementada
		Asegurar que se aplica un nivel de protección adecuado a la información.		1	2	3	4	5	DEPARTAMENTO DE TIC´S	Abril - 2023
		Evitar la divulgación, modificación,		1	2	3	4	5	COMUNIDAD EDUCATIVA	Implementada

		retirada o destrucción de activos no autorizada almacenada en soportes de almacenamiento.							
A9	Control de accesos.	Controlar los accesos a la información y las instalaciones utilizadas para su procesamiento.	4	1	2	3	4	5	COMUNIDAD EDCUATIVA	Abril - 2023
		Garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información y servicios.		1	2	3	4	5	DEPARTAMENTO DE TIC´S	Abril - 2023
		Los usuarios sean responsables de la protección de la información para su identificación.		1	2	3	4	5	COMUNIDAD EDCUATIVA	Abril - 2023
		Impedir el acceso no autorizado a la información mantenida por los sistemas y aplicaciones.		1	2	3	4	5	DEPARTAMENTO DE TIC´S	Abril - 2023

A10	Cifrado.	Se debería desarrollar e implementar una política sobre el uso, la protección y el ciclo de vida de las claves criptográficas a través de todo su ciclo de vida.	1	1	2	3	4	5	DEPARTAMENTO DE TIC´S	Octubre - 2023
A11	Seguridad física y ambiental.	Evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.	2	1	2	3	4	5	COMUNIDAD EDCUATIVA	Abril - 2023
		Evitar la pérdida, los daños, el robo o el compromiso de activos y la interrupción a las operaciones de la institución.		1	2	3	4	5	COMUNIDAD EDCUATIVA	Abril - 2023
A12	Seguridad en la operativa.	Evitar el acceso físico no autorizado, los daños e interferencias a la información de la	5			3	4	5	DEPARTAMENTO DE TIC´S	Abril - 2023

	organización y las instalaciones de procesamiento de la información.					
	Garantizar que la información y las instalaciones de procesamiento de información estén protegidas contra el malware.		3	4	5	DEPARTAMENTO DE TIC´S	Octubre - 2023
	Alcanzar un grado de protección deseado contra la pérdida de datos.		3	4	5	DEPARTAMENTO DE TIC´S	Octubre - 2023
	Evitar la explotación de vulnerabilidades técnicas.		3	4	5	DEPARTAMENTO DE TIC´S	Octubre - 2023
	Se deberían planificar y acordar los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos		3	4	5	DEPARTAMENTO DE TIC´S	Octubre - 2023

		relacionados con la institución.						
A13	Seguridad en las telecomunicaciones.	Evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.	2		3	4	5	DEPARTAMENTO DE TIC´S	Octubre - 2023
		Mantener la seguridad de la información que transfiere una organización internamente o con entidades externas.			3	4	5	DEPARTAMENTO DE TIC´S	Octubre - 2023
A14	Adquisición, desarrollo y mantenimiento de los sistemas de información.	Garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo su ciclo de vida.	2		3	4	5	DEPARTAMENTO DE TIC´S	Octubre - 2023
		Garantizar la seguridad de la información en los entornos de diseño e implementación			3	4	5	DEPARTAMENTO DE TIC´S	Octubre - 2023

		dentro del ciclo de vida de desarrollo de los sistemas de información.								
A16	Gestión de incidentes en la seguridad de la información.	Se deberían evaluar los eventos de seguridad de la información y decidir su clasificación como incidentes.	1	1	2	3	4	5	COMUNIDAD EDCUATIVA	Abril - 2023
TOTAL	**29**									

Nota: Para poder establecer al menos 20 medidas con su nivel de alerta asociado se propuso lo que se refleja en la tabla. Tomada de elaboración propia.

Anexo 3. Certificación de traducción del Resumen

Mg. Yanina Quizhpe Espinoza
Licenciada en Ciencias de Educación mención Inglés
Magister en Traducción y mediación cultural

Celular: 0989805087
Email: yaniqes@icloud.com
Loja, Ecuador 110104

Loja, 13 de mayo de 2023

Yo, Lic. Yanina Quizhpe Espinoza, con cédula de identidad 1104337553, docente del Instituto de Idiomas de la Universidad Nacional de Loja, y certificada como traductora e interprete en la Senescyt y en el Ministerio de trabajo del Ecuador con registro **MDT-3104-CCL-252640**, certifico:

Que tengo el conocimiento y dominio de los idiomas español e inglés y que la traducción del resumen del Trabajo de Titulación **Análisis y propuesta de gestión de riesgo en infraestructura TI en la Unidad Educativa Quevedo,** de autoría del señor Carlos Alberto Bermeo Zamora, con cédula 1105761124, es verdadero y correcto a mi mejor saber y entender.

Atentamente

YANINA BELEN QUIZHPE ESPINOZA
Firmado digitalmente por YANINA BELEN QUIZHPE ESPINOZA
Fecha: 2023.05.13 22:22:54 -05'00'

Yanina Quizhpe Espinoza.
Traductora Freelance

Full text translator: servicios de traducción