UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del proyecto:
Propuesta de seguridad informática para el control de acceso dirigida a la infraestructura para el Colegio Nacional Cutuglagua aplicando la Norma ISO 27001; A9 control de acceso
Línea de Investigación:
Seguridad Informática
Campo amplio de conocimiento:
Tecnologías de la Información y la Comunicación
Autor
Jesús Efraín Tuabanda Cayambe
Tutor
MSc. Pablo Marcelo Recalde Varela

Quito – Ecuador

2023

APROBACIÓN DEL TUTOR

Yo, MSc. Pablo Marcelo Recalde Varela con C.I: 1711685055 en mi calidad de Tutor del proyecto de investigación titulado: **PROPUESTA DE SEGURIDAD INFORMÁTICA PARA EL CONTROL DE ACCESO DIRIGIDA A LA INFRAESTRUCTURA PARA EL COLEGIO NACIONAL CUTUGLAGUA APLICANDO LA NORMA ISO 27001; A9 CONTROL DE ACCESOS**

Elaborado por: **Jesús Efraín Tuabanda Cayambe**, de C.I: **1719302752**, estudiante de la Maestría: en SEGURIDAD INFORMÁTICA de la **UNIVERSIDAD TECNOLÓGICA ISRAEL**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2023

Firmado electrónicamente por:
PABLO MARCEL
RECALDE VARELA

_____

Firma

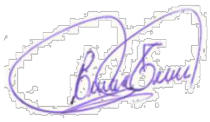
ORCID: 0000-0002-1127-5697

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Jesús Efraín Tuabanda Cayambe con C.I: 1719302752, autor del proyecto de titulación denominado: PROPUESTA DE SEGURIDAD INFORMÁTICA PARA EL CONTROL DE ACCESO DIRIGIDA A LA INFRAESTRUCTURA PARA EL COLEGIO NACIONAL CUTUGLAGUA APLICANDO LA NORMA ISO 27001; A9 CONTROL DE ACCESOS. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., marzo del 2023



Firma

Orcid: 0000-0002-1127-5697

Tabla de contenidos

Índice de figuras

Índice de tablas

INFORMACIÓN GENERAL

Contextualización del tema

Según Cordobés (2018). «En estas fechas se está incorporando la informática en diferentes niveles de educación se ha realizado de manera compulsiva. En la mayor parte de centros educativos, se cree que la informática es una tecnología que ayuda al crecimiento personal y profesional y mediante una computadora podremos adaptarnos a la nueva realidad tecnológica. Por lo tanto, creemos que el gobierno debe tomar acciones que respalde los estudiantes calidad en la educación».

La pandemia azotó al mundo y ha dado paso a una nueva era. En este campo, la seguridad informática inicia una era marcada por el crecimiento explosivo de los ataques contra individuos, pequeñas empresas, grandes corporaciones multinacionales, agencias administrativas gubernamentales e infraestructura crítica. En otras palabras, nadie está excluido del peligro.

Según Elizalde (2021) «En este sentido, cabe señalar que las instituciones financieras, los establecimientos médicos o la infraestructura pública son las principales víctimas de la atención criminal. Lo mismo ocurre con las instituciones educativas. La verdad es que la oportunidad que presenta la pandemia es generosa: sin sistemas basados en la nube, las herramientas de videoconferencia y las actividades de aprendizaje a distancia son invaluables. Inicialmente, no había un acceso de consola bien establecido a la arquitectura de seguridad, y con innumerables usuarios con acceso instantáneo y sin capacitación previa en seguridad, las vulnerabilidades se amplificaron. Atacar es casi obligatorio - inmoral».

A raíz de la pandemia los establecimientos educativos han sufrido ataques informáticos, por un alto porcentaje de personal administrativo, docentes y estudiantes que fueron obligados a cambiar la modalidad de estudio esto permitió abrir una brecha de seguridad, porque no se conoce el acceso a los datos en las redes de las instituciones, esto debido a que muchos profesores y personal administrativo realizan el trabajo remotamente desde su casa u otros lugares lo que ocasionó una ola de ataques, que son aprovechados los delincuentes informáticos aprovechan las vulnerabilidades de equipos personales o de las empresas (sin antivirus, falta de actualizaciones, claves de acceso sencillas, etc.) que no eran supervisados por personal especializado, acompañado de políticas inexistentes, preocupados por resolver inconvenientes generados por los virus y su rápida propagación. (Bartolomé y Monteiro, 2021).

.

Problema de investigación

Entre las medidas de seguridad que dispone cada institución educativa, existen firewalls completamente desactualizados, repitiendo constantemente ciberataques por información completamente confidencial, afectando directamente al personal, profesores y estudiantes de las instituciones educativas.

Según Andrade (2018) «en el país aún existen muchos problemas relacionados a pérdida de información en los establecimientos educativos fiscales dentro del territorio nacional, se basa en que la infraestructura de estas instituciones es diferente en comparación con instituciones privadas que manejan sistemas e infraestructura más modernas y con personal adecuado para el mismo».

¿Cómo se puede disminuir el índice de delitos informáticos en las instituciones educativas?

Objetivo general

- Proponer mecanismos de seguridad informática a aplicarse en los establecimientos educativos.

Objetivos específicos

- Investigar características de índole tecnológico mediante encuestas en el Colegio Nacional Cutuglagua.
- Comparar estándares de seguridad informática mediante un análisis documental para aplicar el estándar más adecuado para la institución educativa..
- Identificar brechas de seguridad informática mediante entrevistas para evitar los riesgos en la institución educativa.
- Proponer los controles que deben aplicarse a la seguridad informática en el establecimiento educativo, caso estudio Colegio Nacional Cutuglagua.

Vinculación con la sociedad y beneficiarios directos

El actual caso de estudio tiene como propósito mejorar los mecanismos de seguridad informática para los colegios del sur de Quito, especialmente como caso de estudio el Colegio Nacional Cutuglagua.

En la actualidad todas las instituciones educativas afrontan problemas de mucho riesgo e inseguridades en la información que conllevan a la pérdida de su confidencialidad e integridad, en los establecimientos educativos públicos y privadas por lo que se determina que deben implementar modelos de seguridad informáticas, que manejen la información de las instituciones educativas que están expuestos a amenazas cibernéticas y riesgos a su infraestructura como a su base de datos, software y hardware con información importante y privada que afecte a la institución. Tarazona (2018)

Según la Escuela Europea de Excelencia (2019) «La seguridad de un activo debe ser cuidado antes que se materialice las amenazas, estos deben ser cuidados que no se realicen robos de información, se puede hacer la diferencia antes de que se produzca tal evento de lo contrario podemos gastar más recursos tecnológicos, económicos al no prevenir tal situación.».

La tecnología es un principal eje en cada una de las empresas y en especial en las instituciones educativas frente a ataques, amenazas y toda clase de delitos informáticos.

Carlos Acuña (2017) define «que los activos más importantes de cada una de las organizaciones, especialmente la información se debe al mal funcionamiento de sus equipos informáticos por lo que son amenazados constantemente con virus y malware que permiten el acceso a dispositivos inteligentes que disponemos en la actualidad que están conectados a Internet, que son una fuente importante de amenazas a la seguridad».

«Hay una relativa preocupación al momento de estudiar en poblaciones que no tienen una adecuada capacitación tecnológica, las mismas que aumentan el desconocimiento tecnológico en zonas rurales que no permite el crecimiento cultural tecnológico» (Ziegler, 2021)**.**

Tomando en cuenta los Objetivos de Desarrollo Sostenible (ODS), la investigación se centrará en el ODS número 4 «garantizar una educación inclusiva, equitativa y de calidad y promover oportunidades de aprendizaje durante toda la vida para todos» ETICENTRE (2019).

Este contribuye a la mejorara de la educación con calidad que es básica para enriquecer con conocimientos modernos y contribuir al desarrollo de las personas.

Aún queda camino por recorrer para que el mundo logre aprovechar plenamente este potencial. Para poder aplicar la investigación a la práctica y sugerir controles que se puedan aplicar a las instituciones educativas a nivel de Ecuador en especialmente en las instituciones del sector sur de la provincia de Pichincha, en el cual identificamos brechas de seguridad que están siendo afectadas, y con este aporte se está ayudando a reducir los ataques informáticos debido al desconocimiento de seguridad aplicables a instituciones educativas.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

El presente capítulo evidencia las características de la seguridad en el colegio Nacional Cutuglagua.

1.1. Contextualización general del estado del arte

Con el apogeo de nuevas técnicas la información se comparte de manera inminente a la sociedad, con el uso de la Internet (Abad, 2020); también se ha presentado un aumento de ataques a organizaciones, las nuevas técnicas usadas por los piratas informáticos han mejorado notablemente, esto conlleva a que el personal de seguridad informática fortalezca sus esfuerzos en mejorar las barreras de protección.

En el ámbito privado y público es importante la protección de la información estos son los activos más importantes, para el acceso a los datos generalmente se usan sistemas de información, al momento de ingresar a estos se debe comprobar la identidad del usuario, validar los perfiles y permitir el ingreso según sea el caso. Švar (2021).

En el transcurso de esta fase se han desarrollado en el tema de protección de infraestructura, sea estos de red de datos, base de datos, servidores, mientras estos últimos son apetecido por piratas informáticos, Si sus datos confidenciales caen en manos de personas inescrupulosas, es posible que exijan un rescate, vendan la información o se enfrenten a varios problemas de confidencialidad de la información. Los ataques cibernéticos pueden desafiar las formas tradicionales en que las organizaciones se defienden y crear inestabilidad. Cano (2020).

Existen modelos de gestión educativa bajo normas técnicas y protocolos de seguridad. Como lo expresa la norma ISO 27001, la cual corresponde a métodos de gestión de riesgos y seguridad enfocados en el uso de las buenas prácticas, siendo una norma internacional se considera importante en la prevención de ataques, además de brindar aseguramiento, totalidad y eficacia de los datos y la información, además de los sistemas tabulan. ISOtools (2019).

Afirma (Soto, 2019). «Existen otras normas que garantizan el cuidado de la información y sistemas de gestión. Como la norma COBIT 5 la cual es utilizada por las instituciones para procesos de negocio, además de mantener la tecnología y la información en estándares de confianza, calidad, y control Teniendo habilitadores prácticos en la gestión como bases, políticas, modelos de referencia, procesos, estructuras organizacionales, cultura, ética, comportamiento, información, servicios, infraestructura, aplicaciones, gente, habilidades, y competencia».

«Además se puede obtener certificaciones de calidad mediante el uso de habilidades en la gestión de las tecnologías. Como las establecidas en ITIL, para mejores prácticas en las tecnologías de la información En las cuales se establece las fases de pericia, diseño, transición, operación, y mejora continua de los servicios, siendo su objetivo principal aumentar la calidad de los servicios tecnológicos» (GlobalSuite Solutions, 2020)

Dentro de la revisión efectuada a las investigaciones realizadas en materia educativa relacionada a la seguridad informática se destaca. La denominada «Propuesta de políticas de seguridad de la información para la institución educativa de educación básica y media del departamento de Boyacá, basadas en la norma ISO 27001:2013» efectuada por los autores Figueroa y Pérez (2017). En la cual se diseñaron políticas de seguridad de información para la institución educativa, para disminuir el peligro que pueden llegar a tener los activos de las Instituciones educativas.

La investigación realizada por el autor Garín (2015), con relación a «La seguridad completa debe gestionarse en los establecimientos educativos, se debe conocer la organización y gestión todo lo relacionado con la seguridad en los centros educativos, para analizar las prácticas concretas de profesores y resto del personal, y también conocer la opinión del personal del establecimiento educativo».

Por otra parte, la investigación denominada «Seguridad Informática para alumnos de la Escuela Secundaria con Software Educativo, un aporte a la educación», realizada por el autor Rodríguez (2009), se determina que existen falencias de la utilización de los sistemas educativos, especialmente en tema de desconocimiento de seguridades informáticas, por ende, los ataques son originados por fallas humanas, de la misma forma la implementación de un software conlleva a la capacitación de la comunidad educativa.

Según el portal ISOtools (2019) «debe contener un sistema de dirección sobre seguridad informática, en donde contemplan parámetros como el período de vida de los datos, además de un software especializado para este proceso». Por otra parte, hay normas que se deben cumplir desde las personas que manejan la información hasta las que administran los sistemas.

En Ecuador la educación está ligada a los parámetros del gobierno de turno y su ente regulador que se radica en el Ministerio de Educación, dentro de los modelos educativos realizados por el sector público, también forman parte como ejemplo para la aplicación del sector particular. Una de las características importantes dentro de los modelos de gestión es la conllevar las tecnologías hacia mejores prácticas y comunicaciones, desde el año 2015 se inició la implementación del proyecto SITEC a través de la plataforma EducarEcuador por parte del (MINEDUC, 2015). Con la finalidad de facilitar los registros académicos, el

incremento de las competencias profesionales en los docentes y el uso de la tecnología para los estudiantes.

Investigaciones previas realizadas

En la ciudad de Quito se encuentra gran cantidad de establecimientos educativos privados y fiscales. Para la siguiente investigación se toma como objeto de estudio el Colegio nacional Cutuglagua perteneciente al cantón Mejía de la provincia de Pichincha que es un establecimiento del sistema fiscal.

La investigación encontró diferentes casos en instituciones educativas de todo el mundo, Y dado que los hogares en su totalidad tienen dispositivos móviles, televisores se debe trabajar mediante el acceso más confiable que son la televisión que llega a toda la población se a de la zona rural o urbana, debido a que la mayor parte no dispone de un computador en su casa para poder realizar tareas de la mejor manera.

Se ha realizado un estudio para este trabajo en diferentes unidades educativas fiscales y privadas del sector sur de la provincia de Pichincha en el cual se concluye que en el ámbito educativo particular no se tiene los mismos problemas que en los establecimientos fiscales.

Esto se debe a que en las instituciones privadas existe un adecuado control de acceso a la red, equipos informáticos tanto como a los profesores, personal administrativo y los estudiantes en los laboratorios.

1.2. Proceso investigativo metodológico

A continuación, una explicación del proceso de investigación a partir de los siguientes elementos:

Investigación Bibliográfica

Arteaga (2020). Define como «Todo trabajo de investigación que necesite recoger información puede utilizar materiales ya publicados, estos pueden ser de índole tradicionales como revistas, periódicos, libros e informes, también puede utilizar grabaciones de audio, video y recursos tecnológicos como blogs datos bibliográficos, sitios web.».

En este trabajo se aplica la búsqueda de información, con lo cual se logró recopilar toda la información necesaria para sustentar los temas que se están desarrollando en el planteamiento del problema, los datos que se han tomado en cuenta fueron obtenidos de fuentes cuyo origen ha sido verificado, además se cita repositorios universitarios que han contribuido con información principal para la obtención de mejores resultados.

La investigación descriptiva

En el presente trabajo se utilizará la investigación descriptiva, la cual es definida por Pazmiño (2019), pág. 27, «como aquella que se dedica al estudio de acontecimientos en tiempo presente, aquellos que están en auge en la actualidad», con el cual se podrá detallar la situación actual de los centros educativos.

Dentro de la investigación planteada se determina la problemática central, la cual se especifica dentro de las instituciones educativas haciendo énfasis en el objeto de estudio que el colegio Nacional Cutuglagua, donde la pérdida de información y ciberataques han resultado en retrasos en crecimiento de las actividades académicas, así como en el resguardo de la información que en su totalidad se ha visto vulnerada por errores humanos de los docentes y personal administrativo que maneja los sistemas informáticos educativos gubernamentales, en tal sentido se plantea la siguiente interrogante; ¿Cómo se está gestionando la seguridad informática en los sistemas de gestión académica y educativa de las instituciones educativas del cantón Mejía, frente a la prevención de ciberataques y pérdida de información?

El principal objetivo de la investigación es poder conocer cómo se está gestionando la seguridad informática en los sistemas de gestión académica y educativa de las instituciones educativas.

Según Hernández (2019), «cada diseño metodológico de la investigación realizada va a permitir seleccionar las herramientas fundamentales para evolucionar la investigación el cual debe definirse la unidad de estudio, muestra, técnicas, población, métodos y procedimientos que se utilizan, adicional si se utilizara alguna alternativa de valoración de estadísticas de los resultados que se obtengan. Por ello la siguiente investigación se define varios puntos»:

Se utiliza una investigación aplicada, en el cual se recolecta la información cuantitativa y cualitativa, pero la investigación es metodología de tipo no experimental.

También se utiliza la investigación descriptiva para determinar la situación actual de la Unidad Educativa, en donde se identifica: activos, riesgos e incidentes.

Seguridad de la Información

La principal acción que tienen las instituciones planteadas por sus objetivos es resguardar la seguridad d ellos datos sin que estos sean vulnerados y usados para sacar provecho para los piratas informáticos. Acurio, (2019, p. 25).

En la actualidad para mantener la confidencialidad, la disponibilidad y la integridad las empresas que usan el internet y cada uno de los avances tecnológicos que existen en la era moderna han provocado las amenazas haciéndoles más vulnerables para las

instituciones que están modernizándose Areitio (2018).

La integridad hace refiere a la información de las instituciones que no se pueden manipular sin el permiso expreso del encargado.

La confidencialidad permite el acceso a las personas que están debidamente autorizadas.

La disponibilidad se basa en la garantía de tener acceso a la información en cualquier momento.

Importancia de la seguridad de los datos

El principal objetivo es asegurar y prevenir todo tipo de incidentes en la proteccion de datos guardados por las instituciones, toda la información que se posee es utilizada para el estudio de datos que implementan en las campañas de marketing con la información guardada. Berumen y Arriaza (2008).

Protección de datos.

Permite el aseguramiento de los datos de una empresa que pueden ser datos de clientes y a la misma vez resguardar la infraestructura, servidores y el cableado que son activos de las empresas. Suárez y Ávila (2015).

Usuarios que tendrán acceso a datos privados mediante procesos o dispositivos autorizados. La información al tener un gran valor se debe asegurar que sea integro que no se deba perder o que deseen cambiar con intenciones de desinformar.

Accesible mediante accesos confiables e inmediatos de la información que tiene.

Identificamos información de manera objetiva mediante la autenticidad.

Gestión de Seguridad de Información

La norma ISO 27001 dispone las mejores prácticas quien dispone de un sistema de gestión de la información. Mediante esta norma se permite resguardar la información de la institución y a la misma vez se crea una cultura de confiabilidad con los clientes, empleados y los proveedores. Detallamos varios pasos de la Gestión de la información.

Los individuos manejan y procesan la información.

La mayor parte presentan vulnerabilidades quienes han sido desempeñadas por personal responsable de la empresa.

La infraestructura y servicios es complementada con las nuevas tecnologías quienes ayudan almacenar, difundir, recuperar y retener información y así mejorar cada una de las actividades.

Aseguramiento de la información bajo las normas vigentes.

Después de identificar las características clave de los distintos tipos de almacenamiento de datos, se identificaron los líderes del mercado y se continuaron identificando las características clave de cada uno, observando las similitudes y diferencias que permiten cada aplicación. verlos como una solución única o crear un modelo especial combinando elementos de cada estudio realizado.

Se estudiaron las particularidades sobresalientes de cada muestra para poder compararlas rápidamente e identificar sus principales características. Si bien las necesidades de las organizaciones no son las mismas, se determinan de acuerdo con los recursos de que disponen.

Una vulnerabilidad es un decaimiento en la seguridad informática donde se pueden introducir otra variante de ataques que comprometen la privacidad, integridad y autenticidad de los datos. Steven (2019).

Dependiendo de alguna situación que se encuentre en la organización o empresa, se puede combinar los sistemas o valores que hay en la actualidad. Cabe destacar que para todos los obstáculos que se presentan, existen varias formas efectivas de solucionar estos problemas. Existen diferentes patrones y niveles de seguridad de la información, detallamos a continuación. Triana (2018).

Gestión de proyectos con PMBOK

Es un patrón integral de gestión de proyectos, basado en un conglomerado de mejores prácticas que se dividen en 9 áreas profesionales divididas en tareas (44 en total), a partir de la gestión de contenidos hasta la gestión de proyectos y materiales. Los componentes del marco PMBOK son aplicables a las necesidades de la institución.

ITIL

E un patrón de TI de mejores prácticas que se enfoca en ofrecer asistencia de calidad para alcanzar el agrado del cliente a un bajo costo. Se parte de una estrategia basada en un proceso-personas-tecnología. Figueroa (2019).

EL MODELO CMMI

Se evalúa el nivel de avance de las organizaciones en el uso de las buenas prácticas en crecimiento y gestión de software. El molde tiene varios niveles principales de madurez; inicial, repetible, definido, administrativo, optimizado. Por lo visto hasta ahora las instituciones suelen llegar al nivel 3. García (2006).

COBIT

Es un patrón utilizado para controlar y administrar las TI. Consta de cuatro áreas organizadas por métodos, las cuales se dividen en funciones de gestión y objetivos.

Entre todos los tipos de seguridad informática o estándares, se seleccionan los siguientes: OSSTMM3, NIST SP 800-30, COBIT 5 e ISO 27001, debido a su existencia y reconocimiento en el mundo de la tecnología, son considerados estándares comunes a seguir en las distintas partes que componen el sistema de seguridad de la información. Murillo (2019)

OSSTMM3

Es un estándar muy completo que es muy utilizado en la evaluación de sistemas de seguridad de la web. Tiene una estructura que describe los pasos a seguir para completar la evaluación.

Existe algunas versiones que incorpora la realización de normativas y desarrollo de buenas prácticas establecidas por el NIST, ISO 27001 - 27002 e ITIL, Este modelo es uno de los más extensos en cuanto al manejo de ensayos a la seguridad y trance de la comunicación en las organizaciones. Guijarro (2018).

Seguridad en:

- Información
- Procesos
- Tecnologías de internet
- Comunicaciones
- Inalámbrica
- Física.

Su finalidad es proporcionar un método científico para estudiar la organización y realizar pruebas de seguridad desde el interior. Guijarro (2018)

OSSTMM para llegar a la auditoria es guiada mediante la intrusión se dispone de varios ejemplos: Blindaje o Hacking ético; Doble blindaje, auditoría de caja negra o pruebas de penetración, de caja gris, de doble caja gris, test tándem o secuencial y prueba inversa. Vásquez (2014).

NIST SP 800-30

Corresponde a un sistema de gestión de riesgos desarrollado en modo de directrices desarrolladas por el Departamento de Comercio de EE. UU. y el Instituto Nacional de

Estándares y Tecnología (NIST) de EE. UU. que proporciona a las empresas orientación sobre seguridad cibernética de manera analítica peligrosa. Nist (2018).

Para brindar liderazgo técnico en estándares nacionales e internacionales las NIST SP 800-30 fomenta métodos de prueba, datos de referencia, prueba de concepto y análisis técnico para promover el crecimiento y la utilización apropiada de la tecnología en cada uno de los sistemas utilizados.

Las NIST SP 800-30 propone varias metodologías, que incorpora los siguientes subprocesos, Torres (2012):

- Características de los sistemas
- Identificar amenazas y vulnerabilidades
- Determinación de probabilidades
- Análisis de impacto
- Determinar los riesgos
- Recomendar controles
- Documentar los resultados

ISO 27001

El estándar de la Organización Internacional de Normalización (ISO) explica cómo se gestiona los activos de una institución. Se basa en el ciclo de mejora continua de Deming (planificar, hacer, verificar, hacer), por lo que la gestión del conocimiento basada en una escala poderosa en constante repetición. Calder (2018).

Tabla 1.

Familia Serie ISO/IEC

Normativa	Contenido
ISO/IEC 27000	Contiene conceptos generales mediante una perspectiva global.
ISO/IEC 27001	Contiene una norma certificable para implementar un SGSI
ISO/IEC 27002	Contiene los objetivos de control de seguridad para mejoras las buenas prácticas.
ISO/IEC 27003	Define la implementación de un SGSI de acuerdo ISO/IEC 27001.
ISO/IEC 27004	Contiene una guía métrica para medir un SGSI.
ISO/IEC 27005	Contiene una guía de la gestión del riesgo en un SGSI.
ISO/IEC 27006	Contiene requisitos y provee guía para auditoría y certificación del sistema.
ISO/IEC 27007	Aporta un marco de seguridad para el crecimiento, implantación y paramantener especificaciones de los Sistemas de Gestión de la SI.
ISO/IEC 27008	Dispone de plataforma estratégica de implementación y operación decontroles según la organización.
ISO/IEC 27009	Contiene indicios de requisitos dependiendo del tipo de organización donde se implementará.
ISO/IEC 27010	Escoge la forma del traslado e intercambio de información con referencia al funcionamiento interno de la organización.

***Nota**: Esta tabla describe la familia ISO/IEC para gestión de seguridad de la información.*

Según ISO 27001 el resultado del proceso para otorgar a los usuarios que tienen autorización para acceder a la información, mientras que se determina que no tendrán acceso usuarios que no tengan permitido ingresar.

«Se especifica el rol de cada usuario que deben tener únicamente acceso a los servicios de red que han sido permitidos. Se puede controlar el acceso por procesos restringidos para controlar un inicio eficaz de acuerdo a las políticas de accesos». ISO 27001 (2020).

A.9.1.1 Política de control de acceso

Establecemos la documentación y revisión periódicamente con unos procesos de control de acceso, contemplando los requerimientos de la organización.

Se refleja las restricciones y derechos sobre los controles de acceso y que controles son utilizados para el uso adecuado.

Para conceder el control de acceso se toma en cuenta quien debe utilizar, para que lo va a ocupar y que porcentaje requiere.

A.9.1.2 Acceso a redes y servicios de red

Suministrar acceso simple permitirá proteger de una manera más eficaz ante dar accesos ilimitados, tal usuario podrá tener acceso a la red y servicios que realmente necesite.

Se aplicará las siguientes políticas.

Los servicios de red

Autorización de quien tienen acceso para que y que fecha.

Evitar accesos sin controles o con su respectivo procedimiento otorgado por el administrador.

A.9.2.1 Registro de usuarios y anulación de registro

Debemos ingresar procesos formales mediante el registro de usuarios, mediante la administración de ID a usuarios con super usuarios y asociar a personas limitadas en ID de accesos mediante la compartición de este.

Mediante el control de identificaciones antiguas se reforzará la supervisión constante.

A.9.2.2 Aprovisionamiento de acceso de usuario

Documentar todos los procesos que requieran asignar o quitar derechos de accesos específicos.

El encargado del sistema de información autorizara el uso de este.

Verifica el acceso cedido que se utilice realmente para el que fue asignado.

A.9.2.3 Gestión de derechos de acceso privilegiado

Administra niveles de accesos con privilegios el cual debe ser controlado estrictamente para evitar robo de información y acceso a los sistemas.

A.9.2.4 Gestión de información secreta de autenticación de usuarios

Contraseñas y claves con cifrado son activos valiosos que se deben controlar mediante procesos formales y secreto para cada usuario otorgado.

A.9.2.5 Revisión de los derechos de acceso del usuario

Accesos a sistemas deben ser revisados y regulados periódicamente debido al cambio de puestos de trabajo o incorporaciones de personal nuevo, por lo que se determina un mayor riesgo.

A.9.2.6 Eliminación o ajuste de los derechos de acceso

Al finalizar un vínculo laboral debe ser determinante para proceder al cambio de claves para el acceso a las instalaciones o información así garantizara el resguardo de la información.

A.9.3.1 Uso de información secreta de autenticación

Se debe asegurar que los usuarios sigan las políticas establecidas sobre confidencialidad de información privilegiada de autenticación.

A.9.4.1 Restricción de acceso a la información

El encargado del sistema tendrá la obligación de delimitar el acceso a los sistemas y aplicaciones que tengan niveles de riesgo altos tales como:

Control de acceso

Nivel de acceso

Diseño de sistemas

Ejecutar y eliminar permisos

Controlar accesos lógicos y físicos de aplicaciones y datos sensibles

A.9.4.2 Procedimientos de inicio seguro

Un inicio seguro permitirá controlar el acceso a los sistemas y aplicaciones en el cual el usuario deberá identificarse, tanto con contraseñas, accesos mediante tarjetas o por accesos biométricos, dependiendo del riesgo que tenga el departamento.

A.9.4.3 Sistema de gestión de contraseñas

Para garantizar que cumplan con niveles fuertes y de manera consistente se debe utilizar un administrador de contraseñas, que proporcionan centralizar los accesos.

A.9.4.4 Uso de programas de utilidad privilegiada

Existen softwares que ayudan administrar contraseñas los mismos que pueden ser atacados por piratas informáticos por lo que se debe restringir a pocos usuarios.

A.9.4.5 Control de acceso al código fuente del programa

Programas que sean de fácil acceso a su código fuente deben estar restringido el acceso para evitar ataques.

Activos de la información

Según ISOtools (2017), Los activos de información pueden entenderse como un conjunto de: personas, tecnologías y procesos, los que conforman un ciclo de vida dentro de la empresa. Pero en el caso del procesamiento de información se almacenan los equipos o servidores

Valoración de Activos

Se valora activos de información, se define una escala a usar criterios para cada valor, loscriterios están limitados en la tabla 1..3, con referencia a la norma ISO/IEC 27005

Tabla 2.

Escala de valoración de activos

Valor	Impacto	Detalle	Total
1	Muy Bajo	No se encuentra perdidas de información.	1-3
2	Bajo	Se encuentra niveles bajos, aun así, no produce perdidas de información.	4-6
3	Medio	Empieza afectar el funcionamiento y produce pérdidas o afectar el prestigio de la institución.	7-9
4	Alto	Afecta el funcionamiento, se produce pérdida de información en la institución y se ve afectado la reputación.	10-12
5	Muy Alto	Afecta el funcionamiento, hay grandespérdidas económicas, la reputación se ve afectada enormemente y existe una incapacidad para cumplimientos legales.	13-15

Nota: Autoría Propia, 2022.

Vulnerabilidades

Estas fallas pueden ser explotadas por un agente causal una condición favorable a un evento negativo, es decir, la vulnerabilidad es la fragilidad de la información o uno de estos, que puede ser extraída por una o más amenazas que inciden en el incumplimiento de uno o más principios de seguridad. Las vulnerabilidades están presentes en los propios activos, es decir, son inherentes a los mismos y pueden ser de carácter tecnológico, procesual y ambiental (Joya & Sacristán, 2017).

Amenazas

Existen amenazas a nivel de épocas que no se puede cambiar mientras avanza la tecnología, seguirán apareciendo nuevas formas de exponer la información. Por lo tanto, quienes no saben lo fundamental que es la información dejan los activos sin atención. Fache (2016).

Probabilidades

Según Konzen (2013), «es probable que ocurra un evento, una escala de 0 a 1que puede vincularse a la frecuencia de ocurrencia o la confianza de que ocurrirá un evento»

Para reconocer las amenazas y vulnerabilidades que generan riesgos en los activos se cuenta con ciertos criterios: la disponibilidad, seguridad e integridad de los activos en función de la probabilidad y el impacto. Para evaluar las amenazas y vulnerabilidades de seguridad, se ha establecido una escala según ISO/IEC 27005, que se encuentra en la tabla 3.

Tabla 3. Escala de valoración de probabilidad

Escala de valoración de probabilidad

Valoración	Probabilidad	Detalle
1	Casi probable	Se produce mínimamente
2	Improbable	Se produce eventualmente
3	Moderado	Se presenta de forma moderada
4	Probable	Se producide habitualmente
5	Muy probable	Se produce muy recurrentemente

Nota: Elaborado por Efrain Tuabanda (2022).

Incidentes de seguridad

García (2020) define como un incidente como un evento variado e inesperado que afectara a las operaciones y procesos que se están realizando sean comerciales o de seguridad, a la misma vez se contempla como una amenaza los procesos comerciales y la seguridad de la información.

Cuatro incidencias que son las más frecuentes:

- Suplantación de identidad o enmascaramiento
- Repetición
- Editar mensaje

- Denegación de servicio

Tratamiento del riesgo

El tratamiento del riesgo permite tomar decisiones frente a riesgos analizados, a continuación, se describen los criterios de tratamiento de riesgos:

Aceptar riesgo: No se realiza ninguna acción, debido a los costos de soluciónque pueden ser más altos que origen del riesgo.

Reducir riesgo: se minimiza y reduce la probabilidad de provocarse un riesgo.

Evitar el riesgo: Se puede eliminar actividades que puedan producir riesgos.

Transferir riesgo: se envía a empresas encargadas que tienen experiencia en el tratamiento del mismo..

Para el tratamiento de riesgos hay que definir criterios de valoración en base a una escala, que sepresentan en la Tabla 4.

Tabla 4.

Escala de tratamiento de riesgo

Valoración	Riesgo	Detalle
1 – 3	Mínimo	Asumir
4 – 5	Bajo	Reducir
6 – 8	Medio	Evitar
9-10	Alto	Transferir

Nota: Elaborado por Efraín Tuabanda (2023)

Dentro del trabajo se utiliza una investigación aplicada en el cual se recolecta información cuantitativa y cualitativa enfocándose como una investigación metodológica no experimental.

Población

Se efectuó una encuesta a todos los docentes y estudiantes del Colegio Nacional Cutuglagua del Segundo año de Bachillerato, de donde se inyectará la información recolectada para su proceso de investigación.

Muestra

En la muestra se obtiene la cantidad de los componentes de la investigación que conforman la comunidad educativa son un total de 50 en los que están comprendidos cinco docentes y cincuenta estudiantes de primero y segundo de bachillerato de la carrera de

Informática, en base a la encuesta se podrá identificar las situaciones de inseguridad que tiene la institución al no contar con un esquema de seguridad de información.

Para el calcular la muestra se procede a utilizar la fórmula que se muestra en la figura 1, sin embargo, elsitio web SurveyMonkey proporciona la herramienta para determinar el número de encuestas. La población es de 55 de lo cual se procede a utilizar el 95% de nivel de confianza y un margen de error del 5%, obteniendo el resultado del tamaño de la muestra de 42 como se muestra en la Figura 1,

Figura 1.

Fórmula de la muestra

$$n = \frac{Z^2 . p . q . N}{NE^2 + Z^2 \ p . q .}$$

Z=Nivel de confianza
N=Población-Censo
p= Probabilidad a favor
q= Probabilidad en contra
e= error de estimación
n= Tamaño de la muestra

Nota: (UNIDAD DE EMPRENDIMIENTO VIRTUAL, 2015) Fuente: http://hachepe57.blogspot.com/2010/05/l-calculo-del-tamano-de-la-muestra.html. Fórmula para calcular la muestra de una población finita.

Figura 2.

Cálculo de tamaño de la muestra.

Nota: El resultado de SurveyMonkey se aplica 55 encuestas.

Técnicas e instrumentos

Se recolecta la información con base en las revisiones de información y documentación de la encuesta aplicable a la institución educativa, donde se recolecta toda la información pertinente que servirá como base para identificar aspectos de seguridad de información al no contar con algún sistema de gestión.

Entrevista

"Es una charla sencilla planificado entre el entrevistador y el entrevistado dende se obtiene información, y su uso es un medio para adquirir conocimiento cualitativo" Hernández (2012) Pág. 78. En el cual se realizará entrevistas a los profesores de la institución educativa.

Encuesta

Se realiza la recopilación de información mediante encuetas presenciales, y posteriormente se tabula los datos obtenidos, el formato de la encuesta se observa en el Anexo 1 hasta el 4, dicha encuesta determina la seguridad de la información que se usa en el uso de dispositivos y la conexión a internet de los estudiantes y profesores del Colegio Nacional Cutuglagua.

1.3. Análisis de resultados

Mediante el procesamiento de los datos recopilados, de la investigación realizada al establecimiento educativo de la provincia de Pichincha, en referencia con la seguridad de la información en sistemas de gestión académica y educativa, se pudo observar la participación general de los participantes, además del interés por el tema de investigación, lo cual se desarrolla a continuación:

Una vez realizada la entrevista a los profesores, para conocer las principales problemáticas que mantiene la institución educativa, en la que se determinó;

Tabla 5.

Tabulación de resultados obtenidos de la pregunta 1.

1. ¿Indique usted su vinculación en el área de TICS de la institución educativa?		
Titular con nombramiento	1	20%
Titular con contrato	1	20%
Encargado	3	60%
Total	**5**	**100%**

Nota: *Fuente propia*

Figura 3.

Tabulación de resultados obtenidos de la pregunta 1.

En la Figura 3 se observa que el 60% de los encuestados solo son encargados del departamento de sistemas, mientras el 20 % es titular con nombramiento y el otro 20% titula con contrato.

Tabla 6.

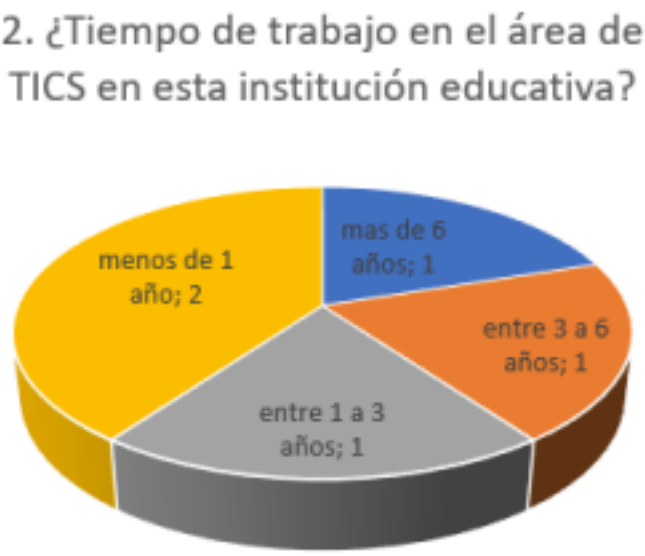
Tabulación de resultados obtenidos de la pregunta 2.

2. ¿Tiempo de trabajo en el área de TICS en esta institución educativa?		
más de 6 años	1	20%
entre 3 a 6 años	1	20%
entre 1 a 3 años	1	20%
Menos de 1 año	2	40%
Total	**5**	**100%**

Nota: *Fuente propia*

Figura 4.

Tabulación de resultados obtenidos de la pregunta 2.



En la Figura 4 se observa que el 40% de los encuestados tiene trabajando en el área de TIC menos de 1 el otro 20% trabaja entre 1 a 3 años, el otro 20% entre 3 a 6 años y el ultimo 20% trabaja más de 6 años.

Tabla 7.

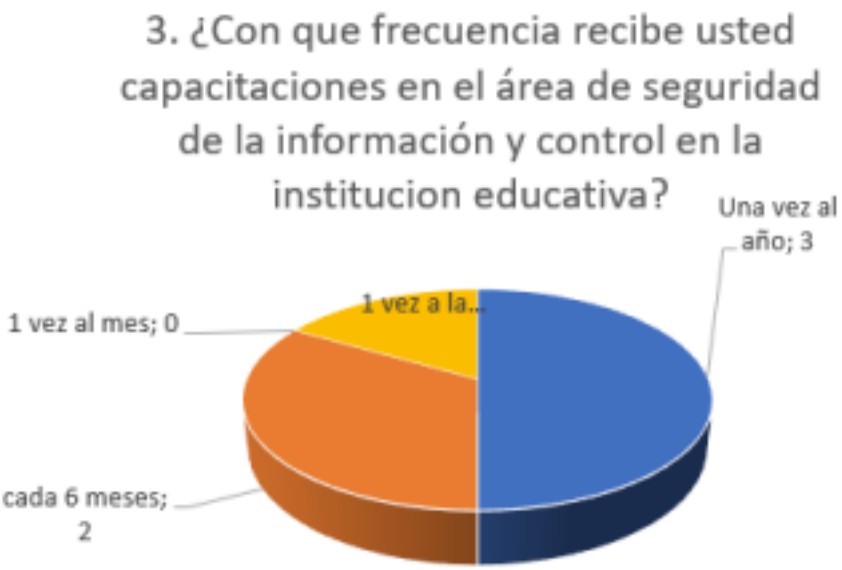
Tabulación de resultados obtenidos de la pregunta 3.

3. ¿Con que frecuencia recibe usted capacitaciones en el área de seguridad de la información y control en la institución educativa?		
Una vez al año	3	60%
cada 6 meses	1	20%
1 vez al mes	1	20%
Total	**5**	**100%**

Nota: *Fuente propia*

Figura 5.

Tabulación de resultados obtenidos de la pregunta 3.



En la Figura 5 se observa que el 60% de los encuestados recibe capacitaciones una vez al año y el otro 20 % tiene capacitaciones cada 6 meses y el ultimo 20 % se capacita cada mes.

Tabla 8. ***4***

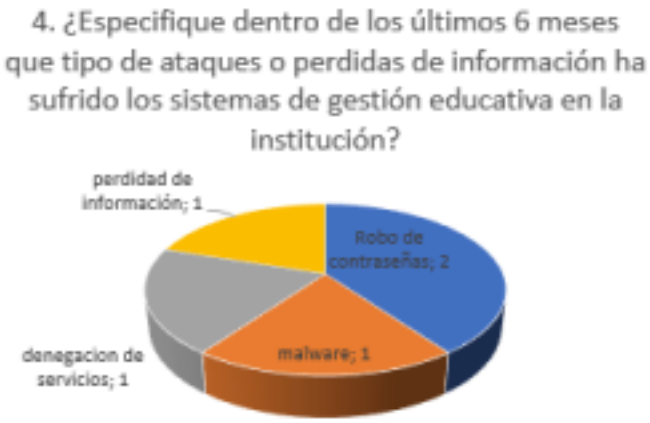
Tabulación de resultados obtenidos de la pregunta 4.

4.- ¿Especifique dentro de los últimos 6 meses que tipo de ataques o perdidas de información ha sufrido los sistemas de gestión educativa en la institución?		
Robo de contraseñas	2	40%
Malware	1	20%
Denegación de servicios	1	20%
Perdida de información	1	20%
Total	**5**	**100%**

Nota: *Fuente propia*

Figura 6.

Tabulación de resultados obtenidos de la pregunta 4.



En la Figura 6 se observa que el 40% de los encuestados comentan que han sido objeto de robo de contraseñas en las instituciones educativas, el otro 20% ha sido víctima de perdida de información, el otro 20% denegación de servicios y el ultimo 20% han sido atacados por malware.

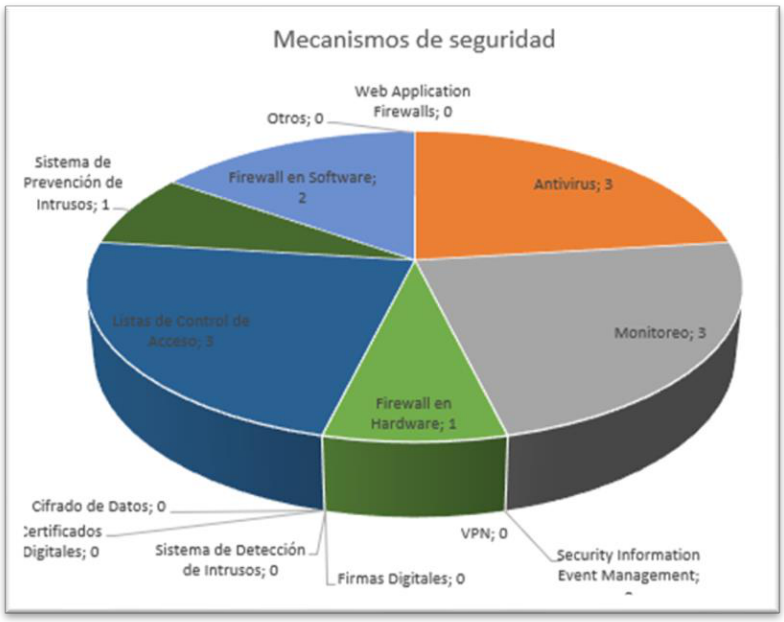
Tabla 9.

Tabulación de resultados obtenidos de la pregunta 5.

Sistemas de seguridad	Cantidad	Porcentaje
Web Application Firewalls	0	0%
Antivirus	5	100%
Monitoreo	5	100%
Security Information Event Management	0	0%
VPN	0	0%
Firewall en Hardware	1	20%
Firmas Digitales	0	0%
Sistema de Detección de Intrusos	0	0%
Certificados Digitales	0	0%
Cifrado de Datos	0	0%
Listas de Control de Acceso	3	600%
Sistema de Prevención de Intrusos	1	20%
Firewall en Software	4	80%
Otros	0	0%
TOTAL	5	100%

Figura 7.

Tabulación de resultados obtenidos de la pregunta 5.



Nota: Fuente propia

En la figura 7 se observa que en el establecimiento educativo existe una variación de porcentajes con relación a los sistemas de seguridad que existen en los mismos tantos sistemas de prevención de intrusos, antivirus, firewall de software. Listas de control de acceso, VPN, Firmas digitales entre otros.

Resumen de la recolección de los datos

Al finalizar la recolección de información y tabular los resultados se concluye que la mayor parte de los encuestados no tienen la capacitación adecuada y el conocimiento adecuado sobre políticas de seguridad, por lo que existe mal uso de sus dispositivos y protocolos y algunos profesores piensan que la responsabilidad solo es del encargado del departamento de informática así evitando responsabilidades.

Mediante la recolección de información ha permitido identificar aspectos que no se había tenido en cuenta en el Colegio Nacional Cutuglagua en el cual se desea implementar la propuesta de seguridad, el cual si es factible debido al requerimiento obligatorio del mismo.

CAPÍTULO II: PROPUESTA

Se desarrollará la propuesta del tema de investigación planteado como: Propuesta de seguridad informática para el control de acceso dirigida a la infraestructura para el Colegio Nacional Cutuglagua aplicando la Norma ISO 27001 A9 Control de accesos.

2.1 Fundamentos teóricos aplicados

Resumen de la recolección de los datos

Realizado el trabajo en las encuestas y entrevistas se obtiene varios resultados los mismos que son tabulados y que nos permite saber a ciencia cierta que los establecimientos educativos tiene brechas que no han sido solucionadas, se ha identificado que está utilizando muchos recursos tecnológicos que permiten el intercambio de información y finalmente se ha identificado que más de la mitad de los usuarios como docentes y estudiantes no están relacionados con algún protocolo de seguridad que permita cuidar la información.

Muchos profesores y estudiantes han sido víctimas de estafas informáticas debido al mal uso de dispositivos ya que aseguran que la responsabilidad cae solo en encargado del departamento de informática.

Debe entenderse que la responsabilidad es todos quienes utilizan los laboratorios incluidos los usuarios que son parte de la Institución educativa por lo que se debe tener conciencia del uso adecuado y así podremos formar parte de la nueva era tecnológica. La técnica de recolección de datos ha sido fundamental el cual permite identificar muchos aspectos de seguridad dentro del establecimiento, por lo que es factible la propuesta.

2.2 Descripción de la propuesta

Para el estudio de este caso, se utilizó métodos de investigación cualitativos y cuantitativos para desarrollar la investigación, el cual permite demostrar los resultados que se logró de la investigación, este permite evaluar mediante un análisis porcentual e interpretar los resultados obtenidos que revela el impacto que tiene el plan informático del fenómeno estudiado, también se utilizó el tipo de diseño no experimental, concretamente el diseño transversal, porque se realizó en un tiempo determinado, en el cual se da un gran impacto en cada estudiante y profesores.

En el proceso de investigación se utilizan métodos teóricos basados en la aplicación del pensamiento y la inferencia para realizar análisis y síntesis, donde: análisis - síntesis e inducción - inferencia, lo que permite encaminar todo el desarrollo de la investigación realizada de lo general a lo específico y viceversa, así como la separación del objeto de investigación en sus componentes, orientaron el proceso de preparación de las herramientas

para su posterior análisis.

Los datos que se recopilaron utilizan información cuantitativa para comprender su impacto en la conciencia de seguridad de la información en el entorno educativo, utilizando cuestionarios como herramienta de recopilación de datos. Se entrevistaron cinco profesores y cincuenta estudiantes. En campo, permite gestionar adecuadamente los resultados de cada estudio. En un enfoque cualitativo, se entrevistó al director del departamento de TI sobre los efectos del programa de seguridad de la información, que facilitó la adquisición de información importante y el seguimiento inmediato, es decir, directamente en el lugar.

Por lo tanto, siempre que se presente un fenómeno de investigación, se debe utilizar una aplicación de notas adhesivas que demuestre las características importantes de la seguridad informática en las instituciones educativas. Esto se hace utilizando un tipo de investigación inductiva y deductiva que examina libros, artículos académicos, revistas y literatura teórica sobre seguridad informática relacionada con Internet y examina los fenómenos existentes en la industria. verdadera naturaleza. y el estado actual de sus instalaciones.

«Entre los métodos utilizados constaron el analítico-sintético en el cual el analítico fue a través de la observación científica de forma directa y estructurada para obtener la información sobre el impacto del plan de seguridad informática, porque permite estudiar la realidad de cómo se encuentra actualmente la unidad educativa y su evolución a través del tiempo, el método sintético, para llegar a la verdad primero separando las partes que intervinieron en el tema investigado y después reuniendo los elementos para completar y demostrar la verdad de cada anomalía». (Ziegler, La Conectividad: un imperativo en la agenda educativa regional, 2021)

a. Estructura general

Actualmente, el departamento tecnológico y destrezas en la comunicación es liderado por el ingeniero Edwin Cocha, quien se vincula con el rectorado que dirige el ingeniero Darío Aimara, las diferentes áreas de la institución no dependen directamente del campo de las tecnologías, que también brindan apoyo para cualquier proceso en cada área de la organización institucional.

Figura 8.

Estructura Organizacional

Fuente: Elaboración propia

Explicación del aporte

En las instituciones dedicadas a la educación, hoy en día utilizan cada vez más los sistemas informáticos para realizar sus actividades, por lo que es necesario velar por la protección de la información y los sistemas de los estudiantes. Están en contra de cualquier tipo de amenaza como acceso no autorizado, virus, etc. Para implementar esta protección, es ideal y recomendable implementar un sistema de gestión de seguridad basado en la norma ISO-27001.

La seguridad informática en los establecimientos educativos cada día conlleva a mejorar estructuras físicas dentro de los establecimientos.

Los problemas que presentan la mayor parte de los establecimientos es por firewall que permiten accesos no autorizados por lo que es necesario generar accesos establecidos para el personal adecuado.

En la actualidad, la informática se encuentra en todos los niveles de educación de una manera acelerada. En la mayor parte de instituciones educativas primarias creen que la informática sólo está basada en una computadora ya que derivan como una herramienta esencial para cada estudiante.

Se tiene un claro ejemplo toda la información que hoy existe en la nube que es administrada por sistemas modernos y de fácil acceso. Estas están ligadas a la necesidad del usuario, en nuestro caso personal administrativo, profesores y estudiantes de cada institución educativa.

Estas herramientas relevantes para todos quienes utilizan deben garantizar que sea seguro y libre de amenazas que dispongan de técnicas y protocolos muy eficaces y dentro de las instituciones educativas los departamentos de TI son los responsables de supervisar el uso adecuado de estas tecnologías.

Para los centros educativos deben complementarse con sistemas de seguridad accesibles y fáciles de usar para reducir accesos no autorizados e inmersión de virus, con los estudiantes familiarizados en tecnología y redes sociales el uso será más efectivo y seguro e innovador.

Es posible que los usuarios, los estudiantes y el personal no estén familiarizados con la tecnología y tengan habilidades técnicas limitadas. Incluso antes de la pandemia, pero sin excepción que requería acceso remoto, los estudiantes y los padres a menudo accedían a los sistemas desde el hogar usando computadoras y teléfonos inteligentes, lo que a menudo introducía vulnerabilidades adicionales. Paradójicamente, la complejidad suele ser un riesgo: los estudiantes con habilidades técnicas pueden intentar atacar solo por diversión o para mostrar sus habilidades.

Entonces, durante la pandemia, algunas fracasaron. En muchos de los casos, los dispositivos que se prestaron a profesores y estudiantes cuando los necesitaban eran vulnerables a los ataques y, a menudo, carecían de actualizaciones de seguridad durante la pandemia. Además, el personal de ciberseguridad no cuenta con suficiente personal o tiene exceso de trabajo, y las plataformas de educación en línea se suman a las preocupaciones de seguridad como si eso no fuera suficiente.

Para ello, Todas las áreas deben involucrarse en la implementación y mantenimiento del uso continuo de los equipos de seguridad. Los buenos modales siempre serán más importantes que los parches. Las certificaciones como ISO también son importantes, pero básicamente son manuales de usuario que nadie lee por ello, se recomienda empezar por lo más sencillo:

Ofrecer capacitación sencilla y eficaz a cada usuario de Internet es una forma de reducir los efectos de fondos y recursos insuficientes.

Un desafío importante que debe abordarse es implementar y proponer protocolos de seguridad confiables seguros de entendimiento común. Igualmente se enseña a los miembros a madurar una cultura de seguridad social conservando una cultura de libertad, que es eficaz para el aprendizaje.

b. Técnicas

Para el presente trabajo, se utilizó la observación y la entrevista, adicionalmente se empleó el método inductivo el cual se ha conformado por tres fases: análisis, identificación y elaboración del plan Gestión de TI.

Análisis. – En este ciclo de análisis se efectúa una evaluación del estado reciente de la organización educativa y del ámbito de referencia COBIT 2019 con la finalidad de definir las mejores prácticas a proseguir en la institución a través de una evaluación sistemática.

Diseño. – Valorando el momento actual de la institución educativa y de COBIT 2019, se seleccionan las técnicas que se adaptan a las necesidades del colegio.

Elaboración. – Se está implementando un programa de desarrollo formal que alinea las metas de la organización con el proceso COBIT en 2019 y permite definir el proceso de manera sistemática.

Situación Actual

Esta sección describe la situación actual del Colegio Nacional Cutuglagua y se utiliza de forma intensiva en el presente trabajo, proporciona un método a seguir para crear un programa de gestión de TI en las instituciones educativas

El Colegio Nacional Cutuglagua ubicada en la ciudad de Quito, es un colegio fiscal que brinda a los adolescentes y jóvenes del cantón Mejía una educación en el aspecto; Inicial; Educación Básica y Bachillerato, el Bachillerato con sus dos opciones: el Bachillerato General Unificado en Ciencias y, el Bachillerato Técnico en; Físico Matemático Comercio y Administración “Informática”.

Tabla 10.

Datos Informativos del Colegio Nacional Cutuglagua

Datos Informativos	
Institución	Colegio Nacional Cutuglagua
Ubicación	Barrio Sta. catalina panamericana sur KM 0
Tipo de educación	Educación Regular
Provincia	Pichincha
Cantón	Mejía
Parroquia	Cutuglagua
Nivel	Inicial; Educación Básica y Bachillerato
Tipo de	Fiscal
Zona	Rural
Número de Docentes	97
Número de Estudiantes	2721

Fuente: Elaboración propia

Identificación en la tabla 10 Los datos informativos institucionales que son de dominio público, para conocer de cerca a la institución educativa.

Tabla 11.

Inventario Tecnológico del Colegio Nacional Cutuglagua

Inventario del Equipo Tecnológico del Colegio Nacional Cutuglagua	
Inventario	**Cantidad**
Computadores de escritorio	35
Laptops	1
Tablets	0
Proyectores	1
Impresora	1
Equipos de telecomunicaciones	0
Escáneres	0

Nota: Elaboración propia

Se puede apreciar en la tabla 11, en la actualidad hay treinta y cinco computadoras de escritorio, una laptop que es asignada al profesor, en el área cuenta con una impresora y un, Adema se ha supervisado que los equipos tecnológicos no poseen con licencias originales de Windows y antivirus.

c. Métodos

Durante el desarrollo se utilizaron métodos basados en conceptos ya conocidos y producidos por otras actividades de investigación, con el fin de evaluar la aplicación se realizaron entrevistas a personas conocedoras del tema, para que de esta manera puedan

brindar sus opiniones acerca de la problemática que se está estudiando, las opiniones brindadas se podrán visualizar en el Anexo 1 hasta él anexo 4.

Tabla 12. Amenazas en Establecimientos Educativos

Amenazas en Establecimientos Educativos

AMENAZAS EN ESTABLECIMIENTOS EDUCATIVOS	
Estado actual	**Impacto**
Amenazas internas	No existe información actualizada que reconozcan amenazas.
Vulnerabilidades de software	Se realiza escaneo de softwares encontrados en los establecimientos, la mayor parte son crackeadas y están expuestas a vulnerabilidades.
Ataques	No hay forma de saber si la red está siendo atacada por un atacante.
Privilegios excesivos	No hay seguridad de cuánto personal tiene privilegios hacia cada una de las redes de la institución.
Abuso de privilegios.	Aún no se define quienes realmente utilizan los accesos a la red institucional.

Nota: Autoría propia

Como se observa en la Tabla 12, Las debilidades en la red de instituciones educativas son el centro de las críticas, los parches de seguridad no se eliminan, no hay formas de controlar la presencia de problemas en el software existente.

2.3 Validación de la propuesta

En el pasado el sistema educativo del Ecuador se ha desarrollado de manera inestable debido a la desigualdad social y económica y la ineficacia de los servidores públicos en la comunidad.. Senplades (2017).

La introducción y uso de la tecnología es ilimitada en todas las áreas, con énfasis especial en la educación. El Colegio Nacional Cutuglagua, en su trabajo diario, es importante la aplicación de TI para sus procedimientos internos, como la comunicación a través de

programas digitales con el personal docente, y la comunicación externa con los programas de educación nacional.

Características de índole tecnológico.

De la encuesta realizada, en la tabla 4 se puede resumir que los colegios del sur de Quito cuentan con lo siguiente:

Tabla 13.

Estándares utilizados en los establecimientos educativos

Estándares utilizados en establecimientos	Colegio 1 Fiscal	Colegio 2 Fiscal	Colegio 3 Fiscal	Colegio 4 Privado	Colegio 5 Privado
Firewall en software	X	X	-	X	X
Antivirus	X	X	x	X	X
Gestión de identidad y el acceso (IAM)	X	X	-	X	X
Auditorías de seguridad periódicas	-	X	-	-	-
Copias de seguridad	X	X	-	-	-
Segmentación de redes y equipos críticos	-	X	-	X	-
IPS Sistema de Prevención de Intrusos	-	X	-	X	X
Adecuación de Permisos	X	X	-	X	X
Vigilancia 24/7	-	-	-	-	X
Security Information Event Management	-	X	-	-	-
Firewall en Hardware	-	X		X	X
Plan de Detección y respuestas a incidentes	X	-	-	X	-
Firmas Digitales	-	-	-	X	-
Listas de Control de Acceso permitidos	-	-	-	X	X
Cifrado de Datos Internos	-	-	-	-	-

Nota: Elaboración propia

La tabla 13, muestra la comparativa de los estándares que utilizan en las instituciones educativas de la provincia de Pichincha. Dejando a cada institución educativa la decisión de su uso acorde a su realidad, teniendo en cuenta las diferentes metodologías como el firewall, encriptación, gestión de identidad y el acceso, copias de seguridad, IPS Sistema de prevención de intrusos, adecuación de permisos, vigilancia veinte y cuatro horas y siete días, plan de detección y respuestas a incidentes estos se muestran optimizados, mostrando una similitud.

Tabla 14.

Comparativa de firewalls recomendados para centros educativos.

FIREWALLS RECOMENDADOS PARA ESTABLECIMIENTOS EDUCATIVOS		
Fortigates		**Cisco ASA**
Esta interfaz de firewall es fácil de configurar. Incluyen acceso a la línea de comandos para administradores avanzados y, por lo general, son fáciles de mantener y modificar.	**CONFIGURACIÓN**	El equipo es fuerte y confiable. Tiene ajustes de configuración flexibles y tiene suficiente potencia y funcionalidad para adaptarse a las necesidades de cada empresa.
Una buena solución VPN, puerta de enlace, enrutador y, por supuesto, firewall. Especialmente para empresas medianas y grandes empresas con usuarios empresariales. Del mismo modo, Fortigate en pequeñas y medianas empresas funciona de la mejor manera.	**SOLUCIONES**	Las soluciones de un firewall de ASA suelen ser las más adecuadas para las pequeñas empresas. (Sin ignorar los grandes) Combinan los firewalls del hardware con una herramienta del software en recurso de seguridad que incluye apoyo de red privada virtual (VPN). antivirus, antispam, antispyware y filtrado de contenidos.
No todos los controles habilitados en el firewall son de gran beneficio en el control del rendimiento.	**RENDIMIENTO**	Ofrece soluciones totales al tener la disposición de integrarse con varias tecnologías de seguridad. Sin que pierda la eficacia de este.
El chasis de hardware se ven limitados por los números que tienen los VPN desde su fabricación.	**RESTRICCIONES DE VPN**	Tiene varios tipos de licencias, que limitan el número de dos sin importar el tipo; clientes versus clientes sslvpn, ipsec, l2tp-ipsec..
El VPN a través de SSL Web Portals simplifica la escala de adaptación para el usuario final, permitiendo una personalización del portal frontal.	**Pros VPN**	Las unidades ASA se conectan fuera de Internet a redes internas y VPN con muy poca sobrecarga y sin pérdida de velocidad de señal.

Nota: Camila Pachón (2022), se respeta derechos de autor

Comparación de estándares de seguridad informática

En la tabla 14, Se revisan algunos aspectos importantes de las mejores prácticas de conservación para cada especie estudiada. Los ejemplos ilustrativos se toman de varios trabajos publicados.

Tabla 15.

Comparativa entre diferentes estándares

Comparación entre estándares

Guía	OSSTMM3	NIST	COBIT 2019	LA ISO 27001
Implementación a través de métodos y recursos.	NO	En la implementación de normas se debe suministra documentos.	Para la implementación de metodologías se debe proporciona documentos.	Suministra métodos para su implementación.
Se orienta a procesos.	Canalizar y suministrar técnicas de evidencias para comprobar y proteger el sistema.	SI	SI	SI
La gestión de riesgos esta establecida en la ejecución de la seguridad.	No	La seguridad.es una norma principal.	Admite controles de seguridad deben aplicarse con una gestión de riesgos.	La seguridad.es una norma principal.
Es aplicable en diferentes empresas	Si	Es más común en empresas de Estados Unidos	No es un programa que de soluciones a nivel global.	Recomendado para empresas de cualquier índole y tamaño.
Objetivos claramente definidos	Si	Antes se debe recabar información para definir los objetivos.	Si	Antes se debe recabar información para definir la meta final.
Definición clara de la gestión	No	No	Si	No
Cobertura de controles	No	Enfocado para la protección de equipos informáticos	Orientado al control en la tecnología informática.	En cada proceso de implementación existe controles que aseguren la seguridad.
Utiliza certificados	No	Solo en Estados Unidos	Si	Si

***Nota*:** Se respeta derecho de autores

En la tabla 15 se puede apreciar varios modelos o estándares que tienen similitud e importancia en cuanto a la gestión de la información. Cada uno tiene un enfoque distinto con aspectos de la misma gestión. Inclusive NIST tiene fuente más local lo que condiciona su aplicación en el ámbito educativo, mientras COBIT, ISO 27001, y OSSTMM3 tienen un origen de entorno global.

Cada modelo en el procedimiento de gestión de la información tiene diferentes factores a considerar al colocar un SGSI (sistema de gestión de la seguridad de la información). La opción de un modelo de un determinado estándar debe abordarse de forma razonable, teniendo en cuenta los beneficios que aportan a la institución educativa. ISO (2018).

Aunque ISO 27001 proporciona una práctica aceptada mundialmente, no significa que sea la única o la mejor práctica para la retención de información. Se debe utilizar un enfoque holístico para implementar un sistema de seguridad de manera efectiva. Alcanzar este nivel requiere del aporte de ciertos modelos de seguridad, cuyas características principales les permiten tener diferentes aspectos que deben ser tomados en cuenta al momento de planificar e implementar sistemas de seguridad informáticos.

El marco de seguridad cibernética de NIST se puede utilizar para apoyar al desarrolla de controles de TI, ISO 27001 debe elegir una herramienta de seguridad informática que considera las necesidades actuales de las personas el cual utiliza un sistema de prevención. Al desarrollar modelos ad hoc para la seguridad informática, se deben considerar las principales recomendaciones de los modelos estudiados.

Brechas de seguridad informática

Para la mitigación de las brechas de seguridad se tienen diferentes estándares el cual se precisa en la Tabla 16.

Tabla 16.

Estándares o brechas de seguridad informática.

Estándares	Brechas de seguridad ESTABLECIMIENTOS EDUCATIVOS PÚBLICOS	ESTABLECIMIENTOS EDUCATIVOS PRIVADOS
Antivirus	Se maneja software de paga, no cuentan con sus respectivas licencias para su correcto funcionamiento dentro de estos encontramos: Avast Panda Antivirus AVG Antivirus	En establecimientos educativos privados se encuentra equipado con Antivirus Eset Nod32 con licencias originales, que permiten el bloqueo de accesos a páginas no autorizadas, navegación en modo incógnito, bloqueo de accesos a dispositivos de almacenamientos externos.
FIREWALL	En establecimientos los Firewalls están predeterminados por defecto por la compañía Microsoft en su versión Windows 10; Windows Defender.	Una de las opciones que manejan las instituciones educativas particulares es MIKROTIK, este es un dispositivo de red que en su arquitectura dispone de un software de enrutamiento, ofrecen una variedad de casos de uso, desde el uso de accesos inalámbricos de la red fijos hasta dispositivos de firewall con funciones de calidad de servicio (QoS).
IPS SISTEMA DE PREVENCIÓN DE INTRUSOS	No cuenta con sistema IPS. Debido a la falta de recursos por parte del estado.	Poseen dispositivos de seguridad y Red denominado Fortinet: que es el que saca más ventaja de cada una de las características naturales de los dos modelos previos, el asimétrico y el simétrico.

Fuente: García (2018)

Identificación de amenazas vulnerabilidades

La Tabla 17 muestra las amenazas potenciales. La colección Amenazas y Vulnerabilidades se ve afectada por el hecho de que actualmente se encuentra en peligro por posibles impactos. En este caso, estas vulnerabilidades identificadas deben abordarse para evitar futuras pérdidas de activos de información para la institución.

Tabla 17.

Identificación de vulnerabilidades y amenazas

ACTIVOS	VULNERABILIDADES	AMENAZAS	CONCLUSION
Infraestructura	Normalmente hay perdida de información debido al cambio de la infraestructura.	Instalaciones en remodelación estructura física.	Se debe a cambio de personal administrativo.
	Construcciones realizadas hace varios años de forma veloz sin seguridades.		Incendio
		Desastres naturales	Terremoto
.	Cableado a la intemperie con accesos a cualquier persona	Servicios básicos	No se tiene control adecuado de la infraestructura
Usuarios	No hay control de la información, accesos	No se maneja adecuadamente la información	Copia y modificación de la información.
Telecomunicación	Manipulan todos los usuarios, cableado sin normativas al aire libre.	Mal estado de los equipos	Equipos sufren daños por cortes eléctricos.
	Conexione eléctricas deficientes	Corte de servicios de telecomunicación.	Falta de actualizaciones de firewall por no contar con servicios básicos.
		Corte de luz por falta de pago.	
	No hay control de acceso a equipos de red.	Claves simples y equipos vulnerables	Los equipos solo disponen claves de fábrica.
	No existe control de autentificación		
Certificaciones	No existe en ningún departamento	Fácil acceso a cualquier departamento para el robo de información.	Se debe canalizar a la implementación de certificaciones.

Fuente: Autoría propia (2023)

Identificación de riesgos

En esta evaluación de los riesgos se aprecia que algunos activos que presentan muy alto riesgo son de vulnerabilidades y amenazas evidentes que si no se toma acciones preventivas o correctivas puede generar pérdidas en los activos de la información. Como se muestra en la figura 13.

Valoración de riesgos

Consideramos la valoración de cada uno de los activos críticos que contiene una lista común de amenazas y con la valoración de P= probabilidad, I= impacto, entonces para el cálculo del riesgo se suman los dos R=.

Tratamiento del riesgo

El tratamiento del riesgo permite tomar decisiones para actuar frente a riesgos analizados, a continuación, se describen los criterios del tratamiento de riesgos:

Aceptar riesgo: se acepta el riesgo sin necesidad de efectuar acción alguna, debido a los costos de solución pueden llegar a ser más caros al origen del riesgo.

Reducir riesgo: se toman acciones para minimizar y bajar el índice que provoque el riesgo.

Evitar el riesgo: tratar de eliminar las actividades que tomen riesgo.

Transferir riesgo: trasladar el riesgo a terceros en este caso se lo hace a: especialistas, empresas, u otras entidades entendidas en el tratamiento de riesgo.

Aplicabilidad de los controles de seguridad

La aplicabilidad se puede ver en el Anexo 6, la cual se representa en una matriz que se define criterios de evaluación para confrontarlos con los controles actuales que maneja la Institución, para posteriormente definir controles de aplicabilidad propuestos por el proyecto en prioridad operativa para establecer las bases para eliminar en la medida posible las amenazas y vulnerabilidades detectadas en la Institución.

Propuesta de SGSI

Los sistemas de gestión son muy necesarios y es importante mencionar que estás políticas son complementarias dentro del Colegio “Nacional Cutuglagua”, por la confidencialidad, integridad y disponibilidad que nos brinda, evitando amenazas y vulnerabilidades de la información esenciales dentro de la comunidad educativa.

Propuesta para el control que deben aplicarse a la seguridad informática en el establecimiento educativo, caso estudio Colegio Nacional Cutuglagua

Luego del estudio y la comparativa entre las metodologías tanto NIST, COBIT, ISO 27001 se escoge para su aplicación la Norma ISO 27001 por lo siguiente:

A medida que las instituciones regresan a las clases presenciales y continúan usando sistemas virtuales, algunos de los cuales se implementaron durante la pandemia, estas sencillas medidas de seguridad ayudarán a las instituciones a navegar a través de muchas mejoras de seguridad. la pandemia presenta una oportunidad para poder ver problemas en su institución. Sin sistemas basados en la nube, las herramientas de videoconferencia y las actividades de aprendizaje a distancia son invaluables.

Inicialmente, no había un acceso de consola establecido a la arquitectura de seguridad, acceso instantáneo para millones de usuarios y ninguna capacitación previa en seguridad, lo que proliferaba las vulnerabilidades.

Establecer un mejor control en el uso de las Tecnologías de la Información y la Comunicación (TIC) en el sector educativo.

Diagnosticar Inexistencia de uso de políticas, normas, estándares de seguridad informática Revisar estrategias de seguridad informática en establecimientos educativos de educación bajo la Norma Iso2701.

Hacer infraestructuras más eficientes

Utilizar eficazmente los recursos financieros

Mejore el valor educativo

Establecer controles de calidad

Implantar prácticas sostenibles

Destaque en el mercado educativo

Mejore la seguridad de los datos

Compartir políticas de seguridad en la institución educativa que abarque varios puntos:

Identificación

Enlistar los equipos, software y datos, que incluye computadoras portátiles, teléfonos inteligentes, tablets y dispositivos utilizados por los profesores y estudiantes.

Funciones y responsabilidades de profesores, estudiantes y personal que tenga apertura a datos importantes de la institución.

Protección

Controlar el acceso a la red y el uso adecuado de las computadoras.

Usar programas que protejan los datos.

Codificar la información delicada que estén en uso o guardados.

Realizar copias de seguridad periódicamente.

Actualizar con regularidad programas, de preferencia automatizar las actualizaciones.

Implementar políticas que permitan la eliminación de archivos electrónicos y dispositivos que no estén siendo utilizados.

Capacitación frecuente sobre ciberseguridad a profesores, alumnos y personal administrativo que usen las computadoras, dispositivos y redes.

Detección

Monitorear las computadoras para detectar el acceso de personas no autorizadas a las computadoras, dispositivos (sean de almacenamiento tipo USB) y software.

Revisar la red para detectarla intromisión de usuarios o conexiones no autorizados.

Investigar actividades inusuales dentro de la red por parte profesores autorizados.

Respuesta

Se debe Implementar un plan para:

Notificar a los profesores, administradores y demás personal cuya información pudiera estar en peligro.

Mantener funcionando adecuadamente las instalaciones.

Informar sobre ataques a la persona encargada y otras autoridades.

Investigar y contener un ataque.

Actualizar las políticas y plan de seguridad.

Preparar para eventos inadvertidos (como emergencias climáticas).

Poner a prueba los planes de prevenciones con frecuencia

Recuperación

Después de un ataque:

Reparar y restaurar equipos y parte de la red que hayan sido afectados.

Mantener informado al personal administrativo, profesores y estudiantes de las actividades de respuesta y recuperación.

Políticas de seguridad de los activos de la información

La Gestión de la Seguridad del colegio debe estar a cargo de un comité técnico, que debe estar formado por el personal de la Unidad Educativa. Este comité tendrá que reunirse de manera periódica, registrando los encuentros realizados.

El Inspector será responsable de comunicar a los usuarios de la Unidad Educativa, las responsabilidades con relación a las Políticas de Seguridad.

Las autoridades o el máximo organismo son quienes deben de comunicar a los docentes y estudiantes a su cargo las obligaciones del cumplimiento de estas regularidades.

Los administradores y usuarios de la Información en la Unidad Educativa tendrán la responsabilidad, conservar actualizada los sistemas y poder otorgar accesos a los profesores y alumnos y personal administrativo.

Encargado del departamento de TIC o profesor encargado de seguridad de la información, debe ser seleccionado por las autoridades y docentes, el mismo que tendrá la responsabilidad de llevar a cabo medidas de seguridad, capacitación y mantener operativo los recursos tecnológicos.

Activos de información

Los activos deben etiquetarse mediante el procedimiento designado como “Clasificación y etiquetado de Información” de acuerdo con lo siguiente.

El departamento de TIC debe disponer de material tecnológico que permita el inventario y determinación de los activos.

Implantar normas y procesos para el uso adecuado de la información ya sea en medios, físicos o digitales.

Recurso humano

Las autoridades y el departamento de TIC en sus procedimientos la planificación y administración deberán hacer una previa investigación de los nuevos usuarios que son parte

de la Unidad Educativa esto incluye a toda la comunidad educativa para eludir riesgos de errores humanos por el uso indebido, robo, fraude, etc.

Reglas de acceso

La institución educativa al ser público, los profesores y alumnos que deseen accesos a los activos deben tener restricciones como:

Correos personales

Video llamadas a través de internet

Redes sociales

Descarga de juegos y programas

Uso de plataformas como Facebook o Netflix

Paginas no autorizadas.

Servicios remotos

Los profesores y estudiantes que manejan la información tanto de sistemas tecnológicos si existe problemas en los sistemas deben tomar las siguientes acciones.

Reportar al departamento tecnológico

Informar sobre posibles inconvenientes que afecten a los equipos informáticos.

Mitigar el incidente desconectando los sistemas.

Dialogar con los profesores para socializar las formas de ataques que existen en la actualidad.

Protección a la infraestructura del establecimiento educativo

Autenticación. Filtros de privacidad que controlan el acceso a personas no autorizadas dentro del establecimiento

Lista blanca. Crear una lista sobre aplicaciones o páginas web que sea permitido el uso para profesores y alumnos dentro del are de estudio, a la misma vez para limitar el tráfico desde adentro hacia afuera y viceversa.

Limitación de administradores, Controlar a las personas que tengan accesos privilegiados para evitar la exposición del sistema o la información del colegio evitando cambios en el sistema.

Segmentación de las redes. Evitar el uso inadecuado de la red tanto a profesores, alumnos y personal administrativo tendrán acceso a redes propias que será controlado por el administrador.

Bloqueo de puertas traseras. Cerrando puertos que no se utilicen permitirán un control adecuado de cibercriminales que desean acceder a la red.

Copias de seguridad. .Es recomendable realizar periódicamente copias de seguridad y guardarlas en el caso de que se viole las seguridades y empiecen a pedir dinero para la devolución de la información.

Auditorías. Para saber el control que se ha implementado y tener la seguridad que esté funcionando y actualizado correctamente en la institución educativa..

Matriz de articulación de la propuesta

En la presente matriz se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

Tabla 8.

Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
ISO 27001	Desarrolla el método de gestión de riesgos enfocados en las buenas prácticas, lo cual en comparación a los sistemas de gestión y educación del Ministerio de Educación presentan mejoras por cuanto no se está efectuando la respectiva capacitación en buenas prácticas de uso de los sistemas educativos lo que como consecuencia produce pérdida de información y ciberataques.	La metodología de investigación fue bibliográfica que permitió tener los conceptos sobre la norma ISO 27001	Fuente bibliográfica	Analiza las características de seguridad que debe poseer según sus normas en un Establecimiento educativo.	Encuestas, entrevistas
ISO 27002	Este es un manual que describe los planes de control y monitoreo recomendados desde una perspectiva de seguridad informática. Este paso no está sujeto a certificación.	La metodología de investigación fue bibliográfica que permitió tener los conceptos sobre la norma ISO 27017	Fuente bibliográfica	Analiza las características de seguridad que debe poseer según sus normas un Cloud Computing	Encuestas
SGSI	Este sistema permite a las organizaciones garantizar que mantengan los activos adecuadamente y que no sean utilizados por terceros	ISO/IEC 27001 define los requerimientos para constituir, implementar, perseverar y modernizar un método de	La clave del SGSI está en diseñar e implementar y dar mantenimiento a los procesos que desean	Se ejecuta y se salvaguarda el secreto e integridad de activos de los establecimientos que estarán disponibles y pueden prevenir los	

	así se evitara fugas de información.	seguridad (SGSI) según el célebre “ciclo de Deming":	gestionar eficazmente la información.	riesgos de perdida de información.
IDS	El sistema de detección de intrusiones: en esta aplicación se detecta en una red accesos que no han sido autorizados.	Este sistema monitorea la entrada de trafico para poder actualizar y comparar con otros ataques conocidos.	El sistema solo emite alertas ante posibles intrusiones, no realiza ninguna mitigación.	Existen ataques espontáneos realizados con herramientas automáticas o por usuarios malintencionados.
IPS	IPS son sistemas que ayudan a prevenir intrusiones a los sistemas de ataques de intrusiones.	Realiza un análisis en el mismo momento que las conexiones y sus protocolos de seguridad detectan que se va a producir o se está produciendo un incidente.	Se reconoce anomalías o patrones sospechosos que permitan el control de los accesos hacia la red, mediante políticas de monitoreo de trafico de contenido.	Realizan alarmas de conexiones sospechosas y a la misma vez desconectan paquetes anómalos.
SIEM	Sistema de gestión de eventos e información de seguridad, Engloba y sistematiza la información de una forma hibrida.	Permite ejecutar un análisis de las alertas de seguridad que tienen los dispositivos en hardware y software.	Recoge los registros de actividad (logs) de los distintos sistemas, los relaciona y detecta eventos de seguridad, es decir, actividades inesperadas o que sospechen que pueden traer problemas	Existen falsos positivos que se descarta dependiendo a la base de datos que se tiene y los informes que registrar en anteriores evaluaciones.

Fuente: Se respeta derecho de autores

CONCLUSIONES

Mediante el procesamiento de los datos recopilados, de la investigación elaborada a los colegios fiscales de la provincia de Pichincha en referencia a la confianza en los sistemas de gestión académica.

La investigación muestra debilidades en las instituciones educativas fiscales donde se determinó que la seguridad informática se encuentra en un segundo plano con respecto a instituciones educativas privadas.

Es importante identificar las brechas de seguridad informática el cual permite resaltar las condiciones actuales de las instituciones educativas fiscales y privadas para aplicar los filtros de seguridad.

La utilización de controles tales como generación de accesos, firewall de contenidos permitirán mejorar la calidad de seguridad informática evitando filtración de información y brindando al personal administrativo, docentes y estudiantes la navegación segura.

RECOMENDACIONES

Se recomienda analizar los métodos de seguridad que se han investigado para poder implementar y mejorar la seguridad en todos los establecimientos educativos a nivel del país.

Es recomendable realizar la protección y segmentación de redes en los colegios que abarque la totalidad de los centros educativos creando varias subredes para profesores, alumnos e invitados.

Es recomendable realizar la prevención de pérdida de datos, mediante sistemas de copias de seguridad para poder establecer con facilidad y rápidamente el correcto funcionamiento.

Es recomendable tener una solución de conectividad y almacenamiento en red en la actualidad existen los servicios y herramientas de Google for Education o Microsoft Office 365 Education.

Se recomienda realizar inducciones o jornadas de sensibilización en temas de seguridad informática a profesores de la institución y a los alumnos.

Se recomienda la implementación de las herramientas de seguridad y el monitoreo de uso constante. Las buenas prácticas valen más que “parches”. Es más, las certificaciones como las normas ISO son de suma importancia, pero si se convierten en simples manuales que nadie usa menos aún lo ponen en práctica, no podrá mejor las seguridades en los establecimientos.

BIBLIOGRAFÍA

Acronis. (22 de febrero de 2021). *Copia de seguridad en la nube vs. copia de seguridad local: ¡necesita ambas!* Obtenido de Acronis: https://www.acronis.com/es-es/blog/posts/cloud-vs-local-backup/

Alonso, C. (5 de marzo de 2020). *¿Cuál es el objetivo fundamental de las normas ISO?* Obtenido de GlobalSuite Solutions: https://www.globalsuitesolutions.com/es/que-son-normas-iso/#:~:text=Las%20normas%20ISO%20son%20un,de%20productos%20en%20la%20industria.

ATICO34. (5 de octubre de 2018). *Hosting pedía*. Obtenido de Hostingpedia: https://hostingpedia.net/copias-de-seguridad.html

BSIGROUP. (4 de junio de 2022). *bsigroup*. Obtenido de bsigroup: https://www.bsigroup.com/es-ES/ISO27017-controles-seguridad-servicios-cloud/

Castillo, G. (30 de junio de 2022). *Innovación digital 360*. Obtenido de Innovación digital 360: https://www.innovaciondigital360.com/big-data/que-son-y-como-funcionan-los-data-center/

CITELIA. (9 de diciembre de 2019). *citelia*. Obtenido de Citelio conéctate con nosotros: https://citelia.es/blog/que-es-cloud-computing-y-como-funciona/

Cloudflare. (27 de marzo de 2020). *cloudflare*. Obtenido de cloudflare: https://www.cloudflare.com/es-es/learning/cloud/what-is-a-cloud-firewall/

Cordoves, L. (2018). La Informática en el mundo actual. *Scielo*, 10.

Elizalde, M. (15 de 12 de 2021). *Instituciones Educativas en Riesgos Informáticos.* Obtenido de Instituciones Educativas en Riesgos Informáticos: https://www.udla.edu.ec/liderazgo/blog/2021/12/15/instituciones-educativas-en-riesgo-informatico/

Escuela Europea de Excelencia. (13 de 11 de 2019). *Escuela Europea de Excelencia*. Obtenido de Escuela Europea de Excelencia: https://www.escuelaeuropeaexcelencia.com/2019/11/listado-de-amenazas-y-vulnerabilidades-en-iso-27001/

ETICENTRE. (30 de agosto de 2019). *ETICENTRE*. Obtenido de ETICENTRE: https://www.eticentre.org/objetivos-desarrollo-sostenible/industria-innovacion-e-infraestructuras/

Fatemeh Khoda Parast, C. S. (2022). *Cloud computing security: A survey of service-based models.* Obtenido de https://www.sciencedirect.com/science/article/pii/S0167404821003977

Fernández, Y. (6 de marzo de 2020). *Ayuda le proteccion datos*. Obtenido de Ayuda le proteccion datos: https://ayudaleyprotecciondatos.es/2022/02/11/encriptacion-datos/#:~:text=La%20encriptaci%C3%B3n%20de%20datos%20es%20un%20proceso%20de,la%20informaci%C3%B3n%20mientras%20viaja%20del%20emisor%20al%20receptor.

Figueroa Pérez, O. (2017). Propuesta de Políticas de Seguridad. En O. Figueroa Pérez, *Propuesta de Políticas de Seguridad* (pág. 58). Colombia: Universidad Nacional Abierta y a Distancia UNAD.

Fursan Thabit, O. C.-G. (2022). *A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing*. Obtenido de International Journal of Intelligent Networks: https://www.sciencedirect.com/science/article/pii/S2666603022000033

García, R. (15 de Julio de 2018). *Media Cloud*. Obtenido de Media Cloud: https://blog.mdcloud.es/tipos-de-encriptacion-en-cloud-computing/

GlobalSuite Solutions. (2020). *¿Qué es ITIL?* España: GlobalSuite.

INTEDYA. (1 de septiembre de 2019). *INTEDYA*. Obtenido de INTEDYA INTERNATIONAL DYNAMIC ADVISORS: https://www.intedya.com/internacional/757/noticia-iso-27000-y-el-conjuntode-estandares-de-seguridad-de-la-informacion.html

KIONETWORKS. (14 de junio de 2022). *KIONETWORKS*. Obtenido de KIONETWORKS: https://www.kionetworks.com/blog/data-center/qu%C3%A9-es-un-data-center

Klusaité, L. (7 de abril de 2022). *NordVPN*. Obtenido de NordVPN: https://nordvpn.com/es/blog/seguridad-cloud-computing/

Martínez, E. (21 de abril de 2021). *Seguridad en América*. Obtenido de Seguridad en América: https://www.seguridadenamerica.com.mx/noticias/articulos/27438/soluciones-de-seguridad-en-data-centers

Moes, T. (25 de marzo de 2018). *SoftwareLab*. Obtenido de SoftwareLab ORG: https://softwarelab.org/es/que-es-un-firewall/

NORMA ISO. (25 de junio de 2019). *normaiso27001*. Obtenido de normaiso27001: https://advisera.com/27001academy/es/que-es-iso-27001/

Pathak, A. (7 de abril de 2022). *geekflare*. Obtenido de geekflare: https://geekflare.com/es/hardware-vs-software-cloud-firewall/

Pazmiño Cruzatti, I. (2019). *Tiempo de investigar, investigación científica 2: cómo hacer una tesis de grado.* Quito: EDITEKA Ediciones.

Ramírez, A. (1 de junio de 2022). *Community*. Obtenido de FS Community: https://community.fs.com/blog/what-is-a-data-center-firewall.html

Sánchez, F. (17 de febrero de 2019). *Smartekh*. Obtenido de Smartekh: https://blog.smartekh.com/4-de-las-principales-problematicas-y-riesgos-en-los-data-center

Tarazona, C. (2018). Amenazas Informáticas y Seguridad de la Información. *Provided by Revistas,* 10.

Zambrano, G. A. (2019). DIAGNÓSTICO DE LAS VULNERABILIDADES INFORMÁTICAS EN. *(Tesis de Ingeniería).* Universidad Tecnológica Israel, Quito.

Ziegler, S. (22 de 02 de 2021). La Conectividad: un imperativo en la agenda educativa regional. *La Conectividad: un imperativo en la agenda educativa regional*, 10. Argentina, Argentina, Argentina: Blog del IICA.

Ziegler, S. (2021). La Conectividad: un imperativo en la agenda educativa regional. *IICA BLOG,* 10.

ANEXOS

ANEXO 1

FORMATO DE ENTREVISTA ESTABLECIMIENTO PÚBLICO

	UNIVERSIDAD TECNOLÓGICA ISRAEL Maestría en Seguridad Informática

El objetivo del presente instrumento es conocer sobre el departamento de TICS. La información aquí registrada es de carácter confidencial y será utilizada exclusivamente con los fines anteriormente mencionados.

Fecha: 01/09/2023

1. Datos Personales

Nombre: Edwin Cocha **Título:** Ingeniero en Sistemas informáticos.		Ingeniería		PhD
		Especialización		Otro

2. Banco de Preguntas

Banco de Preguntas a los encargados del departamento de TICS

¿Indique usted su vinculación en el área de TICS de la institución educativa?

Titular con nombramiento
Titular con contrato
Encargado

¿Tiempo de trabajo en el área de TICS en esta institución educativa?

más de 6 años
entre 3 a 6 años
entre 1 a 3 años
menos de 1 año

¿Con qué frecuencia recibe usted capacitaciones en el área de seguridad de la información y control en la institución educativa?

Una vez al año
cada 6 meses
1 vez al mes
1 vez a la semana
Ninguna

¿Especifique dentro de los últimos 6 meses que tipo de ataques o perdidas de información ha sufrido los sistemas de gestión educativa en la institución?

Robo de contraseñas
Malware
Denegación de servicios
Pérdida de información

GRACIAS POR SU COLABORACIÓN

Firma y Sello

Edwin Cocha

ANEXO 2

FORMATO DE ENTREVISTA ESTABLECIMIENTO PRIVADO

	UNIVERSIDAD TECNOLÓGICA ISRAEL Maestría en Seguridad Informática

El objetivo del presente instrumento es conocer sobre el departamento de TICS. La información aquí registrada es de carácter confidencial y será utilizada exclusivamente con los fines anteriormente mencionados.

Fecha: 09/18/2023

1. Datos Personales

Nombre: Marcelo Salazar	X	Ingeniería		PhD
Título: Ing. En informática y sistemas computacionales		Especialización		Otro

Banco de Preguntas a los encargados del departamento de TICS

¿Indique usted su vinculación en el área de TICS de la institución educativa?

Titular con nombramiento
Titular con contrato
Encargado

¿Tiempo de trabajo en el área de TICS en esta institución educativa?

más de 6 años
entre 3 a 6 años
entre 1 a 3 años
menos de 1 año

¿Con que frecuencia recibe usted capacitaciones en el área de seguridad de la información y control en la institución educativa?

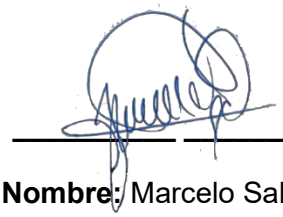
Una vez al año
cada 6 meses
1 vez al mes
1 vez a la semana
Ninguna

¿Especifique dentro de los últimos 6 meses que tipo de ataques o perdidas de información ha sufrido los sistemas de gestión educativa en la institución?

Robo de contraseñas
Malware
Denegación de servicios
Pérdida de información

GRACIAS POR SU COLABORACIÓN

Firma y Sello



Nombre: Marcelo Salazar

ANEXO 3

Entrevista 2

FORMATO DE ENTREVISTA A ESTUDIANTES DE COLEGIOS PRIVADOS

	UNIVERSIDAD TECNOLÓGICA ISRAEL Maestría en Seguridad Informática

El objetivo del presente instrumento es conocer si los estudiantes están familiarizados en el ámbito de seguridad informática. La información aquí registrada es de carácter confidencial y será utilizada exclusivamente con los fines anteriormente mencionados.

Fecha: 11 de agosto de 2022

Datos Personales

Nombre: Jean Pierre Tipan	x	Ingeniería		PhD
Título: Ingeniero en Electrónica y Telecomunicaciones		Especialización		Otro

1.- ¿Sabe usted quién es el responsable de instalar y mantener el software de seguridad en el laboratorio de computación?

- Empleados
- Administrador
- Personal de TIC

2.- ¿Qué versión de Windows está instalada en el equipo que normalmente usan para conectarse a Internet?

- Windows 10
- Windows 8.1
- Windows 8
- Windows 7
- Otros

3.- ¿Qué navegador web usan comúnmente?

- Internet Explorer
- Firefox
- Chrome
- Ópera
- Netscape

4.- ¿Con qué frecuencia utiliza Windows Update?

- Se configura para que se actualice automáticamente
- Al menos una vez al mes
- De vez en cuando, cuando recuerdo
- Nunca
- No sé qué es Windows Update

5.- ¿Tienen algún antivirus instalado en las computadoras del laboratorio?

- Sí
- No
- No sé

6.- ¿Qué antivirus utilizan frecuentemente en el laboratorio?

- Avast
- Microsoft
- ESET
- Symantec
- AVG
- Avira
- Kaspersky
- McAfee

7.- ¿Con qué frecuencia actualizas un software antivirus?

- Se hace automáticamente
- Al menos una vez a la semana
- Al menos una vez al mes

8.- ¿Qué antispyware han utilizado con frecuencia en el laboratorio?

- Norton Internet Security
- McAfee Internet Security / antispyware
- Panda Internet Security
- PC Tools Spyware Doctor

9.- ¿Utiliza algún firewall en las computadoras del laboratorio?

- Sí
- No
- No sé

10.- ¿El personal de TIC monitorea las computadoras todo el tiempo?

- Sí
- No
- No sé

GRACIAS POR SU COLABORACIÓN

Jean PiereTipan

ANEXO 4

Entrevista 3

FORMATO DE ENTREVISTA EN ESTABLECIMIENTO PUBLICO

	**UNIVERSIDAD TECNOLÓGICA ISRAEL** Maestría en Seguridad Informática

El objetivo del presente instrumento es conocer si los estudiantes están familiarizados en el ámbito de seguridad informática. La información aquí registrada es de carácter confidencial y será utilizada exclusivamente con los fines anteriormente mencionados.

Fecha: 11/08/2022

1. Datos Personales

Nombre: Juan Pablo Tigasi	X	Ingeniería		PhD
Título: Estudiante Tercero de Bachillerato		Especialización informática		Otro

2. Banco de Preguntas

1.- ¿Sabe usted quien es el responsable de instalar y mantener el software de seguridad en el laboratorio de computación?

- Empleados
- Administrador
- Personal de TIC

2.- ¿Qué versión de Windows está instalada en el equipo que normalmente usan para conectarse a Internet?

- Windows 10
- Windows 8.1
- Windows 8
- Windows 7
- Otros

3.- ¿Qué navegador web usan comúnmente?

- Internet Explorer
- Firefox
- Chrome
- Ópera
- Netscape

4.- ¿Con qué frecuencia utiliza Windows Update?

- Se configura para que se actualice automáticamente
- Al menos una vez al mes
- De vez en cuando, cuando recuerdo
- Nunca
- No sé qué es Windows Update

5.- ¿Tienen algún antivirus instalado en las computadoras del laboratorio?

- Sí
- No
- No sé

6.- ¿Qué antivirus utilizan frecuentemente en el laboratorio?

- Avast
- Microsoft
- ESET
- Symantec
- AVG
- Avira
- Kaspersky
- McAfee

7.- ¿Con qué frecuencia actualizas un software antivirus?

- Se hace automáticamente
- Al menos una vez a la semana
- Al menos una vez al mes

8.- ¿Qué antispyware han utilizado con frecuencia en el laboratorio?

- Norton Internet Security
- McAfee Internet Security / antispyware
- Panda Internet Security
- PC Tools Spyware Doctor

9.- ¿Utilizan algún firewall en las computadoras del laboratorio?

- Sí
- No
- No sé

10.- ¿El personal de TIC monitorea las computadoras todo el tiempo?

- Sí
- No
- No sé

GRACIAS POR SU COLABORACIÓN

Firma y Sello

Nombre: Juan Pablo Tigasi