UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN
SEGURIDAD DE LA INFORMACIÓN
RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:

ARTÍCULOS PROFESIONALES DE ALTO NIVEL

TEMA:

PROPUESTA DE UNA POLÍTICA DE SEGURIDAD PARA EL USO DE TECNOLOGÍAS QUE PERMITAN DISPONIBILIDAD EN AMBIENTES DE ENSEÑANZA VIRTUALES SINCRÓNICOS ONLINE

AUTORA:

GÉNESIS MAGALY RODRÍGUEZ ACOSTA

DIRECTOR:

JOSÉ LUIS AGUAYO MORALES

CUENCA – ECUADOR
2023

Autora:

Génesis Magaly Rodríguez Acosta
Ingeniera en Sistemas.
Candidata a Magíster en Seguridad de la Información por laUniversidad Politécnica Salesiana – Sede Cuenca.
grodrigueza@est.ups.edu.ec

Dirigido por:

José Luis Aguayo Morales
Ingeniero en Electrónica y Telecomunicaciones.
Magister en Ciberseguridad.
Magister en Sistemas Informáticos Educativos.
Magister en Redes de Comunicación.
jaguayo@ups.edu.ec

DEDICATORIA

Este trabajo se lo dedico con todo el corazón a mi Familia, quienes siempre me apoyan y están conmigo, gracias por su amor y sus consejos. A mi esposo por su paciencia, comprensión y ayuda infinita.

AGRADECIMIENTO

Primeramente, agradezco a Dios por haberme dado la sabiduría y la fortaleza para continuar con mis estudios, a mis padres que son mi guía y ejemplo, y a mi esposo por sus consejos, su apoyo, paciencia y amor incondicional.

Tabla de Contenido

Resumen 7

Abstract 8

1. Introducción 9

2. Determinación del Problema 10

3. Marco teórico referencial 11

3.1 Políticas de Seguridad de Información 11

3.2 Tecnología en el Ecuador 13

3.3 Educación virtual en el Ecuador 13

3.4 Procesos en la educación on-line: 14

3.5 Amenazas Cibernéticas en la educación Virtual: 15

3.6 Normas y marcos de referencia en T.I, S.I y Ciberseguridad 16

3.7 Procedimiento Metodológico para la gestión de la Política de Seguridad de la información 17

3.7.1 Identificar infraestructura 18

3.7.2 Salvaguardas 18

3.7.3 Políticas del Negocio: 19

3.7.4 Sanciones del Código Integral Penal a posibles ataques cibernéticos o de redes que se generen en el Ecuador 20

4. Resultados y discusión 22

5. Conclusiones 29

6. Bibliografía 30

Propuesta de una política de seguridad para el uso de tecnologías que permitan disponibilidad en ambientes de enseñanza virtuales sincrónicos online

Autora:

Génesis Magaly Rodríguez Acosta.

Resumen

Las instituciones educativas impulsaron la educación en línea a raíz de la pandemia, dándole vital importancia al proceso de enseñanza o transmisión de conocimientos mediante el uso de las telecomunicaciones donde el docente y el alumno no comparten un aula física. Algunas características de esta modalidad son: flexibilidad de horarios, trabajo colaborativo, información instantánea; así como desventajas tales como: retrasos por fallas tecnológicas, caídas de la plataforma que provocan indisponibilidad de la información. Estos problemas revelaron vulnerabilidades a ciberataques queponen en peligro algunos datos sensibles de los estudiantes, como información bancaria, información residencial, números de empleados, entre otros. Todas estas posibles amenazas llevan a las instituciones a la obligación de corregir urgentemente estas vulnerabilidades.

Por lo tanto, se necesita una política de seguridad de la información que ayude a reducir los riesgos que afectan la operación, con el propósito de salvaguardar los activos de una empresa ante un daño ocasionado por un ataque. Además, se debe cumplir con la legislación vigente en Ecuador para proteger los datos. Por ello, se sigue la norma ISO 27000, las recomendaciones COBIT 2019 y la metodología Magerit para desarrollar la política de seguridad.

La política que se propone como estándar para las instalaciones, el sistema y el personal sobre el cual se aplica, tiene como objetivo preservar la privacidad y disponibilidad de la información en ambientes síncronos, para lo cual se designan responsabilidades y roles de los empleados y usuarios en el sistema, también se establecen procedimientos para la gestión de incidentes de seguridad, para la gestión de contraseñas y autenticación de usuarios; además de las características mínimas de los recursos informáticos, software y equipos físicos para proteger los datos de la empresa, y finaliza con la valoración económica que muestra la factibilidad de aplicar la política desarrollada en las instituciones educativas.

Palabras clave:

Disponibilidad, Enseñanza, vulnerabilidad, Políticas de Seguridad.

Abstract

Educational institutions promoted online education as a result of the pandemic, giving vital importance to the process of teaching or transmitting knowledge through the use of telecommunications where the teacher and the student do not share a physical classroom. Some characteristics of this modality are: flexibility of schedules, collaborative work, instant information; as well as disadvantages such as: delays due to technological failures, platform crashes that cause unavailability of information. These problems revealed vulnerabilities to cyber attacks that endanger some sensitive student data, such as banking information, residential information, employee numbers, among others. All this possible threats leads institutions to the obligation to correct urgently these vulnerabilities.

Therefore, an information security policy is needed to help reduce the risks that affect the operation, with the purpose of safeguarding the assets of a company before there is damage caused by an attack. In addition, the current legislation in Ecuador must be complied with to protect the data. Therefore, the ISO 27000 standard, the COBIT 5 recommendations and the Magerit methodology are followed to develop the security policy.

The policy that is proposed as a standard for the facilities, the system and the personnel on which it applies, its objective is to preserve the privacy and availability of information in synchronous environments, for which responsibilities and roles of employees and users are designated in the system

Keywords:
Availability, Teaching, vulnerability, Security Policies.

1. Introducción

Una de las particularidades de la transformación digital es el uso de equipos, sistemas, herramientas más conocidas como las TIC, tecnologías digitales e infraestructura de internet o nube. La combinación de estas tecnologías genera un gran impacto en la sociedad, y por causa de la pandemia, la educación on-line se tuvo que implementar de forma inmediata, haciéndose evidente que, la tecnología fue el actor principal para que, las instituciones pudieran continuar con la enseñanza, en este caso online.

La disponibilidad de la información es importante al momento de que los docentes dictan sus clases, por lo que las instituciones de enseñanza sincrónica online deben implementar una política de (Sec.Info.) que contenga los lineamientos para salvaguardar la disponibilidad de la información en los ambientes sincrónicos. Esta política debe basarse en normativas como la ISO 27002 la cuál detalla las buenas prácticas que permiten mantener y resguardar los sistemas mediante procedimientos y políticas.

Por otro lado, hoy en día existen los ciberdelincuentes que pueden causar grandes impactos a las instituciones educativas, ya que pueden robar información causando que no esté disponible para las partes interesadas, por lo que las instituciones deben revisar y remediar las brechas que pueden causar que los ciberdelincuentes exploten una vulnerabilidad que cause un problema de indisponibilidad.

La disponibilidad para el usuario final es uno de los propósitos principales del centro de cómputo así también es importante asegurar quiénes tienen acceso a la información ya que esto también podría generar que la información no esté disponible cuando se requiera, debido a que se pueden efectuar cambios no autorizados.

Por lo mencionado, como resultado se obtendrán los beneficios del uso de tecnologías que permita a las instituciones educativas reforzar su área de redes utilizando controles que permitan salvaguardar la disponibilidad de la información.

2. Determinación del Problema

Durante las clases pueden presentarse problemas en los principios de la Sec.Info., en este caso en específico en la “Disponibilidad”, sea por fallas en la conectividad, en el internet, bajo ancho de banda, problemas de respaldo de la información, o porque no se ejecutaron los procesos batch para actualizar la información, entre otros.

Algunos factores como la falla de almacenamiento de información atenta contra la disponibilidad de la información, especialmente los servicios que se tengan en la nube, para esto los especialistas deben estar muy atentos y se deben crear alertas que permita identificar cualquier anomalía ya que una falla podría causar reducción en el rendimiento del sistema. (SOTWARE ONE, 2020).

Así también, debido al rápido avance e innovación de las herramientas para el procesamiento de información, así como también los mecanismos empleados para las comunicaciones, han surgido riesgos en la tecnología informática. A lo cual es importante levantar el inventario de activos para que estos sean debidamente administrados y preserven la confidencialidad, integridad y disponibilidad de la información, dando lugar a la seguridad de la información (M., 2015)

(Yang, 2002) sugieren la obligación de contar con mecanismos efectivos para el control y la gestión de la seguridad y la privacidad. Tener un control sin una planificación adecuada no ayuda a reducir las amenazas en aulas virtuales. Una analogía a esto es: para mantener una casa o una habitación de datos valiosos, la puerta se cierra con llave, usando la llave y la cerradura como mecanismo de control. Solo las personas autorizadas reciben la clave para acceder a la casa.

Desafortunadamente, sin embargo, la gestión del proceso de entregar la clave a las personas validadas se maneja de manera insuficiente, lo que puede llevar a que la clave termine en manos de personas maliciosas En una situación diferente, la clave también podría perderse o duplicarse y luego ser utilizada por personas no autorizadas. Por lo tanto, no es solo la solución o los controles lo que importa, sino la gestión de seguridad, que determinará el éxito de los controles de seguridad y la solución implementada (Benavides Sepúlveda, 2018)

En los últimos tiempos han existido ataques y/o vulnerabilidades exclusivamente durante la emergencia sanitaria, han resaltado los ambientes e-learning, donde se maneja información reservada o confidencial, estos se encuentran expuestos a troyanos, spyware, acceso no autorizado o a la alteración parcial o total de la información que se almacena estos sistemas. No obstante, la implementación de buenas prácticas de seguridad de la información aplicada por instituciones que regularmente soportan e-learning ha significado un éxito para la gestión académica de forma remota (Monges Olmedo, 2020)

3. Marco teórico referencial

3.1 Políticas de Seguridad de Información:

En la actualidad conectarse a redes sociales, adquirir aplicaciones y software son cada vez más sencillos, lo cual conlleva a compartir todo tipo de información y datos, aumentando el riesgo de que todo los recursos informáticos, financieros y operacionales de una organización sean vulnerados e irrespetados.

La definición más acertada de seguridad nos indica que son todos los métodos posibles y aplicables en la reducción de riesgos que afecten un correcto funcionamiento. Eliminar en su totalidad todo tipo de vulnerabilidad que sea propenso es imposible, pero el objetivo es proteger los activos de una empresa contra un posible ataque.

Los delincuentes informáticos constantemente se encuentran en búsqueda de vulnerabilidades y debilidades en los softwares que han sido diseñados con un fácil acceso en su configuraciones y utilización, lo cual brinda oportunidades de amenazas pudiendo atacar las redes y servidores de una compañía, organización, etc., otorgando una imagen negativa públicamente.
Toda compañía u organización tiene información confidencial, la cual debe ser protegida bajo un plan de S.I donde se pueda controlar, dirigir y medir todos los recursos humanos, su software y el hardware.

Los activos de una organización protegidos en una política de seguridad, como se muestran en la figura 1:

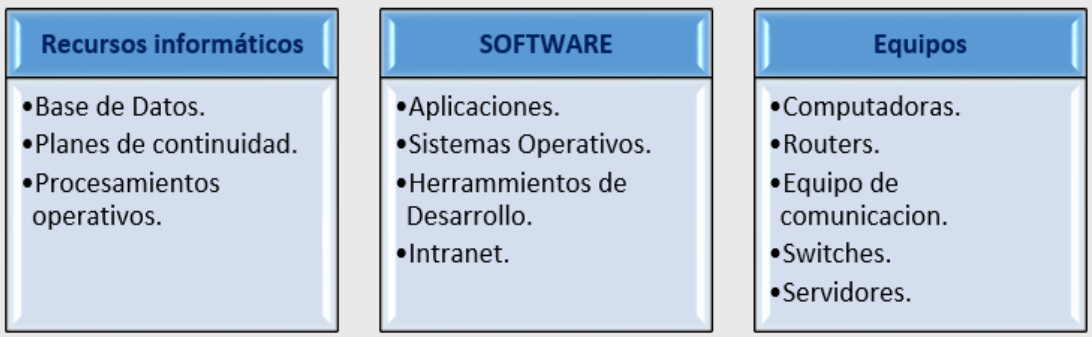


Figura 1 Activos de una organización

Una política de seguridad no solo se basa en conocer las amenazas que una organización puede ser víctima, sino de fijar el inicio, y el origen del evento, así también es importante conocer si el ataque es interno o externo a la institución.

Se define como política de seguridad a las normativas establecidas por una organización que se deben respetar, para el correcto uso de información y recursos,

al igual que una constitución de una estado o país, las políticas de seguridad deben ser claras, precisas, ajustables a cualquier cambio que se presente.

Las políticas de seguridad deben asegurar la CID de la información. Así mismo presentar documentos relativos que contemplen los procedimientos del cumplimiento de reglas, los responsables por niveles o áreas de las organizaciones, el compromiso de la Dirección y las Gerencias de la institución, así como también el documento debe ser presentado a todos los trabajadores de la empresa.

Un correcto uso de las políticas de seguridad debe contener:

- Administración de usuarios, que controle el acceso a los recursos a todo el personal.
- Copias de respaldo, que describa los pasos detalladamente a seguir en la recuperación de información.
- Tratamiento de la información, define el tipo de información y las personas autorizadas en manejarlo.
- Clasificación de la información: Público, Interno y Confidencial.
- Software legal uso de programas con licencias oficiales.
- Servicio de internet y correo electrónico con protección de información.
- Seguridad en la comunicación, descripción detallada de la transmisión y recepción de información externa e interna.
- Auditoría de sistemas, donde se controle y se provenga posibles eventos.
- Continuidad del procesamiento, se establecerán normas a seguir en la recuperación de informáticos en casos críticos.
- Teletrabajo, controlar el acceso remoto a la red fuera de las instalaciones propias.
- Seguridad en las telecomunicaciones, deben existir controles detectivos, preventivos y correctivos para evitar brechas.
- Sanciones por incumplimiento, medidas para proteger los fines de la compañía con sanciones que serán aplicadas por mal uso de recursos.

En su última versión la ISO 27000 tiene como finalidad garantizar la CID de los recursos cumpliendo los requerimientos legales estatales, proporcionando servicios para proteger la data de la empresa. Cabe mencionar que estas normas mediante una planificación basada en el análisis de riesgos y la medición del impacto, les permite a las empresas definir, implementar, monitorear, evaluar la seguridad, generando políticas, normativas y procedimientos para salvaguardar y proteger la información de los procesos y activos de la empresa especialmente los más críticos.

Así también en la Política debe quedar definido los roles y responsabilidades de los ingenieros de la información, es importante q mínimo se cuente el siguiente rol según la ley de Protección de Datos Personales (Corrales, 2022).

- **Oficial de Protección de Datos Personales:** Su función es implementar de

forma efectiva las políticas y procedimientos para cumplir las normas, así también efectuar la implementación de buenas prácticas de gestión de datos personales dentro de la empresa y determinar los controles del programa de protección de datos personas, su evaluación y revisión permanente.

3.2 Tecnología en el Ecuador:

En Ecuador, en el 2009 se fundó el MINTEL, que es el ministerio gestor, con el fin de fortalecer la democracia, la diversificación y la universalización de los servicios y empresas relacionadas con las telecomunicaciones.

El logro más significativo del MINTEL, es el aumento de las conexiones a internet en el país, ya que en el 2006 apenas existían 207,277 usuarios a internet, para inicios del 2013 el número se incrementó a 4,463,390 de usuarios conectados a internet. Este hecho hizo que Ecuador ocupe los primeros puestos de crecimiento en la región (Ofimática, 2020).

Así mismo, en el 2019 Ecuador mejoró su índice de disponibilidad en tecnología de la red y en el 2021, todas las empresas con diferentes modelos de negocio decidieron acelerar sus planes de transformación digital debido a la crisis otorgada en la pandemia.

Sin duda la tecnología crecerá en nuestro país enormemente, por lo cual se necesitará de muchos profesionales con capacitación en el ámbito digital, que no solo brinden superávits económicos a las compañías, sino seguridad en su información privada lo cual a medida que crece considerablemente se puede hacer más vulnerable (Guerra, 2021).

3.3 Educación virtual en el Ecuador:

Se puede definir como educación virtual al proceso de enseñar o transmitir conocimientos mediante el uso de las telecomunicaciones donde el docente y el estudiante no comparten un aula física, en otras palabras, la educación virtual es la evolución de la educación a distancia (Ruiz, 2021).

Actualmente, ha cambiado la forma de estudiar a distancia con las telecomunicaciones. Entre las ventajas de la educación virtual tenemos:

- Permisos a la información instantánea.
- Flexibilidad de horarios y residencia.
- Oportunidad de repetir video clases las veces que sean necesarias.
- Oportunidad de repetir lecciones y actividades.
- Trabajo colaborativo en salas de chat.

Entre las desventajas de la educación virtual tenemos:

- Menos concentración que las clases presenciales.

- Carencia de rutina, ocasionando descontrol en las actividades.
- Requiere más perseverancia y disciplina que clases presenciales.
- Demoras por fallas tecnológicas.
- Indisponibilidad de la información.

La educación virtual utilizando tecnologías se enfrenta a 4 retos muy importantesen su desarrollo los cuales son: Calidad, Alcance, Capacidad de adaptación y Cultura.

3.4 Procesos en la educación on-line:

A continuación, se detallan las características a considerar para cada uno de los actores:

- **Estudiantes:**
  - Tener la facilidad de acceder a la plataforma de una manera sencilla, motivando al estudiante a seguir participando.
  - Accesibilidad a las tareas a efectuar.
  - Fácil interacción con compañeros.
  - Facilidad de acceso al docente para consulta de información y dudas de los estudiantes.

- **Docentes:**
  - Subir materiales, clases y la programación de actividades de una manera sencilla.
  - Poder importar y exportar las actividades, tareas, elaboradas con otro software.
  - Permitir la comunicación individual y/o grupal con los estudiantes.
  - Dar seguimiento a las actividades que realizan los estudiantes permitiendo evaluar, calificar los trabajos enviados, así como su participación.

- **Administración y gestión:**
  - Tener la posibilidad de expandir tanto la cantidad de los estudiantes como de los cursos.
  - Poder administrar las altas y bajas de los estudiantes, así como las restricciones de acceso.
  - Tener la facilidad de solucionar problemas tecnológicos y administrativos.

Ciclo del proceso E-learning:

- Análisis y estudio de la realidad.
- Diseño del proyecto E-learning.
- Instalación de servidor y plataforma.
- Adecuación técnica.
- Experimento con la plataforma.
- Capacitación.

Uno de los elementos importantes del proceso e-learning es la adecuación técnica, la cual está relacionada con los procesos tecnológicos necesarios para la educación on-line:

- Servidores: Se deben tener un servidor dedicado que permita el control de las T.I.
- Dominio web: Corto y concreto de la institución.
- Hosting: Elegir hosting y dominio con el mismo proveedor.
- Pagos electrónicos: La virtualización de estos procesos facilitan la vida a la institución.
- Conectividad: Considerar velocidad en la conexión y capacidad en la transferencia.
- Capacitación: Entrenamientos a los docentes en: herramientas en línea, web y entornos 3D.
- Aulas virtuales: Virtualización de ambientes, integración de tecnologías.
- Portal educativo: Difusión oficial de la información de la institución ante el público ubicación, logros, actividades curriculares, misión, avances académicos.

3.5 Amenazas Cibernéticas en la educación Virtual:

Las instituciones educativas en la modalidad presencial tenían menos probabilidad de sufrir un ataque cibernético, pero a raíz de la pandemia que impulso el cambio a la educación online, demandaban servicios basados en la nube, las video conferencias y el trabajo remoto.
Sin contar con un principio claro en arquitectura de seguridad, con una cantidad de usuarios accediendo sin capacitaciones, ni cuidado de información ni prevención de datos informáticos, la vulnerabilidad se fue agrandando, lo cual ocasionó una necesidad urgente de respuesta inmediata al daño que se puede originar o corregir a tiempo.

En los Estados Unidos en el 2020, los costos de inmovilidad, pérdida y reparaciones, ascendieron alrededor de 273 millones de dólares, siendo el daño más alto en comparación con otras modalidades de negocio.

Fuera del país norteamericano, las instituciones educativas fueron objetos de ataques informáticos, que se resume en la siguiente frase:

“Los delincuentes cibernéticos pueden acceder a una red de investigación ver lo que se está realizando, probando y cómo va el avance de esas pruebas y una de las razones a que pase esto es que las universidades y facultades tienen bibliotecas con un gran número de información de investigación no pública, además cabe indicar que este tipo de información no solo es útil para el gobierno, sino que también tiene un valor económico” (Information, 2021).

Los ataques cibernéticos no solo buscan usar información para espionaje y venta de documentación o material de estudio, los delincuentes tienen otras alternativas como por ejemplo un esquema de correo electrónico de phishing donde el objetivo es solicitar préstamos fraudulentos a estudiantes y empleados, obtener información crediticia y comercial, datos financieros sensibles como acceso a cuenta de bancos.

Dada la relación estrecha entre banco, estudiantes y universidades, el ataque a centros educativos se hace atractivo, y es una manera más sencilla de obtener datos financieros, creando una base de datos para estafas, para los delincuentes el sistema de seguridad de las instituciones educativas es más débil que el de una entidad financiera.

Las Instituciones educativas almacenan una impresionante cantidad de datos financieros, pero el presupuesto de seguridad, software de protección, los planes de contingencia no son comparables a las entidades financieras.

3.6 Normas y marcos de referencia en T.I, S.I y Ciberseguridad:

Citamos las más relevantes normativas y marcos de referencias en el ámbito de la tecnología, ciberseguridad y seguridad, entre ellas se tienen las siguientes:

- **ISO IEC 27032 cybersecurity standard:** Con base a que el presente trabajo de investigación es a fin a una política de seguridad, se considera importante citar las siguientes definiciones incluidos por ISO IEC 27032:

  "La seguridad del ciberespacio o ciberseguridad es garantizar la CID de la información en la nube".

  Es importante considerar herramientas que resguardan la seguridad y brindan soporte a la defensa perimetral, gestión de configuración, continuidad e incidentes.

- **Marco para mejorar la Ciberseguridad de la Infraestructura Crítica – Instituto Nacional de Normas y Tecnología:**

  Facilita a las empresas independientemente de su tamaño y naturaleza del negocio, los lineamientos y directrices para definir una estrategia que permita salvaguardar los activos de las empresas que transmiten, procesan y almacenan información y data relevante.

- **Marco de referencia Cobit 2019:**

  Es el avance más reciente desarrollado por ISACA.
  COBIT 2019 y los objetivos del gobierno tienen que estar alineados a los objetivos de la empresa estos a su vez van a estar relacionados con un proceso y un conjunto de componentes.

Estos objetivos se agrupan en cinco dominios: el primer dominio (EDM) congrega los objetivos de gobierno, y los objetivos de gestión se congregan en cuatro dominios (APO, BAI, DSS, y MEA).

Dominio Alinear, Planificar y Organizar (APO):

- APO13: Gestionar la seguridad.

Dominio Construir, Adquirir e Implementar (BAI):

- BAI04: Gestionar la disponibilidad y la capacidad.
- BAI09: Gestionar los activos.
- BAI10: Gestionar la configuración.

Dominio Entregar, Dar servicio y Soporte (DSS):

- DSS02: Gestionar las peticiones y los incidentes del servicio.
- DSS04: Gestionar la continuidad.
- DSS05: Gestionar los servicios de seguridad.

Bajo lo mencionado, la política de seguridad debe contener controles que permitan principalmente la disponibilidad de la información en ambiente de enseñanza virtuales sincrónicos online, en sus activos, especialmente los más críticos, entre estos controles, podemos detallar los siguientes:

- Supervisar el rendimiento y utilización de las capacidades de los componentes tecnológicos frentes a los umbrales definidos.
- Cuando existan incidentes de disponibilidad, se debe identificar su causa raíz y dar seguimiento para su correcta corrección.
- Monitorear el rendimiento de los componentes tecnológicos críticos.

3.7 Procedimiento Metodológico para la gestión de la Política de Seguridad de la información:

Para alcanzar el objetivo planteado se propone definir en las instituciones educativas un área de S.I., la cual va a estar encargado de salvaguardar el activo más importante como es la información, y a su vez se identifiquen los controles para la disponibilidad de la información. El primer paso es crear una Política de S.I.

Esta Política de S.I. debe estar publicada y socializada con los colaboradores y debe actualizarse conforme a los cambios en la institución, leyes y aspectos

globales. Se debe implementar herramientas como Global Suite, para la aprobación de la Política por las partes interesadas.

3.7.1 Identificar infraestructura:

Para definir las infraestructuras de hardware y software que ayudarán a la disponibilidad de la información es preciso tomar como referencia los activos definidos en el estado del arte como parte de los activos que deben estar protegidos en una Política de S.I.

- Plataformas Web: Plataformas educativas e-learning, Sistemas de gestión educativa, Repositorios Digitales, página web institucional.
- Infraestructura: Servidor Web, Servidor de aplicaciones.
- Redes: Red interna Institucional.
- La Nube: Aplicaciones Web alojadas en servidores externos.

3.7.2 Salvaguardas

Para que las instituciones educativas puedan atenuar los problemas de ciberseguridad es de vital importancia que se defina e implemente controles que brinden seguridad a las aplicaciones web. Detallamos algunas de ellas:

Administración del sistema: Para la gestión de la Política de S.I es preciso que se efectúen las siguientes actividades basado en la ISO27032 (Arévalo, 2022).

- Definición de Roles y Privilegios en los Sistemas (gestión de sesiones).
- Acceso mediante métodos autenticación en la plataforma web.
- Gestión de respaldos de la Información.
- Redundancia.

Plataforma:

Arquitectura física:

- Ejecución de un Firewall interno y externo para la auditoria y autorización de conexiones permitidas.
- Ejecución de una Wireless LAN Controller para los accesos a las aplicaciones web dentro de las instituciones financieras.
- Servidores.
- Storage.
- Cintas.

Arquitectura lógica:

- Las aplicaciones deben contar con protocolos seguros y un certificado digital.
- Herramienta Networker para respaldos.
- Herramientas como Zabixx para monitorear los equipos.

- Herramientas para controlar el mantenimiento de parches de seguridad.

Usuarios:

- Capacitaciones.
- Contraseñas.
- Antivirus.

3.7.3 Políticas del Negocio:

Se deben determinar políticas para el uso y protección de los activos de información, así como el debido manejo y administración de los respaldos de información de las instituciones educativas, así como asegurar el cumplimiento de los estándares y mejores prácticas para el almacenamiento, custodio de la data respaldada, asegurando de esta forma la recuperación y disponibilidad de la información.

Uno de los controles principales que deben estar descritos y aprobados en la política, es el "Respaldo de Información" el cual debe ser definido según los procesos de la Institución educativa, los respaldos pueden ser diarios, mensuales y semanales. La información una vez respaldada puede ser almacenada en discos.

Así también hay que definir y asegurar que se mantengan los respaldos para los siguientes elementos: Sistemas operativos, Base de Datos, aplicaciones y archivos. Y los tipos de respaldos que se utilizarán son: Full, Incremental, Diferencial, Bases de Datos transaccionales.

Es importante que los respaldos sean revisados y verificados periódicamente por un área independiente con el objetivo de asegurar que se tenga la información lista para operar los procesos en el plan de continuidad de negocio.

Una de las opciones es utilizar discos espejos para que la información se almacene simultáneamente en dos o más discos, en otras palabras, si un disco llegará a fallar se encontrará con la información restaurada en el otro disco.

Se debe mantener siempre actualiza la guía de programación de los respaldos y que los operadores tengan accesos a ella.

Así también se menciona que una de las maneras más seguras de reducir los riesgos de disponibilidad de la información es utilizando la tecnología, es decir contar con sistemas alternativos contingentes como:

- Tener computadores con esquema de respaldo (N+1), por si la red falla.
- Contar con abastecimientos de energía alternos.
- Replicación de datos del Storage entre el CCP y CCA, manteniendo un esquema de replicación sincrónico.

La información contenida en los medios de almacenamiento deberá mantenerse de acuerdo con lo establecido en las Políticas de Información de las Instituciones Educativas.

Las cintas obsoletas, que hayan superado el tiempo de reutilización deberán ser destruidas, para cumplir con la ley orgánica de protección de datos personales, usando el procedimiento que se defina para dicha destrucción.

Los responsables de los respaldos deben tener de forma actualizada un inventario en el que se detallen los tapes y su contenido. Así también todos los respaldos deben tener log para corroborar el resultado de ejecución de dicho proceso y constatar que siempre exista espacio suficiente para que no se presente ningún inconveniente.

3.7.4 Sanciones del Código Integral Penal a posibles ataques cibernéticos o de redes que se generen en el Ecuador.

Hoy en día existen ciberdelincuentes que están a la expectativa de las vulnerabilidades que pueden explotar para el robo de información. El Ecuador siendo un país libre y democrático que brinda a sus ciudadanos la libertad total de navegar en redes, páginas, etc., sin restricciones, pero a través del código orgánico integral penal, castiga y pone limitaciones donde las personas deben respetar y no cometer actos perjudiciales a terceros. A continuación, detallamos algunas medidas:

- Cualquier ataque mal intencionado que sea dirigido a compañías privadas y públicas tienen su respectiva sanción, los artículos 232 y 233 del COIP dice que toda persona que destruya, dañe, trabe, ocasione mal funcionamiento de sistemas informáticos, será sancionado con una pena de libertad de 3 a 5 años, estos malos funcionamientos pueden ser ocasionados por diseño, creación y desarrollo de programas maliciosos que ocasionen daños, que destruya sin autorización la infraestructura tecnológica interrumpiendo su correcto uso.

- Cuando se trate de daños en sistemas informáticos del estado o revelación de información que es considerada no pública, la sanción va de 5 a 7 años, si se comprueba que los daños fueron ocasionados por personal que labore en el sector público e interfiera en la seguridad del estado la pena asciende de 7 a 10 años más una declaración de no volver a trabajar en el sector público mínimo de 6 meses.

- Acceder sin consentimiento a un sistema informático y de telecomunicación tiene su 3 respectiva sanción y el artículo 234 del COIP dice la persona que acceda en una parte o de forma completo a un

sistema informático o de telecomunicaciones y se mantenga activo generando modificaciones en la web, desviando o redireccionando tráfico, para ofrecer los mismos servicios que el dueño legítimo será sancionado con una pena privativa de libertad de 3 a 5 años.

Así mismo el estado está facultado a interceptar datos informáticos o de telecomunicaciones bajo los puntos mencionados en el artículo 476 del COIP se puede retener por 90 días con fines investigativos e incluso solicitar una prórroga por 90 días más en casos de sospecha de delincuencia organizada. Todo dato recaudado en la investigación es de información privada no se puede divulgar hasta que un juez analice todo lo recaudado. La intercepción de telecomunicaciones (llamadas, mensajes de texto, mensaje de voz, dirección ip, vídeos, fotos, etc.) no pueden ser realizadas previa autorización de un juez, el cual lo solicita porque considera necesario para la comprobación de infracción o participación en un delito. Solo puede ser utilizada la información necesaria para el proceso legal, el acusado puede solicitar sus grabaciones para su defensa.

- Revelar una base datos que es considerada privada tiene su sanción correspondiente y el artículo 229 del COIP dice que la persona que desee sacar provecho propio o de terceros y decida revelar información registrada por un compañía, archivada, este en una base de datos y se divulga de manera digital, con la intención de perjudicar la privacidad será sancionada con 1 a 3 años, si este acto es realizado por un servidor público, empleados bancarios, empleados de frentes populares la sanción asciende de 3 a 5 años.

4. Resultados y discusión

Para que exista disponibilidad de información en ambientes sincrónicos, es importante que las instituciones educativas aprovechen las tecnologías de información mencionadas en el numeral anterior. Si bien es cierto se debe realizar una compra de hardware y software para la implementación, tenemos que pensar que ser proactivos sale más económico que ser reactivos. Una excelente recomendación es realizar la compra de servidores, al menos ser TIER 2, lo cual se refleja al tener una infraestructura N+1. Es decir, si se necesitan 5 switches se deben comprar 6 para que encaso de una falla se pueda reemplazar el extra por el dañado.

Al adquirir un switch debe considerar cuantos usuarios estarán conectados y cuantos dispositivos necesitan estar conectados juntos esto le ayudará a definir con cuantos puertos debe comprarlo, así también los switches Layer-3 permiten más control sobre la red y permite a un administrador fácilmente separar datos y control de acceso a los diferentes dispositivos. (Franklin, 2019)

Recordemos que los sistemas de seguridad perimetral no pueden dejar de funcionar; si es que lo llegan hacer, los usuarios (docente y alumno) y la información confidencial estarán expuestos a posibles ataques. Los encargados serían los equipos de capa perimetral firewalls y routers que cumplan ciertas características mínimas como las de la figura 2:

- Port Security
- Static Port Security
- Dynamic Port Security
- Sticky Learning
- Maximum MAC Addresses
- Port-Security Violation Actions
- **errdisable recovery**
- 802.1x
- DHCP Snooping
- TACACS+
- RADIUS

Figura 2 Características de seguridad de los switches

Adicionalmente, dentro de la infraestructura existen otras capas de seguridad que son de vital importancia para el ambiente tecnológico como la capa de datos que se encarga del cifrado, capa de aplicación en lo que se refiere al antivirus, la capa de red interna que se centra en los segmentos de red, Ipsec y una de las más importante y críticas la capa humana que es el eslabón más débil por lo cual una de las formas de mantener esto fortalecido, es entrenando, capacitando y concientizando al personal sobre las buenas prácticas de seguridad. A continuación, una breve descripción:

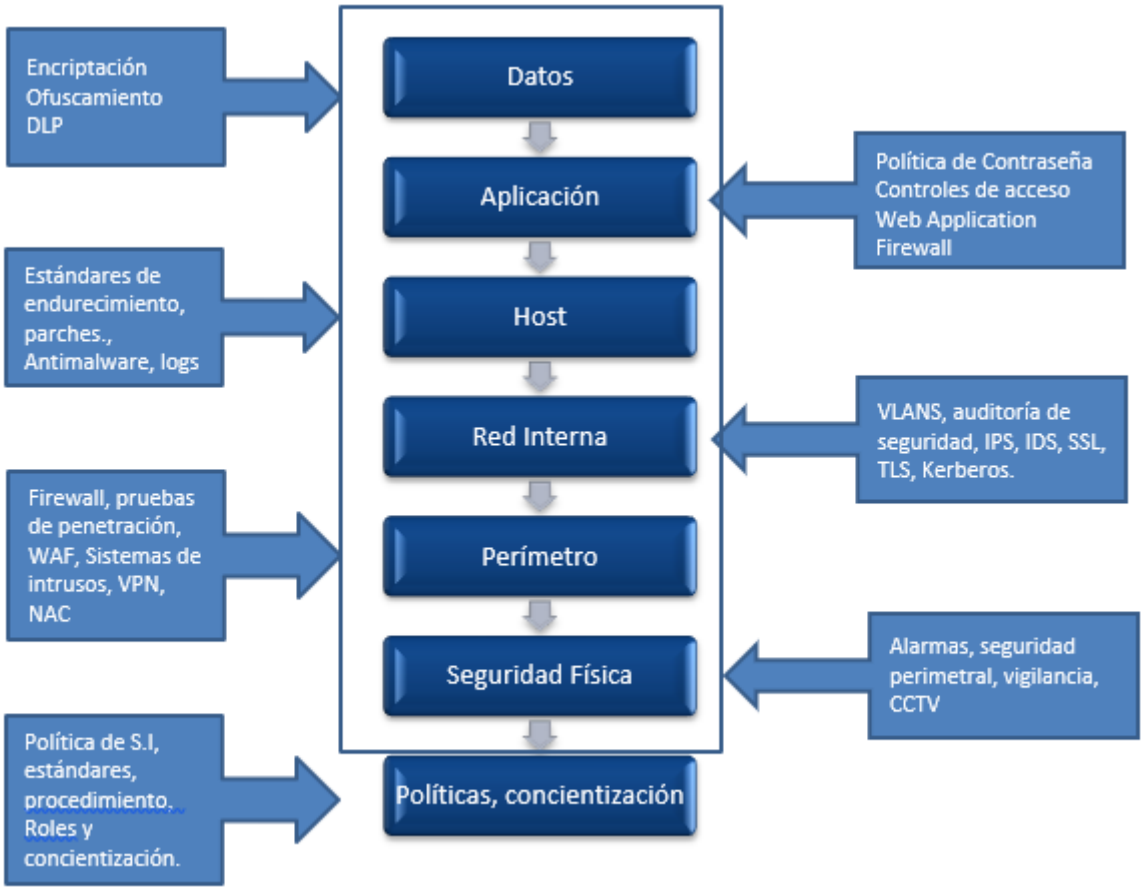


Figura 3 *(Info B. S., 2010)*

Por lo antes mencionado la alta disponibilidad garantiza la continuidad de los servicios, incluso en situaciones de emergencia. Adicionalmente otro punto al cuál hacemos énfasis, es la redundancia el cual está ligado a las implementaciones de alta disponibilidad, específicamente se refiere a un dispositivo adicional que se tendrá como respaldo (activo-pasivo) o equilibrador (en el caso activo-activo).

Estos controles permiten proporcionar a las instituciones educativas 2 puntos importantes:

- **Seguridad:** Tener un firewall redundante, permite que el entorno no esté expuesto a amenazas recurrentes como virus, malware, ransomware, troyanos, etc. Además, los servicios integrados, estarán disponibles, como la encriptación, la protección contra amenazas, la prevención de intrusiones, etc.

- **Productividad:** El firewall es un componente que se puede utilizar para filtrar contenido y bloquear o permitir el acceso a las aplicaciones que son utilizadas por un equipo, otorgando productividad y adherencia a la política de S.I.

Los controles antes mencionados, son basados en la ISO 27002, la cual me permite tener una política de S.I. completa y alineada a uno de los principales pilares de la seguridad como es la "Disponibilidad", esta normativa se certifica cada 2 años, sin embargo, de forma anual el auditor líder realiza una validación del cumplimiento de los controles con el objetivo de supervisar su cumplimiento y que no existan no conformidad y observaciones que puedan llevar a la institución educativa a un incumplimiento y pérdida de la certificación.

Otros controles de la ISO27001:2022, publicada en octubre 2022, que se debe considerar como parte de la política de seguridad de la información son:

- **Controles organizacionales:**

  - Control 5.1 – Políticas para Seguridad de la Información.
  - Control 5.9 – Inventario de activos de información y otros activos asociados.
  - Control 5.30 – Disponibilidad de las TIC para la continuidad de negocio.
  - Control 5.31 – Requerimientos legales, estatuarios, regulatorios y contractuales.
  - Control 5.34 – Protección y Privacidad de la información de carácter personal.

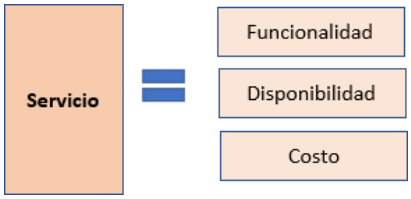
- **Controles tecnológicos:**

  - Control 8.6 – Gestión de capacidades.
  - Control 8.9 – Gestión de la Configuración
  - Control 8.13 – Copias de seguridad de la información.
  - Control 8.14 – Disponibilidad de los recursos de tratamiento de la información.
  - Control 8.20 – Controles de red.

Los controles disminuyeron de 114 a 93 controles.

A continuación, detallamos breves costos representativos de la tecnología, para que las instituciones educativas puedan asignar un presupuesto:

Figura 4 Servicio



Estándar de costos:

Es importante que las instituciones educativas determinen la inversión que se va a efectuar y los beneficios que van a generar adquiriendo un conjunto de equipos que unidos conforman una tecnología a la vanguardia que va a permitir la disponibilidad en

los ambientes sincrónicos online:

Hardware	Firewall, Servidores, Storage, Cintas, Portátiles.
Software	Zabixx, Networker, Symantec, Virtual Patching, Bases de Datos.
Personas	Capacitaciones.
Instalaciones	Oficinas, áreas seguras, electricidad.
Servicios Externos	Servicios de seguridad, outsourcing.
Costos de Capital	Activos físicos de la institución.
Costos Operativos	Relacionados a los procesos diarios del área de T.I.
Costos Fijos	Se mantienen iguales.
Costos Variables	Costos que pueden variar como depreciación de equipos, daños etc.

Tecnología:

Costos del Hardware:

Equipos	Costo Unitario	Total
10 servidores	$100.00	$1000.00
10 portátiles	$600.00	$6000.00
10 discos duros externos	$80.00	$800.00
equipos de oficina (teclados, mouses, reguladores)	$ 300.00	$3000.00

Costos de Software:

Programas	Costo Unitario	Total
Sistemas Operativos	$ 60.00	$ 600.00
Licencias de Office	$ 90.00	$ 900.00
Bases de Datos	$ 1000.00	$ 10000.00
Licencias programas de Seguridad	$150.00	$1500.00
Antivirus	$ 30.00	$300.00
Zabixx	$20000.00	$20000.00
Virtual Patching	$50000.00	$100000.00

Costos de Instalaciones:

Equipos de Oficina	Costos Totales
Instalaciones de equipos de redes	$ 1500.00
14 escritorios	$ 2100.00
14 sillas de oficina	$ 1400.00
2 aires Acondicionados	$ 1200.00

Costos de Hosting:

Área segura	Costos Totales
Servicio de Hosting - Datacenter	$ 10000.00

Servicios externos:

Servicios	Costos Totales
Internet	$1200.00 anuales

Telefonía Fija	$ 600.00 anuales
Mantenimiento de Equipos	$ 300.00 semestrales

Costos de Capital:

Activos físicos	Costos Totales
Hardware	$ 10.800.00
Equipos de Oficina	$ 6200.00

Costos Operativos:

Activos	Costos Totales
Software	$13300.00
Personal	$25000.00

Costos Fijos:

Servicios	Costos Totales
Internet	$1200.00
Telefonía Fija	$ 600.00

Costo variable:

Servicios	Costos Totales
Mantenimiento de Equipo	$300.00

2.- Política y capacitaciones:

Costos de implementación de la política:

Política	Costos	Total
Política de Seguridad de la Información	$ 1000.00	$1000.00
Capacitación de la política	$ 2500.00	$2500.00
Difusión de la política	$ 500.00	$ 500.00

3.- Personas:

Costos de Personal:

Capital Humano	Capacitación	Total
10 especialista de Tecnología	$ 2000.00	$20000.00
2 auditores	$ 1000.00	$2000.00
2 especialistas de seguridad de la información	$ 1500.00	$ 3000.00

Recordemos que es mejor ser proactivos que reactivos ya que siendo reactivos nos puede generar costos más altos e impactos mayores a los activos de la empresa.

Se deben identificar los activos más críticos de la empresa, y con la metodología Magerit podemos definir su nivel de riesgo (Director, 2012):

Valoración de activos:

Nivel	Abreviatura	Valor
Muy alto	MA	500000 $
Alto	A	100000 $
Medio	M	30000 $
Bajo	B	3000 $
Muy bajo	MB	500 $

Clasificación de la vulnerabilidad:

Nivel	Abreviatura	Valor	Descripción
Extremadamente frecuente	EF	0,9973	1 vez cada día
Muy frecuente	MF	0,1425	1 vez cada semana

Frecuente	F	0,0329	1 vez cada mes
Frecuencia normal	FN	0,0055	1 vez cada 6 meses
Poco frecuente	PF	0,0027	1 vez al año
Extremadamente poco frecuente	EPF	0,0003	1 vez cada 10 años

Valoración de impacto

Nivel	Abreviatura	Valor
Crítico	MA	90%
Alto	A	75%
Medio	MA	50%
Bajo	B	20%

Disminución de impacto y vulnerabilidad:

Nivel	Abreviatura	Valor
Alta	A	90%
Media	MA	60
Baja	B	30
Nula	N	0%

Nivel de riesgo:

Nivel	Abreviatura	Valor
Muy alto	MA	300000 $
Alto	A	20000 $
Medio	MA	10000 $
Bajo	B	500 $
Muy bajo	N	100 $

Grupo de activos	Descripción	Valoración cuantitativa	Valoración cualitativa
[D] Datos / Información	copias de respaldo	$30000,00	M
[D] Datos / Información	credenciales	$500000,00	MA
[D] Datos / Información	registro de actividad	$100000,00	A
[HW] Equipos informáticos (hardware)	cortafuegos	$100000,00	A
[HW] Equipos informáticos (hardware)	punto de acceso inalámbrico	$100000,00	A
[Media] Soportes de información	almacenamiento en red	$100000,00	A

Nº	Código	Nombre	Riesgo intrínseco total diario	Riesgo efectivo total diario	Riesgo controlado por salvaguardas
1	AC-003	Credenciales	$ 7.534,25	$ 3.424,66	$ 4.109,59
2	AC-004	Registro de actividad	$ 821,92	$ 452,05	$ 369,87
3	AC-006	Cortafuegos	$ 1.232,88	$ 739,73	$ 493,15
4	AC-007	Punto de acceso inalámbrico	$ 1.232,88	$ 863,01	$ 369,87
5	AC-009	Almacenamiento en red	$ 438,36	$ 356,16	$ 82,20

Activo	Riesgo Inicial	Riesgo Final
Credenciales	MA	M
registro de actividad	A	MB
cortafuegos	A	MB
punto de acceso inalámbrico	A	MB
almacenamiento en red	A	MB

Cálculo del ROSI:

Figura 3 Retorno de la inversión por seguridad de la información ROSI

Pérdidas anuales por incidentes - Sin tratar:	**$1.5000,00**
Pérdidas anuales por incidentes – Residual luego de mitigados:	**$ 600,00**
Ahorro bruto anual por contramedidas.	**$900,00**
Costo inicial contramedidas:	**$250,00**
Costos anuales recurrente contramedidas:	**$70,00**

Con base al cálculo de ROSI podemos identificar que las instituciones educativas deben conocer que, al colocar controles en los sistemas, permite que los mismos sean menos vulnerables y que puedan ser impactados por intrusos, a su vez permite disminuir gastos en caso de que pueda ser atacado. Al tener controles, estos deben ser revisados, darle mantenimiento y tratamiento continuo para corroborar que el control es eficaz y funciona como es debido.

Los controles y el uso de tecnologías permiten grandes beneficios como (Paz, 2008):

- Aprendizaje mediado por ordenador.
- Innovación tecnológica en TICS.
- Acceso rápido y eficaz a la información.
- No obsolescencia de equipos e información.
- Gran capacidad de almacenamiento de información.
- Seguridad en la información.
- Monitoreo de los datos.
- Virtualización.

La Alta Dirección de las instituciones educativas deben evaluar si el proyecto de utilización de tecnologías de información basado en una política se puede efectuar por fases por medio de un proyect, con el objetivo de que se vaya identificando y adquiriendo los recursos necesarios para la implementación de dichas tecnologías

Por ejemplo, la implementación del proyecto por razones económicas o técnicas, se recomienda ejecutarlo por fases, las cuales pueden dividirse en 3 segmentos:

1. **Fase 1** – Adquirir los equipos de seguridad perimetral (Firewall, IPS, IDS, Access Point).
2. **Fase 2** – Adquirir los softwares de antivirus, respaldos, procesos batch, directorio activo, parches.
3. **Fase 3** – Adquirir el hardware como servidores, equipos de oficina y otorgar las capacitaciones al personal humano.

5. Conclusiones

1.- Hemos identificado que existen grandes beneficios al utilizar tecnología avanzada para los ambientes de enseñanza virtual online.

2.- Al implementar una política de S.I. en las instituciones educativas permite salvaguardar la información que es procesada, transmitida y almacenada dentro del proceso, así también concientiza a los usuarios de cómo deben darle tratamiento a la información convirtiéndose en un control efectivo y eficaz para los ambientes de enseñanza virtual online y dando como resultado mantener los controles a un nivel de riesgo aceptable por la institución.

3.- La Alta Dirección de las instituciones educativas propone que el proyecto de implementación de la política de S.I. sea ejecutada por fases, permitiendo identificar cualquier desviación que pueda impactar la seguridad de la institución, así también se pueda medir el nivel de satisfacción de los usuarios.

6. Bibliografía

Arévalo, M. (05 de octubre de 2022). *ISO 27032, el estándar enfocado en ciberseguridad*. (pirani) Recuperado el 20 de marzo de 2023, de https://www.piranirisk.com/es/blog/iso-27032-el-estandar-enfocado-en-ciberseguridad

Calles-García, J., & González-Pérez, P. (2011). *La Biblia del Footprinting.*

Corrales, G. (05 de 05 de 2022). *Funciones del oficial de protección de datos*. Recuperado el 29 de 03 de 2023, de Funciones del oficial de protección de datos: https://es.linkedin.com/pulse/funciones-del-oficial-de-protecci%C3%B3n-datos-gilber-corrales-rubiano?trk=pulse-article

Director, M. A. (2012). MAGERIT – versión 3.0. En M. A. Director, *MAGERIT – versión 3.0* (pág. 127). Madrid: Ministerio de Hacienda y Administraciones Pública.

Franklin. (30 de Julio de 2019). *Que debes saber a la hora de elegir un switch*. Recuperado el 21 de marzo de 2023, de https://www.4netonline.com/ws/que-debes-saber-a-la-hora-de-elegir-un-switch/

Guerra, B. (15 de 12 de 2021). *Instituciones educativas en riesgo informático*. Recuperado el 29 de 03 de 2023, de Instituciones educativas en riesgo informático: https://www.udla.edu.ec/liderazgo/blog/2021/12/15/instituciones-educativas-en-riesgo-informatico/

Information, R. (2021). Obtenido de https://www.udla.edu.ec/liderazgo/blog/2021/12/15/instituciones-educativas-en-riesgo-informatico/

Ocrono, Editorial Cientifico. (2020). Percepcion sobre la educacion virtual ante la pandemia del Covid.

Ofimatica, B. d. (25 de 06 de 2020). *Como a evolucionado la tecnología en el Ecuador*. Obtenido de Como a evolucionado la tecnología en el Ecuador: https://blogdeandreg1.blogspot.com/2020/06/como-evolucionado-la-tecnologia-en-el.html

Ormella., I. C. (s.f.). *El ROI de la Seguridad de la Información.* Obtenido de https://www.angelfire.com/la2/revistalanandwan/rosintro.pdf

Paz, F. E. (Sept de 2008). *Fides et Ratio - Revista de Difusión cultural y científica de la Universidad La Salle en Bolivia*, On-line ISSN 2071-081X. Recuperado el 27 de 03 de 2023, de http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2008000100008

Ruiz, V. (22 de 02 de 2021). *E-learning, Educación, Educación por competencias, Technology* . Recuperado el 29 de 03 de 2023, de E-learning, Educación, Educación por competencias, Technology : https://www.sicom.com.mx/2021/02/22/educacion-virtual-e-learning/

SOTWARE ONE . (2020).

www.elhacker.net. (s.f.). *www.elhacker.net*. Obtenido de https://www.elhacker.net/trucos_google.html

2015, M. (2015). Monges, . Obtenido de M. (2015). Seguridad de la información en plataformas virtuales de e- Learning. ScientiAmericana,

Benavides Sepúlveda, A. &. (2018). Obtenido de Benavides Sepúlveda, A., & Blandón Jaramillo, C. (2018). Modelo sistema de gestión de seguridad de la información para instituciones educativas de nivel básico. Scientia et Technica

M., M. (2015). Revista Multidisciplinaria. Obtenido de Revista Multidisciplinaria.: Monges, M. (2015). Seguridad de la información en plataformas virtuales de e- Learning. ScientiAmericana,

Monges Olmedo, M. R. (2020). Seguridad de la información en plataformas de elearning en tiempos de pandemia COVID-19. Obtenido de Seguridad de la información en plataformas de elearning en tiempos de pandemia COVID-19: http://revistacientifica.unida.edu.py/publicaciones/index.php/cientifica/article/view/9

Yang, C. L. (2002). Proceedings of the 5th IASTED International Multi-Conference Computers and Advanced Technology in Education. Obtenido de Yang, C., Lin, F., & Lin, H. (2002). 'Policy based Privacy and Security Management for Collaborative Eeducation Systems. Proceedings of the 5th IASTED International Multi-Conference Computers and Advanced Technology in Education, (págs. 501-505).