ESTRATEGIA DE ASEGURAMIENTO DE LA INFORMACIÓN A PARTIR DEL ANÁLISIS Y GESTIÓN DE RIESGOS EN LOS PROCESOS ACADÉMICOS Y ADMINISTRATIVOS QUE PUEDEN AFECTAR LAS INSTITUCIONES EDUCATIVAS

ROBERTO SABALZA JUNCO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2023

ESTRATEGIA DE ASEGURAMIENTO DE LA INFORMACIÓN A PARTIR DEL ANÁLISIS Y GESTIÓN DE RIESGOS EN LOS PROCESOS ACADÉMICOS Y ADMINISTRATIVOS QUE PUEDEN AFECTAR LAS INSTITUCIONES EDUCATIVAS

ROBERTO SABALZA JUNCO

MONOGRAFÍA

Director
EDGAR MAURICIO LÓPEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2023

Nota de aceptación

_____
_____
_____
_____
_____
_____
_____
_____

_____
Firma del presidente de Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bogotá, 13 de abril de 2023

DEDICATORIA

A mi familia, mi esposa, mis hijos que siempre han estado a mi lado brindándome su apoyo incondicional, siempre estuvieron presentes en cada paso que he dado en mi carrera educativa y profesional. Con todo mi amor a mi esposa Irene, a mis hijos Leandro y Andrés, gracias por el apoyo y confianza que me han dado durante el proceso en esta nueva etapa en mi vida.

CONTENIDO

Pág.

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

CIBERDEFENSA: Es una evolución de las tecnologías de la información y las comunicaciones que ha provocado un cambio de paradigmas que exige la adopción de procedimientos especializados para neutralizar y controlar las amenazas cibernéticas

CIBERNAUTA: La cibernética es el estudio interdisciplinario de la estructura de los sistemas reguladores. el espacio virtual que existe en las terminaciones dendríticas le hizo imaginar la navegación en un espacio virtual

EXCESO DE CONFIANZA: Cuando una persona no tiene la capacidad de percibir los riesgos que es susceptible de ser víctima de un ataque de seguridad: virus, malware, y los bots maliciosos pueden combinarse en una botnet como se les llama a las redes de que consta de una serie de dispositivos conectados a Internet en los que se ejecutan uno o más bots (a menudo sin que los propietarios de esos sistemas lo sepan) como códigos maliciosos de Internet que pueden programarse (o alterarse) para hackear cuentas de usuario y enviar correos no deseados en busca de datos de contacto o realizar otras acciones malignas para el robo de datos personales, suplantación de identidad, etc. Los usuarios no son conscientes de los riesgos que existen en el mundo físico, y del mismo modo, deben tomar consciencia de los riesgos que existen en el entorno online.

POLÍTICAS APROPIADAS DE SEGURIDAD: Establecer reglas y lineamientos técnicos para el uso controlado de activos de información que minimicen el riesgo de pérdida de dato, accesos no autorizados, divulgación no controlada, duplicación e interrupción intencional de la información.

PERDIDA DE INFORMACIÓN: Situación en la que no podemos acceder a datos importantes almacenados en un sistema informático. Se puede producir por cualquier causa, una avería, un error humano, un borrado accidental o provocado, desastres naturales, incendios, etc.

RANSOMWARE: Es un tipo de malware donde se utiliza el método más habitual para transmitirse es mediante un spam malicioso o mensajes no solicitado, enviando dicho malware por correo electrónico actúa de tal manera que no permite a los usuarios tener acceso a su propia información o acceder a su sistema y mediante soborno exigen el pago del soborno se efectúe mediante criptomonedas o tarjetas de crédito, para que el usuario rescate y acceda de nuevo a su información. Los primeros ransomware se crearon al final de la década de los 80.

RECURSOS INFORMÁTICOS: Un recurso informático es cualquier componente físico o virtual de disponibilidad limitada en una computadora o un sistema de

gestión de la información. Los recursos informáticos incluyen medios para entrada, procesamiento, producción, comunicación y almacenamiento.

RECURSOS FÍSICOS: Es la propiedad tangible, e incluyen instalaciones, oficinas, bodegas, terrenos, maquinaria, equipos y herramientas.

SALVAGUARDAR: Nos permite de una manera más segura y organizada consignar la información que es de gran valor para una compañía, ya que nos permite que en dado caso se genere un daño técnico poder recuperar los datos que creíamos perdidos.

MALWARE: Es un término general para referirse a cualquier tipo de “malicious software” (software malicioso) diseñado para infiltrarse en su dispositivo sin su conocimiento. Hay muchos tipos de malware y cada uno busca sus objetivos de un modo diferente.

PHARMING: Es una famosa combinación entre los términos "phishing" y "farming", clasificándose como un tipo de cibercrimen muy similar al phishing, donde el tráfico de un sitio web es manipulado para permitir el robo de información confidencial. Es decir, un hacker puede instalar un virus o un troyano en la computadora de un usuario que cambia el archivo de hosts de la computadora para dirigir el tráfico fuera de su objetivo previsto, hacia un sitio web falso y aprovecha los principios con los que funciona la navegación por Internet, usando la dirección IP por parte de un servidor DNS para establecer la conexión.

KEYLOGGERS: Es un seguimiento que se realiza y registran todas las teclas que se pulsan en una estación de trabajo, de forma delictiva sin el conocimiento del usuario, que puede estar enfocado en software o hardware, y se puede usar como herramienta lícita de control de TI, tanto profesional como personal, los keyloggers también se pueden utilizar con fines delictivos. Por regla general, son un spyware malicioso que se usa para capturar información confidencial, como contraseñas o información financiera que posteriormente se envía a terceros para su explotación con fines delictivos.

SMISHING: Se manifiesta como una técnica que básicamente consiste en la transmisión de envío de un SMS por un ciberdelincuente a un usuario haciéndose pasar por una entidad legal. Enviando mensaje de incitación o llamar a un número de contacto ganador o acceder a un enlace de una web totalmente falsa buscando un pretexto.

RESUMEN

En el siguiente trabajo se aborda el tema de la seguridad de la información frente a amenazas cibernéticas buscando una estrategia de aseguramiento de la información a partir del análisis y gestión de riesgos en los procesos académicos y administrativos que pueden afectar las instituciones educativas de la ciudad de Bogotá. Mediante una consulta teórica y documental, se realizará la consulta y se pondrá en práctica una estrategia considerando la historia acerca de la ciberseguridad, delitos informáticos, y la seguridad de la información, donde se han evidenciado alertas durante la pandemia COVID-19, amenazas gubernamentales, institucionales, educativas, bancarias entre otras, el resultado no fue favorable teniendo en cuenta la mal praxis de las políticas de seguridad informática, estándares de calidad, tecnología obsoleta y de manera consciente se pretende dar a conocer los diferentes estados de riesgos para así poder determinar en cualquier institución el grado o el nivel del riesgo que se puede materializar mediante un análisis profundo y generar la forma de preservación de la infraestructura tecnológica y de comunicación en que están soportadas la operaciones.

PALABRAS CLAVES

Amenazas, confianza, confidencialidad, políticas, riesgos, salvaguardar.

ABSTRACT

Taking into account that overconfidence is one of the main risks of loss of information in any work or institutional field, it is important that companies or educational institutions make a periodic investment in computer security, as well as in qualified professional personnel in this area., a situation that carries a lower cost than facing a security incident of this style, because, even with current technology, it is very unlikely to recover 100% of the data.

The appropriate security policies within any entity for the information systems implemented, and that in general the corrective measures when they want to be implemented, in many cases it is already too late.

This guide offers computer security measures for the administrative and academic information systems of any educational entity, in order to reduce as much as possible and eliminate the risks, threats and vulnerabilities that have been identified, thus allowing to safeguard the computer resources of an institution and collaborating vertically with the institution in the adaptation of its academic and administrative objectives.

INTRODUCCIÓN

Indudablemente el avance de muchas actividades ilícitas presentadas a nivel institucional, se presentan por la falta de procesos informáticos y que en la actualidad se efectúan rápida y acertadamente, reflejan la importancia en que se aprovecha para el bien y el mal en distintos ataques cibernéticos, de ahí que la inseguridad informática crezca a la par y sea más común en los entornos educativos, se convierte en objeto vulnerable y de fácil ataque de los delincuentes informáticos, se mantienen al acecho buscando robar o dañar información.

El aseguramiento informático a los sistemas académicos, en cuanto a la identificación de vulnerabilidades y amenazas que se presentan en las instituciones educativas, tienen como propósito adoptar políticas apropiadas de seguridad al interior de una institución educativa, con el fin de ofrecer una mejora continua para la seguridad informática en los sistemas de información académicos de cualquier institución educativa, y poder reducir en lo posible mitigar o eliminar los riegos, amenazas y vulnerabilidades que se hayan identificado; permitiendo así salvaguardar los recursos informáticos de las instituciones educativas y restringiendo así la posibilidad de ataques informáticos.

Salvaguardar los recursos informáticos de una institución educativa mediante las amenazas identificadas implementando la norma ISO 27001:2013, una solución que permita investigar rápidamente cualquier actividad sospechosa y altamente maliciosa, a la vez, establecer la mejor manera de enfrentar y mitigar los incidentes.

1 DEFINICIÓN DEL PROBLEMA

En la última década los sistemas de información, utilizan un procedimiento de almacenamiento en una red mundial de servidores remotos conectados para funcionar como un único ecosistema, diseñados para almacenar y administrar datos, y poder ejecutar aplicaciones y facilitar contenidos o servicios, como vídeos, correo electrónico, software de ofimática, redes sociales.[1] La "nube" se utiliza para dar respaldo y copia de la información inmediata en un lugar seguro y de fácil acceso con el fin de recuperación y almacenamiento, gestión y aplicación de información personal y organizacional, de esta manera la información contenida se vuelve sensible para picaros, que vulneran el sistema seguro, robando, manipulando, dañando la información allí contenida, afectando a los usuarios.

Al poner en riesgo la información existente en correos electrónicos, redes sociales, archivos laborales, información de bases de clientes y proveedores, suplantación, pérdida de información estratégica del Estado, generan ansiedad y preocupación en el campo de la ciberseguridad.

En la ciudad de Bogotá, algunas instituciones educativas han sido víctimas de ataques cibernéticos por diferentes razones técnicas, este tipo de problemas se presentan en el campo institucional llámese colegios y/o universidades, instituciones en riesgo inminente, es la consecuencia del exceso de confianza, el desconocimiento de la implementación de políticas apropiadas de seguridad al interior de la Institución. Al interior de las instituciones los sistemas de información están implementados, pero no se hace el correcto seguimiento a las medidas preventivas y correctivas, lo cual conlleva a daños irreversibles al interior en su interior [2].

La seguridad en informática para las instituciones educativas acarrea un costo elevado, teniendo en cuenta que la implementación de tecnología actual la inversión puede ser considerable, generando costos no programados en su presupuesto.

El reciente estudio publicado consultados en revista semana en su sección de Economía "El año de los ciberataques en Colombia" Se registraron notoriamente

[1] AZURE. Que es la Nube. [en línea] Recuperado de https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-the-cloud

[2] LA FM. Colegios en Latinoamérica víctimas de ataques. John Mauricio Aguirre. [Blog] 28 de mayo de 2018. Recuperado de: https://www.lafm.com.co/tecnologia/el-67-de-los-colegios-en-latinoamerica-han-sido-victimas-de-ataques-ciberneticos

más de 23.000 noticias criminales, un 30% más que en el mismo periodo de 2020[3].

La violación de datos personales que se sitúa en el primer lugar, presentando un incremento del 108% con 6.649 denuncias instauradas. La suplantación de sitios web para capturar datos personales, esta modalidad opera bajo enlaces maliciosos para la difusión de códigos dañinos, que puede presentarse a través de phishing, smishing, o pharming y tuvo 2.825 denunciados ante la fiscalía general de la Nación[4].

El hurto por medios informáticos, registró más de 12 mil casos denunciados, el apoderamiento de credenciales para el acceso a servicios de banca online, suplantar al titular del producto bancario y apoderarse del dinero generalmente dispuesto en cuentas bancarias. La propagación de campañas de phishing que contienen archivos adjuntos maliciosos. Las entidades de gobierno con mayor presencia de trámites en línea también se vieron afectadas[5].

La Universidad de los Andes en el año 2015 en la ciudad de Bogotá, presentó el caso de un estudiante utilizando un software registrador de teclas (keylogger), realizando la captura de contraseña de todos los docentes para acceder al sistema de notas y así poder realizar modificaciones y alterarlas, suceden frecuentemente; prueba de ello es el reporte en vivo de ciberincidentes de la Policía Nacional de Colombia, el cual en un periodo de una media hora se evidencian 88 incidentes de seguridad para el Sector de la Educación[6].

Es muy relevante reconocer la importancia de la información que se gestiona, teniendo en cuenta que es uno de los activos más significativos para el funcionamiento de las instituciones educativas, los cuales puede ser de naturaleza operativa. Y por ende concientizar a los usuarios sobre este tipo de ataques.

---

[3] REVISTA SEMANA. Año del ciberataque en Colombia. [revista en línea] 2 de julio de 2021. Recuperado de: https://www.semana.com/economia/empresas/articulo/el-ano-de-los-ciberataques-en-colombia-estas-son-las-alarmantes-cifras/202125/

[4] PORTAFOLIO. Ataques cibernéticos en Colombia. [revista en línea] 8 de junio de 2021. Recuperado de: https://www.portafolio.co/tendencias/aumentan-en-30-los-ataques-ciberneticos-en-colombia-553803.

[5] PORTAFOLIO. Cifras de Ciberseguridad. [revista en línea] 10 de diciembre de 2020. Recuperado de: https://www.portafolio.co/tendencias/cifras-de-ciberseguridad-en-colombia-prenden-alarmas-al-cierre-del-2020-547412

6 UNIVERSIDAD SANTO TOMAS. Hurto por medios informáticos. Mihdí Badí Talero Magnin [Blog] Recuperado de: https://auditoriainterna.usta.edu.co/index.php/120-los-ataques-de-hacking-en-el-sector-educativo.

En la figura 1, se observa una evidencia de modalidad de ataques con sus respectivos porcentajes de incidencias.

Figura 1. Estadística de ataques 1

Fuente: Estadística Ataques cibernéticos: https://www.asuntoslegales.com.co/actualidad/los-ataques-ciberneticos-aumentaron-30-durante-el-primer-semestre-de-este-ano-3198212

1.1 ANTECEDENTES DEL PROBLEMA

Las instalaciones físicas de una institución educativa poseen en su mayoría la disponibilidad y acceso a terceros sin autorización a la red de datos, lo cual puede acarrear Problemas en el acceso a la información de las diferentes dependencias desde los entornos de red y de la información compartida entre los diferentes dispositivos ya que están en riesgo de ser obtenida por terceros sin autorización.

No disponer de políticas de seguridad y no disponer de un cronograma de procesos de Backup para salvaguardar la información de la institución, no disponer de un mapa de revisión y control de las actualizaciones de software y antivirus, no tener un responsable de hacer copias de seguridad y actualizaciones que se realizan de forma periódica y un control de las contraseñas de acceso a las conexiones WIFI que se comparten sin ningún tipo de control con docentes, estudiantes y padres de familia.

1.2 ESTADÍSTICAS SOBRE CIBERATAQUES A RECURSOS EDUCATIVOS.

Estudio realizado por Kaspersky, permite mostrar estadísticas muy importantes sobre los ataques que afectaron a los recursos educativos[7]:

Los recursos educativos afectados con ataques DDoS fue de un 350 y un 500% cifra mayor en febrero a junio del 2020 que en el mismo período en 2019.
La plataforma Zoom más utilizada para estos ataques, con un 5% de usuarios captados con archivos disfrazados bajo el nombre de Zoom. Otras plataformas que se vieron en la misma situación fueron Moodle, Google Class-room, Coursera, Google Meet, Blackboard y edx.

Las amenazas más frecuentes durante el 2020 fueron los descargadores y adware, con 98.77% del total en intentos de infección registrados.

La última actualización del estudio, relacionado a usuarios que se encontraron con amenazas, continuó ascendiendo desde junio de 2020 hasta lograr la cifra de 270.171 para enero de 2021, un 60% más en comparación al periodo de enero a junio de 2020[8].

1.3 FORMULACIÓN DEL PROBLEMA

Debido al problema inminente presentado en la ciberdelincuencia y ataques presentados a las instituciones educativas como colegios, de acuerdo a Informes de amenazas de distintas instituciones educativas en el año 2021 se examinan los eventos de seguridad cibernética más importantes del último año y los problemas que posiblemente afectarán al año próximo. este análisis se deriva de diferentes amenazas a las instituciones y de clientes a lo largo de 2020 y se presenta para beneficios de personas que atentan de manera inescrupulosa[9].

Es importante que la educación formal se acoja al proceso de educación de las nuevas generaciones. En este sentido, el sistema educativo de cada institución procura brindarles aquellos procesos y buenas prácticas no solo los conocimientos académicos elementales, sino también ayudarlos a desarrollar las habilidades para enfrentar diferentes situaciones de ataques cibernéticos teniendo en cuenta los desafíos de esta época. Partiendo de la base de que contar con esas habilidades es importante para los integrantes de una institución, la educación en seguridad informática, dado el rol que ocupa la tecnología en los tiempos actuales

[7] KASPERSKY. Estadísticas de Ciber ataques. [Blog] Recuperado de: https://latam.kaspersky.com/about/press-releases/2020_ataques-d-do-s-contra-recursos-educativos-aumentaron-mas-de-350-durante-el-primer-semestre
[8] WIDEFENSE. Estadísticas de Ataques. Kenneth Daniels. 20 de mayo de 2021 [Blog] Recuperado de: https://widefense.com/blog/los-ciberataques-contra-los-recursos-educativos-en-linea
[9] OBSERVATORIO CIBERSEGURIDAD. Riesgos, avances y el camino a seguir en América Latina y el Caribe. [Articulo] Recuperado de: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

y futuros, Por lo tanto, podría formar parte de la lista de habilidades esenciales del personal tanto administrativa como estudiantil y enfrentar los desafíos de la vida en el mundo cibernético[10].

¿Cuáles pueden ser las mejores prácticas de seguridad informática para la protección de la información en las instituciones educativas?

[10] WELIVESECURITY. Seguridad-informática ¿debería incluirse educación formal? Juan Manuel Harán. 18 de noviembre 2019. [Blog] Recuperado de: https://www.welivesecurity.com/la-es/2019/11/18/educacion-seguridad-informatica-deberia-incluirse-educacion-formal/

2 JUSTIFICACIÓN

Teniendo en cuanta las diferentes situaciones que se presentan a diario en las instituciones educativas, debido al desconocimiento de ciertos procesos que involucran y ponen en riesgo claramente los sistemas de información, software, redes de comunicaciones entre otros.

Hoy en día se ha podido apreciar, como diferentes Instituciones educativas como colegios ofrecen juntamente con su portafolio de servicios, la oportunidad de cargar, actualizar y consultar información en línea y en muchos casos su plataforma no cuenta con certificados de seguridad brindando no solo un servicio a los padres de familia, estudiantes y docentes, sino que también al mismo tiempo, se exponen a los diferentes ataques informáticos prolíferos en la internet.

Es así que de una u otra manera se pretende mitigar las vulnerabilidades y amenazas en las instituciones educativas con el propósito de adoptar políticas y procedimientos apropiados de seguridad al interior de una entidad. Resaltando de manera adecuado mediante unas políticas de seguridad y de endurecimiento de la plataforma y de su sistema de información, para evitar futuros ataques y evitar el riesgo reputacional de la institución.

Teniendo en cuenta la naturaleza de la entidad se pretende conformar un equipo auditor para el desarrollo del proyecto definiendo las tareas principales del líder del proyecto y entregar y dar a conocer los perfiles y responsabilidades e identificar las personas idóneas para tomar cada rol como:

- Personal de seguridad de la información.
- Un representante del área de Tecnología.
- Un representante de sistemas de Gestión de Calidad.
- Un representante del área de Control Interno.

Los ataques cibernéticos han ido en aumento significativamente en las instituciones educativas; más recientemente el ramsomware, con el nombre de WannaCry, golpeó algunas instituciones en Asia, donde hubo informes generalizados de ataques de este ramsomware en colegios, con estudiantes excluidos de sus tesis y trabajos finales cuando se avecinaba la graduación [11].

Las instituciones educativas son tan ricas en objetivos de ataques a menudo, como las escuelas y las universidades son entornos muy conectados, con tasas muy altas de intercambio de archivos. Cada día hay miles, incluso decenas de miles, de estudiantes, académicos y empleados que circulan y utilizan

[11] ACIS. Ataques a Instituciones educativas. Sophos. [Blog]. Recuperado de: https://acis.org.co/portal/content/escuelas-las-m%C3%A1s-afectadas-por-ransomware-el-60-fueron-atacadas-en-2021

computadoras portátiles, tabletas y teléfonos inteligentes para acceder a los datos institucionales cada minuto. Las redes utilizadas pueden ser wifis públicas no seguras, cuentas de datos personales de operadores locales o redes privadas específicas de un departamento. Cada uno de ellos tiene controles de seguridad independientes.

Un segundo factor que pone en mayor riesgo a las instituciones educativas es el hecho de que muchas de ellas tienen sistemas heredados. Muchas Instituciones han existido desde mucho antes del advenimiento de Internet, y aunque crecieron con la tecnología moderna, a menudo tienen enfoques anticuados de la seguridad. La cultura académica es la de compartir, lo que crea naturalmente un ambiente poroso.

El tercer factor principal y el de mayor preocupación es que las escuelas mantengan un rico fondo de información personal de los exalumnos y de valiosa investigación y propiedad intelectual y riesgo de que se piratee la información académica.

Es importante comprender el valor potencial que tiene la investigación académica y la propiedad intelectual. Aunque no es fácil de cuantificar, existe el prestigio y el respeto que las instituciones ganan cuando se logran avances dentro de sus departamentos y en sus campus. Esto es importante tanto para los esfuerzos de recaudación de fondos de los exalumnos como para atraer a los mejores estudiantes, un factor más concreto es el financiero.

En los Estados Unidos, la Ley Bayh-Dole de 1980 estableció por primera vez que se permitía a las universidades beneficiarse de la investigación financiada con fondos federales mediante la venta o concesión de licencias de descubrimientos de investigación a empresas.

Esencialmente, la ley creó una política universal de patentes entre las agencias federales que permite a las universidades retener el título de las invenciones. Desde entonces, éxitos espectaculares como la ganancia inesperada de 1.000 millones de dólares en regalías de Pfizer para Lyrica, su medicamento anticonvulsivo, han abierto los ojos de los cancilleres universitarios que esperan avances similares.

Sin embargo, la transferencia de tecnología no ha sido generalizada, por lo que las escuelas están comenzando a crear nuevas empresas basadas en la investigación, planes de estudios de la fuerza laboral específicos de la industria, investigación patrocinada por la industria y, en algunos casos, consultoría tecnológica, todo ello en un esfuerzo por atraer nuevas fuentes de ingresos. Todas estas iniciativas serán presa de los mismos ataques por parte de actores

malintencionados que utilizan malware para secuestrar material, ya sea para obtener un rescate o para cometer un robo total[12].

[12] MALWAREBYTES. Ransomware. [Blog] Recuperado de: **HTTPS://ES.MALWAREBYTES.COM/RANSOMWARE/**

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar las diferentes estrategias para la gestión de la seguridad de la información en las instituciones educativas, a partir de una revisión de las diferentes iniciativas normativas y estándares, que permitan asegurar la confidencialidad, integridad y disponibilidad de la información.

3.2 OBJETIVOS ESPECÍFICOS

- Evaluar las estrategias propuestas para garantizar la seguridad de la información en las instituciones educativas, a partir de una revisión de iniciativas de ciberseguridad que permita su reconocimiento y posible aplicación.

- Valorar las amenazas y riesgos más comunes que afectan la seguridad de la información de las instituciones educativas, mediante una valoración del impacto generado, para el establecimiento de los controles que reduzcan la probabilidad de impacto.

- Proponer una estrategia para la mitigación del riesgo en la seguridad de la información en instituciones educativas, a partir de la adopción de estrategias, normatividad, estándares y buenas prácticas, que permitan fortalecer la seguridad de la información.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

El presente trabajo tiene como resultados la realización de una estrategia de aseguramiento de la información a partir del análisis y gestión de riesgos en los procesos académicos y administrativos que pueden afectar las instituciones educativas de la ciudad de Bogotá para guiar y poder analizar y poder evaluar el nivel de seguridad de la información y sus procesos estratégicos en el tratamiento de la información basado en la ISO 27001. Por tal razón no podemos confundir seguridad de la información con seguridad informática, ya que este último sólo se encarga del medio informático, pero la información puede ubicarse en diferentes medios y formas, y no solo en medios informáticos.

En la seguridad de la información es importante señalar que su manejo está basado en la tecnología y es necesario saber que riesgos causar o exponer la información confidencial de una institución, como también se encuentra centralizada y puede tener una importancia. Puede ser divulgada, mal utilizada, ser robada, borrada o saboteada. Esto afecta su disponibilidad y la pone en riesgo. La información es poder, y se clasifica como:

- Crítica: Es la información indispensable de toda la operación de la empresa.
- Valiosa: Se considera un activo de la empresa y muy valioso.
- Sensible: Debe de ser conocida por las personas autorizadas Existen dos palabras muy importantes que son riesgo y seguridad:
- Riesgo: Es la materialización o vulnerabilidades identificadas, asociadas con su probabilidad de ocurrencia, amenazas expuestas, así como el impacto que ocasione a las operaciones de negocio.
- Seguridad: Es una forma de protección contra los riesgos.

Para así poder evaluar los riesgos y amenazas con el fin de mitigar la materialización del miso para poder determinar las vulnerabilidades y amenazas existentes en una institución y hacer una estrategia de aseguramiento de la información orientado a los procesos académicos y administrativos.

En la figura 2. Se evidencia el marco referencial de ciberseguridad que plantea el NIST en cuanto a los ataques cibernéticos.

Figura 2. Marco de Ciberseguridad 1

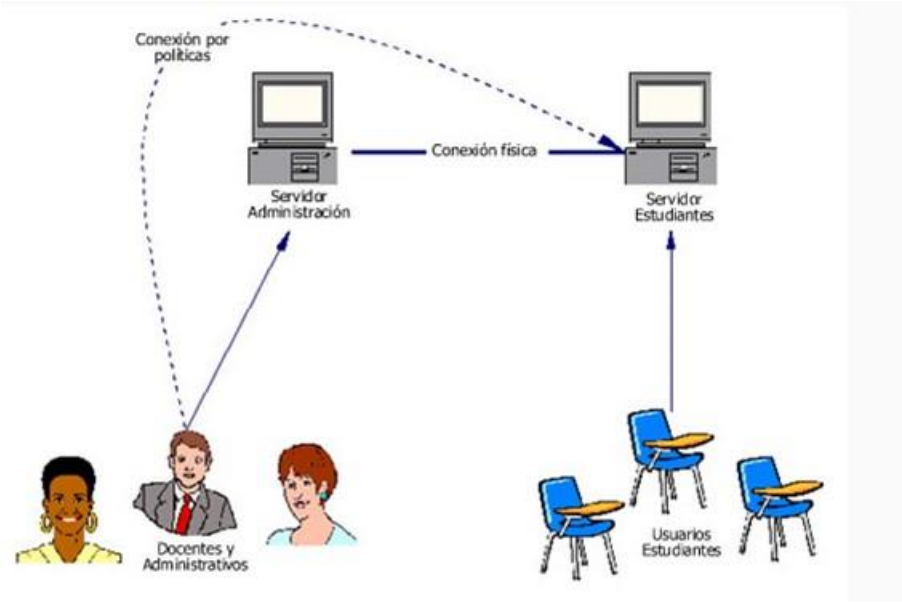
Fuente:https://www.cic.es/preparacion-respuesta-ataques-ciberneticos

Identificación.
Identificar cuáles son los servicios para poder iniciar primero y saber cuáles son las medidas a tomar para implementar Planes directos de Seguridad donde se puedan analizan las vulnerabilidades y los elementos críticos para planificar las contramedidas procedimentales con técnicas adecuadas y realizar lo siguiente:

- Ejecutar y controlar un plan de realización de backups.
- Administrar de manera adecuada el sistema de información.
- Crear un esquema de control de modificar o inactivar usuarios del directorio activo en la red.
- Crear, modificar o inactivar usuarios de VPN y Soporte de VPN
- Administrar y gestionar las cuentas de correo corporativo y listas de correo de la organización.
- Gestionar y actualizar la herramienta de inventario.

En la figura 3. Se muestra el esquema en cuanto a una estructura de una red educativa de manera local y lógica.

Figura 3: Estructura lógica de una red 1



Fuente: https://eduteka.icesi.edu.co/articulos/RedEscolarDatos

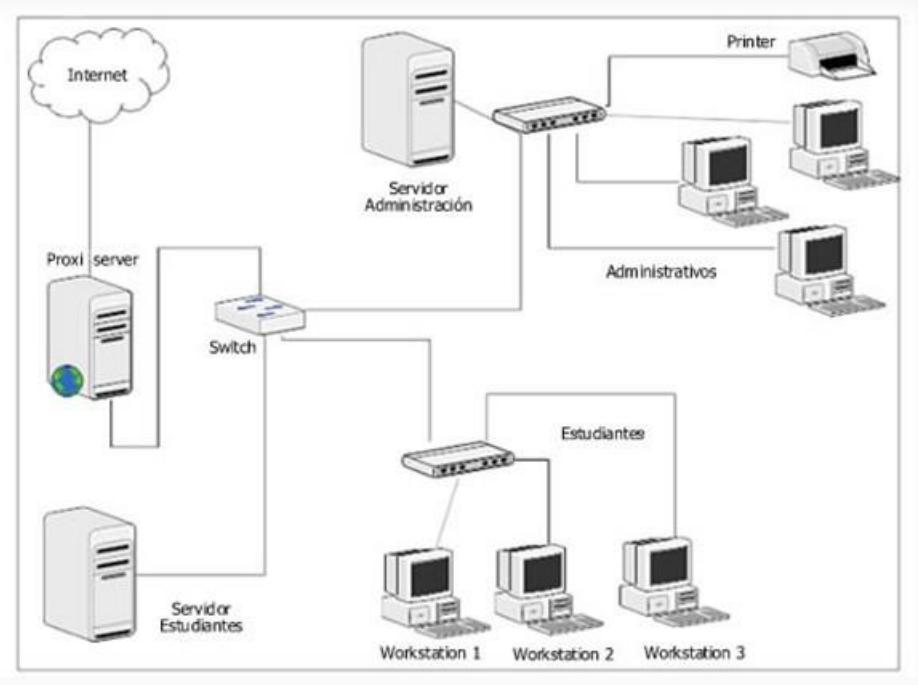
Protección:
Es importante realizar medidas técnicas, firewalls, seguridad de red, antivirus, elementos perimetrales, hacking ético, test de penetración, acciones de Red, donde un equipo atacante ficticio pueda realizar un ataque totalmente simulado para ver si es capaz de penetrar en la organización y ver cuánto daño puede hacer a la formación y la concienciación en un punto muy importante a tener en cuenta en la ciberseguridad, teniendo en cuenta que el eslabón más débil son las personas, ya que si hay alguien que haga clic en un phishing surgen importantes problemas.

- Restringir por completo el acceso de los estudiantes al servidor Administrativo de la institución.
- Instalar en la red escolar de datos dos servidores interconectados: uno para Estudiantes y otro para personal Administrativo.
- Habilitar el ingreso a los usuarios del servidor Administrativo con directorio activo diferente al que utilizan los estudiantes.
- Instalar un administrador de acceso a Internet como firewall para toda la red.
- Controlar el acceso de los estudiantes a servicios públicos de Chat, como a la instalación de aplicaciones free.
- Instalar en el servidor dedicado a Internet dos tarjetas de red: Una para el acceso a Internet y otra para la red LAN.
- Controlar, si es necesario y estableciendo límites de tiempos y horarios específicos de conexión.

- Asignar a los usuarios administrativos un espacio de almacenamiento Ej: 20 MB para cada uno.
- Crear una carpeta pública (común), en el dominio Administrativo, que permita solo el acceso a funcionarios y profesores de la institución.
- Crear una relación de confianza de una vía entre los dos dominios para que desde el dominio Administrativo se pueda ingresar al dominio Estudiantes.

En la figura 4. Se muestra la estructura y planteamiento de seguridad de una red educativa.

Figura 4: Estructura lógica de protección 1



Fuente: https://eduteka.icesi.edu.co/articulos/RedEscolarDatos

Detección:
Es muy importante la monitorización constante en la ciberseguridad, implementación y poder realizar eventos como detectores de ataques de red utilizando herramientas adecuadas para este tipo de amenazas[13].

- Tener programas de seguridad
- Mantener todo actualizado

[13] CIC. Ataques Cibernéticos. [Blog] 18 de noviembre de 2021. Recuperado de: https://www.cic.es/preparacion-respuesta-ataques-ciberneticos/

- Descargar de fuentes fiables
- Tener mucho cuidado a correos no deseados y desconocidos (Spam).

Muchos ataques provienen de la interacción del usuario por omisión. Por tal razón, la mayoría de descarga de archivos maliciosos o ataques Phishing. Por lo tanto, debemos tener siempre presente este tipo de acciones al abrir archivos adjuntos en correos desconocidos o no deseados.

Respuestas:
La recogida de evidencias es importante ante cualquier ataque, como peritaje forense y judicial. hay que tener bien claro y saber cómo hay que gestionar la crisis y recolectar las evidencias como elementos probatorios.

Objetividad:
El objetivo, debe observar los códigos de ética profesional.
Autenticidad y conservación: Mediante la investigación, tener en cuenta que la autenticidad e integridad de los medios probatorios se debe conservar.

Legalidad:
Se debe ser preciso en las observaciones y cumplir con los requisitos establecidos y ser coherente con opiniones y resultados.

Idoneidad:
Todos los medios probatorios deben ser relevantes, auténticos y suficientes para el caso.

Inalterabilidad:
Es necesario establecer una custodia debidamente asegurada que se demuestre que los medios no han sido modificados durante la pericia.

Documentación:
Se Deberá establecerse totalmente por escrito los pasos y procedimientos realizados en el procedimiento pericial.

Recuperación:
Es necesario tener en cuenta la ejecución de planes de Recuperación de desastres, Para poder tener un tiempo de respuesta ante un incidente o ataque, donde se pueden recuperar los datos perdidos y realizar un informe post incidente. Y tratar de dar parte de tranquilidad y en caso de materialización de un incidente, que sea el seguro el encargado de dar cobertura.

- Estudiar el incidente
- Utilización de la herramienta adecuada
- Aplicar la tecnología
- Analizar la infraestructura

- Ejecutar el plan de recuperación
- Restauración de datos

En la figura 5. Se muestra el esquema de recuperación o planes de Recuperación de desastres, Para poder tener un tiempo de respuesta.

Figura 5: Estructura Plan de Recuperación 1

Fuente https://www.shutterstock.com/es/search/information-recovery

4.2 MARCO CONCEPTUAL

Mediante las Especificaciones de la ISO/IEC 27001:2013 y los requisitos necesarios para, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI). Abarca:

Organización de la seguridad de la información:
Organizar la información para lograr el fin que se pretende y poder realizar una auditoría que le permita a una institución evaluar todos sus sistemas de información, desde los centros de información, hasta el hardware y software de la institución, brindando así sistemas confiables y una buena política de seguridad.

Gestión de activos:
Calcular el riesgo para cada activo a partir de la probabilidad que la amenaza se materialice y el impacto de este se menor.

Control de acceso:
Determinar los riesgos de accesos de zonas restringidas no autorizadas e identificado y clasificar las amenazas que se presenten a un impacto en caso de que un riesgo se materialice y poder controlarlo.

Seguridad de los recursos humanos:

Realizar capacitación periódica al personal como evaluar, verificar y recomendar, temas relativos a la planificación, control de la seguridad y adecuación para mejorar el servicio informático en la Institución.
Seguridad física y del entorno:
Enfocar los procedimientos físicos informático adecuados en vista a mejorar la seguridad en cuanto a la seguridad perimetral como implementación de alarmas y cortafuego para la seguridad en la información.

Gestión de la continuidad del negocio:
Permitir mantener planes adecuadamente priorizados, coordinados y probados como realización de backup, antivirus y actualizaciones en los sistemas operativos tanto de pc como de servidores.

4.3 ANTECEDENTES O ESTADO ACTUAL

La empresa Symantec destaca que el 4,2% de los ataques cibernéticos de América Latina y el Caribe durante el 2013, ocurrieron en Venezuela; país que tuvo una infección por malware del 23% en el total de computadoras analizadas. Así mismo registró el 5% del total de spear phishing suscitado en la región.

Durante el año 2015 y 2016, algunas compañías como “Viajes SIS”, presentaron pérdidas económicas más o menos de $50.956.220, dependientes de diferentes fraudes identificados como de invasión de cuentas, dichos fraudes por tele mercadeo y también la fuga se determinó por falsificación de banda magnética, entre otros. Por lo tanto, el trabajo se trazó como propósito determinar la estrategia que debe seguir la compañía “Viajes SIS” para fortalecer e implementar los controles que le permitan mitigar riesgos asociados a fuga de información, fraudes, deterioro de la imagen corporativa, Phishing, con el fin asegurar y proteger los procesos de la entidad.

Estos antecedentes, y formulación del problema en cuanto a su justificación y sus objetivos trazados por la entidad no tuvieron el alcance y fundamentos legales desde los cuales se tomó un punto de referencia para el abordaje de un fraude materializado y la metodología en cuanto a recursos físicos, humanos e institucionales que no realizaron un control para prevenir este riesgo materializado.

Recomendaciones para el control del riesgo Técnico:

- Aumento en la eficiencia de la gestión de los sistemas TI
- Mejoras frente a posibles amenazas contra los sistemas e información confidencial.
- Controles adecuados a nivel de sistemas de la compañía

- Lograr una adecuada segregación de funciones en los diferentes sistemas, bases de datos y servidores. Económico
- Conocer y robustecer los controles existentes, para mitigar la materialización de riesgos como fraudes internos, teniendo en cuenta los datos estadísticos presentados para el 2015 y 2016
- Disminuir los casos de fraudes internos y externos y así reducir las pérdidas económicas.

Importancia de proteger a las escuelas del riesgo cibernético:
Las actuales vulnerabilidades de las instituciones educativas al riesgo cibernético son tan significativas, porque no solo está en juego el robo de identidad, la privacidad de la salud y violaciones a la propiedad intelectual, por nombrar algunos, sino que también se suma la reputación de la empresa y la exposición del grado de responsabilidad que ésta tiene para con los estudiantes, planta docente, colaboradores, padres de familia, entre otros.

Las Instituciones educativas, como cualquier otro tipo de organización, no puede estar expuesta a ningún tipo de ciberdelito. Porque aun cuando se esté retornando a la prespecialidad, no hay certezas de que no se vuelva más a los confinamientos y, con ellos, a la virtualidad. Esto sin dejar de lado que la sociedad, ante la experiencia de la virtualidad, está optando por continuar con algunas de las actividades por estas vías por la conveniencia que le significa. La educación también forma parte de este proceso.

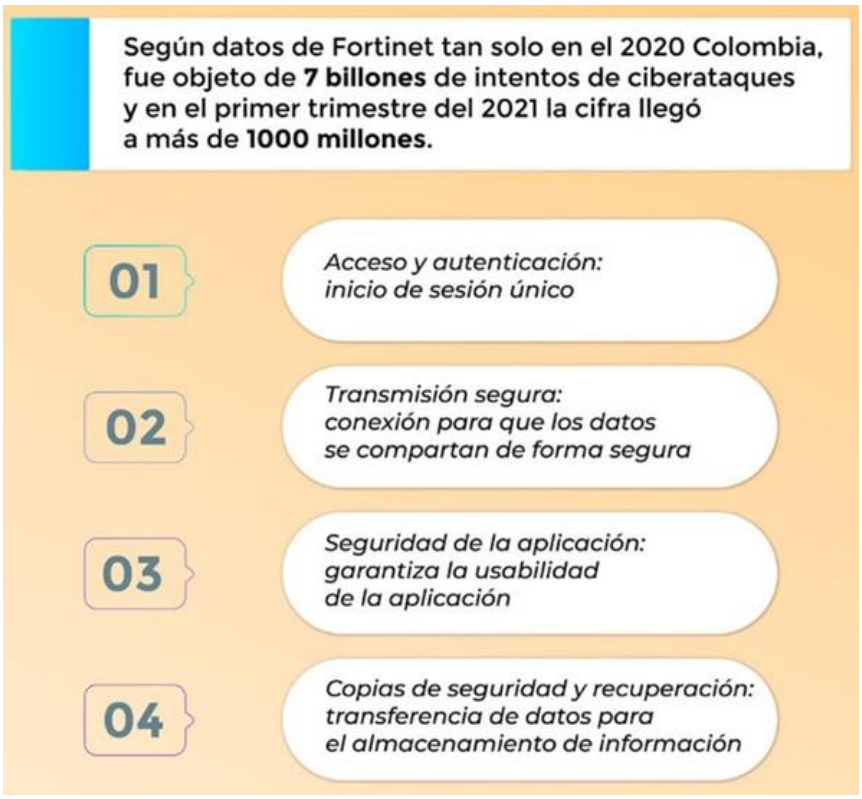
De ahí la necesidad de plantear el tema de la resiliencia de la red, también en el ámbito educativo, y de priorizar a la ciberseguridad en los diseños de las redes de telecomunicaciones. Y así como los gobiernos hoy discuten planes para llevar conectividad al ámbito escolar, también es necesario que lo planteen en el marco de una estrategia de ciberseguridad. Porque si es necesario construir redes, lo es también que sean resistentes frente a ataques o intrusiones, a gestión de desastres, que cuenten con sistemas de respaldo y de recuperación, y con elementos redundantes para que haya continuidad en la educación. Y seguridad para los estudiantes[14].

Lo importante para las instituciones educativas es estar protegidos del acceso a ciberdelincuentes, que afecten la educación en línea a los ciberataques contra los recursos educativos, por tal razón recomienda dos caminos para protegerse. El primero relacionado a la educación en ciberseguridad dirigido a los usuarios a través de persona, además, utilizar una de las herramientas de protección de dispositivos endpoint, más poderosa del mercado.

[14] METODOLOGÍA PARA LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA. [Documento en línea] Recuperado de: https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf

En la Figura 6. Se muestran los principales intentos de ataques cibernéticos

Figura 6: Datos de intentos de ciberataque 1



Fuente: Datos de intentos cibernéticos: https://revistaedu.co/secciones/tematicas-educativas/los-retos-de-seguridad-informatica-que-enfrentan-las-instituciones-de-educacion-en-colombia/2660/

Mediante estos cuatro procesos asegurar la confidencialidad, integridad y disponibilidad de la información con un apoyo tecnológico que se han convertido en los ejes principales a garantizar al interior de cualquier organización. actualmente, el sector educativo tiene el desafío de evitar la vulnerabilidad, fortalecer el acceso, monitorear y garantizar la gestión adecuada, reduciendo las posibilidades de ser siempre víctimas de ataques cibernéticos.

Este tipo de riesgos desafían a la tradicional seguridad física, como lo son los campus, las edificaciones o simplemente el personal de las instituciones. Lamentablemente esto se ha convertido en oportunidades para la puesta en marcha de protocolos de seguridad de la información a través de pasos como la autenticación, la estructura, la secuencia y el cifrado de datos en las organizaciones.

4.4 MEDICIÓN Y EVALUACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN.

Determinar en la institución educativa donde se recomendarán metodologías de medición del Riesgo en forma cualitativa o cuantitativa. Dichas metodologías que deben ser revisadas como mínimo una vez al año, para determinar si miden apropiadamente la probabilidad de ocurrencia del riesgo y su impacto en caso de materializarse el riesgo, frente a cada uno de los factores de incidencias y los riesgos asociados[15].

En la Figura 7. Se muestra gráficamente el proceso del tratamiento del riesgo.

Figura 7: Tratamiento del riesgo 1

Fuente: https://www.normas-iso.com/wp-content/uploads/2012/02/EvaluacionRiesgo.png

La identificación de riesgos será plasmada en los mapas de riesgo o mapas de calor. Este mapa es la representación o descripción de los distintos aspectos tenidos en cuenta en la valoración de los riesgos. Para la elaboración de estos mapas se define un riesgo como un evento determinado por una probabilidad y un impacto específico, por lo que es necesario clasificar el evento dentro de una matriz.

Gestión de los Riesgos: Se debe determinar un tratamiento según los diferentes niveles en el sistema de Gestión de Seguridad y los riesgos asociados a la

[15] NORMAS ISO. Metodologías de medición del Riesgo. [Blog] Recuperado de: https://www.normas-iso.com/iso-27001/

Información según la (ISO:27001) para una garantizar una adecuada gestión de la seguridad de la información en la institución educativa.

Un Sistema de Gestión de Seguridad de la Información se encuentra basado en la norma ISO-27001. Este estándar internacional presenta un sistema de gestión basado en el ciclo de planificar, Hacer, Verificar y Actuar, cuyas siglas en inglés son PDCA. Y la implementación de un Sistema de Gestión que se centra básicamente en la mejora continua.

PLANIFICAR. Definir la política de seguridad y establecer al alcance del SGSI y realizar el análisis de riesgo para seleccionar los controles y definir competencias mediante un mapa de procesos con autoridades y responsabilidades.

HACER: Implantar el plan de gestión de riesgos basada en el SGSI e Implantar los controles

CONTROLAR: Revisar internamente el SGSI para realizar auditorías internas del SGSI y Poner en marcha indicadores y métricas para hacer una revisión por parte de la Dirección

ACTUAR: Adoptar acciones correctivas y adoptar acciones de mejoras[16].

En la figura 8. Se Puede observar el procedimiento lógico y por etapas que permite el mejoramiento continuo del SG-SST del esquema del ciclo PHVA.

[16] NORMAS ISO. Metodologías de medición del Riesgo. [Blog] Recuperado de: https://www.normas-iso.com/iso-27001/

Figura 8: Mapa del tratamiento del ciclo 1

Fuente: PHVA: https://safetya.co/phva-procedimiento-logico-y-por-etapas/

4.5 MARCO LEGAL.

El marco legal de la norma ISO 27001:2013, garantiza que las organizaciones cumplan con los requisitos establecidos por la NTC ISO27001 y además se cumpla de un modo complementario con las buenas prácticas y controles definidos por la ISO 27002, que hace posible que las organizaciones aseguren la confidencialidad y al mismo tiempo la integridad de toda la información que tengan y comprender los requisitos de seguridad de la información de la institución y la necesidad de establecer la política y objetivos en relación con la seguridad de la información[17].

La ISO/IEC 27000:2 permite aplicar un conjunto de estándares desarrollados por ISO (Organización internacional de Estandarización) e IEC (Comisión electrotécnica internacional), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

Algunas de las normas que conforman la serie ISO/IEC 27000 van encaminadas precisamente a documentar mejores prácticas en estos aspectos, y orienta en la adaptación de disposiciones concretas como la norma ISO/IEC 27001, que indica qué requisitos deben conformar un SGSI, pero no estipula cómo cumplirlos.

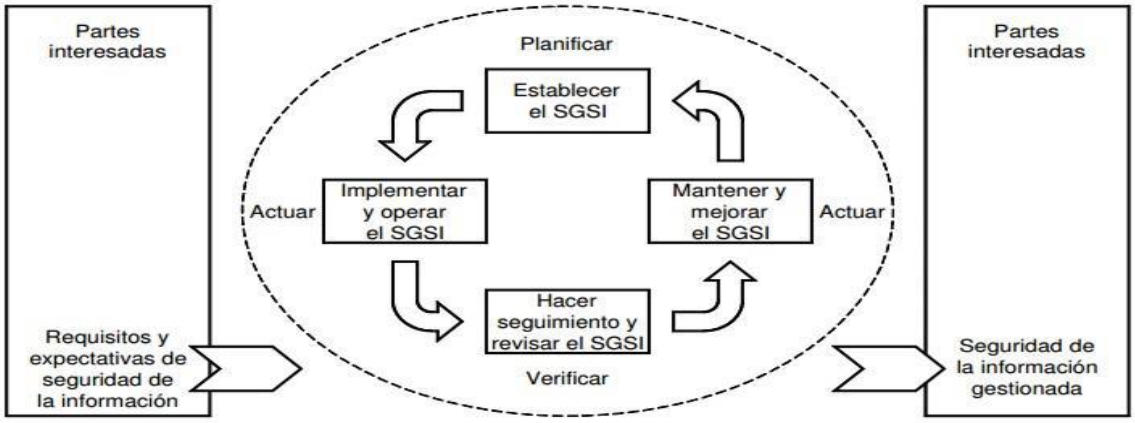
[17] DOCPLAYER. Marco legal. [Blog] Recuperado de: https://docplayer.es/7982301-Norma-tecnica-ntc-iso-iec-colombiana-27001.html

Gracias a esta implementación se posibilita obviar la redundancia en la definición de requisitos, con un valioso ahorro de tiempo en la implantación del SGSI.

La implementación de un SGSI intenta ajustarse en su totalidad a las necesidades y expectativas que exigen las organizaciones hoy en día, por ejemplo, una situación simple requiere una solución de SGSI simple. A la par se puede usar para evaluar la conformidad de las partes interesadas, tanto internas como externas.

En la Figura 9: Se muestra la implementación de un SGSI a la Norma 1

Figura 9: implementación de un SGSI 1



Fuente: Norma Técnica NTC-ISO/IEC colombiana 27001:2013

Esta norma busca proponer un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI), convirtiéndose en una decisión estratégica para las organizaciones que desean proteger sus activos de los sistemas de información.

OBJETIVO GENERAL

Analizar las diferentes estrategias para la gestión de la seguridad de la información en las instituciones educativas, a partir de una revisión de las diferentes iniciativas normativas y estándares, que permitan asegurar la confidencialidad, integridad y disponibilidad de la información.

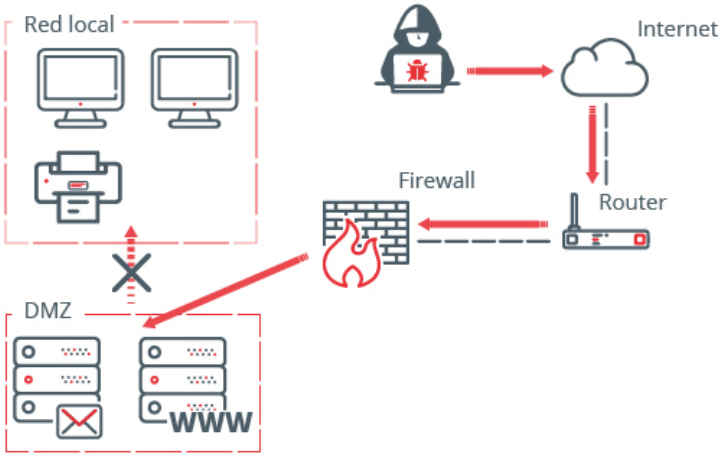
OBJETIVOS ESPECÍFICOS

Evaluar las estrategias propuestas para garantizar la seguridad de la información en las instituciones educativas, a partir de una revisión de iniciativas de ciberseguridad que permita su reconocimiento y posible aplicación.

Evaluar una estrategia de defensa en profundidad donde se implemente el uso de la seguridad perimetral como cortafuegos y creación de DMZ mediante las opciones de configuración del cortafuego, estableciendo en la red que se conecta a un puerto distinto, así como políticas de seguridad efectivas y el uso de soluciones para la detección de intrusiones,

En la Figura 10. Se muestra el esquema de una DMZ,

Figura 10: Estructura normal de una DMZ 1



Fuente: Zona desmilitarizada: https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa.

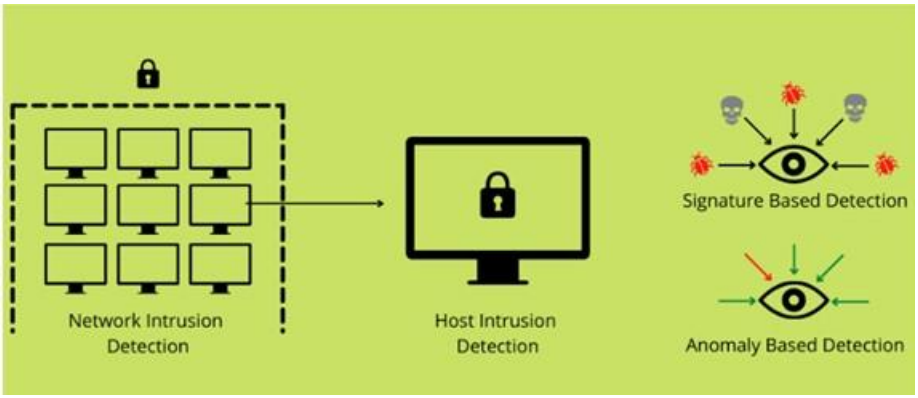
Proponer programas de formación, respuesta ante incidentes y mecanismos para garantizar la seguridad física y mecanismos para la monitorización y alerta de incidentes. Para que de esta manera existan salvaguardas y poder mitigar fallas que existirán y mantendrán el riesgo en niveles aceptables.

- Autenticación de forma correcta usuarios y equipos.
- Aplicar Controles de acceso.
- Implantar IDS/IPS que detectan actividades sospechosas o no autorizadas.
- Implementar Uso de cifrado.
- Adoptar Uso de firmas digitales.

- Segregación de redes/dispositivos.
- Escaneo de vulnerabilidades.
- Monitorización de la actividad de los equipos y de la red.

En la Figura 11: Se muestra el esquema de un sistema de detección de intrusiones (IDS) en seguridad,

Figura 11: Sistema de detección 1



Fuente: https://geekflare.com/es/ids-vs-ips-network-security-solutions/

- Aplicar habilidades, conocimientos, herramientas y técnicas aplicada a las actividades propias, de manera que se cumplan las expectativas de seguridad
- Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación de la entidad.
- Generar un respectivo cronograma para la implementación del Modelo de Seguridad y privacidad de la información.
- Planear y hacer seguimiento a las tareas, con fechas, respectivos costos y plan de trabajo de los objetivos definidos.
- Gestionar en el proyecto de la entidad, definiendo roles, responsabilidades que cada usuario debe entregar a con tiempos definidos.
- Coordinar todas las actividades diarias del equipo y así proporcionar un apoyo administrativo
- Cumplir con la implementación del Modelo de Seguridad y privacidad de la Información para la entidad[18].

[18] MIN-TIC. ROLES Y RESPONSABILIDADES. Seguridad y Privacidad de la información. [Documento en línea] Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf

Determinar las medidas y técnicas utilizadas para controlar y salvaguardar la información que se manejan dentro de la institución educativa y poder identificar una fuga o daño de información en el sistema de seguridad de la información estableciendo. Además, una pieza clave para que las instituciones puedan actualmente llevar a cabo sus operaciones con el minino o ningún riesgo, ya que la información manejada es esencial y considerada como el activo más importante para la actividad que desarrollan, es importante establecer los roles y responsabilidades.

Evaluar responsabilidades y los roles que dependerán de las metas establecidas para cada una y diferentes actividades, que van a desarrollar los roles y responsabilidades de los funcionarios encargados de desarrollar la implementación de los objetivos, para elegir de forma eficiente y adecuada un responsable en el proceso o medida de seguridad de la información, las funciones de cada rol asignas al personal de la entidad. Debe contar con una constante vigilancia en cuanto al ejercicio asignado en cada uno ya que, en el momento de la ejecución de las tareas, se debe generar un sobredimensionamiento de las actividades, es así que se pueda garantizar primordialmente cada una de las funciones realizadas y también el análisis minucioso del desarrollo de cada uno de los roles independientes[19].

Determinar en cuanto a las responsabilidades de las personas o la persona responsable de la seguridad de la información y los datos en una institución y se debe tratar de implementar políticas de cara a proteger diversas cuestiones como los sistemas, las comunicaciones o los activos de la institución de las posibles amenazas tanto internas como externas.

El responsable de la Seguridad de la Información de la institución no necesariamente tiene que delegarse a un funcionario de la institución, sino que puede delegarse o tercerizarse mediante una organización externa competente y profesional en el tema, no obstante, es necesario que la institución nombre a un responsable que vigile el proceso en cuanto a la seguridad que mediante a sus funciones asignadas tenga en cuenta lo siguiente.

- Listar las medidas de seguridad y organizativas.
- Identificar los riesgos de proveedores o de terceros.
- Adquisición para determinados productos o de servicios de seguridad.
- Planificación para el aseguramiento de la continuidad de operaciones.
- Implementar un análisis de riesgos y de la gestión de los mismos.
- Implementar los planes para las mejoras continua.
- Asegurar las interconexiones de sistemas que sean necesarias.

[19] MIN-TIC. ROLES Y RESPONSABILIDADES. Seguridad y Privacidad de la información. [Documento en línea] Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf

En la figura 12: Se simboliza y se muestra la seguridad la responsabilidad de la información.

Figura 12: Responsabilidades en la seguridad 1

Fuente: https://letslaw.es/el-responsable-de-la-seguridad-de-la-informacion/

Mediante el esquema de la implementación de la seguridad de la información es importante tener en cuenta el motivo de la publicación del Real Decreto 43/2021, donde regula la denominada “Ley NIS”, de seguridad de las redes y sistemas de información.

Valorar las amenazas y riesgos más comunes que afectan la seguridad de la información de las instituciones educativas, mediante una valoración del impacto generado, para el establecimiento de los controles que reduzcan la probabilidad de impacto.

Identificar las acciones para la prevención de los riesgos y amenazas y poder evitar aquellos incidentes que existen y controlarlos, evitando así que una eventualidad o desastre que provoquen daños en el sistema de información se materialice, y garantizar que se mantengan los tres principios de la triada CID. Es importante conocer las vulnerabilidades y amenazas que se centran sobre la información y encontrar algunos de los riesgos netamente básicos que pueden afectar a algunos de los principios de la triada que puede generar pérdidas tanto económicas Legal o físicas para la información.

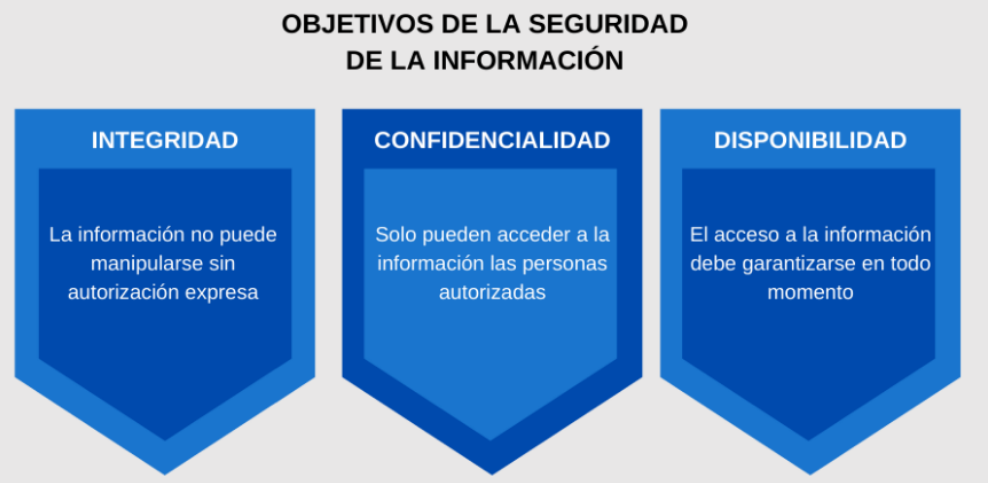
Confidencialidad.
Controlará el riesgo que permite que la información sea divulgada a terceros o entidades o personal no autorizados, de manera que exista un control donde solo

puede acceder a ella aquellas personas que cuenten con la debida autorización y de forma netamente controlada.
Integridad.
Vigilar Si el activo o la información que se maneja en la institución son alterados sin autorización ya que puede generar sanciones de las entidades de control y poner en tela de juicio y riesgo a la Imagen Institucional, Si el activo o la información son alterados sin autorización puede afectar la disponibilidad Financiero o la información requerida para la debida administración y toma de decisiones.

Disponibilidad.
Revisar permanentemente los activos de información como regulaciones impartidas por control para asegurar la disponibilidad de la información en la institución, con el fin de tener permanente la seguridad y el hábito de salvaguardar la información y adoptar medidas de seguridad que se pueda acceder a la información en cualquier momento necesario sin ninguna interrupción [20].

En la figura 13: Se muestra el objetivo de la seguridad de la información de manera esquemática.

Figura 13: Seguridad de la información 1



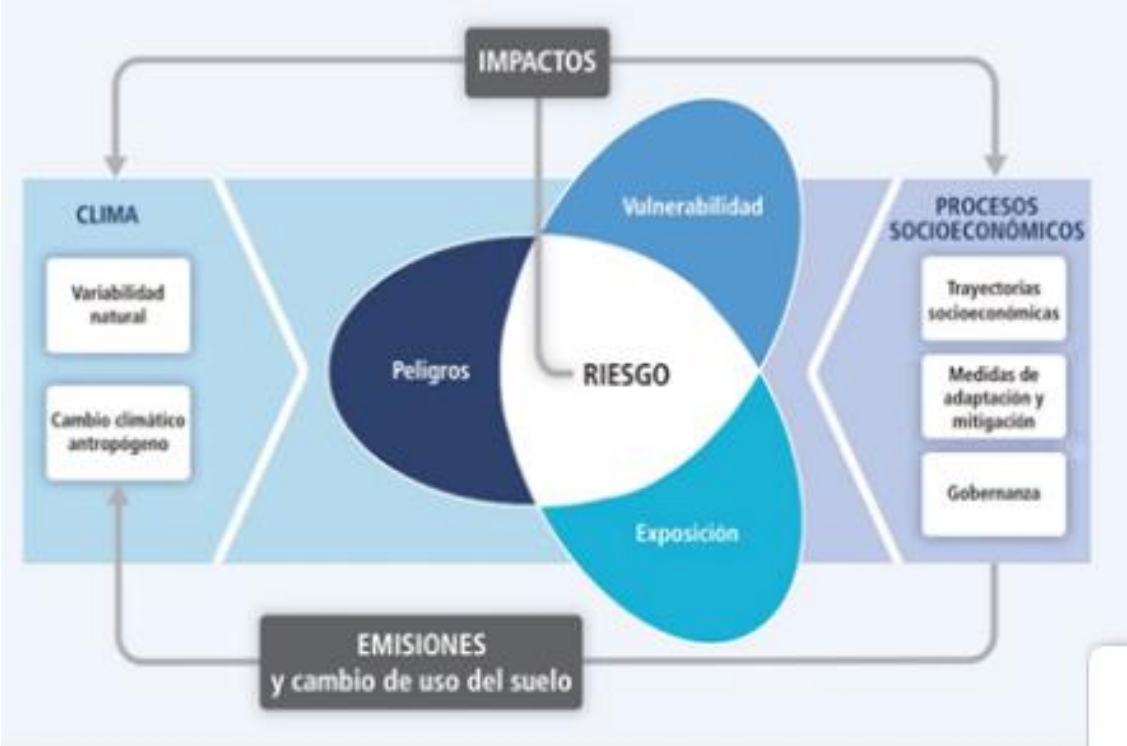
Fuente: Seguridad de la información: https://ayudaleyprotecciondatos.es/2020/07/14/seguridad-de-la-informacion/#Que_es_la_seguridad_de_la_informacion_Definicion_y_Conceptos_basicos

[20] Ayudaley. Objetivos de la seguridad de la información. 14 de julio de 2020. [Blog]Recuperado de: https://ayudaleyprotecciondatos.es/2020/07/14/seguridad-de-la-informacion/#Que_es_la_seguridad_de_la_informacion_Definicion_y_Conceptos_basicos

Es muy importante tener en cuenta las vulnerabilidades o predisposiciones en que se puede ver afectado negativamente la información y los aspectos que conforman la vulnerabilidad ya que son muchos, pero en los sistemas humanos están relacionados con las condiciones sociales. La falta de infraestructura y recursos para enfrentar, y luego reducir las consecuencias o eventos que afecten los recursos de un sistema.

En la figura 14. Se observa lo relacionado con las condiciones sociales. La falta de infraestructura.

Figura 14: Eventos del riesgo 1



Fuente: https://www.minambiente.gov.co/cambio-climatico-y-gestion-del-riesgo/amenaza-vulnerabilidad-y-riesgo-desde-la-tercera-comunicacion-nacional-de-cambio-climatico/

De acuerdo a lo plasmado anteriormente, dentro de contexto del Modelo de Seguridad y Privacidad de la información, un tema muy importarte, es la Gestión de riesgos la cual es utilizada para la toma de decisiones. Por otra parte, Teniendo en cuenta que el contexto organizacional de esta guía aseguramiento de la información y en sí, las instituciones educativas, y la metodología en la cual se enfoca los diferentes modelos del Riesgo es buscar una integración a lo que se pretende desarrollar divulgar en una entidad educativa es buscar un modelo de

Gestión de riesgo, y de este modo aprovechar el trabajo en la identificación del mismo para ser complementados con los Riesgos de Seguridad[21].

Para la evaluación de riesgos en seguridad de la información, es muy importante la clasificación de activos de información y realizar la gestión de riesgos ya que se consideran con nivel de clasificación dependiendo de los criterios de clasificación; es decir: Confidencialidad, Integridad y Disponibilidad y se tengan en cuenta las siguientes calificaciones:

En la figura 15. Se observa la relacionados el criterio de clasificación del riesgo.

Figura 15: Criterios de clasificación 1

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

- Definir acciones de control para prevenir daños futuros en el sistema de la institución
- Identificar las acciones de preparación para enfrentar un eventual desastre
- Llevar a cabo una evaluación básica de riesgos en cuanto a las amenazas

Amenazas:
Evaluar la importancia de tener en cuenta la norma ISO 27001, en donde a través de una adecuada practica poder establecer de forma consciente el estado de la seguridad de la información en la organización y apoyarse mediante la norma 27001 para un mejor tratamiento de las diferentes amenazas y adecuar un proceso de mejora continua, para poder obtener un control de auditoría en la institución educativa y mejorar sus procesos y alcanzar un excelente estándar de calidad.

[21] MIN-TIC. ROLES Y RESPONSABILIDADES. Seguridad y Privacidad de la información. [Documento en línea] Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf

- Falla de fábrica en hardware o software
- Daños o falla en suministro eléctrico y equipos de regulación eléctrica, que pueden ocasionar daños en el dispositivo.
- Aumento de temperatura en la sala donde se ubican los equipos.
- Inicio de sesión no autorizado.
- Perdida de confidencialidad de información, por permitir acceso de terceros a una red sin segmentar.
- Instalación de software no autorizado.
- Parches de actualizaciones de seguridad sin instalar.
- Daños falla en suministro eléctrico y equipos de regulación eléctrica, que pueden ocasionar daños en el dispositivo
- El equipo no se encuentra en una zona segura.
- Equipo abierto a manipulación de terceros, lo que puede ocasionar que se conecten al dispositivo e ingresar alguna carpeta compartida no regulada dentro del mismo segmento.

Es importante adecuar un plan de acción para este tipo de amenazas y así poder mitigar el riesgo:

- Determinar las Causas potencial de un incidente no deseado, que puede causar daños a un sistema o a la institución.
- Conocer cuál es el fenómeno de origen natural o humano que amenazan
- Analizar un adecuado control en los procesos de auditoría para atacar sus riesgos y determinar diferentes amenazas.
- Identificación de vulnerabilidades y amenazas sobre los activos asociados a la información, así como su respectivo impacto.
- Definición de los riesgos de seguridad.
- Establecer la cuantificación de la probabilidad de ocurrencia del riesgo y el impacto que puede generar para la organización la materialización del riesgo.
- Construir la matriz de riesgos inherente.
- Diseñar el plan de tratamiento y gestión de riesgos de seguridad de la información[22].

Proponer una estrategia para la mitigación del riesgo en la seguridad de la información en instituciones educativas, a partir de la adopción de estrategias, normatividad, estándares y buenas prácticas, que permitan fortalecer la seguridad de la información.

[22]CONEXIÓN ESAN. Las cuatro etapas para la mejora continua en la organización. [Blog] Recuperado de: https://www.esan.edu.pe/conexion-esan/las-cuatro-etapas-para-la-mejora-continua-en-la-organizacion/

Se llevará a cabo la propuesta estratégica de la planificación del manejo y mitigación del riesgo que afectan la seguridad de la información mediante la adopción de diferentes fases:

- Fase Diagnostico: En esta fase se permite identificar el estado actual de la institución educativa con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.
- Fase Planificación (Planear): En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los riesgos.
- Fase Implementación (Hacer): En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas y aterrizadas.
- Fase Evaluación de desempeño (Verificar): Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.
- Fase Mejora Continua (Actuar): Se analizarán los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones[23].

En la figura 16. Se muestra el esquema de la estrategia de implementación

Figura 16: Ciclo de Estrategia 1

Fuente: https:/www.mintic.gov.co/gestionti/615/articles5482_Modelo_de_Seguridad_Privacidad.pdf Bogotá

[23] MIN-TIC. ROLES Y RESPONSABILIDADES. Seguridad y Privacidad de la información. [Documento en línea] Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf

En cuanto a los resultados de las fases de planeación, y fase de implementación deberá ejecutarse las siguientes actividades:

Procedimientos de Seguridad de la Información.
La institución educativa desarrollará y formalizará los procedimientos que faciliten gestionar la seguridad de la información en cada uno de los procesos definidos en la institución que describan los procedimientos mínimos que se deberían tener en cuenta para la gestión de la seguridad al interior de la institución.

Roles y Responsabilidades de Seguridad y Privacidad de la Información.
La institución definirá mediante un proceso administrativo ya sea mediante circular o decreto, los roles y las responsabilidades de seguridad de la información en los diferentes niveles tanto operativos o directivos, que enfoquen la correcta toma de decisiones y adecuada gestión para permitir el cumplimiento de los objetivos de la institución.

Inventario de activos de información.
La Institución educativa generara un inventario de activos de información actualizado y enfocada en una metodología de gestión de activos que permita a su vez definir la criticidad de la información y sus responsables, custodios y usuarios que permita brindar información relacionada para poder llevar a cabo la realización de las actividades de cada responsable.

Identificación, Valoración Y Tratamiento de Riesgos.
La Institución definirá una metodología de gestión del riesgo enfocada a procesos y procedimientos, que le pueda identificar, tratar y evaluar los seguimientos a los riesgos de seguridad de la información a los que estén expuestos los activos, así como la declaración de aplicabilidad. Para adoptar una integración apropiada en la gestión del riesgo respecto en cuanto a los criterios de evaluación como impacto, probabilidad y niveles de riesgo emitidos por la institución educativa[24].

[24] MIN-TIC. ROLES Y RESPONSABILIDADES. Seguridad y Privacidad de la información. [Documento en línea] Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf

5 ALCANCE DE LA ESTRATEGIA EN TÉRMINOS DE LOS ROLES, RESPONSABILIDADES, FUNCIONES QUE CUMPLEN LAS INSTITUCIONES EDUCATIVAS DE ACUERDO A LOS ACTIVOS DE INFORMACIÓN Y A LAS TECNOLOGÍAS UTILIZADAS.

Al dar a conocer el alcance de una estrategia para un sistema de gestión de seguridad informática debemos contemplar a que están expuestas las instituciones educativas en cuanto a sus recursos tecnológicos, se hacen necesario la creación de directrices que orienten las políticas de seguridad con documentos que constituyen la base del entorno de la seguridad de una institución educativa y definir las responsabilidades, los requisitos de seguridad y las funciones, normas y políticas a seguir por los funcionarios de la institución, según un estudio realizado recientemente, 8 de cada 10 equipos se encuentran infectados con algún tipo de código malicioso. Ante estos datos tan alarmantes, de inseguridad se intenta describir los pasos prioritarios que una institución, debe implementar para proteger su entorno. Es necesario enfatizar en la necesidad de un cambio de concepción, que conlleva al funcionario adoptar medidas proactivas en la gestión de la seguridad.

Para desarrollar el alcance y los objetivos propuestos con metodología a implementar se enmarca las fases de inicio, análisis y diseño, donde cada etapa determina una serie de actividades destinadas a lograr los resultados mediante las cuales se describen a continuación.

En la Tabla 1, se evidencia la fase 1 de inicio de un análisis del riesgo incluyendo una revisión y aprobación y su respectivo cronograma.

Tabla 1: Fase 1 de Inicio 1

FASE 1 - INICIO
Elaboración de la propuesta del análisis de riesgos de la información sobre la aplicación. Revisión y aprobación de la propuesta por parte de la institución educativa o empresa propietaria del software. Elaboración de cronogramas de actividades a realizar.

En la Tabla 2, se muestra la fase 2 de análisis donde se realiza un levantamiento de la información en cuanto a (Desarrollo, Soporte y Consultoría).

Tabla 2: Fase 2 Análisis 1

FASE 2 – ANÁLISIS
Realizar el Levantamiento de información empleando las siguientes técnicas: Entrevistas con los actores relevantes del aplicativo de gestión de documental (Gerencia y áreas involucradas (Desarrollo, Soporte y Consultoría). Revisión de la infraestructura física existente donde se alberga el aplicativo de la institución. Reconocimiento de la infraestructura existente de red bajo la cual se establece el acceso al aplicativo al personal de desarrollo, consultoría de la entidad y clientes externos. Realización de pruebas con cuenta creada y valida con diversos roles para detectar las vulnerabilidades en cuanto a seguridad de la información del aplicativo.

En la Tabla 3, se muestra la fase 3 de diseño para una metodología a implementar para realizar el análisis de riesgos.

Tabla 3: Fase 3 de Diseño 1

FASE 3 – DISEÑO
Definir la metodología a implementar para realizar el análisis de riesgos de seguridad de la información sobre el aplicativo. Identificación y clasificación de los activos de información, empleando el modelo de clasificación de los activos descrito en la metodología MAGERIT. Determinar las vulnerabilidades y amenazas de los activos de información correspondientes a la aplicación. Definir los riesgos de seguridad de la información detectados en el aplicativo, empleando la metodología MAGERIT de análisis y gestión de riesgos de los sistemas de información. Definir con la dirección el nivel de aceptación de los riesgos de seguridad de la información. Diseñar la política de seguridad de la información para la empresa propietaria del software de gestión documental. Diseñar el plan de tratamiento y gestión de riesgos de seguridad de la información. Socializar los resultados obtenidos ante la dirección de la empresa y/o Universidad.

CONCLUSIONES

Determinar de manera clara y argumentativa el aseguramiento que proporcionará las medidas de seguridad de la informática de manera correcta aplicando la norma ISO/ 27001, como también a los sistemas de información administrativos y académicos de cualquier entidad educativa, con el fin de reducir en lo posible y mitigar los riegos, amenazas y vulnerabilidades que se hayan identificado, permitiendo así salvaguardar los recursos informáticos de una institución y colaborando verticalmente con la divulgación de sus objetivos académicos y definir las responsabilidades para proteger su entorno que conlleva a desarrollar unas mejores y buenas medidas en la gestión de la seguridad de los sistemas informáticos de la institución.

Actualmente las entidades educativas están expuestas a una gran cantidad de amenazas que vulneran sus sistemas informáticos, de allí la importancia de mantener la seguridad de estos, puesto que las consecuencias de un ataque informático pueden poner en riesgo la integridad de la información. Asimismo, los ataques informáticos tienen gran incidencia negativa en varios sectores de la información de cada organización, ya que esta se podría ver modificada inadecuadamente.

En consecuencia, las Instituciones se ven afectadas por problemas relacionados con la seguridad informática, ya que evidentemente la seguridad en Internet afecta de forma excesiva a las organizaciones que operan en la web. Por lo antes expuesto, en el presente informe se logrará evidenciar la profundización sobre las normas ISO 27001 las vulnerabilidades, a partir de los riesgos identificados de; análisis y resultados obtenidos sobre el ambiente controlado.

RECOMENDACIONES

- Identificar las vulnerabilidades y amenazas sobre los activos asociados a la información, así como su respectivo impacto.

- Recolectar información general a cerca de los sistemas de información de la organización.

- Concientizar sobre lo elemental en seguridad informática (por ejemplo, contraseñas seguras) y sobre temáticas como cyberbullying o grooming.

- Recomendar auditorías internas para conocer el estado de la seguridad, evitar brechas y actualizar permisos de administradores.

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.

- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).

- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos.

- Utilizar métodos más ágiles y establecer una junta de compromiso con la certificación bajo la norma ISO 27001 dependiendo del nivel de recursos y la gestión necesaria para simplificar y agilizar los procedimientos que usa un software sobre la gestión de la norma ISO 27001.

- Generar una cultura para una mejora continúa basada en la norma ISO 27001 2013 que encierre el concepto de mejora continua, involucrando todo el personal para mejorar la seguridad de la información con mucho compromiso.

- Establecer en la plataforma de aprendizaje en línea o aplicación de videoconferencia contraseña difícil para el uso de las mismas cuando se utilicen ambos, es importante que cada contraseña sea diferente.

- Aprender a reconocer correos electrónicos de phishing para evitar el robo de información personal del usuario. Para detectarlos, algunos de estos sitios tienen errores ortográficos, enlaces rotos, correo electrónico no oficial, entre otras.

- Proteger todos los dispositivos con algunas herramientas de protección muy confiable para acceder a recursos educativos. De esta forma, se evita el riesgo

de ser víctima de ataques cibernéticos que puedan poner en riesgo la educación en línea en instituciones educativas.

DIVULGACIÓN

El desarrollo del presente proyecto de grado será dado a conocer en colaboración de la biblioteca de la Universidad Nacional Abierta y a Distancia – UNAD, a través de su aplicativo en línea, en donde se publicará un archivo PDF correspondiente al documento final presentado ante los jurados, posterior a la sustentación de este (Si es informe técnico por seminario o créditos de maestría, no tiene jurado); con el fin de que todos los estudiantes de la Universidad que se encuentren interesados en el tema de medidas de seguridad informática a los sistemas de información administrativos y académicos puedan acceder al documento.

BIBLIOGRAFÍA

ACIS. Ataques a Instituciones educativas. Sophos. [En línea]. 2021. Disponible en: https://acis.org.co/portal/content/escuelas-las-m%C3%A1s-afectadas-por-ransomware-el-60-fueron-atacadas-en-2021

AGUIRRE. El 67% de los colegios en Latinoamérica han sido víctimas de ataques cibernéticos. [En línea] 28 de mayo de 2018. Disponible en: https://www.lafm.com.co/tecnologia/el-67-de-los-colegios-en-latinoamerica-han-sido-victimas-de-ataques-ciberneticos

ÁLVAREZ BASALDÚA, Luis Daniel. Seguridad en informática (auditoría de sistemas). Tesis de grado para obtener el título de maestro en ingeniería de sistemas empresariales. México, D. F. 2005. Universidad iberoamericana.

ASUNTOS LEGALES. Antecedentes de asuntos legales. Cristian Acosta Argote [En línea] 9 de julio de 2021. Disponible en: https://www.asuntoslegales.com.co/actualidad/los-ataques-ciberneticos-aumentaron-30-durante-el-primer-semestre-de-este-ano-3198212

AYUDALEY. Objetivos de la seguridad de la información. 14 de julio de 2020. [En línea] Disponible en: https://ayudaleyprotecciondatos.es/2020/07/14/seguridad-de-la-informacion/#Que_es_la_seguridad_de_la_informacion_Definicion_y_Conceptos_basicos

AZURE. Que es la Nube. 2022. [en línea] Recuperado de https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-the-cloud

CÁMARA DE COMERCIO DE PASTO. Políticas de Seguridad Informática y de la Información. [En línea]. [consultado el 14 de junio de 2020] Disponible en: https://www.ccpasto.org.co/wp-content/uploads/2017/07/d-gt_01_v1-politicas_seg_informatica_informacion.pdf

CAPITALIST. Gestión de la Seguridad de la Información ISO 27001:2013. [En línea] noviembre 2022. Disponible en: https://capitalis-it.com/gestion-de-la-seguridad-de-la-informacion-iso-27001/

CIBERSEGURIDAD. Metodologías de Evaluación de Riesgos Cibernéticos. [En línea] 2020. Disponible en: https://ciberseguridad.com/herramientas/metodologias-evaluacion-riesgos-ciberneticos/

CIC. Ataques Cibernéticos. [En línea] 18 de noviembre de 2021. Disponible en: https://www.cic.es/preparacion-respuesta-ataques-ciberneticos/

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. [5, enero 2009]. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”-… Diario Oficial Bogotá D.C., 2009 No. 47.223. p 1 – 4. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

CONEXIÓN ESAN. Las cuatro etapas para la mejora continua en la organización. [En línea] 4 de mayo de 2016. Disponible en: https://www.esan.edu.pe/conexion-esan/las-cuatro-etapas-para-la-mejora-continua-en-la-organizacion/

CORREA LÓPEZ, Jhullián. Manual de Políticas y Estándares en seguridad informática versión 1. INTENALCO educación superior. [Manual] Disponible en: https://www.academia.edu/11353025/Pol%C3%ADticas_y_Est%C3%A1ndares_de_Seguridad_Inform%C3%A1tica_Versi%C3%B3n_01_Jhulli%C3%A1n_Correa_L%C3%B3pez_Sistemas_Intenalco.

DESARROLLO DE LA NORMA DE ASEGURAMIENTO DE LA INFORMACIÓN ISO 27001. Antecedentes. 2019. [En Línea] Disponible en: https://repository.unilibre.edu.co/bitstream/handle/10901/17900/PROYECTO%20DE%20GRADO%20DESARROLLO%20DE%20LA%20NORMA%20DE%20ASEGURAMIENTO%20DE%20LA%20INFORMACION%20ISO%2027001%20PARA%20%E2%80%9CVIAJES%20SIS%E2%80%9D.pdf?sequence=1&isAllowed=y

DOCPLAYER. Marco legal. [En línea] 22 de marzo de 2006. Disponible en: https://docplayer.es/7982301-Norma-tecnica-ntc-iso-iec-colombiana-27001.html

ESCUELA COLOMBIANA DE INGENIERÍA JULIO GARAVITO. Manual de políticas. [En línea]. [consultado el 14 de junio de 2020] Disponible en: https://www.escuelaing.edu.co/escuela/importantDoc/Manual-politica-seguridad-dela-Informacion.pdf

ESQUIVEL SUAZO, María Luisa. Seguridad informática. Instituto tecnológico de Tijuana, Tijuana México, mayo de 2011. Disponible en: https://sites.google.com/site/scesquivelsuazomarialuisa/7-conclusiones/5-2-marco-historico.

FIDUAGRARIA. Manual de Riesgos de Seguridad de la Información, [En Línea] Julio 2018. Disponible en: http://www.fiduagraria.gov.co/wp-content/uploads/2014/12/Amenazas-y-riesgos-en-el-manejo-de-la-informacion.pdf

GALLO OÑATE, Antonio Rafael, Diagnóstico de cumplimiento del modelo gestionado por el sistema de administración de la seguridad de la información de

gobierno en línea – SASIGEL alineado con la norma 27000 para el instituto nacional de formación técnica profesional de la guajira. Monografía Trabajo de Grado para optar al Título Académico de Especialista en Seguridad Informática. Valledupar, Cesar 2014. Universidad Nacional Abierta y a Distancia – UNAD. Escuela de ciencias básicas, tecnología e ingeniería (ECBTI).

GARCÍA, Roberto de Miguel. Criptografía clásica y moderna, Séptima Ediciones, [En línea] 2009. Central, Disponible en: http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3182091

GOBIERNO DE ESPAÑA. MAGERIT - Versión 3.0. Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I - Método. (M. d. Públicas, Ed.). octubre de 2012. Disponible en: http://administracionelectronica.gob.es/

GONZÁLEZ, M. L., & Fuentes, G. D. T. J. M. Sistemas seguros de acceso y transmisión de datos (MF0489_3). Madrid, España IC Editorial. Pag 07 - 88 2014. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/44100?page=1

HEALTHY CHILDER. Seguridad en las escuelas durante la pandemia de COVID-19. [En línea] 28 de septiembre de 2022. Disponible en: https://www.healthychildren.org/Spanish/health-issues/conditions/COVID-19/Paginas/return-to-school-during-covid-19.aspx.

IMPACTO TIC. Ciberataque a la U. del Bosque, una señal de alerta para el sector educativo. Jaime Dueñas. [En línea] 1 de julio de 2021. Disponible en: https://impactotic.co/ciberataque-a-la-u-del-bosque-una-senal-de-alerta-para-el-sector-educativo/

INCIBE. Políticas para la gestión de contraseñas [En línea]. 2020. Disponible en: https://www.incibe.es/sites/default/files/contenidos/politicas/fichas/contrasenas.pdf

INFONET ENTERPRISE. Seguridad Cibernética, Tecnología. Principales modalidades de ciberataques en 2021. 9 de julio de 2021. Disponible en: https://infonetenterprise.com.co/inicio/f/principales-modalidades-de-ciberataques-en-2021?En líneacategory=Seguridad+Cibern%C3%A9tica

INSTITUCIONES SLD. Metodología para la Gestión de la Seguridad Informática. [en línea] agosto 2013. Disponible en: https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRAN COLOMBIANO. Análisis de los riesgos de seguridad de la información. Carmen Elizabeth Fajardo Díaz. [En

línea] 2017. Disponible en: https://alejandria.poligran.edu.co/bitstream/handle/10823/995/3.%20Documento%20Final%20Opci%C3%B3n%20de%20grado%20II.pdf?sequence=1&isAllowed=y

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRAN COLOMBIANO. Gestión de identidad proyecto de implementación de gestión de identidad. Mariano Moreno. 2017 [En Línea] Disponible en: https://pdfcoffee.com/trabajo-de-gestion-de-identidad--2-pdf-free.html

INSTITUTO COLOMBIANO DE CRÉDITO EDUCATIVO Y ESTUDIO TÉCNICO EN EL EXTERIOR ICETEX, Manual de Políticas de Seguridad Digital. [En línea] 2020.
Disponible en: https://portal.icetex.gov.co/Portal/docs/default-source/documentos-el-icetex/biblioteca/manuales-de-la-entidad/m11-manual-politicas-seguridad-digital.pdf

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS ICONTEC. Norma Técnica Colombiana NTC-ISO-IEC 27001:2013. [En línea] 2013. Recuperado https://www.icontec.org/eval_conformidad/certificacion-iso-27001-sistemas-de-gestion-de-seguridad-de-la-informacion-2/

ISO 27001:2013. Fases De Auditoria Inicial ISO 27001:2013. [En línea] 2013. Disponible en: https://normaiso27001.es/1-auditoria-inicial-iso-27001-gap-analysis/.

ISOTOOLS EXCELLENCE. Consejos Para Implementar La Norma ISO 27001. [En línea] 16 de junio de 2016. Disponible en: https://www.pmg-ssi.com/2016/06/10-consejos-para-implementar-la-norma-iso-27001/

ISOTOOLS EXCELLENCE. Aspectos claves de su diseño e implementación ISO 27001:2013. [En línea], 2019. www.isotools.org s.f. 23 p. Disponible en: https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

KASPERSKY. Estadísticas de Ciber ataques. [En línea] 2020. Disponible en: https://latam.kaspersky.com/about/press-releases/2020_ataques-d-do-s-contra-recursos-educativos-aumentaron-mas-de-350-durante-el-primer-semestre

LA FM. Colegios en Latinoamérica víctimas de ataques. Las escuelas, colegios y universidades son objetivos muy atractivos para los piratas informáticos. John Mauricio. [En línea] 2017. Disponible en: https://www.infocyte.com/es/En línea/2017/09/20/malware-and-its-impact-in-educational-institutions/

MINTIC. Ley 1341 de 2009, [En Línea]. Agosto 2015. Disponible en: http://www.mintic.gov.co/portal/604/articles-3707_documento.pdf

MALWAREBYTES. Ransomware. [En línea] agosto 2021. Disponible en: https://es.malwarebytes.com/ransomware/

MIN-TIC. ROLES Y RESPONSABILIDADES. Seguridad y Privacidad de la información. [en línea] 25 de abril de 2016. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf

NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). [En Línea]. agosto 2016. Disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

NORMAS ISO. Metodologías de medición del Riesgo. [En línea] agosto 2021. Disponible en: https://www.normas-iso.com/iso-27001/

OBSERVATORIO CIBERSEGURIDAD. Riesgos, avances y el camino a seguir en América Latina y el Caribe. [En línea] noviembre 2020. Disponible en: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

OSTEC. Principios básicos de la seguridad de la información. [En línea] 07 de julio de 2021. Disponible en: https://ostec.En línea/es/seguridad-informacion/principios-basicos-de-la-seguridad-de-la-informacion/#:~:text=Para%20que%20sea%20posible%20mantener,%2C%20integridad%2C%20disponibilidad%20y%20autenticidad.

PORTAFOLIO. Ataques cibernéticos en Colombia. [revista en línea] 8 de junio de 2021. Disponible en: https://www.portafolio.co/tendencias/aumentan-en-30-los-ataques-ciberneticos-en-colombia-553803.

PORTAFOLIO. Cifras de Ciberseguridad. [revista en línea] 10 de diciembre de 2020. Disponible en: https://www.portafolio.co/tendencias/cifras-de-ciberseguridad-en-colombia-prenden-alarmas-al-cierre-del-2020-547412

PUBLICATIONS. Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe. [En línea] Julio 2020. Disponible en: https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

REVISTA EDU.CO. Los retos de seguridad informática que enfrentan las instituciones de educación en Colombia. [En línea] 19 de agosto de 2021.

Disponible en: https://revistaedu.co/secciones/tematicas-educativas/los-retos-de-seguridad-informatica-que-enfrentan-las-instituciones-de-educacion-en-colombia/2660/

REVISTA SEMANA. Año del ciberataque en Colombia. [en línea] 2 de julio de 2021. Disponible en: https://www.semana.com/economia/empresas/articulo/el-ano-de-los-ciberataques-en-colombia-estas-son-las-alarmantes-cifras/202125/

REVISTA SEMANA. La Universidad Javeriana confirma que sufrió ataque informático en Bogotá y Cali. [En Línea] 23 de noviembre de 2021. Disponible en: https://www.semana.com/nacion/articulo/la-universidad-javeriana-confirma-que-sufrio-ataque-informatico-en-bogota-y-cali/202153/

REVISTA SEMANA. El año de los ciberataques en Colombia, estas son las alarmantes cifras. 2 de julio de 2021. [En Línea]. Disponible en: http://www.elmundodelastics.net/2009/07/9-pasos-para-implementar-la-seguridad.html#.WA12OGVX_IU

SMARTEKH. Herramientas para garantizar la seguridad en el uso de plataformas digitales. [En línea] 6 marzo 2022. Disponible en: https://En línea.smartekh.com/herramientas-para-garantizar-la-seguridad-en-el-uso-de-plataformas-digitales

UNIVERSIDAD DEL ROSARIO. Preparación en Colombia para los ciberataques. noviembre 2017. [En línea] Disponible en: https://www.urosario.edu.co/UCD/Colombia-no-esta-preparada-ante-un-ciberataque/

UNIVERSIDAD SANTO TOMAS. Hurto por medios informáticos. Mihdí Badí Talero Magnin [En línea] 2020. Disponible en: https://auditoriainterna.usta.edu.co/index.php/120-los-ataques-de-hacking-en-el-sector-educativo.

UNIVERSIDAD SANTO TOMAS. Auditoría Interna. Mihdí Badí Talero Magnin [en línea]. 2018. Disponible en: https://auditoriainterna.usta.edu.co/index.php/120-los-ataques-de-hacking-en-el-sector-educativo

WIDEFENSE. Estadísticas de Ataques. Kenneth Daniels. [En línea] 20 de mayo de 2021. Disponible en: https://widefense.com/En línea/los-ciberataques-contra-los-recursos-educativos-en-linea

WIDEFENSE. Educación digital: Los ciberataques contra Recursos Educativos en línea. Kenneth Daniels. [En línea] 20 de mayo de 2021. Disponible en: https://www.widefense.com/recursos/ciberseguridad/recursos-educativos-linea/.

WELIVESECURITY. Seguridad informática ¿debería incluirse educación formal? Juan Manuel Harán. [En línea] 18 de noviembre 2019. Disponible en: https://www.welivesecurity.com/la-es/2019/11/18/educacion-seguridad-informatica-deberia-incluirse-educacion-formal/

WELIVESECURITY. Advierten sobre el crecimiento de ciberataques a instituciones de educación inicial y primaria. Juan Manuel Harán. [En línea] 11 de diciembre de 2020. Disponible en: https://www.welivesecurity.com/la-es/2020/12/11/advierten-crecimiento-ciberataques-apuntan-instituciones-educacion-inicial-primaria/

Fecha de Realización:	13/04/2023
Programa:	Seguridad en Informática
Línea de Investigación:	Monografía
Título:	Estrategia de aseguramiento de la información a partir del análisis y gestión de riesgos en los procesos académicos y administrativos que pueden afectar las instituciones educativas
Autor(es):	Sabalza Junco Roberto
Palabras Claves:	Amenazas, confianza, confidencialidad, políticas, riesgos.
Descripción:	Indudablemente el avance de muchas actividades ilícitas presentadas a nivel institucional, se presentan por la falta de procesos informáticos y que en la actualidad se efectúan rápida y acertadamente, reflejan la importancia en que se aprovecha para el bien y el mal en distintos ataques cibernéticos, de ahí que la inseguridad informática crezca a la par y sea más común en los entornos educativos, se convierte en objeto vulnerable y de fácil ataque de los delincuentes informáticos, se mantienen al acecho buscando robar o dañar información. El aseguramiento informático a los sistemas académicos, en cuanto a la identificación de vulnerabilidades y amenazas que se presentan en las instituciones educativas, tienen como propósito adoptar políticas apropiadas de seguridad al interior de una institución educativa, con el fin de ofrecer una mejora continua para la seguridad informática en los sistemas de información académicos de cualquier institución educativa, y poder reducir en lo posible mitigar o eliminar los riegos, amenazas y vulnerabilidades que se hayan identificado; permitiendo así salvaguardar los recursos informáticos de las instituciones educativas y restringiendo así la posibilidad de ataques informáticos. Salvaguardar los recursos informáticos de una institución educativa mediante las amenazas identificadas implementando la norma ISO 27001:2013, una solución que permita

	investigar rápidamente cualquier actividad sospechosa y altamente maliciosa, a la vez, establecer la mejor manera de enfrentar y mitigar los incidentes.

Fuentes bibliográficas destacadas:

ACIS. Ataques a Instituciones educativas. Sophos. [En línea]. 2021. Disponible en: https://acis.org.co/portal/content/escuelas-las-m%C3%A1s-afectadas-por-ransomware-el-60-fueron-atacadas-en-2021

AGUIRRE. El 67% de los colegios en Latinoamérica han sido víctimas de ataques cibernéticos. [En línea] 28 de mayo de 2018. Disponible en: https://www.lafm.com.co/tecnologia/el-67-de-los-colegios-en-latinoamerica-han-sido-victimas-de-ataques-ciberneticos

CÁMARA DE COMERCIO DE PASTO. Políticas de Seguridad Informática y de la Información. [En línea]. [consultado el 14 de junio de 2020] Disponible en: https://www.ccpasto.org.co/wp-content/uploads/2017/07/d-gt_01_v1-politicas_seg_informatica_informacion.pdf

CAPITALIST. Gestión de la Seguridad de la Información ISO 27001:2013. [En línea] noviembre 2022. Disponible en: https://capitalis-it.com/gestion-de-la-seguridad-de-la-informacion-iso-27001/

DESARROLLO DE LA NORMA DE ASEGURAMIENTO DE LA INFORMACIÓN ISO 27001. Antecedentes. 2019. [En Línea] Disponible en: https://repository.unilibre.edu.co/bitstream/handle/10901/17900/PROYECTO%20DE%20GRADO%20DESARROLLO%20DE%20LA%20NORMA%20DE%20ASEGURAMIENTO%20DE%20LA%20INFORMACION%20ISO%2027001%20PARA%20%E2%80%9CVIAJES%20SIS%E2%80%9D.pdf?sequence=1&isAllowed=y

DOCPLAYER. Marco legal. [En línea] 22 de marzo de 2006. Disponible en: https://docplayer.es/7982301-Norma-tecnica-ntc-iso-iec-colombiana-27001.html

ESCUELA COLOMBIANA DE INGENIERÍA JULIO GARAVITO. Manual de políticas. [En línea]. [consultado el 14 de junio de 2020] Disponible en: https://www.escuelaing.edu.co/escuela/importantDoc/Manual-politica-seguridad-dela-Informacion.pdf

ESQUIVEL SUAZO, María Luisa. Seguridad informática. Instituto tecnológico de Tijuana, Tijuana México, mayo de 2011. Disponible en: https://sites.google.com/site/scesquivelsuazomarialuisa/7-conclusiones/5-2-marco-historico.

Fuente: Estadística Ataques cibernéticos: https://www.asuntoslegales.com.co/actualidad/los-ataques-ciberneticos-aumentaron-30-durante-el-primer-semestre-de-este-ano-3198212

Fuente: https://www.cic.es/preparacion-respuesta-ataques-ciberneticos

Fuente: https://eduteka.icesi.edu.co/articulos/RedEscolarDatos Fuente https://www.shutterstock.com/es/search/information-recovery Fuente: Datos de intentos cibernéticos: https://revistaedu.co/secciones/tematicas-educativas/los-retos-de-seguridad-informatica-que-enfrentan-las-instituciones-de-educacion-en-colombia/2660/	
Contenido del documento:	En el siguiente trabajo se aborda el tema de la seguridad de la información frente a amenazas cibernéticas buscando una estrategia de aseguramiento de la información a partir del análisis y gestión de riesgos en los procesos académicos y administrativos que pueden afectar las instituciones educativas de la ciudad de Bogotá. Mediante una consulta teórica y documental, se realizará la consulta y se pondrá en práctica una estrategia considerando la historia acerca de la ciberseguridad, delitos informáticos, y la seguridad de la información, donde se han evidenciado alertas durante la pandemia COVID-19, amenazas gubernamentales, institucionales, educativas, bancarias entre otras, el resultado no fue favorable teniendo en cuenta la mal praxis de las políticas de seguridad informática, estándares de calidad, tecnología obsoleta y de manera consciente se pretende dar a conocer los diferentes estados de riesgos para así poder determinar en cualquier institución el grado o el nivel del riesgo que se puede materializar mediante un análisis profundo y generar la forma de preservación de la infraestructura tecnológica y de comunicación en que están soportadas las operaciones.
Marco Metodológico:	Alcanzar de manera clara un análisis del riesgo inherente y establecer diferentes atributos de controles y acciones de tratamiento de riesgos para garantizar el aseguramiento y las medidas de seguridad de la información de manera correcta aplicando la norma ISO/ 27001
Conceptos adquiridos:	**SALVAGUARDAR:** Nos permite de una manera más segura y organizada consignar la

	información que es de gran valor. **MALWARE**: Es un término general para referirse a cualquier tipo de “malicious software” (software malicioso). **PHARMING:** Es una famosa combinación entre los términos "phishing" y "farming", clasificándose como un tipo de cibercrimen muy similar al phishing. **SMISHING:** Se manifiesta como una técnica que básicamente consiste en la transmisión de envío de un SMS por un ciberdelincuente
Conclusiones:	Determinar de manera clara y argumentativa el aseguramiento que proporcionará las medidas de seguridad de la informática de manera correcta aplicando la norma ISO/ 27001, como también a los sistemas de información administrativos y académicos de cualquier entidad educativa, con el fin de reducir en lo posible y mitigar los riegos, amenazas y vulnerabilidades que se hayan identificado, permitiendo así salvaguardar los recursos informáticos de una institución y colaborando verticalmente con la divulgación de sus objetivos académicos y definir las responsabilidades para proteger su entorno que conlleva a desarrollar unas mejores y buenas medidas en la gestión de la seguridad de los sistemas informáticos de la institución. Actualmente las entidades educativas están expuestas a una gran cantidad de amenazas que vulneran sus sistemas informáticos, de allí la importancia de mantener la seguridad.