ANÁLISIS DE LOS PRINCIPALES RIESGOS DE CIBERSEGURIDAD EN LOS ESTUDIANTES DE BÁSICA SECUNDARIA EN COLOMBIA

VICENTE OMAR MONTILLA MONTILLA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

PASTO - NARIÑO

2025

ANÁLISIS DE LOS PRINCIPALES RIESGOS DE CIBERSEGURIDAD EN LOS ESTUDIANTES DE BÁSICA SECUNDARIA EN COLOMBIA

VICENTE OMAR MONTILLA MONTILLA

Proyecto de Grado – Monografía presentado para optar por el título de

ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Ing. CHRISTIAN REINALDO ANGULO

Asesor de Trabajo de Grado II

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

PASTO - NARIÑO

2025

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

A Dios Todopoderoso, por regalarme el don de la vida, todas mis facultades y fortalezas para poder día a día aunar esfuerzos para cumplir con todas las actividades propuestas en esta nueva etapa de estudio.

También ofrezco todo el trabajo realizado a mis padres, aunque ya no están conmigo aquí en la tierra, estoy seguro de que desde el cielo continúan presentes en cada día de mi vida, gracias por los valores inculcados y por seguir siendo una luz en mi camino.

A quien ha sido mi apoyo y motivación, a mi querida esposa por su comprensión y aliento constante en este nuevo camino académico.

AGRADECIMIENTOS

Sea la oportunidad para agradecer a mi universidad UNAD - Pasto, por brindarme la oportunidad de regresar a sus aulas y profundizar en mi formación académica a través de la Especialización en Seguridad Informática, en la modalidad virtual. Esta experiencia ha contribuido al desarrollo de mis habilidades, conocimientos, a mi crecimiento profesional, personal y valoro notoriamente su contribución con la educación.

También expreso mis más sinceros agradecimientos a cada uno de los tutores por su orientación, colaboración y asesoría que han sido fundamentales para culminar con éxito esta nueva fase de formación académica, que me ha permitido ampliar mis conocimientos como Ingeniero de Sistema; profundizando en áreas acordes a los nuevos desafíos de la Informática.

Quiero agradecer a mis compañeros en los diferentes equipos de trabajo. Su apoyo y motivación me permitieron superar desafíos, crear un ambiente de trabajo positivo, muy productivo y alcanzar mis objetivos.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

ACCESO: proceso principal en la ciberseguridad que involucra diversas situaciones para legalizar: autenticación, autorización y auditoría, por parte de los interesados para acceder a recursos digitales de una empresa.

ADWARE: clase de software malicioso que muestra anuncios no deseados en una computadora o dispositivo. Aunque no siempre es dañino, puede ralentizar el rendimiento del sistema y, en algunos casos, redirigir a sitios web maliciosos.

AMENAZAS: comprometen la privacidad, seguridad, confidencialidad de los datos, de los sistemas informáticos, de una persona, un grupo y por consiguiente el lugar y ambiente de trabajo.

AMENAZA INFORMÁTICA: riesgo alto y característico que afronta una persona u organización concerniente con la pérdida de datos, daños irremediables o pérdida de sistemas informáticos.

ATAQUE INFORMÁTICO: el ciberataque, se refiere a cualquier maniobra dañina, cuyo objetivo es desequilibrar un sistema informático y pretende conseguir el control puede ser por software maliciosos, malware virus, etc.

ATAQUE CIBERNÉTICO: es cualquier esfuerzo intencional para robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos a través del acceso no autorizado a una red, sistema informático o dispositivo digital.

AUTENTICACIÓN MULTIFACTOR (MFA): método de seguridad que exige a los usuarios proporcionar dos o más formas de verificación para acceder a una cuenta o sistema. Es como añadir un candado extra a tu puerta: hace mucho más difícil que alguien entre sin tu permiso.

BIG DATA: conjuntos de datos extremadamente grandes y complejos que no pueden ser gestionados ni procesados de manera eficiente utilizando herramientas tradicionales de procesamiento de datos.

BOTNET: red de dispositivos, como computadoras y otros dispositivos conectados a Internet, que han sido infectados con malware y son controlados de forma remota por un atacante.

BOTS: programas automatizados que realizan tareas específicas en Internet, y pueden clasificarse en diferentes categorías según su propósito y funcionalidad.

CARNADA: conocida como baiting en inglés, es un tipo de ataque de ingeniería social que utiliza dispositivos de almacenamiento, como USB, para atraer a las víctimas y comprometer sus sistemas; utilizando tácticas engañosas para lograr su objetivo.

CATFISHING: una práctica engañosa en la que una persona crea un perfil falso en línea con el objetivo de iniciar una relación romántica con otra persona. Suele estar construido con información falsa o robada, incluyendo fotos, nombres e incluso historias de vida.

CERTIFICADO DIGITAL: fichero electrónico generado por una autoridad de certificación. Se utiliza para verificar la identidad de la persona titular, confrontar su firma o cifrar mensajes dirigidos a ella.

CIBERDELITO: actividad delictiva que se realiza a través de Internet o utilizando recursos tecnológicos.

CIBERATAQUE: acción realizada por una o varias personas por medio de herramientas informáticas, con el fin de dañar un sistema informático o una red informática.

CIBERSEGURIDAD: conjunto de tecnologías y servicios que protegen a una empresa de cualquier agresión o pérdida de datos.

El CIO: responsable de desarrollar una estrategia tecnológica alineada con los objetivos comerciales de la empresa. Identifica y prioriza las necesidades tecnológicas, así como establece la dirección y los objetivos a largo plazo para la infraestructura y las soluciones de tecnologías de la información y la comunicación.

CICLO DEMING: también conocido como PDCA (Plan, Do, Check, Act) o PHVA (Planificar, Hacer, Verificar, Actuar), es una metodología de gestión de la calidad diseñada por W. Edwards Deming.

CÓDIGO MALICIOSO: programas planteados para crear una vulnerabilidad en los diferentes sistemas, logrando ocasionar daños, robar datos o acceder sin autorización; toman diversas formas, por ejemplo troyanos, virus, gusanos, entre otros.

CRACKER: persona que se aprovecha de sus conocimientos para romper o vulnerar la seguridad de un sistema**,** generalmente para obtener un beneficio económico.

CUANTIFICACIÓN DE RIESGOS: proceso que consiste en medir y asignar un valor numérico a las amenazas que pueden afectar los objetivos de una organización.

DELITO INFORMÁTICO: tiene que ver con la sustracción de datos, en los diferentes ataques a los sistemas, tanto a personas o de entes de carácter público o privado; afectando con ello los procesos, sus redes y los datos.

DIRECCIÓN MAC (control de acceso medio): Es una dirección física, o un identificador exclusivo que se le da a un equipo de hardware de red donde el fabricante determina y tiene su propia dirección MAC, en el instante de su fabricación.

E-LEARNING: variedad de actividades formativas de educación y capacitación que se imparten a través de un dispositivo conectado a la red, Se lo conoce de diferentes formas: formación online, teleformación, aprendizaje electrónico o aprendizaje virtual.

EXPLOID: programa, técnica o fragmento de código diseñado para aprovechar una vulnerabilidad en un sistema informático. Su objetivo principal es obtener acceso no autorizado, ejecutar comandos o alterar el comportamiento normal de un sistema, red, software o hardware.

GAP: o análisis de brechas, consiste en una evaluación del desempeño real de una empresa, con la cual se busca contrastar el punto en que se encuentra, el punto al que quiere llegar en su desarrollo y crecimiento como organización.

GOBIERNO DIGITAL: implica la implementación de tecnologías de la información y la comunicación (TIC) en las actividades gubernamentales para aumentar la eficiencia, transparencia y accesibilidad de los servicios públicos.

GROOMER: persona adulta que realiza acoso sexual a niña, niño o un adolescente por medio de internet.

GUSANOS: son programas maliciosos que se esparcen de forma autónoma a través de redes y sistemas, sin necesidad de intervención humana. Se replican y se envían a otros sistemas conectados, lo que puede llevar a una propagación rápida y dañina.

HACKER: o pirata Informático es una persona con grandes habilidades y conocimientos, en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora, en modificar sistemas, pero que los usa para detectar brechas de seguridad en los mismos.

HACKTIVISMO: Derivado de combinar las palabras 'Hack' y 'Activismo', el hacktivismo es el acto de irrumpir en un sistema informático con fines políticos o sociales.

HASHCAT: herramienta de recuperación de contraseñas de alto rendimiento y de código abierto, ampliamente utilizada en el ámbito de la ciberseguridad para el cracking de hashes de contraseñas.

HUNTING: técnica que se usa tanto phishing, la carnada y el hacking de correo electrónico para obtener infinidad de datos de la víctima, sin el mayor esfuerzo.

ISO/IEC 27001: norma o estándar internacional que establece los requisitos para la gestión de la seguridad de la información (SGSI):

INGENIERÍA SOCIAL: técnica utilizada por ciberdelincuentes para manipular a las personas y obtener información confidencial o acceso a sistemas.

JOHN THE RIPPER: herramienta de código abierto adoptada para la recuperación y auditoría de contraseñas, ampliamente reconocida en el campo de la ciberseguridad.

MALWARE: abreviatura de "malicious software" (software malicioso), se refiere a cualquier programa o archivo diseñado con la intención de causar daño a un sistema informático, red o dispositivo.

MAGERIT: metodología de análisis y gestión de riesgos de la información desarrollada por el Consejo Superior de Administración Electrónica.

MEHARI: método armonizado. Base de datos conocimientos y procedimientos para el Análisis de Riesgos en los sistemas de seguridad de la información para descubrirlos a tiempo.

MITM: (man in the middle) tipo de ciberataque en el que un atacante intercepta y potencialmente altera la comunicación entre dos partes que creen que están comunicándose directamente entre sí

NIST: marco de Ciberseguridad que ayuda a los negocios de todo tamaño a comprender mejor sus riesgos de ciberseguridad, administrar y reducir sus riesgos, y proteger sus redes y datos.

OCTAVE: se basa en la operatividad de la organización y considera la seguridad informática como un tema que va más allá de lo técnico.

PDCA: Ciclo PDCA: herramienta para la mejora continua. PDCA son las siglas en inglés de Plan, Do, Check, Act, que en español se traduce como Planificar, Hacer, Verificar, Actuar. Es un ciclo de mejora continua empleado en diversos campos para resolver problemas, optimizar procesos y alcanzar objetivos.

PAYLOAD: en ciberseguridad, se refiere a la parte del malware que ejecuta la acción maliciosa prevista después de que un exploit ha comprometido exitosamente un sistema.

PHISHING: ataque cibernético que utiliza técnicas de ingeniería social para engañar a las personas y obtener información sensible, como credenciales de acceso o datos personales.

PHARMING: ciberataque que busca redirigir el tráfico web de un sitio legítimo a un sitio falso, creado por los atacantes con el objetivo de robar información personal o financiera.

RANSOMWARE: tipo de malware que secuestra datos de un usuario o una organización, impidiendo el acceso a ellos hasta que se pague un rescate.

RIESGOS: posibilidad de que suceda un evento negativo y que la amenaza se convierta en un desastre; consiguiendo que cause daños o pérdidas a mediana o gran escala.

RIESGO INFORMÁTICO: riesgos que puede enfrentar una persona u organización, como ataques cibernéticos a su red o los sistemas ya sea por errores humanos, ataques externos y vulnerabilidades en los sistemas; resultando una pérdida o robo como consecuencia del daño ocasionado.

SEGURIDAD DE LA INFORMACIÓN: conjunto de normas para proteger los datos e información al interior de una organización, con el propósito de realizar actividades encaminadas al control y la protección de los activos lógicos.

SITIO WEB: o Portal Web se refiere a un conjunto de páginas web conectadas en el entorno de Internet, conocido como World Wide Web.

SGSI: conjunto de políticas, procedimientos y controles diseñados para garantizar la confidencialidad, integridad y disponibilidad de la información de una organización.

SMS O SMISHING: emplea un mensaje de texto en su teléfono móvil o inteligente, proporcionándoles un presente de 'agradecimientos' para que sus víctimas puedan realizar la actualización de sus datos de su tarjeta de crédito.

SPOOFING: o suplantación de identidad, es un tipo de ciberataque en el que un atacante se hace pasar por una persona o entidad de confianza para obtener información privada.

SPYWARE: software malicioso diseñado para recopilar información sobre las actividades de un usuario sin su consentimiento. Puede registrar pulsaciones de teclas, capturar contraseñas o rastrear la navegación web, lo que plantea graves preocupaciones de privacidad.

SOLARWINDS: empresa estadounidense que se especializa en el desarrollo de software para la gestión de redes, sistemas y la infraestructura de tecnología de la información (TI). Fundada en 1999, la compañía tiene su sede en Austin, Texas.

TIC: abarcan una amplia gama de tecnologías que incluyen computadoras, dispositivos móviles, redes de telecomunicaciones, software y servicios relacionados que facilitan la comunicación y el acceso a la información. Se utiliza para describir tanto las tecnologías de la comunicación (radio y televisión) como las tecnologías de la información (computadoras y software).

TRÁFICO DE RED: unidades pequeñas que se mueven a través de una red informática en un momento dado. Este tráfico es primordial para situaciones encaminadas a la medición y para un control de simulación.

TROYANOS: son programas que se disfrazan como software legítimo, pero contienen código malicioso. Una vez en el sistema, este tipo de riesgos de ciberseguridad pueden permitir el acceso no autorizado o robar información.

VIDEOLLAMADAS: también conocidas como videoconferencias a través de una aplicación informática, para reproducir entrada y salida de video y mediante la comunicación entre dos o más usuarios se convierte en una comunicación bidireccional y moderna.

VIRUS: se adjunta a programas legítimos o archivos y se propaga al ejecutar el programa o abrir el archivo infectado. Estos pueden dañar archivos, corromper sistemas y propagarse a través de medios de almacenamiento compartidos, como unidades USB.

VISHING: una contracción de "voice phishing" (phishing por voz), es un tipo de ataque cibernético que mediante llamadas telefónicas o mensajes de voz engaña a las personas; obteniendo información personal y financiera sensible.

VULNERABILIDAD: “susceptibilidad o fragilidad física, económica, social, ambiental o institucional que tiene una comunidad de ser afectada o de sufrir efectos.

VULNERABILIDAD INFORMÁTICA: cualquier error, debilidad o falla en el hardware o el software, en el código de un sistema o dispositivo; comprometiendo el riesgo de seguridad, mediante la labor de un atacante o hacker y con ello implicando la integridad y confidencialidad de los datos que procesa un sistema.

RESUMEN

Actualmente, los jóvenes se enfrentan a diferentes retos tecnológicos, que son considerados como una ayuda académica, pero desafortunadamente pueden ser empleados con otros propósitos. De allí la importancia de que tanto padres e hijos conozcan los diferentes aspectos que encierra la ciberseguridad y sobre los riesgos significativos para los menores de edad, debido a que logran ser vulnerables a la exposición a una variedad de contenido inadecuado para su edad.

La tesis destaca los principales riesgos de ciberseguridad en los estudiantes de Básica Secundaria en Colombia, para la mitigación de riesgos y vulnerabilidades, en la población juvenil de los grados 9, 10 y 11, a través de una investigación teórico-descriptiva concreta, se pretende realizar un análisis del problema y objeto de estudio de los diferentes tipos de ataques cibernéticos y para que posteriormente se haga énfasis en el mundo de la ciber educación que involucre la apropiación de buenas prácticas informáticas para proteger, generar conciencia individual y colectiva al igual el derecho a la protección de la intimidad, a conocer y estar al tanto de las leyes colombianas vigentes que trabajan al cuidado del bienestar de los menores de edad.

Con esta propuesta pretendo prevenir y alertar de todos los posibles riesgos que corren los menores de edad y de esta forma reducir las dificultades y problemas que puedan surgir con su integridad moral y física. Está en manos de la ciberseguridad que se informe de los conceptos de seguridad y privacidad, con el fin de fomentar el cuidado y protección de datos personales garantizando un futuro seguro donde la información veraz y oportuna sea una herramienta reconociendo ante todo el valorar de la vida, la armonía familiar y social.

ABSTRACT

Young people face different technological challenges and although these are considered an academic aid, they can be used for other purposes. It is necessary that both parents and children know the different aspects of cybersecurity and the inherent risks of social networks to minors.

This thesis points out the main cybersecurity risks in Basic Secondary students in Colombia, for the mitigation of risks and vulnerabilities, so that the youth population of grades 9, 10 and 11, through a specific theoretical-descriptive investigation, carry out an analysis of the problem and object of study of the different types of cyber-attacks. It's clearly possible to speak about cyber education involves the appropriation of good computer practices to protect and make each user aware of the pros and cons of social networks and we have to generate awareness for protection of information, the right to privacy and to know the current Colombian laws and regulations that work for the welfare of minors.

With this proposal I wish to prevent and warn of all possible risks that this sector of youth runs with their integrity moral and physic. It is in the hands of cybersecurity to be informed of the concepts of security and privacy, to promote the care and protection of personal data, guaranteeing a safe future where accurate and timely information is a valuable tool allowing to value life, family and social harmony.

INTRODUCCION

En esta era digital, en un mundo cada vez más interconectado, la ciberseguridad se ha convertido en un tópico fundamental para muchos sectores de la sociedad y de manera especial en el contexto educativo.

Los estudiantes de básica secundaria en Colombia, están cada vez más expuestos a la tecnología; al demostrar sus habilidades y conocimientos, se enfrentan a riesgos cibernéticos que pueden comprometer su seguridad emocional, seguridad física, la pérdida de privacidad, el secuestro de datos personales, la difusión de información falsa, el acoso, la violencia; entre otros. Por eso, la ciberseguridad en la educación es vital para proteger la privacidad y seguridad de los datos, prevenir el ciberacoso, garantizar el funcionamiento adecuado de la infraestructura y fomentar una cultura de seguridad digital.

No cabe duda que las redes sociales se han transformado para los menores de edad en esos espacios atractivos y a veces secretos donde ellos son sin lugar a duda los protagonistas, porque en esos encuentros se relacionan con otros semejantes, que aparentemente emplean un lenguaje propio, los mismos gustos, juegos, una misma jerga que los identifica y es precisamente en ese entorno donde se acepta sus gustos e intereses, aquí no son criticados, ni rechazados.

La investigación documental se presenta como una herramienta esencial para identificar y comprender estos riesgos. A través de un análisis exhaustivo se puede obtener una visión clara de las amenazas más comunes que enfrentan los estudiantes y sus familias en el entorno digital. Este conocimiento no solo permite diseñar estrategias efectivas para mitigar esos riesgos, sino que también promueve una cultura de responsabilidad digital y conciencia cibernética en la comunidad educativa.

Es indispensable analizar y profundizar sobre los diferentes aspectos relacionados con la ingeniería social, que se pueden originar a través del error humano; llevando al delito cibernético, a las estafas de "hackeo de humanos" y consiguiendo que los usuarios desprevenidos expongan datos, propaguen infecciones de malware o den acceso a sistemas restringidos.

Los ataques pueden ocurrir en línea, en persona a través de otras interacciones y de allí que se enfatizará en las diferentes técnicas de Ingeniería Social que son necesarias tener presente como: vishing, phishing, pharming, grooming, entre otros, que pueden dar origen a graves consecuencias y por eso es necesario mitigar los riesgos existentes e implementar un correcto uso de la tecnología de la información y tener presente sus diferentes tácticas, con el propósito de estar alerta y salvaguardar los intereses de los menores de edad.

Dentro de este contexto social y familiar, se hace necesario que adolescentes estén cada vez más acompañados en todos esos procesos de información, comunicación porque

sólo la guía y orientación de padres de familia y de los docentes permitiría que ellos conozcan de peligros del empleo de Internet y que posteriormente afectarían sus vidas, su confidencialidad; producto del interactuar con extraños en situaciones que tienen que ver con juegos, hacer amigos, redes sociales y dispositivos informáticos; para dar paso a que las instituciones educativas, los padres de familia y los menores de edad estén involucrados en la educación, la seguridad en línea, a través del diálogo, la conversación franca, abierta y honesta sobre los diferentes riesgos cibernéticos.

En esta monografía quedará plasmado una serie de recomendaciones dirigidas al estudiantado, al sector educativo, a todos los padres de familia con miras a proteger y mitigar estas amenazas; para ello se registra algunas plataformas útiles para estudiantes y que es necesario conocer y poder aplicar no sólo en el núcleo familiar, sino también en el sector educativo.

Es fundamental familiarizarse con ciertas indicaciones para el control parental del material que diariamente utilizan los alumnos en Internet y finalmente se hace énfasis en ciertas normas de comportamiento que los usuarios de los servicios online, es preciso que conozcan y practiquen y aquí se refleja en la netiqueta como una herramienta que complementa la ciberseguridad en los menores de edad.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Desde que los delitos informáticos fueron incorporados en el Código Penal hace casi trece años, se ha observado una notable disparidad entre la cantidad de sucesos que ocurren diariamente y los casos que verdaderamente son llevados a juzgado.

En 2021, se registraron más de 48,000 denuncias relacionadas con infracciones tecnológicas, lo que representa un aumento notable del 21% registrado; en relación con el año anterior, señala un progreso en el avance de la ciberseguridad y la sensibilización acerca de salvaguardar la información. Además, se presentó un incremento considerable en la ciberdelincuencia, que ocurrió durante la época de COVID-19, una rápida expansión del universo digital.

"En Colombia, la Ley 1273 de 2009 creó nuevos tipos penales relacionados con los delitos informáticos y la protección de información y datos y estableció penas de prisión hasta de diez años y multas hasta de 1.500 salarios mínimos vigentes" [1] Es esencial tener en cuenta que estos actos delictivos pueden perpetrarse haciendo uso de las Tecnologías de la Información y la Comunicación (TIC). A continuación, algunos ejemplos, de estas conductas ya consideradas como delitos:

- La propagación masiva de correos no deseados, denominado Spam.
- Uso del método Spoofing, destinado a alterar la identidad del remitente, mediante mensajes o correos electrónicos.
- Se envían o se infiltran archivos de espionaje de manera oculta.
- Seguimiento o incluso sustracción de datos de sistemas particulares, empleando troyanos.
- La proliferación de virus de computación.

Enfatizando la importancia de seguir potenciando las habilidades de investigación de la fiscalía general de la Nación, en lo que respecta a los crímenes definidos en el Título VII bis e incorporados a través de la Ley 1273 del 2009, así como a los variados ataques cibernéticos planteados desde el año 2001. Para los progresos de Colombia en el campo de Ciberseguridad, con el objetivo de luchar en las diferentes modalidades del

[1] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 (5, enero, 2009). De la Protección de la información y de los datos [en línea]. José Camilo. Ley de Delitos Informáticos en Colombia. Delta Asesores. [Consultado: mayo 16 de 2023]. Disponible en: https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

ciberespacio, nuestra nación se adhirió al Convenio de Budapest al ser reconocido como un acuerdo internacional ya que establece:

- Definiciones exactas para varios delitos informáticos.
- Promueve la colaboración global, se involucra de forma activa en la batalla contra la ciberdelincuencia.
- Ofrece un marco jurídico que ayuda de manera significativa a enfrentar los desafíos de la criminalidad cibernética y la seguridad en internet.

1.2 FORMULACIÓN DEL PROBLEMA

¿Es necesario establecer los riesgos y amenazas a los que se ven expuestos los estudiantes de los grados 9º, 10º y 11º al estar en contacto con las diferentes redes sociales?

2. JUSTIFICACIÓN

Nos encontramos en la era de la información, aquí los estudiantes menores de edad, se encuentran inmersos, tienen que convivir en un nuevo escenario de conflicto el ciberespacio, donde surgen comportamientos y acciones que resultan desconcertantes porque hay confusión en los límites que se deben tener de los valores adquiridos y en especial del respeto; hay confusión al intentar rescatar lo positivo y eso termina llevando a una realidad lamentable, la delincuencia.

Hay que tener presente que en este contexto existe una organización macro como es la familia y en varias ocasiones, los adolescentes de la Básica Secundaria se encuentran solos en este espacio virtual y con esa necesidad inmensa por conocer de allí, que a diario utilizan la tecnología como recurso fundamental de conocimiento, de juego y diversión; es por eso que con el desarrollo de la monografía se pretende dar a conocer los principales riesgos de ciberseguridad en los estudiantes de Básica Secundaria en Colombia, para protegerlos y a su entorno familiar, mitigando los riesgos existentes, al usar las redes sociales, juegos y dispositivos informáticos.

Es urgente que se identifique y examine los riesgos en línea, a los que los estudiantes están expuestos en su vida cotidiana, con el propósito de proporcionar pautas para crear entornos virtuales más seguros. Tener en cuenta que la familia como núcleo fundamental es la más afectada; entonces mi propósito es plantear prácticas de seguridad, con el fin de que sirva de guía a docentes, a los padres de familia y al entorno estudiantil.

3. OBJETIVOS

3.2 OBJETIVO GENERAL

Analizar los principales riesgos de ciberseguridad en estudiantes de básica secundaria en Colombia, para mitigar los peligros existentes, mediante un correcto manejo de la tecnología de la información.

3.3 OBJETIVOS ESPECÍFICOS

- Identificar los riesgos en ciberseguridad mediante investigación documental para la protección de los estudiantes de básica secundaria en Colombia y su entorno familiar.

- Explicar las herramientas de ciberseguridad que protegen la confidencialidad, integridad y disponibilidad de la información para una navegación segura de los estudiantes al usar equipos personales e institucionales.

- Proponer buenas prácticas de seguridad de la información para que sirvan de guía a los docentes, padres de familia y el entorno estudiantil.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

Para entender el tema y el propósito de la monografía del trabajo de grado, primero es necesario tener en cuenta la relevancia del concepto de ciberseguridad y entender su repercusión en diversos contextos sociales; de esta manera, se buscarán los medios para salvaguardar estos datos tan importantes para los estudiantes y el sector educativo; claro está, considerando las diversas normas vigentes, entre las que se incluye la ISO 27001, que proporciona los requisitos necesarios para establecer un Sistema de Gestión de Seguridad de la Información.

4.1.1 Riesgos de Seguridad de la Información

Es primordial salvaguardar los datos y sistemas de una organización porque los riesgos pueden surgir de varias amenazas, vulnerabilidades y fallos humanos. Estos son aspectos constantes en el mundo digital contemporáneo; a medida que la dependencia de los sistemas informáticos, las amenazas y la protección de nuestros datos se intensifica.

4.1.1.1 Casos de uso de la cuantificación de riesgos cibernéticos

Cuando se trata de implementar de manera práctica esta técnica de medición de riesgos, estos son algunos ejemplos de uso:

- **Definición y evaluación de estrategias de ciberseguridad**: analiza y evalúa la eficacia de diversas tácticas de seguridad. Esta metodología contribuye a ajustar y perfeccionar las prácticas de seguridad actuales, obteniendo datos de gran relevancia para la asignación de prioridades en los Planes Estratégicos de ciberseguridad.
- **Evaluación en términos cuantitativos de la postura de riesgo de ciberseguridad**: evalúa las posibles pérdidas económicas en caso de un ciberataque o que se concreten los distintos escenarios de riesgo propuestos. Promueve la realización de elecciones fundamentadas acerca de las medidas de mitigación.

- **Priorización de inversiones en seguridad:** ayuda a las organizaciones a identificar las áreas más críticas asigna recursos de manera óptima, permite evaluar diferentes escenarios y determinar dónde invertir para maximizar la protección.
- **Es un aliado más en los procesos de Deal:** ofrece información de gran utilidad durante los procesos de M&A, obteniendo con detalle los riesgos y su correspondiente cuantía para ajustar las valoraciones de acuerdo con los resultados obtenidos.

4.1.1.2 ¿Qué es la gestión de riesgos cibernéticos?

Es el proceso de identificación, asignación de prioridad, gestión y monitorización de los riesgos vinculados a los sistemas de información.

En la actualidad, compañías de todas las industrias se apoyan en las tecnologías de la información para realizar labores comerciales esenciales, enfrentándose a peligros como los cibercriminales, fallos de los trabajadores, catástrofes naturales y otras amenazas a la ciberseguridad.

Estos riesgos tienen el potencial de desmantelar sistemas vitales o generar problemas de otras maneras, lo que resulta en la pérdida de ingresos, el hurto de información, perjuicio a la reputación a largo plazo y sanciones legales; sin embargo no pueden ser erradicados, porque pueden contribuir a disminuir el impacto y la probabilidad de amenazas.

- **El proceso de gestión de riesgos de ciberseguridad**

Es un proceso complejo y constante, motivo por el cual las compañías se encuentran con dudas acerca de las estrategias de los criminales y sus propias vulnerabilidades. Entre las metodologías empleadas para evaluar y gestionar estos riesgos se encuentran OCTAVE, MAGERIT y MEHARI, que asisten en la detección de vulnerabilidades y en la formulación de planes de mitigación.

El Instituto Nacional de Estándares y Tecnología (NIST) recomienda que las instituciones lleven a cabo un análisis constante de su gestión de riesgos para adaptarse a desafíos emergentes. La estrategia para la ciberseguridad del NIST (NIST CSF) y la estrategia para la administración de riesgos (NIST RMF) son herramientas fundamentales en este método. Los medios tecnológicos pueden contribuir a disminuir el impacto y la probabilidad de amenazas.

- **¿Por qué es importante la gestión del riesgo cibernético?**

Conforme se expanden los ambientes tecnológicos, también lo hace la superficie de ataque, incrementando así la susceptibilidad a ataques cibernéticos. Las acciones de

administración de riesgos asisten a las entidades en la identificación y priorización de las amenazas más críticas, mejorando de esta manera la distribución de recursos. Esto implica acatar normativas como el RGPD y el estándar PCI DSS, lo que resulta decisivo para prevenir penalizaciones. Las técnicas empleadas comprenden el marco de administración de riesgos del NIST (NIST RMF) y otros estándares como la ISO 27001. Además, es esencial llevar a cabo un inventario de activos, detectar posibles riesgos y definir controles apropiados.

La formación continua del personal y la implementación de un equipo de respuesta a incidentes son características clave para fortalecer la postura de seguridad en cualquier organización.

- **Todo lo que deberías saber de la gestión de riesgos en ciberseguridad**

¿Quieres hacer que la ciberseguridad sea algo sencillo y potente para tu negocio? Presta mucha atención a las siguientes líneas, porque te vamos a contar cómo gestionar los riesgos de ciberseguridad, así como algunas recomendaciones al respecto.

¿Si desea convertir la ciberseguridad en algo simple y eficaz para su empresa?

Es necesario tener presente las siguientes recomendaciones.

- **Recomendaciones para aumentar la ciberseguridad:**

    - Concientizar al personal de la entidad, ya que los fallos humanos son los responsables de la mayoría de los ataques en ciberseguridad.
    - Detecta y rectifica tus vulnerabilidades antes, durante y después de establecer medidas de protección contra ataques.
    - Proteger los datos a través de copias de seguridad y recuperación de datos.
    - Elabora y desarrolla un plan de recuperación que garantice la continuidad de la organización.
    - Configura y controla el acceso de los usuarios a las diferentes aplicaciones locales o en la nube.
- **Comportamientos que provocan riesgos de ciberseguridad en la empresa**

    - Dejar los dispositivos abiertos.
    - Usar redes sociales en equipos de empresa.
    - Utilizar dispositivos externos.
    - No realizar auditorías de ciberseguridad.
    - Enviar emails en masa a los clientes.
    - Carecer de información acerca de incidentes o problemas con los equipos de la empresa.
    - Falta de copias de seguridad, uso indebido de permisos y contraseñas,
    - Abrir emails o archivos adjuntos de individuos desconocido.

- Equipos sin antivirus y actualización de software.

- **Ventajas de gestionar correctamente los riesgos de ciberseguridad**

Reduce el peligro de pérdida de datos en la entidad, potenciar la imagen de la empresa, mejorar la experiencia del usuario, incrementar la ciberseguridad, mantener la continuidad en el funcionamiento y servicio, garantiza el respeto de las regulaciones de la organización, incrementa su competitividad, previene que la información sea divulgada a personas o sistemas no autorizados, reduce costos y simplifica.

- **Cómo gestionar los riesgos**

La estrategia más eficaz para gestionar los riesgos en ciberseguridad consiste en realizar un análisis de GAP en función de las normas estándar de seguridad de la información, como ISO27001, ENS o DORA. Este tipo de evaluación se realiza mediante una actualización del SGSI (Sistema de Gestión de la Seguridad de la Información). De esta manera, se pueden identificar los riesgos e instaurar controles, además se define un plan de acción, que permita valorar la eficacia de los controles implementados y la gestión del Plan de Acción para abordar los riesgos excedidos, los "incumplimientos" y las "no conformidades" detectadas. Existen herramientas que promueven la automatización de estas tareas.

4.1.2 Teorías de ataques de seguridad

La protección de la información se ve amenazada y puede poner en riesgo la integridad, la privacidad y la disponibilidad de la información. Los atacantes exploran continuamente nuevas maneras de aprovechar las vulnerabilidades, por lo que resulta complejo mantenerse al día con las más recientes técnicas y estrategias de ataques informáticos.

4.1.2.1 ¿Qué es un ataque cibernético?

Un ataque cibernético se refiere a cualquier intento deliberado de sustraer, descubrir, modificar, desactivar o eliminar datos, aplicaciones u otros recursos mediante el acceso no permitido a una red, sistema de computación o aparato digital. Los creadores de amenazas realizan ataques informáticos por diversas razones, que van desde hurtos simples hasta acciones bélicas. Implementa diferentes estrategias, tales como ataques de software maliciosos, fraudes de ingeniería social y hurto de contraseñas, para conseguir acceso no permitido a sus sistemas.

Los ataques cibernéticos poseen la habilidad de alterar, perjudicar e incluso destruir compañías. Una filtración de datos tiene un costo medio de 4.35 millones de dólares. Este

desembolso abarca los gastos para identificar la filtración y reaccionar ante ella, el periodo de parada y la duración de la inactividad.

De acuerdo con una proyección, para 2025, el crimen cibernético generará 10.5 billones de dólares anuales en la economía global.

- **¿Por qué ocurren los ataques cibernéticos?**

Existen tres categorías principales: delictivos, políticos y personales.

Los ciberdelincuentes intentan conseguir ganancias financieras mediante el hurto de dinero, la extracción de datos o la interrupción de actividades de negocio. Tienen la capacidad de acceder a una cuenta bancaria para robar dinero de manera directa o emplear tácticas de ingeniería social para engañar a las personas para que les transfieran dinero, siendo esa otra forma de hurtos de identidad, comercializarlos en la red sombría o conservarlos para solicitar rescates.

La extorsión es otra estrategia popular. Los hackers usan ransomware, ataques de denegación distribuida del servicio (DDoS) u otras tácticas para secuestrar datos o dispositivos hasta que una empresa pague un rescate. Según el X-Force Threat Intelligence Index, el objetivo de 27 % de los ataques cibernéticos es extorsionar a sus víctimas.

Las personas que actúan por motivos personales, como empleados descontentos, quienes buscan principalmente una retribución por algún desdén percibido son capaces de sustraer dinero, datos íntimos o alterar los sistemas de una empresa.

Los atacantes de procedencia política suelen tener conexiones con la guerra, el terrorismo en el ciberespacio o el "hacker ismo". En el conflicto cibernético, los miembros de las naciones a menudo atacan a las instituciones gubernamentales o a la infraestructura esencial de sus oponentes. Por ejemplo, desde el comienzo del conflicto bélico entre Rusia y Ucrania, ambas naciones han sufrido una serie de ataques informáticos contra entidades esenciales. Entre las motivaciones menos comunes de los ataques cibernéticos podemos mencionar el espionaje corporativo, en el que los hackers roban propiedad intelectual para obtener una ventaja desleal sobre sus competidores.

- **¿Quién está detrás de los ataques cibernéticos?**

El delito organizado, entidades gubernamentales e individuos pueden desencadenar ataques informáticos. Se pueden categorizar los actores de amenazas en: amenazas externas y amenazas internas.

  - **Amenazas externas:** no tienen autorización para utilizar una red o dispositivo, pero lo realizan de alguna manera. incluyen grupos delictivos organizados, hackers profesionales, organizaciones respaldadas por el gobierno, hacktivistas y hackers entusiastas.

- **Amenazas internas:** son usuarios que poseen un acceso legítimo y autorizado a los recursos de una entidad y utilizan de manera indebida sus privilegios, ya sea de manera deliberada o accidental. Esta categorización incluye empleados, consumidores, proveedores con acceso al sistema y empleadores.

- **¿Cuál es el objetivo de los ataques cibernéticos?**

Los actores de amenazas suelen infiltrarse en las redes de computación en busca de algo concreto. Los objetivos compartidos comprenden:

- Dinero
- Información económica de las compañías
- Catálogos de clientes
- Recopilación de listas de clientes
- Información de los clientes, incluyendo datos de identificación personal (PII) u otros datos personales de carácter confidencial.
- Dirección de email y claves para iniciar sesión.
- Propiedad intelectual, tales como secretos de negocio o diseños de artículos.

- **¿Cómo afectan los ataques cibernéticos a las empresas?**

Si logran su objetivo, los ataques informáticos pueden perjudicar a las entidades hasta el punto de provocar un período de inactividad, pérdida de información y pérdida de dinero. Ejemplos:

- Los ciberdelincuentes poseen la habilidad para utilizar malware o ataques de interrupción del servicio para causar fallos en el sistema o el servidor. Este lapso de suspensión puede conllevar interrupciones en el servicio y pérdidas financieras considerables.

- En el caso de los ataques de inyección SQL posibilitan a los hackers modificar, suprimir o sustraer información de un sistema.

- Los ataques de ransomware pueden desactivar un sistema hasta que la empresa pague un rescate al atacante.

- Al referirse a los ataques de phishing, éstos permiten a los ciberdelincuentes engañar a las personas con el fin de transferirles dinero o información personal.

Las personas afectadas por ataques cibernéticos también pueden sufrir efectos que van más allá del objetivo directo. En 2021, DarkSide, una banda de ransomware, realizó un ataque contra la empresa Colonial Pipeline, dueña del mayor tubo de aceite de Estados Unidos. Los atacantes ingresaron a la red empresarial utilizando una contraseña vulnerada. El oleoducto, que provee el 45% del gas, gasóleo y combustible para aviones

a la costa este de Estados Unidos, se cerró, provocando de esta manera una escasez generalizada de combustible. Los criminales informáticos solicitaron un pago de casi 5 millones de dólares en la criptomoneda bitcoin, lo que Colonial Pipeline finalmente pago.

- **Las principales causas que pueden generar un ataque cibernético**

Ingeniería social para manipular mediante chantajes a los trabajadores más hábiles con el propósito de obtener accesos a sistemas esenciales con información confidencial de gran relevancia para la organización.

- Empleados malintencionados: que cooperaban con ciberdelincuentes con el propósito de perjudicar a la empresa con fines de lucro o por razones de anarquía.
- Fallas de seguridad en los sistemas informático: provocados por los programadores al diseñar los sistemas y que son utilizados por los atacantes.
- Propagación de datos confidenciales: por los empleados de manera accidental o deliberada, frecuentemente el eslabón más vulnerable de la cadena suelen ser los mismos trabajadores de las empresas.
- Pérdida o robo de aparatos electrónicos: que protegen información privada de la organización mediante el uso de datos confidenciales a través de empleados o infiltrados.
- Poco control por parte de terceros: normalmente ocurre que empresas que llevan a cabo alguna actividad tercerizada que podría ser objeto de ataque o utilizada como un caballo de troya para alcanzar el objetivo.

4.1.2.2 ¿Cuáles son los tipos comunes de ataques cibernéticos?

- **Ataques de denegación del servicio:** este tipo de ataques de denegación de servicio (DoS) y de denegación de servicio distribuida (DDoS) agotan los recursos de un sistema con tráfico de datos fraudulento. El flujo de información satura el sistema, obstaculizando la respuesta a solicitudes legítimas y reduciendo la habilidad del sistema para funcionar.

  La diferencia entre los ataques de DoS y los de DDoS se basa solo en que los primeros utilizan un solo origen para generar tráfico fraudulento, mientras que los últimos utilizan múltiples orígenes. Estas últimas suelen llevarse a cabo mediante una botnet, una red de dispositivos conectados a Internet e infectados con malware bajo la gestión de un hacker. Las botnets pueden incluir portátiles, teléfonos inteligentes y Internet de las cosas (IoT). Frecuentemente, las víctimas desconocen cuándo éste se ha activado y secuestrado sus equipos.

- **Cuenta comprometida:** una cuenta comprometida es el producto de ataques donde los hackers se apropian de la cuenta de un usuario legítimo para llevar a

cabo acciones perjudiciales. Los criminales informáticos tienen múltiples formas de infiltrarse en la cuenta de un usuario. Son capaces de sustraer credenciales mediante ataques de phishing o adquirir bases de datos de contraseñas sustraídas de la Red Roja. Son capaces de emplear herramientas de ataque de contraseñas como **Hashcat y John the Ripper** para descifrar contraseñas codificadas u estructurar ataques de fuerza bruta, donde operan scripts automatizados o bots para crear y verificar posibles contraseñas hasta que una funcione.

Esta cuenta surge a raíz de ataques en los que los hackers se usurpan de la cuenta de un usuario legítimo para realizar acciones dañinas. Las técnicas de infiltración de los ciberdelincuentes en la cuenta de un usuario son diversas. Es su habilidad para robar credenciales a través de ataques de phishing u obtener bases de datos de contraseñas extraídas de la red oscura. En estos escenarios, emplean scripts automatizados o bots para generar y analizar numerosas contraseñas hasta que una sea implementada.

- **Ataques de intermediario (MitM):** también conocido como "ataque de escucha subrepticia", un hacker intercepta de manera secreta las conversaciones entre dos individuos o entre un usuario y un servidor. Los ataques de MitM generalmente se realizan mediante redes de Wi-Fi públicas no seguras.

  Los hackers pueden acceder y leer los correos de un usuario o incluso modificarlos de manera secreta antes de que arriben al receptor. En un ataque de captura de sesiones, el hacker interfiere en la conexión entre un cliente y un servidor que alberga activos de gran relevancia, como una base de datos privada de la compañía. El hacker sincroniza su dirección IP, lleva al servidor a creer que es un usuario auténtico en una sesión legítima.

- **Ataque a la cadena de suministro:** los hackers se infiltran en una empresa, dirigiendo sus ataques hacia sus proveedores de software, proveedores de materiales y otros proveedores de servicios. Un caso ilustrativo en 2020, las autoridades gubernamentales de Rusia ingresaron al proveedor de software SolarWinds y difundieron malware a sus usuarios, asumiendo que se estaba actualizando el software. Malware otorgó a los espías rusos la posibilidad de acceder a la información privada de varias agencias gubernamentales estadounidenses.

4.1.3 Teorías de Ingeniería Social

¿Qué es ingeniería social?

Se vincula con el acto ilegal de obtener información a través de la manipulación psicológica. Los atacantes se presentan como personas. organismos legítimos, o empleados de una empresa o instituciones financieras, con la finalidad de obtener la confianza de la víctima y conseguir que esta revele datos delicados. Este tipo de ataques informáticos representan aproximadamente el 98%, resaltando de esta manera su prevalencia y efectividad.

4.1.3.1 Principios de la Ingeniería Social

- **El usuario es el Eslabón más frágil:** sostiene que, en cualquier sistema de defensa, los seres humanos son el pilar más frágil.
- **Manipulación Emocional**: utilizan emociones tales como el miedo, la necesidad, la culpa o la curiosidad para influir en las decisiones de sus víctimas; logrando que las personas actúen de manera impulsiva y sin hacer una reflexión crítica sobre ello**.**
- **Construcción de Confianza**: los agresores se presentan como figuras de autoridad o de seguridad con el objetivo de ganar la confianza de las víctimas.
- **Recolección de datos:** previo a realizar un ataque, los ciberdelincuentes tienden a indagar en profundidad en sus víctimas para recolectar información relevante que les facilite ajustar su método y hacerlo más convincente. Esta fase puede incluir la recopilación de datos a través de redes sociales o en comunicados previos.
- **Explotación de Vulnerabilidades Psicológicas**: los atacantes se valen de las falencias psicológicas y sociales, tales como el deseo humano de asistencia, la ignorancia en ciberseguridad o la presión social, para influenciar a sus víctimas.
- **Desensibilización a la Seguridad**: muchas personas desconocen el verdadero valor de su información personal o el peligro que implican sus acciones en internet. Esto permite que los atacantes consigan sus metas sin que las víctimas se perciban amenazadas.
- **Urgencia y Escasez**: generar un sentimiento de urgencia (por ejemplo, sosteniendo que una oferta es escasa) puede impulsar a las personas a actuar de

manera precipitada sin tener en cuenta las repercusiones, lo que es una táctica habitual en los ataques de ingeniería social.

4.1.3.2 Fases de un ataque en ingeniería social.

- **Preparación del entorno:** en esta etapa el atacante recolecta datos acerca del contexto en el que pretende realizar el delito informático. Esto conlleva examinar la entidad objetivo y los trabajadores que podrían estar vulnerables a la manipulación.
- **Análisis de la organización y los empleados:** el atacante se adentra en la entidad y lleva a cabo un estudio minucioso de los trabajadores. Busca datos acerca de las jerarquías, las obligaciones laborales, las interacciones entre los trabajadores y cualquier otro dato que pueda ser beneficioso para el ataque. Además, tiene la posibilidad de investigar mediante fuentes públicas y redes sociales para recolectar datos personales acerca de los trabajadores.
- **Planificación de posibles vectores:** una vez que se ha recopilado la información requerida sobre la organización y sus empleados, el atacante comienza a planificar los potenciales objetivos de su ataque, lo que se parece a la tercera fase de un ataque en el ámbito de la ingeniería social. Esto implica identificar las deficiencias o vulnerabilidades en el sistema de seguridad de la organización, así como los procedimientos y estrategias que se podrían utilizar para capitalizar dichas debilidades.
- **Seleccionar víctimas:** el atacante selecciona a las víctimas de forma exacta que serán el objetivo principal del ataque. Se basa en la información obtenida en las etapas anteriores y podría necesitar la identificación de empleados que puedan ser más susceptibles a ser manipulados o que tengan acceso a datos sensibles o privilegiados.
- **Desarrollo del pretexto:** escogidas las víctimas, el atacante elabora un motivo persuasivo para ejecutar el ataque, lo que conduce a la última de las etapas de un ataque de ingeniería social que consiste en llevar la creación de una historia o un escenario imaginario que facilite al atacante construir una relación de confianza con la víctima y convencerla para que lleve a cabo acciones que favorezcan al atacante.

4.1.3.3 ¿Cuáles son las consecuencias de la ingeniería social?

Los efectos de la ingeniería resultan perjudiciales para los usuarios individuales y las organizaciones. Para los primeros, podría conllevar la pérdida de dinero y/o cuentas de

usuario, sumado a las dificultades psicológicas derivadas de este tipo de ataques, se suma la pérdida de confianza o el sentimiento de culpabilidad y vergüenza que genera ser víctimas de ciertos tipos de ingeniería social.

Para las organizaciones, supone la amenaza de sufrir otros tipos de ciberataques, como el ransomware, y tener acceso a la red interna de la entidad, desde la cual pueden llevar a cabo diferentes acciones: el robo de datos delicados, la eliminación de información crucial o el hurto de dinero, o las potenciales extorsiones para no revelar la información extraída.

4.1.3.4 ¿Existe alguna herramienta informática para protegernos de la ingeniería social?

No, los ataques de ingeniería social son muy difíciles de identificar. Los ciberdelincuentes usan diferentes técnicas psicológicas y sociales, distintos tipos de dispositivos y plataformas para engañar a las personas.

4.1.3.5 ¿Qué canales utilizan los ciberdelincuentes para los ataques de ingeniería social?

Los delincuentes cibernéticos manipulan y engañan a las personas mediante:

- Llamadas telefónicas
- Visita personal a la vivienda de las victimas
- Aplicaciones de mensajería instantánea
- Correos electrónicos
- Plataformas sociales

4.1.3.6 ¿Qué porcentaje de hackers utiliza la ingeniería social?

La ingeniería social es un táctica empleada frecuentemente por los hackers, en aproximadamente el 90% de los ataques que resultan exitosos.

4.1.4 Autores académicos y expertos reconocidos en ciberseguridad

“Alrededor del 68 % de las filtraciones en una encuesta de 2024 se debieron a factores humanos, como el engaño de una persona mediante una estafa de ingeniería social o un error. En 2023, esta cifra fue del 74 %”[2]

> “La ciberseguridad, la práctica de proteger sistemas, redes y datos de ataques maliciosos, es esencial para salvaguardar la seguridad y la privacidad de los niños y adolescentes en el mundo digital. Los menores son particularmente vulnerables a los ciberataques, ya que pueden carecer de la experiencia o el conocimiento para identificar las amenazas en línea. Por lo tanto, es responsabilidad de las instituciones educativas y los padres educar a los niños sobre ciberseguridad y proporcionarles las herramientas que necesitan para protegerse a sí mismos y a sus datos”[3]

“El ciberdelito representa un reto, ataca en diferentes sectores, tanto públicos como privados que utilizan el ciberespacio y las nuevas tecnologías como herramientas para el desarrollo de las actividades cotidianas, teniendo presente el ambiente escolar como uno de los escenarios más propensos a este tipo de amenazas, sobre todo la población constituyente, pues cada actor de la comunidad educativa representa un factor de riesgo”[4]

[2] JONES, Anthony. Estadísticas de ciberseguridad sobre errores humanos.(2024). [consultado 9 de septiembre 2025]. Disponible en: https://www.ispartnersllc.com/blog/human-error-cybersecurity-statistics/

[3] TRIGOSO, Javier R. Protegiendo el futuro digital: La importancia de la ciberseguridad en la enseñanza primaria y secundaria. [consultado 12 de septiembre 2025]. Disponible en: https://www.linkedin.com/pulse/protegiendo-el-futuro-digital-la-importancia-de-en-y-trigoso-trigoso-dkbhe/

[4] CASTILLO, Jaquelin. Análisis de la ciberseguridad en espacios educativos pertenecientes a la Fuerza Aeroespacial Colombiana. [consultado 15 de septiembre 2025]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/9234359.pdf

5 MARCO LEGAL

En los años recientes, la legislación sobre Ciberseguridad en Colombia se ha robustecido para enfrentar los retos y peligros vinculados a los ataques cibernéticos. A continuación, se citan algunas normativas pertinentes.

5.1 LEY DE PROTECCIÓN DE DATOS PERSONALES

Se enfoca en la claridad de las bases de datos y en el derecho cuando la información personal será recopilada para un objetivo concreto, específicamente comercial. La Ley de Protección de Datos Personales (Ley 1581 de 2012) reconoce y salvaguarda el derecho que todos tenemos de conocer, actualizar y rectificar los datos que se han recolectado sobre nosotros en bases de datos o archivos que sean susceptibles de ser tratados por organismos públicos o privados.

> "Los datos personales están conformados por aquella información asociada a ti y que permite tu identificación; por ejemplo: tu número de identificación, lugar de nacimiento, estado civil, edad, lugar de residencia, trayectoria académica, laboral y/o profesional. Existe también información relacionada con datos personas que es sensible como tu estado de salud, tus características físicas, ideología política, vida sexual, religión, entre otros aspectos".[5]

5.2 NORMATIVA 620 DE 2020

Esta ley establece normas sobre delitos informáticos en Colombia y define las categorías penales vinculadas al acceso no autorizado a sistemas de computación, daño informático, sabotaje informático, uso de software malintencionado, entre otros.

Este reglamento acata la Ley 1273 de 2009 y dicta normas concretas acerca de la salvaguarda de la información y los sistemas de información en el contexto de las instituciones públicas. Fue un hito para que en Colombia se empezara a entender amenazas como los ataques de denegación de servicios (DDoS), la totalidad de la seguridad digital, la vulnerabilidad de infraestructuras vitales, entre otras cuestiones de seguridad. La legislación dicta reglas acerca de crímenes informáticos en Colombia y establece las clases penales vinculadas con el acceso no permitido a sistemas de computación, perjuicio y sabotaje informático, empleo de software malintencionado, entre otras.

[5] DIAN. GOV.CO. Protección de datos personales. [consultado 29 de octubre de 2024]. Disponible en: https://www.dian.gov.co/atencionciudadano/Seguridad-de-la-Informacion/Paginas/Proteccion-de-datos-personales.aspx

5.2.2 El Manual de Gobierno Digital

Documento que incluye las directrices para la puesta en marcha de la política. Es un dispositivo centralizado, normalizado y de uso sencillo que establece las pautas y regulaciones para la implementación de la política de Gobierno Digital en Colombia y para las entidades públicas porque proporciona una guía sobre cómo utilizar las tecnologías de la información y la comunicación (TIC) para mejorar la gestión pública y la calidad de vida de los residentes. Las disposiciones que lo apoyan son:

5.2.3 Decreto 767 del 16 de mayo de 2022.

La nueva política de Gobierno digital fue impartida mediante este decreto, que establece:

- Directrices básicas de la Política de Gobierno Digital en Colombia y sustituye el Capítulo 1 del Título 9 de la Sección 2 del Libro 2 del Decreto 1078 de 2015.
- Transformación Digital de ciudades y regiones inteligentes.
- Innovación Digital Pública: dentro del contexto de la Política de Gobierno Digital.
- Política de Gobierno Digital en Colombia: vista como una táctica gubernamental destinada a optimizar la oferta de servicios estatales y fortalecer la relación entre ciudadanos e instituciones públicas mediante la utilización de las TIC.

Figura 1. Política de Gobierno Digital

Fuente: GOBIERNO DIGITAL MINTIC. Política de Gobierno Digital. [Consultado el 10, junio, 2023], Disponible en: https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/

La implementación del gobierno digital implica el uso de diversas herramientas y metodologías que facilitan la transformación digital de las entidades públicas. La siguiente tabla presenta un resumen de las herramientas y tecnologías clave que las instituciones gubernamentales pueden emplear para impulsar su transformación digital y ofrecer servicios más eficientes y accesibles a los ciudadanos.

Tabla 1. Herramientas implementación del gobierno digital

HERRAMIENTAS	DESCRIPCION
MANUAL DEL GOBIERNO DIGITAL	• Determina lineamientos, modelos y acciones a producir.
MARCO DE ARQUITECTURA EMPRESARIAL	• Solucionar problemas u oportunidades empresariales complejas.
SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	• Programa de competencias en innovación de los servidores públicos para la generación de valor público.
MÁXIMA VELOCIDAD:	• La gamificación es una estrategia que busca desarrollar una serie de desafíos centrados en la política GB.
DATA SANDBOX	• Espacio para experimentar, probar y desarrollar proyectos piloto de analítica y Big Data.
SOFTWARE LIBRE	• Para resolver necesidades y/o problemas de la administración pública.
DATOS ABIERTOS	• Impulsa y faculta las condiciones para usar y generar valor, partiendo de datos abiertos de Gobierno.
RED CIO	• Facilita la interacción entre los responsables de tecnología pública y una comunidad de cooperación.
CENTRO DE CONTACTO	• Centro de atención, supervisión y apoyo para el Gobierno Digital a través de un centro de llamadas.
GUIA IMPLEMENTACIÓN GOBIERNO DIGITAL	• Documento que presenta las directrices, modelos y medidas a implementar para el avance de los componentes transversales vinculados con el Gobierno Digital.
ACUERDO MARCO DE PRECIOS	• Permite a las instituciones estatales obtener productos y servicios de Tecnología de la Información mediante la Tienda Virtual del Estado de Colombia.
ADOPCIÓN DE IPV6	• Determina los lineamientos y políticas para que las empresas del gobierno aprueben con éxito IPv6.
AUTODIAGNÓSTICO	• Herramienta para medir y determinar el avance hacia la implementación y puesta en marcha de las políticas de gobierno digital.

Fuente: GOBIERNO DIGITAL. TIC. [Consultado el 12, noviembre, 2024], Disponible en: https://gobiernodigital.mintic.gov.co/portal/Biblioteca/

5.2.4 Decreto 338 de 2022

Este decreto establece la política de seguridad digital, de igual forma puntualiza las competencias y funciones del gobierno para proteger los sistemas informáticos, redes, infraestructuras y servicios digitales en el ciberespacio colombiano.

> "El 26 de mayo de 2015, el Gobierno Nacional y el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), expidió el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital y crear el modelo y las instancias de Gobernanza de Seguridad Digital. El objetivo de este decreto se centró en promover el uso y apropiación de las TIC entre los ciudadanos, las empresas, el Gobierno y demás instancias nacionales como soporte del desarrollo social, económico y político de la Nación".[6]

Entre sus objetivos se encuentran:

- Recomendar al gobierno medidas estratégicas para responder y recuperarse de acciones que comprometan o amenacen los sistemas informáticos y redes.
- Apoyar la adecuada articulación y coordinación entre entidades, autoridades y órganos para optimizar el ejercicio de sus competencias y funciones.
- Fortalecer las habilidades de las partes interesadas para identificar, administrar y mitigar los peligros de seguridad digital.

5.2.5 Ley 2489 de 2025

Se define los principios y reglas para salvaguardar y asegurar los derechos de los niños, niñas y adolescentes en Colombia. Los aspectos más destacados de la ley en cuanto a la protección de los menores en el ambiente digital:
Artículo 1: establece que la ley busca como objetivo generar espacios digitales seguros y sanos para niños, niñas y adolescentes en Colombia, mediante una política pública que coordine esfuerzos entre entidades del gobierno, padres de familia, organizaciones y la sociedad en general, con el fin de proteger sus derechos, fomentar costumbres tecnológicas saludables y evitar peligros en línea.
Artículo 6: señala que el Ministerio de Educación, en colaboración con el Ministerio de Tecnologías, definirá directrices para que las entidades educativas incorporen estrategias en sus programas académicos, fomentando habilidades tecnológicas, socioemocionales en los jóvenes y niños, para identificar y prevenir riesgos en los entornos digitales.

[6] TUS DATOS.CO ¿Qué es el Decreto 338 (15, diciembre, 2022). Establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital. [Consultado el 10, junio, 2023]. Disponible en: https://www.tusdatos.co/blog/que-es-el-decreto-338-2022

5.2.6 Ley 1273 de 2009

Hace frente y contrarresta varios delitos informáticos. Esta ley establece:

- Efectuar cambios en el código penal para proteger la información y los datos, e incluye sistemas que utilizan tecnologías de información y comunicaciones.
- Colombia ha utilizado instrumentos eficientes para luchar contra el problema de los delitos informáticos, en diversas áreas como: la integridad, la privacidad, la administración de datos y los sistemas de computación.
- Creó nuevas categorías de delitos informáticos y protección de información y datos: en este marco, aplica sanciones de cárcel y específicas a quienes perpetran estos crímenes. El Título VII BIS, también conocido como "de salvaguarda de la información y los datos", se incorporó al Código Penal de Colombia mediante la citada legislación, con sentencias de cárcel que oscilan entre 48 y 120 meses, y multas que oscilan entre 200 y 1500 salarios mínimos legales.
- Penalizaciones que se encuentran entre los 200 y 1500 sueldos mínimos legales mensuales actuales.
- El acto de llevar a cabo realizar actos delictivos mediante dispositivos tecnológicos, electrónicos o telemáticos, tal como se indica en el artículo 58 del Código Penal.
- Destaca la implementación de nuevas categorías de penalizaciones para los crímenes informáticos y la protección de la información y datos, con condenas de prisión que varían entre 48 y 120 meses, y multas que varían entre 200 y 1500 salarios mínimos legales; sanciones entre los 200 y 1500 salarios mínimos legales mensuales vigentes.

A continuación, se menciona los siguientes artículos:

- Artículo 269ª: Abuso de acceso a un sistema informático.
- Artículo 269b: impedimento ilegal de un sistema informático o red de telecomunicación
- Artículo 269c prohíbe la captura de datos.
- Artículo 269d: daños informáticos.
- Artículo 269e: Aplicación de software espía.
- Artículo 269f: hurto de datos informáticos.
- Artículo 269g: falsificación de datos informáticos.

5.3 MARCO CONCEPTUAL

En esta sección se tratarán los conceptos de ciberseguridad, ciberdefensa, ciber inteligencia, seguridad de la información y seguridad digital pueden categorizarse como grupos de recursos, herramientas o habilidades que los gobiernos o la población poseen para enfrentar los variados riesgos y amenazas del mundo digital, que se corresponden con respuestas reactivas o preventivas de cada autoridad, o grupo de individuos.

Definir la forma en que los usuarios protegen su información de la vulnerabilidad, identificar las acciones más comunes de robo de datos y examinar datos de virus.

5.3.1 ¿Qué es Ciberseguridad?

El futuro de la tecnología ya está presente, sin embargo, conlleva riesgos significativos a menos que entienda cómo resguardarse ante amenazas cibernéticas y violaciones de datos, proteger las redes, los equipos y los datos frente a ataques, daños o acceso no autorizado, mediante diferentes medios como computadoras, redes informáticas, o smartphones; por lo tanto, es vital proteger la información, prevenir su hurto y aplicar una serie de medidas para garantizar que la información se envíe de un lugar a otro y conservar su integridad.

> "La ciberseguridad tiene el fin de proteger a los ciudadanos que interactúan en espacios digitales y los activos de Estado en el Ciberespacio y comprende el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para dicho fin".[7]

Diversas tecnologías en desarrollo que aportan significativos y novedosos beneficios tanto para las compañías como para las personas, y a la vez ofrecen nuevas oportunidades para que los actores de riesgo y los ciberdelincuentes realicen ataques cada vez más sofisticados.

- La aplicación a gran escala del cloud computing puede intensificar la complejidad en la gestión de redes y elevar el riesgo de errores en la configuración de la nube, de API no protegidas y de otras vías que los piratas informáticos pueden explotar.
- Más trabajo remoto, empleo mixto y políticas de "lleva tu propio dispositivo" (BYOD) implican un incremento en las conexiones, dispositivos, aplicaciones y datos que los equipos de seguridad deben resguardar.

[7] GOV. CO, Colombia aprende. Seguridad Digital. [Consultado el 15, junio, 2023]. Disponible en: https://www.colombiaaprende.edu.co/recurso-coleccion/seguridad-digital#

- La expansión del Internet de las cosas (IoT) y los aparatos conectados, muchos de los cuales carecen de seguridad o están mal protegidos por defecto, pueden propiciar el secuestro por parte de actores malintencionados.
- El avance de la inteligencia artificial (IA), en particular la IA generativa, presenta un panorama de riesgos completamente inéditos que los piratas informáticos ya están utilizando mediante la administración de estímulos y otras tácticas. Según una reciente investigación del IBM Institute for Business Value, solo el 24% de las iniciativas de Inteligencia Artificial generativa poseen protección.

5.3.1.1 Los datos son importantes, pero ¿por qué?

En este siglo, la información se convierte en un tesoro y en un capital, dado que forman parte del derecho sagrado a la privacidad y a la vida privada. Así pues, todos los usuarios de internet tienen la obligación de considerar los datos como un bien personal que les pertenece a sí mismo, por lo que poseen el derecho a que las leyes los salvaguarden. Este derecho constitucional, vinculado a la protección y seguridad de la información personal, es estipulado por la Superintendencia de Industria y Comercio. Esta tiene la obligación de definir, regular la privacidad, investigar y sancionar el incumplimiento.

Los datos están transformándose en un recurso valioso para cambiar significativamente el sector educativo; incrementando la eficiencia y la experiencia del alumno en diversas instituciones educativas y se anticipa que su utilización seguirá en aumento. La información se ha convertido en un proceso de innovación e inspección de datos, con el propósito de simplificar la toma de decisiones; en tanto, los maestros poseen la habilidad de implementar procesos de evaluación, seguimiento de mejoras, modificar sus responsabilidades, prácticas y contenidos educativos mediante el análisis de datos.

5.3.1.2 Importancia de los datos dentro del contexto educativo

Dentro del contexto educativo, los datos potencian tanto la enseñanza y el aprendizaje para cumplir y decidir los siguientes aspectos:

- **Toma de decisiones fundamentadas:** posibilitan que las entidades educativas adopten decisiones fundamentadas en pruebas, por ejemplo, determina las áreas que necesitan mejoras, estudiando, modificando los métodos de enseñanza, los estándares de evaluación y la distribución de los recursos requeridos para potenciar toda la tarea.

- **Personalización del aprendizaje:** permite reconocer patrones en el comportamiento y rendimiento de los estudiantes; de esta manera, se

elaborarían intervenciones particulares para aquellos que requieren asistencia extra, promoviendo de esta manera la retención y el rendimiento académico.

- **Monitoreo del progreso estudiantil:** ayuda a realizar un seguimiento constante del progreso de los alumnos; asiste en la identificación de dificultades, sugiere y elabora soluciones viables para cada circunstancia.
- **Mejora continua:** proporcionan fundamento para un perfeccionamiento constante en el ejercicio de la instrucción. La transformación debe iniciarse con la actitud y el crecimiento profesional del equipo docente hasta la implementación e innovación de los programas de enseñanza.
- **Innovación en técnicas de enseñanza:** el estudio de grandes cantidades de información (big data) facilita la exploración.

5.3.2 El Sistema de Gestión de la Seguridad de la Información (SGSI)

El Sistema de Administración de Seguridad de Datos, ISMS), es el acrónimo de Sistema de Gestión de Seguridad de la Información y se refiere a un conjunto de políticas y procedimientos destinados a administrar de manera sistemática la información confidencial de una entidad. Es viable tanto en compañías de gran envergadura como en empresas de pequeña y mediana dimensión. Esta herramienta facilita la identificación y gestión de los riesgos vinculados a la gestión cotidiana de los datos. Al implementar un SGSI, las entidades pueden eliminar estos riesgos o implementar acciones apropiadas para reducir sus impactos.

> "El objetivo de un SGSI es minimizar el riesgo y garantizar la continuidad del negocio limitando proactivamente el impacto de una brecha de seguridad. Básicamente, busca lograr un sistema de prácticas por parte de todo el personal de la empresa para que esta no pierda información. Un SGSI generalmente aborda tanto el comportamiento y los procesos de los colaboradores, como los datos y la tecnología. No es solo un sistema de protección contra ciber ataques, va mucho más allá"[8]

La puesta en marcha de un SGSI posibilita que las organizaciones detecten, administren, disminuyan las amenazas a la información; asegurando de esta manera la continuidad del negocio, la observancia de las normativas y regulaciones actuales. Se segmenta en diversas etapas:

- Planificación: identificar requisitos y establecer un plan para el SGSI.
- Implementación: desarrollar políticas y procedimientos.
- Evaluación: revisar la eficacia del SGSI.
- Mejora continua: aplicar mejoras basadas en las evaluaciones realizadas.

[8] LOPEZ, Tania. SGSI: ¿Qué es y Cómo Implementarlo? [Consultado el 20, enero, 2023]. Disponible en: https://blog.innevo.com/que-es-sgsi

5.3.2.1 Norma ISO 27001 y SGSI

Para obtener la certificación ISO 27001, las organizaciones deben ajustar sus SGSI (sistemas de gestión de seguridad de la información) a los requerimientos de la norma ISO 27001. El objetivo de estas exigencias es apoyar a las organizaciones en la formación, preservación y perfeccionamiento continuo de su posición SGSI. La regulación se basa en el ciclo de gestión PDCA (Planificar, Realizar, Comprobar, Actuar), el cual permite a las organizaciones establecer, implementar, evaluar y mejorar de forma continua su SGSI.

> "La Organización Internacional de Estandarización, o ISO por sus siglas en inglés, es una de las organizaciones más reconocidas en el mundo en cuanto a estándares internacionales se refiere. ISO posee un conjunto de normas, en distintas áreas de la tecnología, comercio e industria. Una de esas normas es la norma 27001, la cual hace referencia a las políticas y procedimientos de la seguridad informática".[9]

El objetivo principal de la ISO 27001 es definir un esquema para gestionar la seguridad de la información, lo que incluye: reconocimiento y administración de riesgos.

Las entidades que consigan la acreditación ISO 27001 se caracterizan por su dedicación a la administración segura de la información, lo que conlleva la puesta en marcha de un sistema de gestión de seguridad de la información (SGSI) que se adhiere a las normativas internacionales. Esta acreditación no solo evidencia que las entidades poseen políticas y procesos sólidos para salvaguardar la información, sino que también garantiza que han llevado a cabo un estudio detallado de los peligros vinculados a la información que gestionan.

5.3.2.2 Componentes del SGSI

El SGSI es el principal enfoque de la norma ISO/IEC 27001. Dicho enfoque ayuda a una organización o empresa a preservar tres componentes claves:

- **Confidencialidad:** teniendo en cuenta que la información es propiedad de la compañía, garantizando que únicamente individuos autorizados tengan acceso a ella. Esto ocurre porque la información corporativa es privada y confidencial, no puede ser divulgada a terceros, como entidades, empresas o personas.
- **Integridad:** los datos deben permanecer exactos e inalterables, así como los procedimientos encargados de su utilización. La integridad asegura que la información sea precisa e inalterable y no se altere sin el consentimiento de la empresa.
- **Disponibilidad:** implica que cualquier modificación necesita ser copiada y registrada. En un SGSI, la disponibilidad permite que personas, empresas o

[9]ESGINNOVA GROUP. Concepto y definición de las siglas de ISO. [Consultado el 26, enero, 2023]. Disponible en: https://www.nueva-iso-14001.com/2020/12/concepto-y-definicion-de-las-siglas-de-iso/

procesos autorizados accedan a la información corporativa; asegurando que los sistemas estén disponibles.

5.3.2.3 Implementación del SGSI. Ciclo Deming y fases

La puesta en marcha de un SGSI se fundamenta en el Ciclo de Deming, reconocido como el método más empleado para el diseño del plan de mejora continua, con el objetivo de solucionar problemas, implementar ideas innovadoras y potenciar la calidad. Su nombre proviene de Edwards Deming, un autor y estadista que contribuyó de manera significativa a su evolución. Sin embargo, también se le conoce como ciclo PHVA, que en inglés se traduce como Planificar, Realizar, Comprobar y Actuar, o PDCA (Planificar, Realizar, Comprobar y Actuar).

En la siguiente tabla se hace énfasis en las fases del ciclo Deming con las respectiva explicación y herramientas.

Tabla 2. Fases Ciclo Deming

FASES	EXPLICACION	HERRAMIENTAS
Planificar (Plan)	- Se reconoce el problema, o acción. - Se definen objetivos para cumplir y alcanzar (como las SMART). - Se delegan tareas para lograr estos objetivos. - Se definen los métodos e instrumentos.	- Diagrama de Gantt: Organización y monitorización de tareas y proyectos. - AMFE: evaluación modal de errores y consecuencias. - Generación de ideas (brainstorming): de todos los empleados. - Utilización del enfoque 5 W (Quién, Qué, Dónde, Cuándo, Por qué).
HACER (DO)	Los empleados empiezan a efectuar cambios para lograr los objetivos establecidos, siguiendo instrucciones previas y bajo supervisión. - Ejecutar un experimento piloto. - Implementar las políticas y controles previamente establecidos. Realizar un ensayo piloto. - Verificar y aplicar las correcciones. - Aplicar las modificaciones al plan inicial, si el desenlace no resultó positivo. - Anotar la labor efectuada y los resultados obtenidos. - Formar al equipo que requiera la implementación de las soluciones desarrolladas.	Gráficos de control: Monitorean la variabilidad del proceso y ayudan a identificar desviaciones en tiempo real Método de evaluación: Se llevan a cabo ensayos a escala reducida para medir la eficacia de las modificaciones sugeridas
VERIFICAR (Check):	- Vigilar y evaluar el desempeño del SGSI para asegurar su eficacia, de manera constante. - Se comprueba si la mejora aplicada ha alcanzado el objetivo mediante instrumentos de control. - Gestionar elementos fundamentales como la calidad del producto o la operatividad de maquinaria y equipos.	Diagrama de Pareto, Check lists o KPI's.
ACTUAR (ACT)	- Ajustar el plan de mejora. - Modificar el plan de optimización. - Se normaliza la resolución del problema y se definen las circunstancias para su preservación. - Normalización de la respuesta al problema. - Si el objetivo se alcanzó en la prueba piloto, se establecerá de forma definitiva; en caso contrario, se implementará un nuevo ciclo PDCA. - Se realimenta al volver a la primera fase. - Ejecutar las modificaciones necesarias para mejorar el sistema.	Análisis estadístico: Herramientas como SPSS o R serían de utilidad para analizar datos y validar resultados

Fuente: Ciclo PDCA: ¿cuáles son los pasos y cómo funciona? [Consultado el 14, octubre, 2024]. Disponible en:https://www.sydle.com/es/blog/ciclo-pdca-61ba2a15876cf6271d556be9

Para aplicar los principios del ciclo Deming se usan herramientas de mejora.

Figura 2. Ciclo Deming

Fuente: S/fa). Researchgate.net. (enero,2021). Ciclo de Deming (PDCA). [Consultado: 15 octubre,2024]. Disponible en: https://www.researchgate.net/figure/Figura-1-Ciclo-de-Deming-PDCA-Fuente-Elaboracion-propia_fig1_359416383

5.3.2.4 Ventajas y desventajas del ciclo Deming

El Ciclo de Deming es una herramienta eficaz para el perfeccionamiento continuo en las organizaciones, no obstante, su implementación demanda un estudio detallado para reducir sus desventajas y potenciar sus beneficios.

Tabla 3. Ciclo Deming ventajas y desventajas

VENTAJAS	DESVENTAJAS
• Incremento de la confianza: los usuarios y asociados se sienten más seguros al estar informados sobre la protección de sus datos. • Su uso es sencillo, puede incorporarse en cualquier proceso y ayuda a garantizar que las mejoras sean sustentables. • Continuidad del negocio: diseñar planes de recuperación para mantener las operaciones en funcionamiento, si se producen incidentes. • Gestión dinámica de riesgos: facilita una actualización continua frente a amenazas que surgen. • Mejora la imagen de la entidad: la percepción tanto interna como externa de la misma a través de la implementación de un SGSI. • Puede asistir a las organizaciones en la consecución de sus metas y optimizar su desempeño. Usuarios y asociados se perciben más confiados al conocer la salvaguarda de sus datos.	• No sirve para resolver emergencias. Lentitud en la implementación. • Su aplicación puede requerir tiempo, funciona bajo condiciones que estén controladas. • Cada etapa del ciclo se llevará a cabo con cuidado y exactitud para obtener los resultados esperados. • El ciclo sólo resulta efectivo si todos los trabajadores son conscientes de su uso y se involucran en él. • Sin la implicación de todas las partes comprometidas, es posible que el ciclo Deming se desmorone. • Las variables externas e imprevistos que surjan tendrían un impacto negativo en los resultados.

Fuente: SIMPLIROUTE. (julio,2022). Ciclo de Deming: Etapas, Importancia y Ejemplos. [Consultado: 18 octubre,2024]. Disponible en: https://simpliroute.com/es/blog/ciclo-de-deming

5.3.3 Payload

En el campo de la ciberseguridad, el payload de carga útil alude a la sección de un paquete que alberga los datos fundamentales que se pretende enviar, distinguiéndolos de los datos de encabezado y otros metadatos. En situaciones perjudiciales, la carga útil representa el segmento de un ataque que realiza acciones perjudiciales, como la instalación de malware, el robo de datos o el cifrado de archivos en el contexto de un ataque de ransomware.

Carga útil: sinónimo directo de payload, se utiliza en la parte activa que realiza acciones maliciosas en un ataque. La carga útil es una parte integral del malware que ejecuta las funciones dañinas al instalarse en el sistema.

Exploit: se refiere a la vulnerabilidad que es aprovechada por el payload; mientras el exploit abre la puerta, el payload realiza el daño.

5.3.4 Metodologías de Análisis de Riesgos

Las metodologías son fundamentales en ciberseguridad ya que ofrecen un método ordenado y sistemático para detectar, evaluar y administrar los riesgos asociados a los sistemas de información de una empresa facilitando la anticipación de amenazas, la creación de estrategias de defensa efectivas y la asignación prioritaria de recursos para mitigar vulnerabilidades de forma preventiva, algunas metodologías pueden ser:

5.3.4.1 Magerit

Se trata de un marco creado por el Consejo Superior de Administración Electrónica del Gobierno español. Se vuelve un instrumento esencial para las estructuras organizativas que desean establecer un marco robusto para la administración de riesgos en sus sistemas de información; de esta manera, aseguraría un uso seguro y eficiente de las tecnologías digitales en el sector público.

Su objetivo principal es tratar y gestionar los riesgos vinculados al empleo de tecnologías de la información (TI), evidentemente con un énfasis especial en las entidades públicas administradoras. Este enfoque se basa en la importancia de salvaguardar los recursos de información, asegurar la continuidad y proporcionar servicios de seguridad en el sector público.

> "El método MAGERIT, son las siglas de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administraciones, dicho método cubre la fase AGR (Análisis y Gestión de Riesgos). Si hablamos de Gestión global de la Seguridad de un Sistema de Seguridad de la Información basado en ISO 27001, MAGERIT, es el núcleo de toda actuación organizada en dicha materia, ya que influye en todas las fases que sean de tipo estratégico y se condiciona la profundidad de las fases de tipo logístico".[10]

El Consejo Superior de Informática ha asumido la tarea de crear la primera versión de MAGERIT, motivando de esta manera su implementación ante la creciente dependencia de la sociedad en las Tecnologías de la Información. MAGERIT tiene una fuerte relación con la generación en la que se emplean los medios electrónicos, informáticos y

[10] ESGINNOVA (16 marzo, 2015). GROUP.ISO 27001: El método Magerit. [Consultado: 19 octubre,2024]. Disponible en: https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/

telemáticos, produciendo beneficios para los empleados y la comunidad. Esto puede provocar varios peligros que necesitan ser disminuidos a través de acciones de seguridad que promuevan la confianza.

Tabla 4. Objetivos Metodología Magerit

OBJETIVOS DIRECTOS	OBJETIVOS INDIRECTOS	TAREAS A REALIZAR
Es necesario sensibilizar a los encargados de las compañías de información sobre la presencia de riesgos y la importancia de manejarlos	Preparar a la entidad para procedimientos de evaluación, auditoría, certificación o acreditación, lo cual puede ser esencial para acatar regulaciones y estándares.	Análisis de riesgos, que facilita la identificación de los recursos que posee la Organización y calcular lo que podría suceder.
Proporcionar un enfoque sistemático para evaluar los peligros que surgen del uso de tecnologías de la información y comunicaciones.	Contribuir al fortalecimiento general de las habilidades de la organización en la administración de riesgos, aunque no se enfocan específicamente en la detección o reducción de riesgos particulares.	Gestión de riesgos, con el objetivo de organizar una defensa minuciosa y lógica, para prevenir cualquier eventualidad negativa y estar listos para frenar emergencias, resistir incidentes y seguir funcionando en las mejores condiciones; dado que nada es ideal, el riesgo se reduce a un nivel residual que la dirección asuma.
Ayudar en el reconocimiento y organización del tratamiento adecuado para mantener los riesgos bajo control.		

Fuente: ESGINNOVAGROUP Metodología Margerit para el análisis e identificación de riesgos en SGSI). [Consultado: 21 octubre,2024]. Disponible en: https://www.pmg-ssi.com/2021/07/metodologia-margerit-para-el-analisis-e-identificacion-de-riesgos-en-sgsi/

Se detallan los procedimientos y etapas fundamentales utilizadas en esta metodología.

Para representar la información sobre Magerit y sus métodos sistemáticos de análisis de riesgos, se puede utilizar un diagrama de flujo que ilustra las fases y pasos clave del proceso. A continuación, se presenta un esquema simplificado:

Texto

Flow chart TD

A [Inicio y Preparación] --> B [Análisis de Activos]
B --> C[Análisis de Amenazas]
C --> D[Análisis de Vulnerabilidades]
D --> E[Análisis de Riesgos]
E --> F[Tratamiento de Riesgos]
F --> G[Seguimiento y Revisión]

A -->|Definir objetivos y alcance| H[Identificación de Activos]
H -->|Valorar activos| B
H -->|Identificar amenazas| C
H -->|Evaluar vulnerabilidades| D
H -->|Estimar impacto y probabilidad| E
H -->|Implementar medidas| F

Descripción del diagrama

Inicio y Preparación: definir los objetivos y el alcance del análisis.

Análisis de Activos: identificación y valoración de activos relevantes para la organización.

Análisis de Amenazas: registro de amenazas que pueden afectar a los activos.

Análisis de Vulnerabilidades: evaluación de las debilidades en los sistemas que podrían ser explotados.

Análisis de Riesgos: valoración del riesgo mediante la combinación del impacto y la probabilidad.

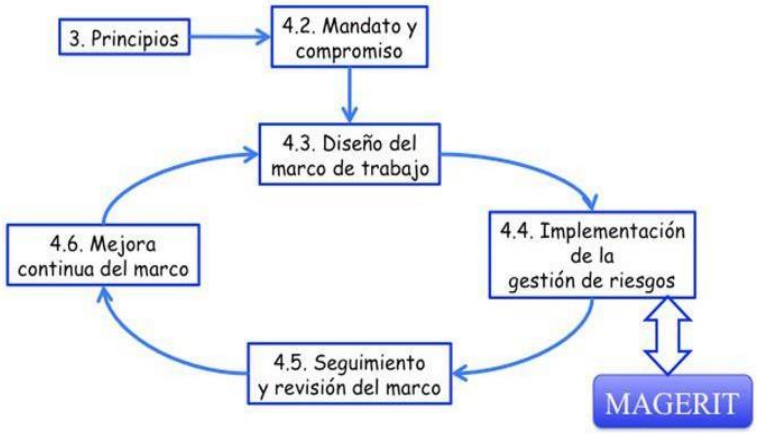
Tratamiento de Riesgos: desarrollo e implementación de medidas para mitigar los riesgos.

Seguimiento y Revisión: monitoreo continuo, revisión del análisis y las medidas implementadas.

Teniendo en cuenta la terminología de la normativa ISO 31000, MAGERIT revela al “Proceso de Gestión de los Riesgos”, sección 4.4 (“Implementación de la Gestión de los Riesgos”) dentro del “Marco de Gestión de Riesgos”. En otras palabras, MAGERIT implementa y desarrolla el Proceso de Gestión de Riesgos; teniendo en cuenta un marco

de trabajo para que los órganos de gobierno realicen decisiones teniendo en cuenta los peligros derivados del uso de tecnologías de la información.

Figura 3. Procesos de Gestión Metodología Magerit



Fuente: PAE Portal Administración Electrónica.). [Consultado: 21 octubre,2024]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Figura 4. Ventajas y desventajas de la Metodología Magerit

METODOLOGÍA	ÁMBITO DE APLICACIÓN	VENTAJAS	DESVENTAJAS
MAGERIT	Gobierno, compañías grandes comerciales y no comerciales, Pymes.	Alcance completo en el análisis y gestión de riesgos. Está bien documentada en cuanto a recursos de información, amenazas y tipos de activos. Utiliza un completo análisis de riesgo cuantitativo y cualitativo. Es libre y no requiere autorización para su uso. Divide los activos de la organización en diferentes grupos, para identificar más riesgos y poder tomar contramedidas para evitar así cualquier riesgo. Se centra en tres objetivos: concientizar sobre la existencia de los riesgos y de la necesidad de atajarlos a tiempo, ofrecer un método sistemático para analizar tales riesgos, ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación. Permite que el proceso esté bajo control en todo momento y contempla aspectos prácticos para la realización de un análisis y una gestión de riegos efectiva. Posee una buena base documental en tres libros: El método, Catálogo de elementos y Guía de técnicas, que son de acceso público. Posee herramientas para el análisis de riesgo como PILAR.	En su modelo no involucra los procesos, recursos, ni vulnerabilidades. Posee falencias en el inventario de políticas. Se considera una metodología costosa en su aplicación.

Fuente: ALEMAN N. Helena y RODRÍGUEZ B. Claudia. Metodologías Para el Análisis de Riesgos en los SGSI.). [Consultado: 22 octubre,2024]. Disponible en: https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

5.3.4.2 Octave

La metodología OCTAVE está relacionada con las siglas de Evaluación Operativa Crítica, Amenaza, Activo y Vulnerabilidad (evaluación operativa crítica, de amenazas, de activos y de debilidad). Por esta razón, se trata de un método para el análisis y administración de riesgos. El propósito del centro es asegurar los sistemas de computación dentro de una organización o empresa.

El marco conceptual que sirvió como base para la primera estrategia de OCTAVE fue expuesto en 1999 por el Instituto de Ingeniería de Software (SEI) en la Universidad de

Carnegie Mellon. El fin de esta metodología era abordar los desafíos de seguridad que el departamento de defensa de los Estados Unidos estaba enfrentando

A través de la implementación de la metodología OCTAVE, diversas personas de los sectores empresariales, de los departamentos de tecnologías de la información y del sector operativo colaborarán de forma conjunta. Se llevará a cabo con el enfoque centrado en las necesidades definidas por la seguridad. En este contexto, se deben balancear tres elementos como los riesgos operativos, la tecnología y las prácticas de seguridad.

OCTAVE está dirigido a empresas de medio y gran tamaño con un número de empleados superior a 300 y que cumplen las siguientes características:

- Organigrama de varios niveles
- Disponen de su propia infraestructura IT
- Tienen capacidad para evaluar vulnerabilidades

Figura 5. Ventajas y desventajas Metodología Octave

METODOLOGÍA	ÁMBITO DE APLICACIÓN	VENTAJAS	DESVENTAJAS
OCTAVE	Pymes, organizaciones públicas y privadas.	Es autodirigible. Se puede desarrollar por empleados de la misma organización, utilizando un equipo multidisciplinario. Involucra a todo el personal. Construcción de los perfiles de amenazas basados en activos. Identificación de la infraestructura de vulnerabilidades. Desarrollo de planes y estrategias de seguridad. Comprende las etapas de análisis y gestión de riesgos. Involucra procesos, activos, dependencias, recursos, vulnerabilidades, amenazas y salvaguardas. Relaciona amenazas y vulnerabilidades. Uso interno: gratuito. Posee tres métodos Octave, Octave-s y Octave allegro, adaptables a una organización.	No tiene en cuenta el principio de no repudio de la información. Utiliza muchos documentos en el proceso de análisis de riesgos. Se requiere de amplios conocimientos técnicos. No define claramente los activos de información. Uso externo: se debe comprar la licencia al SEI si se quiere implementar la metodología a un tercero.

Fuente: ALEMAN Novoa, Helena y Claudia Rodríguez Barrera. Metodologías Para el Análisis de Riesgos en los SGSI. [Consultado: 23 octubre,2024]. Disponible en: https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

- **Objetivos**

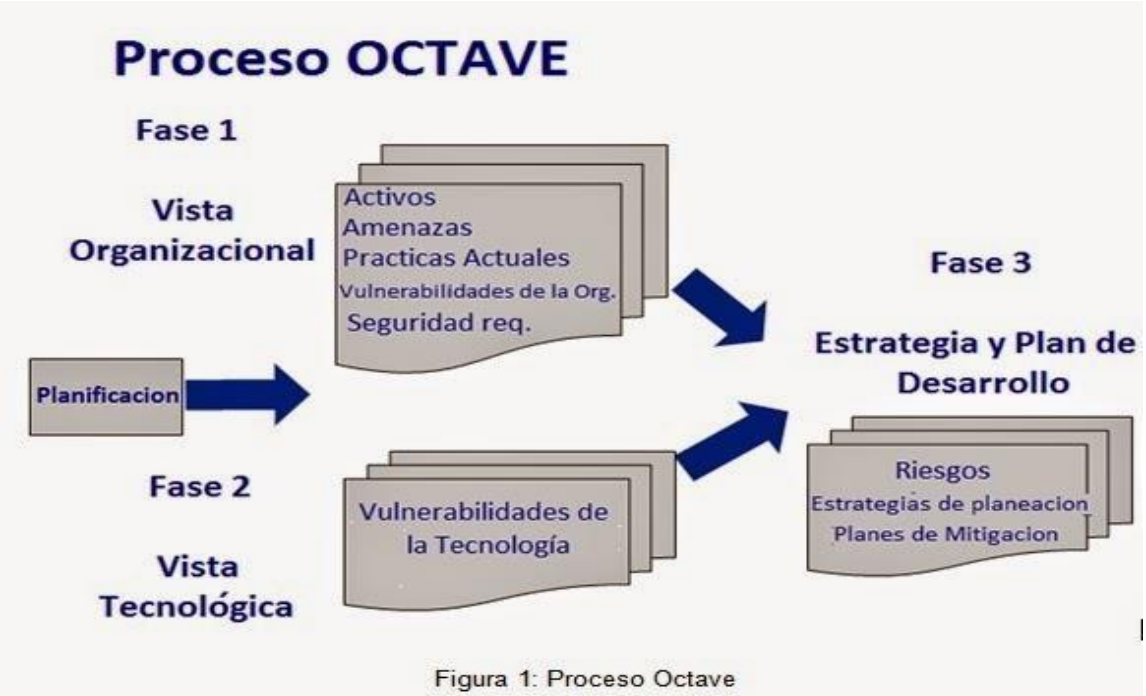
Analizar la metodología OCTAVE en los elementos de riesgos operativos y en las prácticas de seguridad e implica que para que las compañías y organizaciones puedan tomar las decisiones adecuadas respecto a la salvaguarda de la información basándose en riesgos como la privacidad, la integridad o la disponibilidad de los bienes relacionados con la información esencial, la tecnología será evaluada con relación a las distintas prácticas de seguridad.

La metodología OCTAVE se desarrolló en la Universidad Carnegie Mellon de Pensilvania, en los Estados Unidos. Esto se hizo en el Centro de Coordinación del Instituto de Ingeniería de Software. OCTAVE está compuesta por tres fases diferenciadas:

- La metodología OCTAVE cuenta con 3 fases:

    - Identificación de Activos: de mayor importancia para el manejo de información. Es vital identificar todos los recursos que conforman la compañía y respaldan los servicios de computación, así como todos los medios que guardan datos.
    - Análisis de la infraestructura: para completar el estudio efectuado en la etapa inicial, el equipo de análisis de riesgos debe realizar una evaluación de la infraestructura, ya sea tecnológica o física, que aloja la información de la empresa, y también detectar todas las amenazas que podrían poner en riesgo la seguridad de tal infraestructura.
    - Análisis de riesgos: por último, el equipo responsable del análisis de riesgos tiene la responsabilidad de evaluar todas las amenazas e identificar los riesgos más relevantes para la compañía. Será esencial desarrollar un plan de mitigación para los riesgos más altos, implementando controles o mejoras a los ya existentes con el objetivo de disminuir el grado de riesgo de aquellos activos que se han identificado previamente como críticos.

Figura 6. Procesos Metodología Octave



Fuente: Metodología y análisis de riesgos. [Consultado: 23 octubre,2024]. Disponible en: https://metodologiasanalisisriesgos.blogspot.com/p/metodologia.html

6. DESARROLLO DE LOS OBJETIVOS

6.1. IDENTIFICAR LOS RIESGOS EN CIBERSEGURIDAD MEDIANTE INVESTIGACIÓN DOCUMENTAL PARA LA PROTECCIÓN DE LOS ESTUDIANTES DE BÁSICA SECUNDARIA EN COLOMBIA Y SU ENTORNO FAMILIAR

La mayoría de naciones siguen enfrentando retos importantes en el campo de la ciberseguridad, impulsados por el incremento de diversas amenazas y ataques cibernéticos que comprometen la seguridad de los estudiantes menores de edad, la familia y, en consecuencia, las instituciones educativas; en el caso de Colombia, nuestro país también se encuentra en esa situación y los usuarios menores de edad son más vulnerables a riesgos de ciberseguridad como: phishing, malware y diversas actividades maliciosas en línea, producto de la creciente dependencia de la tecnología y la digitalización.

Sin embargo, el primer paso en este proceso es comprender qué es un riesgo en ciberseguridad, con el propósito de mitigar su impacto y diseñar unas medidas de seguridad y políticas efectivas de protección para los estudiantes del proceso educativo.

> "Un riesgo en ciberseguridad es la posibilidad de que ocurra un evento indeseable que ponga en peligro la confidencialidad, la integridad o la disponibilidad de los sistemas y datos. Estos riesgos pueden manifestarse de diversas formas, desde ataques de malware que intentan infiltrarse en redes corporativas hasta el robo de datos personales mediante técnicas de phishing. Los riesgos en ciberseguridad están siempre presentes, y su naturaleza cambiante y sofisticada exige que los profesionales en esta disciplina estén constantemente actualizados y preparados para enfrentar las últimas tendencias y tácticas utilizadas por los actores maliciosos" [11]

[11] STRUCTURALIA. ¿Qué es un riesgo en ciberseguridad y cómo prevenirlos?(31, agosto, 2023). [blog]. [Consultado el 2, septiembre, 2023].Disponible en: https://blog.structuralia.com/que-es-un-riesgo-en-ciberseguridad

Enseguida se indica los riesgos en ciberseguridad con los que pueden verse perjudicados los estudiantes y el entorno educativo.

Tabla 5. Riesgos de ciberseguridad en Jóvenes

RIESGO	DESCRIPCION
Ingeniería Social en jóvenes	Técnica de engaño mediante phishing, pharming vishing, para que se comparta información confidencial como: Datos personales, información personal, claves, suelen suplantar a entidades bancarias, servidores de correo electrónico o redes sociales.
Acceso no autorizado	Este tipo de riesgo implica que personas no autorizadas accedan a nuestros datos, redes, sistemas y sitios físicos.
Riesgos de Malware	Software malicioso que afecta la información de los dispositivos y equipos de los jóvenes a través de: • Virus • Ransomware • Gusanos • Troyanos • Spyware • Adware • Enlaces maliciosos
Riesgo derivado del error Humano	Instalación y mala configuración en hardware y software. Este riesgo relacionado con debilidades en los sistemas, software y configuraciones, de igual forma como las malas acciones y decisiones en la gestión.
Falta de Capacitación de ciberseguridad En los colegios	Riesgo relativo a: • Actualización de software • Dispositivos IoT • Descargas • Visita de sitios web inapropiados. • Correos electrónicos maliciosos • Juegos en línea.

Fuente: Ciberseguridad para niñas, niños y adolescentes [Consultado el 2, septiembre, 2024]. Disponible en: https://www.gob.mx/gncertmx/articulos/tips-y-recomendaciones-de-ciberseguridad?state=published

6.1.1 Ingeniería social en jóvenes

Se reconoce como el arte del engaño, busca captar nuestra atención, utilizando un elemento casi común, la curiosidad. De esta manera, se facilita que nuestras interpretaciones sean manipuladas por individuos ajenos y se lleve a cabo lo que ellos deseen. La ingeniería social representa un peligro considerable en el campo de la ciberseguridad, dado que se fundamenta en la manipulación psicológica de individuos con el fin de adquirir información sensible o llevar a cabo acciones que ponen en riesgo la privacidad de los datos.

> "La ingeniería social es una técnica de manipulación que aprovecha el error humano para obtener información privada, acceso a sistemas u objetos de valor. En el caso del delito cibernético, estas estafas de "hackeo de humanos" tienden a hacer que los usuarios desprevenidos expongan datos, propaguen infecciones de malware o den acceso a sistemas restringidos. Los ataques pueden ocurrir en línea, en persona y a través de otras interacciones" [12]

6.1.1.1 Tácticas de Ingeniería Social

- Manipulación en línea: método psicológico de engaño en línea, con el objetivo de conseguir datos; puede realizarse mediante mensajes de texto y correos electrónicos, foros, chats y redes sociales.
- Vishing: mediante llamadas telefónicas, como encuestas, los ciberdelincuentes obtienen de los alumnos datos delicados.
- Phishing: utilizan emails que parecen seguros para obtener contraseñas y otros datos característicos de los jóvenes.
- Carnada: los ciberdelincuentes dejan dispositivos infectados con software perjudicial en lugares públicos, y cuando alguien lo conecta, ellos tendrán acceso al dispositivo.
- Hunting: método que emplea tanto el phishing, la carnada y el hacking de emails para recopilar numerosos datos del afectado, sin el máximo esfuerzo.
- Pharming: se relacionan con la víctima, a través de redes sociales, con el principal objetivo de conseguir todos los datos personales.
- Perfiles falsos en redes sociales: son tan reales que con éstos se procede al engaño y acceder información personal.
- Manipulación cara a cara: para conseguir aspectos como situaciones del pasado, o presente, o contraseñas frecuentes y dar paso a su privacidad informática.
- Sesgos cognitivos: los jóvenes pueden ser vulnerables cuando ingresan con confianza a fuentes que aparentan ser fiables.

[12] KARPESKY. ¿Qué es la Ingeniería Social? 2024. [Consultado: 20 octubre,2024]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

Figura 7. Características Ingeniería Social

Fuente: Diagrama elaboración propia, con base en el siguiente link. PROOFPOINT. Que es la ingeniería social. 2024. [Consultado: 21 octubre,2024]. Disponible en: https://www.proofpoint.com/es/threat-reference/social-engineering#.

6.1.1.2 Tecnologías de seguridad para combatir la Ingeniería social

- Configuración de Privacidad: establecer las opciones de privacidad en tus redes sociales para limitar la exposición de tus datos personales.
- Contraseñas Seguras y Únicas: para cada cuenta es necesario emplear contraseñas sólidas y diversas, que deben ser ajustadas con regularidad. Sería recomendable considerar el uso de un administrador de contraseñas para mantener su seguridad.
- Autenticación Multifactor (MFA): en caso de que sea viable, se debe activar en dos pasos. Así, se incorpora una capa adicional de protección, porque se va solicitar un segundo proceso de verificación adicional a la de tu contraseña.

- Comprobación Independiente: en caso de recibir un mensaje o una llamada que requiera de información, es necesario emplear un método diferente para verificar su verdad.
- Mantén el Software Actualizado: garantizar la actualización del software antivirus y antimalware y que todos los dispositivos y aplicaciones estén actualizados con los más recientes parches de seguridad.
- Educación Continua: acerca de métodos habituales de ingeniería social y participa en formación si laboras en una entidad.
- Protección con Enlaces y Archivos Anexos: no hacer clic en vínculos o descargues archivos anexos de emails o mensajes sospechosos, puede que contengan malware o te redirijan a páginas fraudulentas.

6.1.1.3 Phishing

Desde mediados de los años 90, el término phishing se ha empleado para detectar a los hackers que emplean emails engañosos para "pescar" datos de usuarios desafortunados. La finalidad de los ataques de phishing consiste en sustraer o perjudicar información sensible, manipulando a los usuarios para que revelen sus datos personales, tales como contraseñas y números de tarjetas de pago.

Este tipo de ciberataques se fundamenta en la falsificación de identidad y es visto como una de las formas más frecuentes de ingeniería social; utilizando la manipulación psicológica y el engaño. Los actores de amenaza se disfrazan como entidades o personas de prestigio para engañar al personal de la educación, y de esta manera, conseguir que lleven a cabo acciones determinadas.

> "El phishing es un tipo común de ciberataque que se dirige a las personas a través del correo electrónico, mensajes de texto, llamadas telefónicas y otras formas de comunicación. El término phishing en inglés se pronuncia igual que la palabra fishing, literalmente pescar. Un ataque de phishing tiene como objetivo engañar al destinatario para que realice la acción deseada por el atacante, como revelar información financiera, credenciales de acceso al sistema u otra información sensible".[13]

6.1.1.4 Tácticas del phishing

- SMS o smishing: emplea un mensaje de texto en su teléfono móvil o inteligente, proporcionándoles un presente de 'agradecimientos' para que sus víctimas puedan realizar la actualización de sus datos de su tarjeta de crédito.
- Voz o vishing: los fraudulentos utilizan la tecnología VoIP (VoIP).

[13] ARCE AGUILAR Mariana. Riesgos de ciberseguridad: qué son, ejemplos y cómo prevenirlos. [blog]. [Consultado el 2, septiembre, 2023]. Cybersecurity Engineer. Disponible en: https://www.deltaprotect.com/blog/riesgos-de-ciberseguridad-ejemplos-y-prevencion

- Ataques de "catphishing": es una nueva estrategia de phishing, los atacantes generan perfiles falsos en páginas de citas con el fin de engañar a las víctimas.
- En redes sociales: requieren a través de plataformas de mensajería como Facebook Messenger, LinkedIn, Instagram, TikTok, X, que actualicen sus credenciales de acceso o datos de pago.
- Ataques por medio de redes sociales: con estrategias de phishing en las redes sociales, mediante el envío de mensajes privados con enlaces malintencionados y conducir a las víctimas a páginas web engañosas para sustraer datos íntimos.
- Correo electrónico: uno de los métodos más habituales, de los atacantes consiste en dirigir mensajes engañosos con el objetivo de que las víctimas hagan clic en estos enlaces.
- Ataques a cuentas de LinkedIn: los ciberdelincuentes emplean cuentas de LinkedIn comprometidas para distribuir vínculos de phishing mediante mensajes privados.

6.1.1.5 Mejores prácticas de seguridad para ayudar a combatir el phishing:

- Los programas antivirus y antimalware identifican y neutralizan el código o archivos malintencionados en los emails de phishing.
- Filtros sofisticados de correo electrónico, posibilitan la restricción de mensajes. Los filtros web presentan alertas e impiden el acceso a páginas web malintencionadas conocidas (lista negra).
- El correo no deseado puede identificar correos electrónicos sospechosos de phishing, utilizando datos de estafas previas y algoritmos de aprendizaje automático.
- Implementación de certificados digitales y firma digital para corroborar la identidad de los remitidos.
- Comprobación de dominios y direcciones email para identificar fraude.
- Instrumentos para el análisis de URL y sitios web para identificar páginas fraudulentas.
- Sistemas de seguimiento y alerta precoz ante acciones sospechosas.
- Implementación para el acceso a sistemas y cuentas a través de una autenticación de dos factores.
- Herramientas de análisis de URL y sitios web para detectar sitios fraudulentos.
- Formación y sensibilización de los usuarios mediante formación y concienciación acerca de los peligros y estrategias del phishing.
- Simulación de ataques de phishing, con el fin de evaluar la capacitación de los trabajadores.
- Coordinación con otras compañías y autoridades para informar y bloquear páginas web de phishing.

Figura 8. Cómo evitar ser víctima de phishing

Fuente: X.COM (17 de enero, 2020). Cómo evitar ser víctima de phishing. [Consultado el 26, septiembre, 2023]. Disponible en: https://x.com/UIDIFGETabasco/status/1218323402944966656

6.1.1.6 Phishing y las operaciones realizadas en línea

- Una de las estrategias más habituales es el phishing, que recopila información delicada. En el robo se recolecta datos personales como: nombre de usuario, contraseña, números de tarjetas de crédito, entre otros, utilizados por el usuario para identificarse en un sitio web, ya sea para una transacción, un pago de servicio o una transferencia bancaria.
- Otra modalidad de hurto en la red es el PHARMING, un phishing más avanzado y más difícil de detectar. Con el uso de un troyano (un software de espionaje pequeño), se modifica un archivo del sistema de un equipo con la finalidad de redirigirlo hacia una dirección web determinada.
- En esta tercera técnica de robo de información de Internet se emplean programas llamados KEYLOGGER, que se reinstalan en los equipos.

- Otra forma de robo en la red es el pharming, que es un phishing sofisticado y más complicado de identificar. Mediante un troyano (un pequeño software espía), se altera un archivo del sistema de un ordenador con el objetivo de desviarlo a una dirección web específica.

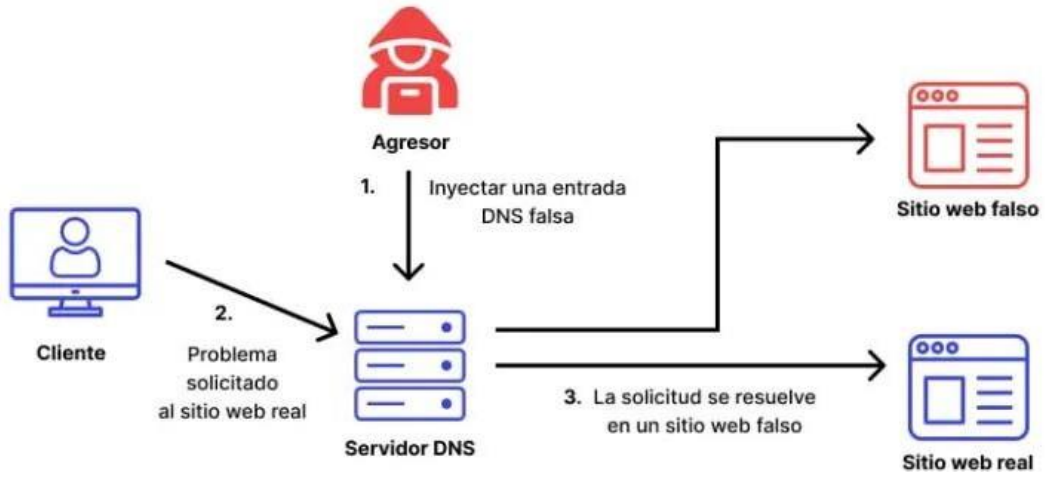
6.1.1.7 ¿Qué es el pharming?

Es similar al phishing, sin embargo, en pharming se proyectan redes mucho más extensas y cualquier persona puede tropezar con una página web de pharming, a través del engañado de una página web de confianza.

> "El pharming, una voz compuesta por phishing y pharming, es una estafa en línea que consiste en dirigir a las personas a páginas web fraudulentas que imitan páginas auténticas. Las estafas de pharming intentan convencer a las personas para interactuar con páginas web falsas y parecidas con el fin de recopilar sus datos personales, como correos electrónicos y contraseñas, o infectar sus ordenadores con malware"[14]

El pharming es un método de ciberataque que consiste en alterar el proceso de resolución de nombres de dominio (DNS) con el objetivo de redirigir a los usuarios a páginas web engañosas, dando la impresión de ser reales. Esta técnica es vista como más amenazante que el phishing, dado que no necesita que la víctima haga clic en un enlace falso; en cambio, el usuario es redirigido automáticamente a una página web engañosa al tratar de entrar a un sitio web auténtico.

Figura 9. Cómo funciona el Pharming



[14] BODNAR Danielle. AVAST. ¿Qué es el pharming y cómo puede protegerse de él? (7, octubre, 2016). [sitio web]. [Consultado el 3, julio, 2023]. Disponible en: https://www.avast.com/es-es/c-pharming

Fuente: WALLARM. Ataque Pharming en acción [imagen]. [Consultado el 22, septiembre, 2024]. Disponible en: https://lab.wallarm.com/what/ataque-pharming-que-es/?lang=es

- **Como combatir el Pharming:**

  - Evitar acceder a links y descargar archivos de procedencia incierta.
  - Implementa un antivirus en tus aparatos digitales.
  - Verifica que la dirección electrónica se haya redactado de manera adecuada.
  - Implementar una aplicación que permita bloquear ventanas emergentes en los lugares a los que concedes autorización.
  - Se aclara en no abrir emails de los cuales no sea posible verificar su autenticidad u origen.
  - Prevenir hacer clic en publicidad o ventanas emergentes que te señalen que has obtenido un viaje, premio o sorteo.
  - Asegura que el enlace electrónico al que accedes tenga un "candado" al inicio del enlace y que inicie con https://.
  - Se alerta sobre el acceso a tus cuentas personales y la divulgación de datos personales, si utiliza aparatos de uso público o vinculados a redes públicas.
  - Evitar contraseñas fáciles de deducir tus contraseñas o NIPs. No se aconseja el uso de fechas de nacimiento, números de teléfono o cualquier información relacionada con tu identidad
  - Emplea instrumentos para generar comprobaciones de múltiples pasos.
  - Buscar la utilización de una VPN (Red Privada Virtual, o red privada virtual).

La ingeniería social es un término más amplio que abarca diversas tácticas utilizadas para manipular a las personas. El grooming, sexting y ciberbullying son tácticas que se relacionan con la ingeniería social y que pueden manifestarse en entornos digitales, llegando a representar riesgos o amenazas significativas en el ámbito educativo de la ciberseguridad.

6.1.1.8 Grooming

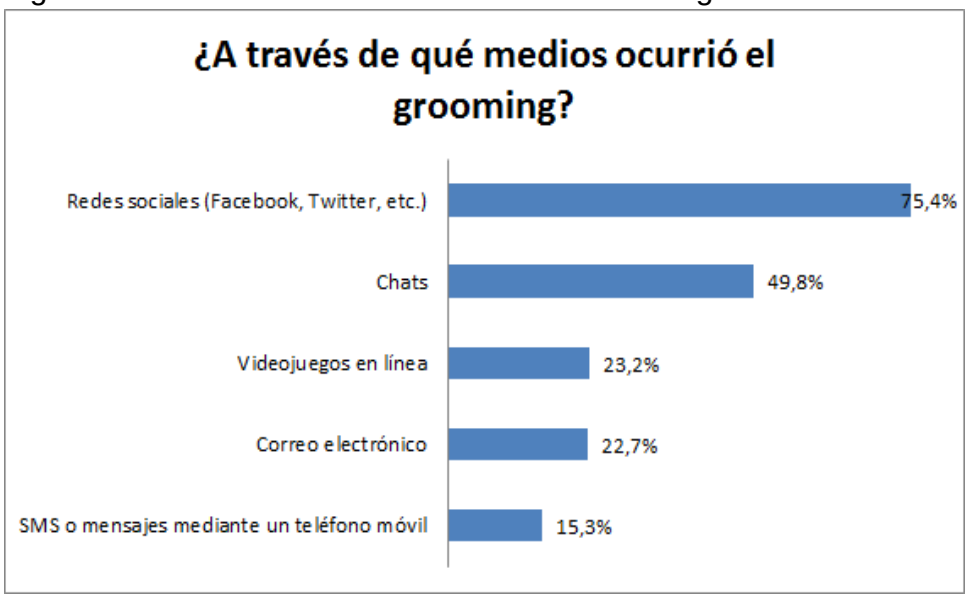
Es una clase de acoso y abuso hacia jóvenes y niños que ha ganado mucha fuerza y se ha popularizado el empleo de las TIC, mediante las redes sociales y todo se da inicio por los chats a través de simple e informal conversación virtual. Aunque la definición de este riesgo no se registra en el diccionario de la Real Academia Española (RAE). Sin embargo,

este concepto está vinculado a la seguridad y la integridad de los niños y los adolescentes.

> "Se trata de una actividad delictiva en la que un adulto busca mantener un contacto con un adolescente o niño con el fin de llegar a un encuentro sexual. Debido a la naturaleza de este comportamiento, su práctica en la era tecnológica moderna se ha vuelto cada vez más frecuente. La víctima se expone de manera constante a un abuso de carácter sexual sin que se dé cuenta. Por lo general, la interacción inicial se produce a través de portales virtuales (redes sociales, etc.) o cuando el adulto consigue un contacto directo con el joven, como puede ser mediante su número telefónico".[15]

Se constituye en riesgo cuando el contacto telemático con una persona menor de edad atenta, con su propia naturaleza, contra la integridad sexual. En este gráfico, se puede observar los medios más empleados para llevar a cabo el grooming.

Figura 10. Medios de comunicación del Grooming



Fuente: GOUJON A. Welivesecurity.com. [Consultado noviembre 15, 2023]. Disponible en: https://www.welivesecurity.com/la-es/2013/03/13/grooming-683-encuestados-cree-amenaza-muy-frecuente/

[15] UNIVERSIDAD INTERNACIONAL DE VALENCIA. ¿Qué es el grooming y por qué es tan peligroso?.(12, enero, 2023).[sitio web].[Consultado el 22, septiembre, 2024]. Disponible en: https://www.universidadviu.com/pe/actualidad/nuestros-expertos/que-es-el-grooming-y-por-que-es-tan-peligroso

- **Tácticas del ‘online grooming**

Mediante tácticas de manipulación y engaño, el atacante forja un lazo de confianza con la niña, niño o joven y usualmente exagera su edad, interpretándolo como si fuera la edad de la víctima. El agresor puede realizar obsequios, oír las dificultades de sus víctimas y luego esa información la emplea para persuadirlos. Este tipo de comportamiento, conocido como grooming, se caracteriza por la habilidad del agresor para presentarse como alguien amigable y accesible. A continuación, se amplían algunos aspectos clave de este fenómeno:

- El aislamiento de la víctima: pretende intimidar a los familiares, amigos y otros individuos próximos.
- Conversaciones sobre sexo: valiéndose de la confianza se inicia conversaciones sexuales gradualmente, pero lo crítico es que el joven se acostumbre a la temática sexual y al vocabulario adecuado.
- Las solicitudes de índole sexual: son la meta principal del grooming en línea. En esta fase el criminal utiliza la manipulación, las amenazas o el chantaje para que la víctima envíe material sexual, relate fantasías sexuales o culmine con un encuentro físico.

> “Por ello, la Secretaría de Seguridad y la empresa de telefonía móvil WOM Colombia, con el acompañamiento de la Secretaría de Educación, lanzaron la estrategia “Alerta en línea”, que iniciará en las instituciones educativas distritales, ubicadas en las localidades de Suba, Ciudad Bolívar, Santa Fe, Antonio Nariño y Los Mártires y de la que harán parte estudiantes, docentes y padres de familia, con talleres formativos teórico-prácticos, acompañados de charlas informativas y videos educativos para prevenir situaciones que puedan afectar física o emocionalmente a niños, niñas y adolescentes”.[16]

Esta estrategia cuenta con el acompañamiento de la Mesa de Expertos Contra el Cibercrimen, liderada por la Secretaría de Seguridad, donde se articulan acciones conjuntas con la Fiscalía General de la Nación y la Dirección Especializada contra delitos informáticos y el centro cibernético de la policía nacional, con la que se ha logrado Las Fases del Online Grooming.

[16] REVISTA SEMANA. Lanzan estrategia para prevenir el ‘grooming’, el ‘sexting’ y el ciberacoso en Bogotá.(6, septiembre, 2023). [sitio web]. [Consultado el 3, noviembre, 2023]. Disponible en: https://www.semana.com/nacion/bogota/articulo/lanzan-estrategia-para-prevenir-el-grooming-el-sexting-y-el-ciberacoso-en-bogota-este-ano-ya-van-214-capturados/202324/

- **Clases de Groomers**

En la siguiente tabla, se ha sintetizado las clases de groomers con sus diferentes características.

Tabla 6. Clases de Groomers

No.	CLASES DE GROOMERS Y SUS CARACTERÍSTICAS	
1	CYBER SEX	• Realiza actividades de masturbación sin necesidad de reunirse físicamente con la víctima e incitan al menor a hacerlo. • Hablan en diferentes redes sociales durante meses, interesándose por el físico. • Le solicitan al menor de edad, fotos sexuales de esos momentos.
2	BUYERS	• La táctica es utilizar a terceras personas para tráfico y explotación sexual Infantil. • No se exponen y sus interacciones son cortas. • Negocia los términos del encuentro sexual, como el precio, el lugar o los actos sexuales que podrá realizar. • Buscan conseguir fotos sexuales de los menores de edad por los que paga.
3	SCHEDULERS	• En este caso las personas intentan organizar reuniones físicas sin tener actividades cibersexuales previas. • Buscan una conexión sexual rápida y para conseguirlo, no se exponen ni duelen pedir fotos sexuales explícitas. • Esperan un tiempo para solicitar un encuentro mediante interacciones cortas.
4	CYBER-SEX SCEDULERS	• Las y los depredadores sexuales virtuales buscan tener encuentros sexuales tanto virtuales como físicos. • Intentan fomentar una relación online en la que hablan con la víctima durante meses. • Solicitan material sexual explícito online.
5	EMOCIONAL	• Se caracteriza por establecer una relación emocional con la víctima. • Buscan ganarse su confianza y afecto para luego manipularla y obtener lo que quieren.

Fuente: Tipos de groomers y sus características. [Consultado el 4, noviembre, 2023]. Disponible en: https://www.asociacionrea.org/tipos-de-groomer-y-sus-caracteristicas/

- **Tecnologías de seguridad para combatir el grooming**

  - Se insiste en no proporcionar a personas desconocidas información, imágenes o fotos comprometedoras a través de chat, ya que frecuentemente quedan visibles en la web y se propagan por internet, lo que resulta complicado de eliminar y mantener en circulación tanto en el presente como en el futuro.
  - Usar la cámara web cuando están conversando con individuos desconocidos puede ser dañino, ya que pueden estar grabando y la imagen es una información personal que necesita atención y resguardo. El desconocido la propaga en internet o puede emplearla posteriormente en actos de extorsiones.
  - En los distintos aparatos: móvil, tableta, portátil u ordenador de escritorio.
  - En las contraseñas para los distintos dispositivos es importante fusionar letras y números, que se puedan recordar con facilidad, a la vez que sean complicados de robar.
  - La contraseña es privada y no debe ser divulgada, ni a amigos ni familiares; excepto para los niños o niñas menores de edad, quienes la compartirán con sus progenitores.
  - Es importante tener en cuenta emplear la misma contraseña para todas las cuentas que posea, porque si alguien ingresa, podría acceder con facilidad.

6.1.1.9 Sexting

Esta práctica muy popular y cada vez más común, involucra el intercambio de asuntos y contenido multimedia de naturaleza íntima o sexual, a través de vídeos, imágenes, GIFs y otros archivos. Conlleva riesgos significativos como la perdida de la confidencialidad de la información, debido a que una vez que estas imágenes se envían, el emisor pierde el control sobre su distribución.

> "La palabra sexting viene de la combinación en inglés de las palabras sex (sexo) y texting (texteo, envío de mensajes de texto mediante teléfonos móviles). La práctica surge del uso de tecnologías digitales y consiste en la circulación de un contenido sexual a través de dispositivos móviles (celulares, tabletas) y que se da mediante diversas aplicaciones (WhatsApp, Facebook, Instagram, Twitter, Snapchat, etc.)" [17]

[17] TODXS ¿Qué es sexting o sextorsión? [sitio web]. Sí nos reímos, nos reímos todxs, Asociación Civil. [Consultado el 25, septiembre, 2024]. Disponible en: https://nosreimostodxs.com/que-es-el-sexting-o-sextorsion/?

- **Tácticas del sexting**

Tener presente estas tácticas para así evitar varios riesgos de ciberseguridad y que incluyen:

- Intercepción de mensajes: en redes no seguras, mostrando información delicada.
- Phishing: mediante engaños buscan obtener información específica o ingresar a cuentas, utilizando estrategias de sexting con el objetivo de manipular.
- Malware: transmiten archivos o vínculos perjudiciales, pero con contenido atractivo y consiguen infectar dispositivos, archivos o vínculos malintencionados.
- Capturas de pantalla: los individuos logran capturar y difundir contenido personal, que se expone sin el permiso del afectado.
- Fugas de datos: en este escenario, si la aplicación en uso presenta una vulnerabilidad de seguridad, los mensajes se vuelven accesibles para terceros.
- Medidas de seguridad: es esencial para mitigar estos riesgos y proteger tu privacidad.
- Desconfía de enlaces y archivos: no hagas clic en enlaces sospechosos y evita abrir archivos de origen desconocido.
- No almacenes contenido sensible: evitar guardar fotos o mensajes comprometidos en su dispositivo; o de lo contrario asegurarse de usar aplicaciones que protejan estos archivos con contraseñas.

- **Tecnologías de seguridad para la prevención del sexting**

  - Resulta imprescindible disponer de sistemas de bloqueo y filtros de seguridad, para prevenir que individuos sin consideración ingresen a los materiales almacenados.
  - Desarrollar claves seguras, mediante la mezcla de números, símbolos y letras en mayúsculas y minúsculas.
  - Alterar la contraseña en promedio cada tres meses, no compartirla por ninguna razón, ya sean familiares o amigos.
  - En caso de que no se utilice la cámara web durante el chat, se alerta a taparla, solo de esta manera se previene la captura de imágenes.
  - Realizar un respaldo de las imágenes y eliminarlas de los distintos aparatos, tabletas o netbooks.
  - En caso de hallarse material sexual vinculado a niños, niñas y adolescentes, es necesario interponer una denuncia en las oficinas de policía o fiscalías adyacentes.
  - Interactuar con los sistemas de denuncia en línea, para pedir la supresión de determinados contenidos y de esta manera pedir la supresión de los datos.

- Implementar filtros de protección en los navegadores para prevenir la propagación de contenido violento o dirigido a los adultos.
- Usa plataformas de mensajería seguras que ofrezcan encriptación de excelente calidad, como Signal o WhatsApp.
- Configura la privacidad: revisa el software limitando quien puede ver los datos.

- **Consecuencias más complejas del sexting.**

  - **Ciberbullying:** actitudes agresivas hacia el personaje principal que causan la humillación pública.
  - **Extorsión y chantaje**: el contenido puede emplearse como mecanismo de extorsión, y para prevenir su divulgación se solicitará cualquier "recompensa" (económica o de otra naturaleza).
  - **Grooming y acoso sexual:** en estos escenarios de hostigamiento sexual, es habitual la extorsión para exigir más contenidos, o incluso un contacto sexual directo.
  - **Riesgos físicos:** Los mensajes enviados pueden utilizarse por los agresores para escoger a sus víctimas. Varios de los contenidos exhiben componentes que simplifican su ubicación, como: domicilio, sitio de estudio, geolocalización o incluso el sitio donde se han registrado.

6.1.1.10 Ciberbullying

Es la utilización de recursos telemáticos (principalmente teléfonos móviles, internet y videojuegos en línea) para instaurar el hostigamiento entre pares. Se distingue por su carácter digital y puede expresarse en múltiples formas, tales como el envío de mensajes intimidatorios, la propagación de rumores o la divulgación de datos personales sin el permiso correspondiente.

> "Se conoce como ciberbullying (del inglés bullying, acoso o matonaje), ciberacoso o acoso virtual al uso de las plataformas y medios de comunicación digitales con fines de ejercer violencia emocional y psicológica sobre un individuo o un grupo de ellos, a través de ataques personales constantes, divulgación de información privada o de información falsa, generalmente por parte de agresores amparados en el anonimato"[18]

[18] CONCEPTO. ¿Qué es el ciberbullying? (29, marzo, 2021).Concepto, características y cómo prevenirlo).[sitio web].[Consultado: 26, septiembre, 2024]. Disponible en: https://concepto.de/ciberbullying/

- **Tácticas empleadas en el Ciberbullying**

Las formas que adopta son muy variadas y sólo se encuentran limitadas por la pericia tecnológica y la imaginación de los menores acosadores, lo cual es poco esperanzador. Algunos ejemplos concretos podrían ser los siguientes:

- Difundir en la web una imagen comprometida (auténtica o realizada a través de fotomontajes) de datos sensibles, elementos que pueden dañar o hacer avergonzar a la víctima.
- Establecer un perfil o lugar ficticio en representación de la víctima, en plataformas sociales o foros, en el que se relaten en primera persona eventos personales, solicitudes explícitas de relaciones sexuales.
- Inscribir a la víctima, con fotografía incluida, en un sitio web donde se busca votar a la persona más guapa, a la menos perspicaz... y otorgarle puntos o votos para que se encuentre en las primeras posiciones.
- Notificar la dirección de email en ciertos sitios para prevenir que sea objeto de spam, o de interacciones con desconocidos.
- Usar su clave de correo electrónico, luego modificarla, de manera que su dueño legítimo no pueda estar al tanto y le resulte complicado leer los mensajes que se hallan en su buzón, así se está infringiendo su privacidad.
- Enviar mensajes amenazantes por e-mail o SMS, hostigar y vigilar a la víctima en los lugares de Internet en los que se relaciona de forma habitual induciendo a que sienta vulnerable.
- Difundir ciertos rumores donde a la víctima se le atribuya una conducta censurable, agresiva u ofensiva, con el objetivo de que los demás implementen sus propios métodos de venganza o hostigamiento.
- Dejar comentarios agresivos en foros o interactuar de manera ofensiva en chats, confundiéndose con la víctima.

- **Tecnologías de IA efectivas para Identificar el Ciberbullying**

Emplear la opción "Restringir" para resguardar de manera discreta la cuenta sin que el individuo involucrado lo conozca, filtrar los comentarios en tus propias publicaciones, cambiar la configuración para que solo se puedan enviar mensajes directos a las personas seleccionadas, entre otros.

No obstante, la inteligencia artificial (IA) se ha consolidado como un recurso esencial en la identificación y prevención del ciberacoso. En seguida se exponen las tecnologías más eficaces en este entorno:

- Identificación de patrones: los algoritmos de machine learning analizan volúmenes de datos históricos para identificar patrones asociados con el ciberbullying y mejorando su precisión con el tiempo.

- Procesamiento del Lenguaje Natural (NLP): analizan el contenido textual, es decir, insultos, amenazas, reconocen el lenguaje hostil y patrones del ciberacoso.
- Detección proactiva: acceden a las plataformas para detectar comportamientos sospechosos antes de que se intensifiquen. Allí analizan comentarios, mensajes y publicaciones en redes sociales.
- Modelos de Deep Learning: empleando redes neuronales, capturan relaciones complejas en los datos e identifican el contenido perjudicial.
- Análisis de Texto: las técnicas de NLP permiten analizar el contenido textual para identificar lenguaje hostil y patrones relacionados con el ciberacoso. Esto incluye la detección de insultos, amenazas y otros tipos de discurso dañino
- Patrullas en línea: compuestas por educadores y padres, ayudan a supervisar interacciones y detectar comportamientos abusivos, complementando la tecnología automatizada.
- Colaboración entre plataformas: la cooperación entre empresas tecnológicas y organizaciones no gubernamentales permite mejores prácticas y optimizar las herramientas disponibles para la detección del ciberbullying.

6.1.2 Malware

Es un software malintencionado creado para perjudicar sistemas de computación, sustraer información o tomar el control de equipos, incorpora tipos como ransomware, rootkits, phishing, cryptojacking, entre otros, estos ataques de malware generalmente utilizan fallos en sistemas o ingeniería social para infectar equipos. Es esencial la ciberseguridad para resguardarse de estas amenazas y los vectores de ataque comprenden correos electrónicos malintencionados, programas descargados de fuentes no confiables, por eso para la prevención se debe actualizar los programas informáticos y fomentar la educación en seguridad informática.

6.1.2.1 Ransomware

En 1996, se denominaba al ransomware como "extorsión criptoviral", una noción propuesta por Moti Yung y Adam Young de la Universidad de Columbia. Luego, los ataques de ransomware comenzaron a ganar popularidad con la aparición de Bitcoin, Ethereum, Litecoin y otras variantes de monedas digitales que emplean ciertos métodos de encriptación para validar, proteger las transacciones, supervisar y regular la generación de nuevas copias.

El ransomware es una categoría de software malicioso, representando un peligro tanto para el individuo como para el aparato. Su denominación no es casual: "ransom", el término que emplea para iniciar su negocio, es una palabra inglesa que traduce "rescate"

> "El ransomware es un tipo de malware (software malicioso) que cifra y/o roba y pide un rescate, normalmente exigido en criptomoneda, como el bitcoin. Los ataques de ransomware suelen cifrar archivos para negar a las víctimas el acceso a sus datos a menos que paguen antes de una fecha límite, después de la cual pueden perder el acceso a los datos cifrados de forma permanente. El pago exigido a cambio de una clave de descifrado puede oscilar entre cientos y millones de dólares".[19]

- **Tácticas del Ransomware**

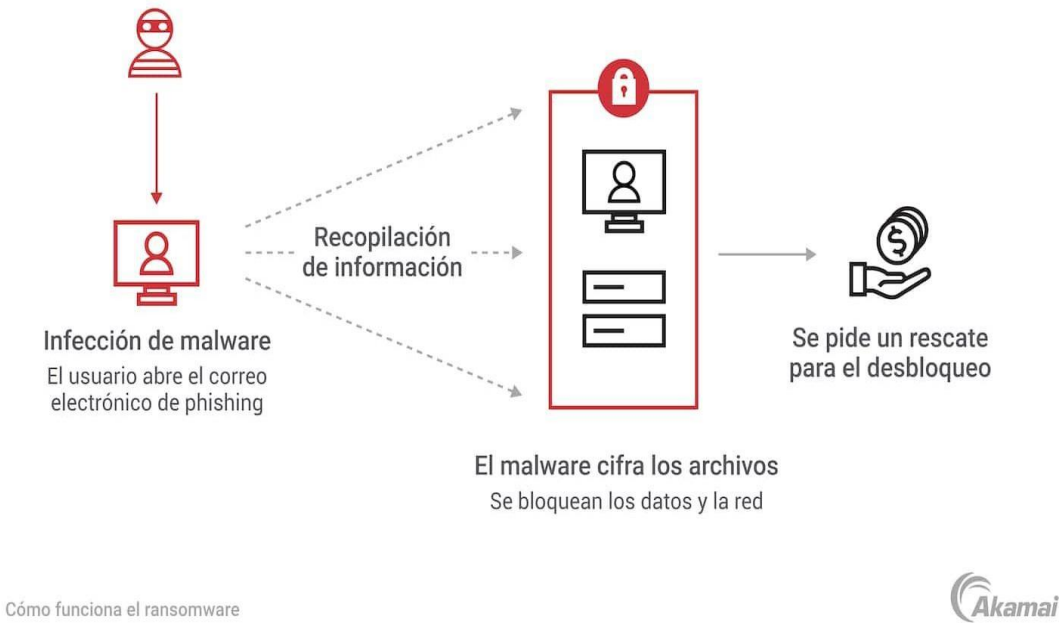
El Ransomware funciona habitualmente mediante:

- Una entidad auténtica y legítima o alguien que diferencia a la víctima,
- Por medio de diversos correos electrónicos de phishing.
- Diversa publicidad infectada que se han enviado.
- En la página web se registró malware.
- Una estafa donde el cliente, al hacer clic en un enlace malintencionado o al abrir un archivo, se ve engañado.
- En los ataques de ransomware contra un tercero, las actividades estarían orientadas a bloquear, capturando documentos, fotografías y datos personales o financieros.
- En el escenario alternativo, criptoransomware, los rehenes son los datos que solicita un resguardo.
- En las entidades, se enfoca en la pérdida de capital, pero lo más grave y alarmante es el buen nombre de la empresa.
- Cuando los ciberdelincuentes encriptan datos, utilizando ransomware de cifrado, pueden necesitar un rescate por los datos que se transforman en prisioneros.
- Los cibercriminales que manejan el ransomware no siempre restablecen los archivos cifrados a la entidad, incluso después de haber pagado el rescate mencionado.
- Otro famoso agente de infección por ransomware se favorece a través de los protocolos de escritorio remoto (RDP), lo que significa que un hacker que ha logrado acceder a las credenciales de acceso podría utilizarlas para verificar los

[19]ZPEDIA. ¿Qué es el Ransomware? [sitio web]. [Consultado el 20, julio, 2024]. Disponible en: https://www.zscaler.es/resources/security-terms-glossary/what-is-ransomware

terminales dentro de una red empresarial o personal. Lamentablemente, este procedimiento facilitaría la descarga y la ejecución directa.

Figura 11. Cómo Funciona el Ransomware



Fuente: AKAMAI. Cómo funciona el ransomware. [imagen]. [Consultado el 20, julio, 2024]. Disponible en: https://www.akamai.com/es/glossary/what-is-ransomware

- **Ejemplos de Ransomware**

Entre los innumerables tipos y grupos de ransomware, algunos de los más comunes y conocidos son:

Tabla 7. Tipos de Ransomware

No.	TIPO	EXPLICACIÓN
1.	CRYPTOLOCKER 2014	Debido a la colaboración internacional de empresas de seguridad y fuerzas del orden y al éxito, han aparecido varios imitadores de cryptolocker.
2.	WANNACRY 2017	Ransomware de naturaleza criptogusana. La meta está enfocada en el sistema operativo Microsoft Windows. Impactó a más de 300 000 sistemas a nivel global.
3.	GANDCRAB	De acuerdo con el reporte Ransomware in Global Context de Virus Total, desde 2020, esta familia ha liderado los ataques de ransomware, con un 78,5 % de las muestras recolectadas.
4.	REVIL/SODINOKIBI MAYO 2020 HASTA OCTUBRE 2021	Famoso por sustraer enormes volúmenes de información tanto en el ámbito jurídico como del entretenimiento, incluyendo el ataque a Kaseya VSA. Es vinculado a una variedad de colectivos que han afectado áreas como la atención sanitaria, el sector público y la educación, especialmente de Estados Unidos.
5.	RYUK	Se relaciona con una serie de grupos que han impactado a sectores como la asistencia médica, el sector público y la educación, en especial en los sistemas escolares de EE. UU.
6.	EVIL CORP	Se encarga de Dridex, un malware que se propaga mediante emails de phishing, famoso por sustraer claves bancarias. Vinculado desde aquel momento con otras variantes de ransomware como WastedLocker, BitPaymer y DoppelPaymer
7.	CLOP	Ransomware es el autor de múltiples ataques importantes a compañías en áreas como la educación y la salud, donde han encriptado información delicada y requerido rescates elevados para su liberación.

Fuente: ZSCALER ¿Qué es el ransomware? [Consultado el 21, agosto, 2024]. Disponible en: https://www.zscaler.com/es/resources/security-terms-glossary/what-is-ransomware

- **Mejores prácticas de seguridad para la prevención de ransomware**

Cuando se trata de ransomware, la mejor forma de actuar es la prevención. La CISA, la Agencia de Seguridad de Infraestructura y Ciberseguridad, y el FBI, con el fin de

salvaguardar las diferentes organizaciones del ransomware realizan las siguientes recomendaciones:

- Efectuar una copia de seguridad de los equipos informáticos, con la finalidad de recuperar su sistema a su estado inicial.
- Adquirir las copias de seguridad de forma independiente, tanto a través del disco duro externo como en la nube, para prevenir la necesidad de tener acceso a través de una red.
- La modernización y evaluación de los dispositivos son medidas para eliminar vulnerabilidades en programas y sistemas operativos.
- Organizar con los empleados varias sesiones regulares y obligatorias de concienciación sobre ciberseguridad; con la finalidad de mantenerse al día acerca de las amenazas actuales y las prácticas de seguridad más significativas.
- Resulta fundamental tener precaución con el correo electrónico (aunque sea de remitentes reconocidos) y si son desconocidos, el procedimiento requiere verificar la identidad del remitente antes de abrirlo.
- La actualización y revisión de los equipos son procedimientos a considerar para eliminar vulnerabilidades en aplicaciones y sistemas operativos.
- Elaborar un plan de continuidad para la reparación en caso de sufrir un ataque por ransomware.
- Resulta esencial utilizar programas antivirus y antimalware, con el objetivo de que los usuarios frenen las amenazas y se evite la propagación de más daños.
- Implementación de una actitud de protección diseñada de manera autónoma en la nube para resguardar a los usuarios, las aplicaciones y la información confidencial de estos ataques, sin importar dónde se conecten o qué dispositivos estén empleando.
- Usar una cuarentena de sandbox gestionada por inteligencia artificial para retener e inspeccionar el contenido sospechoso antes de permitir su paso al receptor
- Realizar una revisión completa del tráfico encriptado con SSL/TLS para asegurar que no existan amenazas ocultas.

6.1.2.2 Riesgos de Malware

Entre los tipos de riesgos de ciberseguridad, este se refiere a la amenaza de software malicioso que puede infectar sistemas y redes como:

- **Virus:** un virus informático se adjunta a programas legítimos o archivos y se propaga al ejecutar el programa o abrir el archivo infectado. Estos pueden dañar archivos, corromper sistemas y propagarse a través de medios de almacenamiento compartidos, como unidades USB.

- **Gusanos:** son programas maliciosos que se esparcen de forma autónoma a través de redes y sistemas, sin necesidad de intervención humana. Se replican y se envían a otros sistemas conectados, lo que puede llevar a una propagación rápida y dañina.
- **Troyanos:** programas que se disfrazan como software legítimo, pero contienen código malicioso. Una vez en el sistema, pueden permitir el acceso no autorizado o robar información.
- **Spyware:** tipo de software malicioso diseñado para recopilar información sobre las actividades de un usuario sin su conocimiento o consentimiento. Puede registrar pulsaciones de teclas, capturar contraseñas o rastrear la navegación web, lo que plantea graves preocupaciones de privacidad.
- **Adware:** clase de software malicioso que muestra anuncios no deseados en una computadora o dispositivo. Aunque no siempre es dañino, puede ralentizar el rendimiento del sistema y, en algunos casos, redirigir a sitios web maliciosos.

6.1.3 Acceso no autorizado

El acceso no autorizado a la información de los estudiantes tiene un impacto significativo en su privacidad, lo que puede derivar en diversas consecuencias negativas. A continuación, se analizan las implicaciones de este riesgo en el contexto educativo.

6.1.3.1 Impacto en la privacidad de los estudiantes

- **Robo de Identidad**: cuando los datos personales de los estudiantes son accesibles sin autorización, existe un alto riesgo de robo de identidad. Los cibercriminales pueden utilizar esta información para hacerse pasar por el estudiante, lo que puede resultar en fraudes financieros y problemas legales.
- **Acoso y Chantaje**: la exposición de información sensible puede llevar a situaciones de acoso. Los delincuentes pueden utilizar datos personales para amenazar o chantajear a los estudiantes, creando un ambiente hostil y perjudicial para su bienestar emocional.
- **Exposición de Información Sensible**: datos como registros académicos, información médica y detalles familiares pueden ser vulnerables al acceso no autorizado. Esta exposición no solo compromete la privacidad del estudiante, sino que también puede afectar su reputación y relaciones personales.
- **Desconfianza en las Instituciones**: la falta de medidas adecuadas para proteger la información personal puede generar desconfianza entre los estudiantes y las

instituciones educativas; afecta la relación entre ambos y disminuye la participación activa de los estudiantes en actividades académicas y sociales

El acceso no autorizado tiene un impacto profundo en la privacidad de los estudiantes, seguridad personal, bienestar emocional y rendimiento académico. Es fundamental que tanto las instituciones educativas como los propios estudiantes tomen medidas proactivas para mitigar estos riesgos.

En los colegios colombianos se subrayan la necesidad urgente de mejorar las medidas de ciberseguridad en el sector educativo. Es esencial que las instituciones implementen políticas robustas, capaciten a estudiantes y al personal sobre ciberseguridad, y establezcan protocolos claros para proteger la información sensible y garantizar un entorno seguro para todos.

6.1.3.2 Tipos de Datos Más Vulnerables en Ciberataques en Colegios Colombianos

- **Datos Personales:** se incorpora nombres, direcciones, números de identificación y datos de contacto del alumno e información personal; la vulnerabilidad de estos resulta atractiva para los ciberdelincuentes para el hurto de identidad y fraudes, debido a la ausencia de medidas de protección.
- **Registros Académicos:** incluye calificaciones, notas, asistencia y otros datos académicos pertinentes; la vulnerabilidad está vinculada a los registros académicos, los cuales pueden ser alterados por alumnos o intrusos externos para modificar notas u obtener acceso a información delicada.
- **Datos Financieros:** la información vinculada a cuentas bancarias, pagos académicos y datos económicos de alumnos y trabajadores; es particularmente atractiva para los ciberdelincuentes por su capacidad para emplearse en estafas financieras.
- **Credenciales de acceso:** las claves y nombres de usuario para plataformas educativas y redes sociales; si se fragmenta esta vulnerabilidad de acceso no permitido a estas claves, permitiría a los intrusos ingresar a cuentas personales, poniendo en riesgo la seguridad del usuario.

6.1.3.3 Impactos negativos ciberataques sector educación Colombia

Un hacker es un individuo con habilidades avanzadas en tecnología de la información que investiga, explora y descubre vulnerabilidades en sistemas informáticos y redes comunicativas; a pesar de que puede contener significados negativos, como "pirata informático", también hace referencia a aquellos que emplean sus capacidades para incrementar la protección de los sistemas. Esta clase de personas utilizan sus habilidades

tecnológicas para infiltrarse en sistemas o redes de forma ilícita y causan serios perjuicios a la seguridad informática en el ámbito educativo y otros contextos.

A continuación, se describen algunos de los daños e impactos que causan los hackers:

- **Robo de información confidencial:** obtienen acceso a información reservada, tales como registros escolares, datos financieros y personales de alumnos, docentes y trabajadores, permitiéndoles cometer fraude, hurto de identidad y otros delitos.
- **Interrupción del servicio:** perturban el funcionamiento de las redes y sistemas de computación, que afecta el rendimiento de las instituciones educativas y dificultan la obtención de datos relevantes, como planes de estudio y apuntes, lo que demora el proceso de educación.
- **Difusión de malware:** introducen malware en sistemas y redes, afecta la funcionalidad de los dispositivos y sistemas informáticos. También se propaga a través de redes y sistemas, causándoles un gran daño.
- **Acoso cibernético:** uno de los temas más graves, cuando sobrepasa la seguridad informática sector educación, es llegar a usar los datos de las redes sociales y otros medios de comunicación para acosar a estudiantes, profesores y empleados.
- **Falsificación de identidad:** utilizando estrategias de ingeniería social para recopilar datos personales, como contraseñas y números de tarjetas de crédito, aprovechan los datos para falsear la identidad de alumnos, docentes y trabajadores de los centros educativos.

6.1.4 Riesgo derivado del error Humano

El error humano es uno de los factores más significativos de las vulnerabilidades en la ciberseguridad, constituyendo cerca del 95% de las infracciones de seguridad. Este fenómeno hace alusión a actos no deseados o elecciones equivocadas hechas por los trabajadores que pueden provocar la divulgación de datos o fallos de seguridad .

El error humano representa aproximadamente el 95% de las violaciones de seguridad debido a acciones involuntarias o decisiones incorrectas realizadas por los usuarios que pueden resultar críticas en la exposición de datos o brechas de seguridad y en el caso de los colegios puede tener consecuencias significativas.

A continuación, se detallan las causas más comunes de estos errores:

- **Configuración incorrecta de seguridad en los dispositivos:** muchos estudiantes pueden establecer en forma incorrecta las configuraciones de privacidad y seguridad en sus dispositivos y cuentas, dejando vulnerabilidades abiertas, dando paso al origen de brechas que los atacantes pueden explotar para que malware o virus se propaguen

dentro del equipo, afectando la confidencialidad e integridad de la información de los usuarios y sistemas.

- **Comportamiento Imprudente en Redes Sociales:** los jóvenes en muchas ocasiones comparten información sensible en redes sociales o con compañeros, sin considerar las implicaciones de seguridad, al verse amenazada la integridad de la información trayendo como consecuencia la exposición de datos sensibles que puede ser utilizada por los ciberdelincuentes para realizar ataques dirigidos o acoso.
- **Envío incorrecto de información sensible:** los estudiantes pueden enviar accidentalmente documentos con información sensible a destinatarios incorrectos, esto puede resultar en brechas de datos significativas y violaciones de la privacidad.
- **Conexión de dispositivos no autorizados:** al conectar los alumnos sus dispositivos personales, como USB o portátiles, a la red escolar sin autorización, puede introducir malware en la red escolar y dar acceso no autorizado a información sensible.

6.1.5 Falta de Capacitación en ciberseguridad

La ausencia de formación en ciberseguridad tiene un rol vital en la prevención de peligros cibernéticos, que son una de las principales razones de incidentes de seguridad en las instituciones educativas. Los menores de edad son especialmente susceptibles en cometer infracciones que pueden poner en riesgo la seguridad de la privacidad e integridad de la información.

Enseguida se detallan los aspectos clave de cómo la educación puede mitigar estos errores y mejorar la postura de ciberseguridad en las instituciones educativas.

6.1.5.1 Importancia de la educación en ciberseguridad

- **Desconocimiento sobre amenazas cibernéticas:** la falta de capacitación y conciencia sobre ciberseguridad impide en los estudiantes identificar las diversas amenazas cibernéticas como el phishing, el malware, ransomware o el uso inseguro de redes Wi-Fi públicas, este desconocimiento aumenta la probabilidad de que caigan en trampas cibernéticas o comportamientos sospechosos y sean víctimas de ataques exponiendo la información personal y académica a riesgos innecesarios.
- **Falta de actualización de software:** las niñas y niños a menudo no actualizan sus dispositivos y aplicaciones, ignorando las notificaciones de actualizaciones, contribuyendo a una posible vulnerabilidad de ataque, esta falta de atención deja a sus equipos tecnológicos vulnerables a exploits y malware que podrían haberse evitado con parches de seguridad.

- **Evitar descargar software potencialmente malicioso:** los menores de edad no deben descargar programas o archivos si no se conocen su procedencia. Puede tener adjunto un archivo infectado que afecte los datos o sistema del equipo tecnológico y ponga en riesgo la seguridad de la información.
- **Uso de contraseñas débiles:** un sinnúmero de estudiantes utiliza contraseñas simples o comunes, como "123456","password", fechas de nacimiento y reutilizan las mismas contraseñas en múltiples cuentas, facilitando el acceso autorizado a sus cuentas y sistemas, permitiendo que los ciberdelincuentes comprometan su información sensible.
- **Clics en enlaces maliciosos:** los estudiantes pueden ser víctimas de trampas de phishing al hacer clic en vínculos dudosos en emails o mensajes de texto, lo que podría llevar a la descarga de malware o al hurto de credenciales, poniendo en riesgo la privacidad e integridad de los datos personales.
- **Pérdida de datos sensibles:** los menores de edad pueden perder información importante, como tareas y proyectos, si no realizan copias de seguridad o no resguardan correctamente sus dispositivos electrónicos. Lo anterior provocaría tensión emocional e impactaría de manera adversa su rendimiento escolar.
- **Riesgos de seguridad asociados con dispositivos IoT en instituciones:** los aparatos del Internet de las Cosas (IoT) consiguen impactar la seguridad de las niñas, niños y jóvenes en instituciones educativas, brindan ventajas considerables en cuanto a aprendizaje y administración educativa, pero también conllevan riesgos que deben ser tenidos en cuenta.

Esencialmente, cualquier objeto físico puede transformarse en un dispositivo IoT si tiene la capacidad de conectarse a Internet para recolectar y manejar información.

Algunos de estos riesgos y su impacto en la seguridad de los menores de edad:

- **Falta de actualizaciones y mantenimiento dispositivos IoT:** muchos dispositivos IoT requieren actualizaciones periódicas para mantener su seguridad. Sin embargo, estas actualizaciones pueden ser pasadas por alto, causando un impacto en la falta de mantenimiento que puede dejar a los dispositivos vulnerables a exploits conocidos, facilitando de esta forma el acceso no autorizado y ataques cibernéticos.

- **Riesgos físicos asociados con dispositivos conectados:** algunos aparatos de IoT, como cámaras y sensores, pueden ser manejados únicamente si no cuentan con la seguridad correcta, lo que podría facilitar intrusiones no autorizadas o el uso indebido de dispositivos que comprometen la seguridad física del ambiente académico.

- **Cámaras de videovigilancia:** utilizadas para monitorear la seguridad en la institución y prevenir intrusiones; un posible riesgo se da si las cámaras están conectadas a una

red insegura, las cuales pueden ser pirateadas, permitiendo a los atacantes acceder a imágenes y videos que comprometen la privacidad e integridad de los estudiantes.

Los estudiantes se encuentran con múltiples peligros al utilizar internet, redes sociales y dispositivos tecnológicos que amenazan su privacidad, integridad y disponibilidad de sus datos. Entre los que se destacan son: el acceso a información poco confiable y perjudicial, así como la exposición a contenidos inapropiados y riesgosos, entre los más comunes esta la pornografía infantil, la violencia, el ciberacoso, acicalamiento y fraudes. En numerosas ocasiones, la interacción de personas desconocidas en internet puede llevar a situaciones de explotación o involucramiento en acciones ilícitas. Por esta razón, es importante que tanto jóvenes como padres y docentes estén informados sobre estos riesgos e implementen acciones preventivas.

6.2. EXPLICAR LAS HERRAMIENTAS DE CIBERSEGURIDAD QUE PROTEGEN LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN PARA UNA NAVEGACIÓN SEGURA DE LOS ESTUDIANTES AL USAR EQUIPOS PERSONALES E INSTITUCIONALES.

En un mundo cada vez más interconectado, donde las amenazas a la seguridad informática son cada vez más sofisticadas, por lo tanto, se hace necesario que los equipos personales de los estudiantes y de las instituciones educativas en general adopten unas medidas proactivas para salvaguardar sus datos y su privacidad, los estudiantes pueden beneficiarse de diversas herramientas de ciberseguridad, tanto gratuitas como privadas. Estas herramientas son fundamentales para proteger integridad, confidencialidad y disponibilidad de la información personal y evitar posibles ataques cibernéticos, garantizando un entorno digital más seguro.

Algunas de las herramientas más relevantes que pueden utilizar los menores de edad en sus equipos personales y las instituciones en sus equipos y redes para mantenerse al tanto de las mejores prácticas en ciberseguridad para una navegación segura en la red internet.

6.2.1 Herramientas de Control Parental

Esta clase de herramientas pueden ser beneficiosas para minimizar los riesgos mientras el niño aprende a manejarse en la red, por otra parte, brindan un respaldo en el aprendizaje digital de los niños, restringiendo las funcionalidades y el alcance de sus aparatos al conectarse a la red.

Muchas de las herramientas que se mencionan en el siguiente gráfico, solo funcionan en presencia de un adulto porque los menores pueden aprender a eliminar estos controles. Es importante tener presente que no todas las herramientas disponibles impiden el acceso a contenido inapropiado para menores de edad; por eso es importante seleccionar una herramienta de control parental con la que se pueda filtrar y bloquear contenido inapropiado; que sirven de apoyo en el aprendizaje digital de los menores, pero limitan el alcance de sus equipos cuando están conectados a Internet.

Figura 12. Herramientas control parental

Fuente: LISA Institute. [blog]. Herramientas de control parental [Consultado el 30, noviembre, 2023]. Disponible en: https://www.lisainstitute.com/blogs/blog/guia-practica-control-parental-hijos-consejos-ventajas-herramientas-riesgos

Es necesario que los padres de familia establezcan relaciones con sus hijos e hijas de los grados 9o. 10o y 11o, el amor y el diálogo, que faciliten esclarecer, guiar y disipar interrogantes sobre algunas acciones que pueden representar un riesgo para los niños. Es imprescindible implementar acciones para supervisar parentalmente el material que los menores de edad emplean diariamente en Internet. Sin embargo, no debe limitarse a eso, sino que este procedimiento debe tener como complemento el diálogo y la confianza, para que ellos se motiven a comunicar cuando algo les resulta molesto.

> "El control parental se define como el conjunto de herramientas que favorecen el control sobre el uso de Internet y de dispositivos electrónicos, es decir, que evitan el acceso de los menores a contenidos inapropiados en la red. Actualmente, los menores tienen acceso a través de los dispositivos electrónicos a cualquier tipo de contenido en Internet, lo que puede causar en ellos serios problemas en su desarrollo psicosocial". [20]

Algunas de las razones por las que establecer un control parental es muy beneficioso:

- Proteger a los hijos e hijas del contenido inapropiado en las redes para que la experiencia sea positiva.
- Bloquear algunas páginas de web o tipos de búsquedas.
- Disminuir las descargas para asegurar la seguridad de los dispositivos.
- Luchar contra el hostigamiento en línea y otros crímenes perpetrados a través de Internet.
- Limitar contenidos o apps que no sean apropiados para su edad.

[20] LISA Institute. [blog]. [Consultado el 30, noviembre, 2023]. Disponible en: https://www.lisainstitute.com/blogs/blog/guia-practica-control-parental-hijos-consejos-ventajas-herramientas-riesgos.

Tabla 8. Herramientas Parentales

HERRAMIENTAS PARENTALES	VENTAJAS
ANTIVIRUS FAMILIAR	• Proporciona herramientas que enseñan hábitos seguros, inteligentes y saludables en Internet. • Brinda información que le contribuye a fomentar un equilibrio saludable entre Internet y los dispositivos de sus hijos. • Para monitorear los sitios y contenidos que ven sus hijos así naveguen en forma más segura. • Bloquea contenido perjudicial o inapropiado. • Con la función "Advertir" genera una advertencia a los niños para que no visiten sitios web peligrosos o dañinos. • Tiene buen filtro para configurar los sitios web, de acuerdo a las edades de los menores. • Los padres tendrán la ventaja de elegir cuáles son las categorías que se bloquean y cuáles si se permiten. • Crea límites de uso diario en bloques de media hora o una hora. • Mamá y papá pueden crear unas listas con las normas o reglas, para gestionar su tiempo en la web. • Opción de bloqueo instantáneo, para que los menores de edad dejen el móvil. **Desventajas:** • Poca flexibilidad de la herramienta del tiempo para controlar cualquier aplicación. • El plan gratuito es sólo por 30 días.
GUARDIÁN FAMILIAR **Estas aplicaciones vinculan el dispositivo de su hijo con su propio dispositivo.**	• Permite crear un rastreo de su hijo o hija en tiempo real con el uso de IA-Inteligencia Artificial. • Indica el nivel de la batería del equipo. Los riesgos que corren los menores de edad en los chat y redes sociales. • Por rastreo GPS se va actualizando en tiempo real la ubicación exacta de su hijo. • Muestra a los padres cuando sus hijos están siendo objeto de acoso cibernético. • Revela el tiempo que los menores de edad están con el dispositivo móvil.
KEYLOGGER	• Es capaz de usarse tanto en Android, Windows o Mac. • Aplicación de código abierto y brinda a los padres una lista de los sitios web que visitan los niños. • Revela que palabras clave escribe el menor cuando busca en el internet e informan un listado de app que más frecuenta. • Controla los distintos destinatarios de mensajes de texto, el registro de llamadas. **Desventajas** No dispone de filtros web
QUSTODIO	• Herramienta gratuita y con varias ventajas. • Gestiona el teléfono inteligente delante de la pantalla. • Para conocer el tiempo que pasan a diario los chicos en los móviles (jugando, navegando). • El tiempo que ellos o ellas permanecen en páginas web. • Tiene varios filtros que les ayudará a los padres a administrar mientras navegan. **Desventajas** Se puede usar en un solo teléfono móvil.
SERVICIO DE SISTEMA DE NOMBRES DE DOMINIO (DNS) Y CORTAFUEGOS	• App gratuita, fácil de instalar y configura para que los padres puedan supervisar como sus hijos usan sus móviles. • Ofrece de forma gratuita 300.000 consultas mensuales. • Opera como un servidor normal de DNS. • Tiene varias funciones como el modo seguro y el restringido de YouTube. • Bloquear anuncios y rastreadores en sitios web y aplicaciones. • Proteger contra amenazas de seguridad como malware, ataques de phishing y cryptojacking. **Desventajas** No funciona con WhatsApp

Fuente: Herramientas de control parental y herramientas para padres [Consultado el 28, noviembre, 2023]. Disponible en: https://www.udlap.mx/habilidadesdigitales/consejosdeseguridad.aspx?id=HerramientasDeControlParental

6.2.2 Herramientas de educación en ciberseguridad para estudiantes

Es esencial salvaguardar la confidencialidad y privacidad de los alumnos. Es habitual en las escuelas y colegios la recolección de información personal, académica para garantizar que dichos datos estén resguardados frente al acceso no permitido. El establecimiento de políticas de privacidad precisas y el encriptado de datos son componentes esenciales para proteger la información delicada del estudiante.

Hay múltiples alternativas que fusionan teoría y práctica para tornar el aprendizaje de la ciberseguridad más atractivo y eficiente para los jóvenes. Varias tácticas y herramientas que pueden emplearse para instruir a los alumnos en temas de ciberseguridad.

6.2.2.1 CyberStart

Es una plataforma educativa interactiva y entretenida creada para instruir a jóvenes, en particular a alumnos de nivel secundario, en el intrigante universo de la ciberseguridad. Mediante juegos y retos, facilita el desarrollo de habilidades fundamentales que resultarán de gran utilidad al incursionar en este ámbito. Proporciona una variedad de retos y juegos que pueden ser finalizados de manera individual o grupal. Los retos suelen surgir en contextos reales donde los jóvenes deben aplicar sus habilidades de ciberseguridad para solucionar un problema.

- **¿Por qué es interesante CyberStart?**

A continuación, se presentan las razones por las cuales CyberStart es considerado interesante y relevante:

- Resulta entretenido: CyberStart convierte el proceso de aprendizaje en una experiencia cautivadora y adictiva, debido a sus juegos y retos.
- Resulta práctico: las competencias que obtienes en CyberStart resultan muy valiosas en la vida real, independientemente de si deseas cursar una profesión vinculada a la ciberseguridad o simplemente salvaguardar tus equipos.
- Es fácil de alcanzar: proporciona un método gratuito y sencillo para comenzar en la ciberseguridad, sin requerir de habilidades previas.
- Se adquieren: principios fundamentales de ciberseguridad, operación de redes, métodos de protección de sistemas y definición de amenazas de ciberseguridad.
- Destrezas prácticas: como el rompecabezas de contraseñas, la identificación de vulnerabilidades en sistemas y la solución de problemas.
- Pensamiento crítico: examina circunstancias, establece razonamientos de forma coherente y toma decisiones estratégicas.
- Cooperación en equipo: trabaja en conjunto colabora con otros estudiantes para resolver problemas complejos.

- **Beneficios al usar CyberStart.**

  - Presentación entretenida de la ciberseguridad: CyberStart convierte el aprendizaje en un juego, en un tema atractivo y estimulante para la juventud, a través de desafíos y juegos, los estudiantes desarrollan habilidades encaminadas al conocimiento de técnicas en ciberseguridad.
  - Fomento de competencias fundamentales: mediante retos y juegos, los alumnos fomentan habilidades orientadas al entendimiento de técnicas de ciberseguridad, a la solución de problemas, al razonamiento crítico y al trabajo colaborativo.
  - Acceso sin costo: en varias naciones, como Estados Unidos, hay programas que proporcionan acceso sin costo a CyberStart para jóvenes de secundaria, transformándose en una oportunidad asequible para todos.
  - Promoción de las nuevas generaciones profesionales: CyberStart aporta a la capacitación de una nueva generación de expertos en ciberseguridad, siendo esencial para abordar los retos en aumento en este ámbito.
  - CyberStart ayuda a crear conciencia sobre la importancia de protegerse en el mundo digital. Aumento de la conciencia sobre la ciberseguridad permitiendo que la ciberseguridad sea más accesible y divertida.
  - Identificación de talentos: en el caso de jóvenes con un talento especial para la ciberseguridad, brindándoles las herramientas y el apoyo necesarios para desarrollar sus habilidades.

- **¿Qué temas cubre CyberStart?: encierra una amplia gama de temas relacionados con la ciberseguridad, incluyendo:**

  - Conceptos básicos de redes: diseño de redes y protocolos de comunicación.
  - Seguridad de sistemas operativos: ¿cómo proteger sistemas operativos como Windows, Linux?
  - Seguridad de aplicaciones: ¿cómo identificar y prevenir vulnerabilidades en aplicaciones web y móviles?
  - Criptografía: los fundamentos de la criptografía y ¿cómo se utiliza para proteger la información?
  - Conciencia de la seguridad: ¿cómo protegerse de las amenazas cibernéticas más comunes, como el phishing y el malware?

6.2.2.2 Google Interland

Juego interactivo creado por Google, tiene como objetivo instruir a las niños y niños acerca de la ciberseguridad de forma entretenida y didáctica. La iniciativa del mismo se

relaciona con la iniciativa "Sé magnífico en Internet", cuyo objetivo es fomentar una ciudadanía digital consciente y segura. Interland se puede visitar mediante navegadores web, lo que posibilita a los niños divertirse desde cualquier aparato con acceso a la red.

- **¿Por qué es interesante Google Interland?** Este juego interactivo es interesante por las siguientes razones:
    - **Educación entretenida:** facilita a los menores de edad el aprendizaje de ciberseguridad de forma atractiva. Mediante cuatro juegos breves, los niños tratan temas fundamentales como el establecimiento de contraseñas seguras, la detección de perfiles falsos y el comportamiento cordial en internet, todo ello mientras se divierte.
    - **Fomento de competencias fundamentales:** a través de Interland, los niños y niñas aprenden a compartir datos personales de forma segura, se instruye a los jóvenes a reconocer correos electrónicos, perfiles fraudulentos, promueve la cordialidad y el respeto hacia otros usuarios en la red, contribuyendo a generar un ambiente digital más favorable.
    - **Accesibilidad y gratitud:** está disponible en varios idiomas, es una herramienta de fácil acceso para todos los niños, independientemente de su contexto socioeconómico.

- **Beneficios Educativos:**
    - **Aprendizaje Interactivo:** usando minijuegos y retos, los menores de edad, pueden adquirir nociones básicas de ciberseguridad al mismo tiempo que se divierten. Cada juego contiene interrogantes y exámenes que potencian el aprendizaje.
    - **Diseño Atractivo:** gracias a sus gráficos vibrantes y controles sencillos, el juego es fácil de entender para los más pequeños.
    - **Conciencia Informática:** Interland no solo enseña a los niños a utilizar la red de manera segura, y asiste a los padres en la comprensión de los peligros vinculados con el uso de la tecnología por parte de sus hijos.
    - **Formulación de cinco fundamentos esenciales:** este juego revolucionario forma parte de la serie "Se genial en Internet", también de Google. El objetivo está orientado a que los niños adquieran cinco valores de Internet; compartir de manera cautelosa, evitar ser víctimas de engaños, y salvaguardar sus datos personales.

- **Características del Juego**

Comparte información personal, crea contraseñas seguras, identifica perfiles falsos y promueve el buen comportamiento en línea. Cuenta con cuatro emocionantes minijuegos, los niños aprenderán estas lecciones vitales de una manera divertida y atractiva.

- **Cuatro Mundos de Tema:** Google Interland se divide en cuatro aventuras, cada una centrada en un elemento crucial de la seguridad en internet:
- **Río de Realidad:** los jugadores aprenden a identificar fraudes y emails engañosos, además de las medidas a adoptar frente a circunstancias inusuales. Implica a mantenerse distanciado de perfiles falsos y estafas.
- **Torre del Tesoro:** este mundo los niños y niñas se centran en la creación de contraseñas seguras y proporciona consejos sobre cómo proteger información personal.
- **Montaña Sensata:** los niños adquieren conocimiento de la relevancia de divulgar información personal de forma responsable y las repercusiones de dicho acto. Mindful Mountain, en la que los niños se enfocan en compartir datos en línea con aquellos en quienes tienen confianza.
- **Reino Amable:** su estrategia consiste en fomentar conductas positivas en las redes sociales; enseñando a los menores de edad a ser amables y a lidiar con el ciberacoso.

6.2.2.3 Línea de Ayuda de INCIBE Instituto Nacional de Ciberseguridad

El Instituto Nacional de Ciberseguridad (INCIBE) ofrece un servicio esencial conocido como "Tu Ayuda en Ciberseguridad", que se centra en brindar asistencia gratuita y confidencial a los usuarios de internet y tecnología. Este servicio es especialmente relevante en un contexto donde la seguridad en línea se ha convertido en una preocupación primordial para individuos y familias referente al uso seguro de Internet para menores, así como orientación para resolver conflictos relacionados con ciberacoso y redes sociales.

- **¿Por qué es interesante INCIBE?**

Protección integral: proporciona un servicio de asistencia al usuario en el que puedes solucionar cualquier pregunta vinculada a la ciberseguridad, desde cómo resguardar tus claves hasta qué acciones adoptar si te afecta un ciberataque.

- Información actualizada

  Brindan comunicación sobre las amenazas más recientes, herramientas y recomendaciones para resguardarse de ellas.

  Respuestas prácticas: en circunstancia crítica, se procederá a orientar paso a paso para resolver el problema de la forma más eficiente.

  Soluciones prácticas: en una situación comprometida, se buscará una guía para solucionar el problema de la manera más eficaz.

- Confianza y seguridad

  Asistencia gratuita: todos los servicios ofrecidos por INCIBE son sin costo alguno, propone la posibilidad de obtener información y asistencia de alta calidad sin tener que pagar más.

  Confidencialidad: las consultas son tratadas, garantizando la protección de tu privacidad.

  Experiencia: los profesionales de INCIBE cuentan con una amplia experiencia en el campo de la ciberseguridad, asegurando recibir asesoramiento experto.

- Promoción de un entorno digital seguro:

  Concienciación: INCIBE trabaja para sensibilizar a la población sobre los riesgos de la ciberseguridad y la importancia de adoptar medidas preventivas.

  Colaboración: trabajan en estrecha colaboración con otras instituciones y empresas para crear un entorno digital más seguro para todos.

- **Beneficios al usar INCIBE.**

  - Resolución de dudas: referente a cómo proteger tus dispositivos, contraseñas seguras, phishing, etc., ofreciendo respuestas claras y concisas.
  - Soluciones a problemas: en el caso de ser víctima de un ciberataque (como hackeo, virus, suplantación de identidad, lo guiarán en los pasos a seguir para mitigar los daños y recuperar el control.
  - Información sobre ciberseguridad: proporcionan consejos y herramientas para mejorar la seguridad en línea y proteger los datos personales.
  - Confidencialidad: las consultas son tratadas de forma reservada y segura.
  - Gratuidad: en relación con el servicio, éste es completamente gratuito.
  - Atención personalizada: por parte de profesionales en ciberseguridad.

- **Características**

  - Promueve saberes y prácticas adecuadas en ciberseguridad para la efectiva salvaguarda de individuos y empresas.
  - Monitoreo constante de las amenazas informáticas y crea instrumentos para identificarlas de manera oportuna.
  - Proporciona servicios de respuesta a incidentes con el objetivo de asistir a las víctimas en la recuperación de su control sobre sus sistemas.
  - Realiza estudios de las tendencias más recientes en ciberseguridad y crea tecnologías innovadoras para luchar contra las amenazas.

- Coopera con otras entidades tanto nacionales como internacionales para robustecer la ciberseguridad a escala mundial.

6.2.2.4 PicoCTF

Plataforma educativa gratuita sin costo para aprender y desarrollar habilidades, a través de un enfoque gamificado basado en el modelo de "captura la bandera" (Capture the Flag, o CTF), en la que los participantes deben solucionar una serie de retos relacionados con ciberseguridad para conseguir "banderas" (fragmentos de texto que actúan como evidencia de que has completado el reto), que van desde la criptografía y el análisis de redes, hasta la ingeniería inversa y el aprovechamiento de vulnerabilidades.

> "Alejándose de los modelos educativos tradicionales, el picoCTF pone un fuerte énfasis en proporcionar una plataforma abierta a personas de todos los orígenes y niveles de habilidad. A través de iniciativas como picoGym y asociaciones con entidades en todo el mundo, incluidas Japón, Canadá y África, el picoCTF ha democratizado el acceso a oportunidades de aprendizaje en ciberseguridad, permitiendo que un espectro más amplio de participantes se involucre con el campo"[21]

- ¿Por qué picoCTF es interesante? El uso de picoCTF mejora una variedad de habilidades específicas que son concluyentes para el desarrollo en el campo de la ciberseguridad. Las habilidades más relevantes que los participantes pueden desarrollar al utilizar esta herramienta son:
  - **Resolución de problemas:** reta a los usuarios a detectar y solucionar dificultades complejas vinculadas a la ciberseguridad; promoviendo competencias esenciales en la detección de vulnerabilidades y en la elaboración de soluciones eficaces, aspectos cruciales en el entorno laboral.
  - **Pensamiento crítico y analítico:** es tarea de los participantes examinar datos, valorar diversas perspectivas y tomar decisiones basadas en conocimiento. Este tipo de reflexión crítica es esencial para enfrentar circunstancias complicadas en el ámbito de la ciberseguridad y en otras áreas como el Análisis Forense.
  - **Trabajo en equipo y colaboración:** picoCTF fomenta la colaboración entre participantes, permitiendo que trabajen juntos para resolver desafíos y así desarrollar habilidades interpersonales y de trabajo en equipo.

[21] BALAZ, Martin. picoCTF: Revolucionando la Educación en Ciberseguridad a Través de la Inclusividad. julio 2024. Disponible en: https://be3.sk/es/uncategorized-en/picoctf-revolucionando-la-educacion-en-ciberseguridad-a-traves-de-la-inclusividad/3859/

- **Adaptabilidad y aprendizaje continuo:** donde los participantes deben actualizar sus conocimientos constantemente para mantenerse al día con las tendencias de ciberseguridad.
- **Manejo del estrés y toma de decisiones bajo presión:** contribuye al desarrollo de resiliencia y capacidades para tomar decisiones ágiles en situaciones de presión.

- **Beneficios de PicoCTF: contribuyen al desarrollo de las habilidades prácticas de los usuarios, así:**
  - **Aprendizaje práctico:** los participantes desarrollan habilidades técnicas al resolver problemas que simulan situaciones del mundo real en ciberseguridad.
  - **Inclusión y diversidad:** picoCTF ha sido diseñado para atraer a una amplia gama de estudiantes, incluyendo iniciativas específicas para aumentar la participación de mujeres y grupos.
  - **Crecimiento global:** picoCTF ha crecido significativamente, con más de 27,000 participantes globales en sus competencias.

- **Características de picoCTF: ofrece una serie de características diseñadas para hacer que el aprendizaje sea divertido y desafiante.**
  - **Problemas diversos:** picoCTF presenta un extenso abanico de retos que abarcan distintos campos de la ciberseguridad, desde la criptografía y el análisis de redes hasta la ingeniería inversa y el uso de vulnerabilidades.
  - **Complejidad progresiva:** los retos se estructuran en niveles de complejidad. Comienza con lo más elemental y progresa progresivamente hacia los más sofisticados. Esto es perfecto para los novatos en el ámbito de la ciberseguridad.
  - **Formato de captura de bandera (CTF):** la plataforma se distingue por utilizar el formato CTF, en el que los participantes deben solucionar retos para conseguir "banderas" (fragmentos de texto) que actúan como evidencia de que han completado el reto.
  - **Aprendizaje práctico:** esta plataforma educativa facilita la implementación práctica de los conocimientos. Los retos te exigen razonar de manera crítica y solucionar problemas.
  - **Actualizaciones constantes:** Los desafíos y recursos de picoCTF se actualizan regularmente, lo que garantiza que siempre tengas nuevos retos y oportunidades de aprendizaje.

6.2.2.5 La Oca del Phishing

El juego de mesa conocido como La Oca Antifraudes es una herramienta educativa diseñada para enseñar a los jugadores, especialmente a los estudiantes, sobre los diferentes tipos de fraudes en línea, tales como el phishing, smishing y vishing. Este enfoque lúdico tiene como objetivo no solo entretener, sino también informar y capacitar a los jugadores para que reconozcan y eviten situaciones de riesgo en el mundo digital.

A continuación, se presentan sus características y beneficios:

- **¿Por qué la Oca del Phishing es interesante? Por varias razones que la han convertido en una herramienta educativa, efectiva y atractiva, tales como:**
    - **Aprendizaje divertido:** el método de juego de mesa hace que la enseñanza de la ciberseguridad sea divertida y fácil de comprender. Los participantes pueden gozar al mismo tiempo que aprenden, lo que simplifica la memorización de información y promueve un enfoque positivo hacia la educación en seguridad digital.
    - **Conciencia sobre fraudes:** el juego está concebido para instruir a los interesados en diferentes formas de estafas en línea, como el phishing, el smishing y el vishing. Al lidiar con circunstancias simuladas, los jugadores potencian sus capacidades para reconocer y prevenir potenciales peligros en su cotidianidad.
    - **Fomento de competencias esenciales:** durante el juego, quienes participan tienen que responder a preguntas y tomar decisiones basadas en información, lo que fomenta el razonamiento crítico y la habilidad para valorar riesgos. Estas competencias son fundamentales no solo en el ámbito de la ciberseguridad, sino en numerosos aspectos de la vida diaria.
    - **Interacción social:** el juego de la Oca Antifraudes se realiza en grupo, promoviendo así la interacción social y el trabajo colaborativo. Esto posibilita que los jugadores debatan tácticas y compartan saberes, potenciando de esta manera la experiencia educativa.
    - **Accesibilidad:** este pasatiempo no tiene costo se puede descargar de manera gratuita, lo que lo hace asequible para un extenso público y fomenta la educación en ciberseguridad a gran escala.
    - **Refuerzo de conceptos fundamentales:** mediante cuestionamientos sobre ciberseguridad, los jugadores fortalecen conceptos relevantes vinculados a la salvaguarda de datos y la seguridad en internet; contribuyendo a formar una base firme de saberes que pueden ser utilizados en contextos reales.
    - **Fomento de un uso seguro de Internet:** la Oca Antifraudes, al instruir a los jugadores en la identificación y protección de fraudes, ayuda a establecer una cultura de seguridad digital más robusta entre los participantes.

- **Beneficios de jugar a la oca del phishing.**
    - **Sensibilizar sobre fraudes:** los jugadores aprenden a reconocer diferentes tipos de fraudes en línea, lo que les ayuda a protegerse mejor en su vida cotidiana.
    - **Aprendizaje divertido:** utilizando un formato de juego, se hace más atractivo y accesible el aprendizaje sobre ciberseguridad, especialmente para jóvenes y familias.
    - **Desarrollo de habilidades críticas:** los participantes desarrollan habilidades críticas para evaluar situaciones potencialmente peligrosas en el entorno digital.
    - **Interacción social:** al ser un juego de mesa, fomenta la interacción social entre amigos y familiares, lo que puede hacer que el aprendizaje sea más efectivo y memorable.
    - **Recursos gratuitos:** está disponible para descarga gratuita en plataformas como INCIBE, lo que permite a cualquier persona acceder a él sin costo alguno.

- **Características principales de la oca antifraudes**
    - **Formato de juego de mesa:** se basa en el clásico juego de la oca, donde los jugadores avanzan por un tablero al responder preguntas y enfrentar desafíos relacionados con la ciberseguridad.
    - **Enfoque educativo:** enseñar a los jugadores a reconocer diferentes tipos de fraudes, como phishing, smishing y vishing, mediante preguntas que ponen a prueba sus conocimientos.
    - **Interacción social:** promueve la participación grupal, lo que posibilita que amigos y familiares se diviertan en equipo, incentivando el aprendizaje en equipo y el debate sobre asuntos de seguridad digital.
    - **Preguntas y respuestas:** contiene un conjunto de interrogantes que tratan aspectos fundamentales de cómo detectar correos electrónicos fraudulentos, mensajes falsos y llamadas no deseadas.
    - **Accesibilidad:** se puede descargar sin costo, lo que facilita que cualquier individuo, incluyendo instituciones educativas y familias, pueda tener acceso al juego sin ningún gasto.
    - **Fortalezas críticas:** los jugadores potencian sus habilidades para valorar situaciones que podrían ser peligrosas en el ambiente digital, potenciando su habilidad para tomar decisiones basadas en información.

- **Conciencia sobre seguridad digital:** ayuda a establecer una cultura más robusta de seguridad digital entre los involucrados.
- **Diversión y aprendizaje:** fusiona el ocio con la enseñanza, convirtiendo el aprendizaje en ciberseguridad en algo cautivador y recordable.
- **Desarrollo de habilidades críticas:** los jugadores desarrollan habilidades para evaluar situaciones potencialmente peligrosas en el entorno digital, mejorando su capacidad para tomar decisiones informadas.

6.2.3 Herramientas de ciberseguridad usadas en equipos y redes institucionales

La ciberseguridad conocida también como seguridad de datos o protección digital incluye todas las áreas de la defensa de una entidad, sus trabajadores y sus bienes frente a los peligros cibernéticos.

> "La ciberseguridad se refiere a cualquier tecnología, práctica y política para prevenir los ataques cibernéticos o mitigar su impacto. La ciberseguridad tiene como objetivo proteger los sistemas informáticos, las aplicaciones, los dispositivos, los datos, los activos financieros y las personas contra el ransomware y otros programas maliciosos, las estafas de phishing, el robo de datos y otras amenazas cibernética".[22]

Los tres pilares de la ciberseguridad, a menudo representados por el acrónimo "CIA", a continuación, se explican.

Confidencialidad: mantener la privacidad de la información, asegurando que sólo los usuarios autorizados puedan acceder a archivos y cuentas.

Integridad: la comunicación sólo deben cambiarla las personas o los procesos adecuados.

Disponibilidad: la información debe ser visible y accesible siempre que sea necesario.

Dentro de la ciberseguridad es clave el empleo de las diferentes tecnologías informáticas para garantizar protección de datos y sistemas en un entorno digital cada vez más complejo y amenazante.

Las tecnologías de la información (TI), optimizan y simplifican los procesos en varios sectores, que se relacionan en el campo educativo, empresarial, gubernamental, de la salud, entre otros. Estas herramientas son relevantes ya que posibilitan el manejo eficaz de la información y pueden incrementar la eficiencia y productividad en diversos sectores, favoreciendo así el crecimiento y el éxito constante de la mayoría de las entidades.

[22] Gregg Lindemulder, Matt Kosinsk. Que es la ciberseguridad. Gregg Lindemulder, Matt Kosinsk. IBM. Disponible en: https://www.ibm.com/mx-es/topics/cybersecurity

> "La TI abarca esencialmente todos los aspectos relativos a la informática dentro de la empresa, lo que incluye el estudio, la conceptualización, el desarrollo, la ejecución y el soporte de los sistemas de información. La TI también puede referirse a los sistemas en sí, específicamente a las aplicaciones de software y al hardware físico en el que se ejecutan. Por último, la TI incluye la gobernanza de TI, que garantiza que las tecnologías de la información se utilicen correctamente para ayudar a la organización a alcanzar sus objetivos y, al mismo tiempo, gestionar los riesgos"[23]

Hay varios tipos de Tecnologías de Información (TI), que comprenden:

Hardware: elementos físicos de un sistema de computación, tales como ordenadores, portátiles, teléfonos inteligentes, servidores, entre otros.

Software: programas y sistemas operativos empleados en los dispositivos de computación.

Redes: encargados de conexión entre aparatos informáticos que facilitan la transferencia de datos.

Seguridad informática: técnicas utilizadas para proteger los sistemas informáticos y la información almacenada.

Cloud computing: entrega de servicios informáticos a través de internet, lo que permite el acceso remoto y la escalabilidad de recursos.

Base de datos: sistema que admite almacenar, administrar y recuperar información estructurada.

Inteligencia artificial: desarrollo de sistemas y algoritmos que permiten a las máquinas aprender y mejorar en su desempeño.

Los equipos tecnológicos empleados en ciberseguridad son esenciales por diversas razones que aseguran la integridad de los datos en un ambiente digital cada vez más complicado y peligroso. La selección adecuada y la implementación efectiva de estas herramientas son fundamentales para establecer una defensa sólida contra una amplia gama de amenazas cibernéticas, incluidos el malware, el phishing, el ransomware y los ataques de denegación de servicio (DDoS), entre otros.

Protección de información sensible: los cortafuegos, antivirus y sistemas de detección de intrusiones son fundamentales para proteger datos sensibles, tales como personales y financieros, previniendo accesos indebidos y hurtos de información.

Prevención de ciberataques: herramientas como escáneres de vulnerabilidades y plataformas de protección de puntos finales; consiguen identificar y mitigar amenazas emergentes antes de que puedan producir daño. La ciberseguridad posibilita que las

[23] SERVICENOW ¿Qué es la Tecnología de la Información Ti? Disponible en: https://www.servicenow.com/es/products/itsm/what-is-information-technology.html

entidades se protejan de ataques avanzados como el ransomware y el phishing, salvaguardando de esta manera su funcionamiento y previniendo futuras pérdidas.

Algunas de las herramientas más relevantes que pueden utilizar las instituciones y usuarios en sus equipos y redes, para una navegación segura en la red internet y prevenir riesgos de posibles ataques cibernéticos.

6.2.3.1 Herramientas de Filtrado Web

El filtrado web es esencial para controlar el acceso a contenido en Internet, mejorar la seguridad y aumentar la productividad en diversas entidades y algunas de las herramientas más populares y efectivas para el filtrado web. Estas herramientas proporcionan una sólida defensa para los usuarios individuales y corporativos contra una amplia gama de amenazas en línea. En la siguiente tabla se analiza en detalle el valor y la importancia de la filtración web.

> "Los filtros web también se utilizan a menudo como herramienta para la prevención de malware, ya que bloquean el acceso a los sitios que comúnmente alojan este tipo de software, como los relacionados con pornografía o juegos de azar. Los filtros más avanzados pueden incluso bloquear la información que se envía por Internet para evitar que se divulguen datos confidenciales"[24]

[24] KASPERSKY. ¿Qué es un filtro web? 2025. Disponible en: https://latam.kaspersky.com/resource-center/definitions/web-filter?

Tabla 9. Herramientas de Filtrado Web

No	HERRAMIENTAS	DESCRIPCIÓN	CARACTERÍSTICAS
1	CISCO UMBRELLA	Solución en la nube que proporciona defensa frente a amenazas y filtrado de contenido.	Monitoreo de tráfico, defensa frente a malware y regulación del acceso a páginas web no autorizadas. Significa la implementación de algoritmos avanzados para anticipar las amenazas antes de que afecten a la red.
2	DNSFILTER	Servicio en la nube que simplifica la filtración de contenido web mediante una interfaz fácil de usar, con opciones analíticas avanzadas.	Proporciona planes elementales y avanzados con capacidades analíticas sofisticadas. Una base de datos que se actualiza constantemente. Emplea el reconocimiento en tiempo real de amenazas, phishing, malware y virus, junto con el uso de herramientas de Inteligencia Artificial.
3	FLASHSTART	Solución de filtrado basada en la nube que no requiere hardware adicional.	Facilita geobloqueo, restricciones programadas. Cuenta con una extensa lista negra, con bloqueos temporales, es decir, definidos en instantes concretos. Permite el uso de las redes sociales en un tiempo distinto al horario de trabajo.
4	UNTANGLE NG FIREWALL COMPLETE	Instrumento completo que fusiona filtrado web con otras características de seguridad.	Monitoreo de aplicaciones, adaptación de normativas y una extensa base de datos de direcciones IP de alto peligro.
5	FILTRADO COMPLETO DEL CONTENIDO DE INTERNET CON FAMISAFE	Aplicación de control parental innovadora y altamente capacitada que facilita la filtración del contenido que sus hijos ven en el dispositivo, conscientes de que sus padres supervisan su actividad en línea.	Comprobar el registro de viaje de sus hijos, incluso de forma privada u oculta. Detecta o impide contenido de riesgo en línea, tales como páginas de juegos de azar, juegos de apuestas o aplicaciones de pornografía, en los smartphones de los niños. Vigila digitalmente a los niños a través de coordenadas GPS y confirma su localización en tiempo real. Ubicado para plataformas móviles de iOS y Android. Define un límite de tiempo frente a la pantalla para que los niños duerman a una hora adecuada, programando el tiempo que permanece frente a la pantalla.
6	FUNAMO INTERNET FILTER	Herramienta que incrementa sus habilidades para llevar a cabo diversas funciones de control parental, como gestionar el tiempo de pantalla, limitar el uso de algunas aplicaciones y establecer filtros de	Controla todas las operaciones que se llevan a cabo en el teléfono móvil. Reconoce y documenta el registro de mensajes de texto, llamadas, aplicaciones empleadas y páginas web previamente visitadas. El filtro de Internet opera en la nube y tiene la capacidad de hacer ajustes en línea que se sincronizarán de manera automática con las configuraciones del móvil de su hijo. .

Tabla 10. Herramientas de Filtrado Web (Continuación)

No	HERRAMIENTAS	DESCRIPCIÓN	CARACTERÍSTICAS
		Búsqueda segura y adecuada para la edad.	Está accesible para dispositivos Android de manera gratuita
7	PUMPIC FILTRO DE INTERNET TELÉFONOS INTELIGENTES.	Se utiliza para filtrar la información en línea para dispositivos móviles smartphones y tabletas. Limita cualquier tipo de acceso a cualquier página web que incluya contenido de carácter explícito o inadecuado	Es posible bloquear efectivamente sitios web de acuerdo con los ajustes de edad previamente establecidos. Incorpora diversas tácticas para filtrar. Comprenden listas blancas, listas negras y bloqueo de términos obscenos en las páginas web. Efectúa la supervisión parental sobre los menores. Define geo-cercas, confirma la localización, maneja el dispositivo inteligente del niño de manera remota e incluso supervisa todos los registros de mensajes de texto y llamadas. No posee un precio, es lícito, funciona de manera visible y es compatible con la plataforma Android.
8	MMGUARDIÁN CONTENT FILTER	Es una aplicación de filtrado que tiene la capacidad de bloquear o limitar ciertos sitios web en el dispositivo móvil de su hijo, monitoreando sus acciones en línea.	Ejecuta la filtración de contenido activo mientras su hijo navega en línea, resguardándolo de ciberacosadores y contenido dirigido a adultos. Identifica mensajes de texto, llamadas y todas las operaciones del teléfono móvil. No es posible desinstalar sin su consentimiento mediante una contraseña maestra previamente establecida por el agente. Es sin costo y adecuado para todos los smartphones Android.

Fuente: FLASHSTART. Software de Filtrado Web Empresarial: los mejores filtros web para empresas. [Consultado: 20 de enero de 2024]. Disponible en: https://flashstart.com/es/software-de-filtrado-web-empresarial-los-mejores-filtros-web-para-empresas/

6.2.3.2 Herramienta de Seguridad SIEM

SIEM, Gestión de Eventos e Información de Seguridad: en sistemas de vigilancia y control previene e identifica incidentes de seguridad que afectan la disponibilidad, integridad y privacidad de la información.

¿Cómo funcionan las herramientas SIEM?

Las herramientas SIEM recopilan, agregan y analizan volúmenes de datos de las aplicaciones, dispositivos, servidores y usuarios de una organización en tiempo real para que los equipos de seguridad puedan detectar y bloquear ataques. Utilizan reglas predeterminadas para ayudar a los equipos de seguridad a definir amenazas y generar alertas; permitiendo una actuación inmediata para evitar sus consecuencias o minimizar sus daños.

Las herramientas SIEM recolectan, añaden y examinan cantidades de información de aplicaciones, dispositivos, servidores y usuarios de una entidad en tiempo real, para que los equipos de seguridad identifiquen y bloqueen ataques, emplean reglas preestablecidas para asistir a los equipos de seguridad en la identificación de amenazas y la generación de alertas, logrando intervención inmediata y así mitigar los daños efectos.

Ventajas de utilizar SIEM

Las herramientas SIEM proporcionan numerosos beneficios que pueden reforzar la posición de seguridad general en una entidad. Entre ellas se incluyen las siguientes:

- Una perspectiva centralizada sobre los riesgos potenciales.
- Detecta y reacciona en tiempo real.
- Inteligencia avanzada en materia de amenazas.
- Creación de informes y auditoría del cumplimiento normativo.
- Elaboración de informes y auditoría sobre el cumplimiento de las normas.
- Mejora de la transparencia al monitorear usuarios, aplicaciones y equipos.

Para ofrecer este entorno de detección y respuesta ante amenazas, un SIEM pasará por este proceso:

Recopilación de datos: una plataforma SIEM recogerá registros, otros datos de sistemas y soluciones de seguridad a lo largo de la red de la organización y los agrupará en un único lugar central.

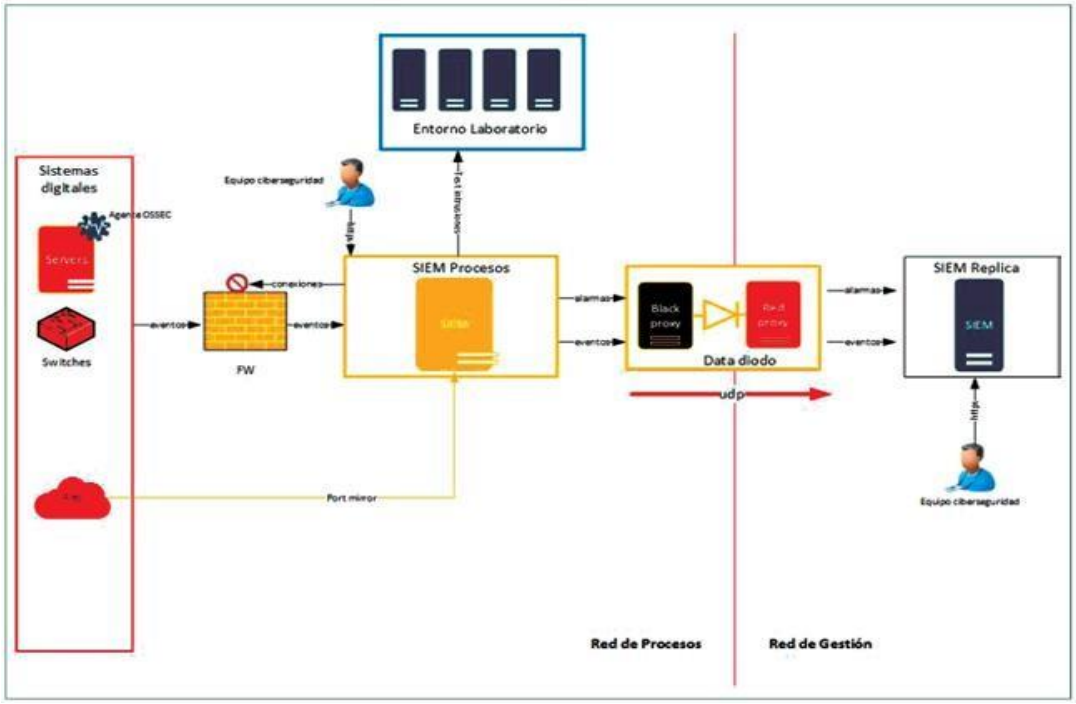
Agregación y normalización de datos: la información recolectada por un SIEM puede provenir de diversos sistemas, presentarse en diversidad de formatos y así llevar a cabo las comparaciones y análisis correspondientes.

Implementación de políticas y análisis de datos: al tener un conjunto de datos único y consistente, la solución SIEM puede iniciar la búsqueda de señales de riesgos de

ciberseguridad en la información. Incluyendo la identificación de problemas preestablecidos, mencionados en las políticas, como otras posibles señales de ataque identificadas a través de patrones ya establecidos.

Elaboración de alertas: cuando una solución SIEM identifica un peligro de ciberseguridad, alerta al equipo de seguridad de la organización. Se puede alcanzar este objetivo mediante la creación de una alerta SIEM y utilizar las integraciones con sistemas de emisión de boletines, reportes de errores o aplicaciones de mensajería.

Figura 13. Estructura del Sistema SIEM



Fuente: HIDALGO C., Roberto. Buenas prácticas en la implantación de siem en infraestructuras críticas. [Consultado: 10 de enero de 2024]. Disponible en: https://www.revistanuclear.es/wp-content/uploads/hemeroteca/384/NE384-06.pdf

¿Qué beneficios ofrece el uso de herramientas SIEM de código abierto?

Las herramientas SIEM de código abierto proporcionan rentabilidad, claridad y habilidad para personalizarse. Facilitan a las entidades la modificación del código fuente para ajustarlo a requerimientos particulares y son compatibles con otras herramientas de seguridad para potenciar la seguridad general.

¿Qué distingue a las herramientas SIEM de código abierto de las que poseen licencia?

Las herramientas SIEM de código abierto generalmente son gratuitas y facilitan la personalización, mientras que las herramientas licenciadas suelen proporcionar un soporte completo, funciones sofisticadas e interfaces de uso sencillo. Las soluciones de licencia también ofrecen una implementación más ágil, aunque a un costo superior en comparación con las de código abierto.

¿Cuáles son las características que debo dar prioridad en la herramienta SIEM de software libre?

Las funciones como la correlación de eventos, este monitoreo se da en tiempo real, las habilidades de alerta, los reportes de cumplimiento y las alternativas de integración con herramientas de seguridad ya existentes son valoradas. Se resalta la sencillez de manejo y la habilidad para gestionar grandes cantidades de datos de forma eficiente.

Herramientas SIEM de código abierto en 2025

- **SIEM de Cisco System:** la solución SIEM de Cisco unifica los datos de registro y eventos de múltiples dispositivos de red, lo que posibilita a las entidades detectar posibles amenazas y responder de forma eficiente. Su funcionamiento se basa en capturar e interpretar eventos en toda la red, organizando los datos para estudio y respuestas.

Si ocurre un incidente de seguridad, el sistema añade información pertinente para determinar la severidad de la amenaza y promover respuestas oportunas.

Características:

- **Agregación de datos centralizada:** herramienta que recolecta registros e información de sucesos de diferentes fuentes, tales como aplicaciones, bases de datos, servidores y cortafuegos.
- **Detección de amenazas en tiempo real:** emplea normas establecidas y aprendizaje automático para filtrar y dar prioridad a las alertas, enfocándose en problemas de seguridad de gran relevancia.
- **Reacciones automatizadas:** Cisco se acopla a las tecnologías de orquestación, automatización y respuesta de seguridad (SOAR) para realizar respuestas automáticas a incidentes de acuerdo con políticas establecidas.
- **Mejora de la visibilidad:** la solución ofrece datos acerca de sucesos de seguridad al vincular datos con fuentes de inteligencia sobre amenazas, lo que potencia la habilidad para monitorear y reaccionar ante estas amenazas.

- **SIEM de ritmo logarítmico:** LogRhythm SIEM solución de seguridad creada para potenciar la identificación de amenazas y las habilidades de reacción dentro de las entidades. Incorpora diversas funciones de seguridad, como gestión de registros, análisis de seguridad y seguimiento de puntos finales en una plataforma unificada, lo que simplifica que los equipos de seguridad gestionen y reaccionen a las amenazas de forma eficaz.

Características:

- **Monitoreo constante:** LogRhythm utiliza analítica Automatizada de Máquinas para ofrecer información en tiempo real acerca de sucesos de seguridad y proporciona a los equipos priorizar a las amenazas basándose en sus niveles de riesgo.
- **Administración del ciclo de vida de las amenazas:** esta función facilita la administración de amenazas de nivel extremo a nivel extremo, posibilitando a las entidades identificar, reaccionar y recuperarse de las amenazas en una sola plataforma.
- **Gestión de registros de alto rendimiento:** la plataforma puede procesar terabytes de datos de registros diariamente, ofrece acceso inmediato para investigaciones y admite búsquedas estructuradas y no estructuradas.
- **Monitoreo en redes y puntos de finalización:** LogRhythm ofrece datos detallados referente a las acciones en la red y los puntos finales mediante sensores forenses incorporados.

- **IBM QRadar SIEM:** IBM QRadar SIEM incorpora y examina la información de seguridad de toda la infraestructura tecnológica de una entidad. Recopila archivos y datos de varias fuentes, analiza estos datos y aplica las normas de correlación para identificar potenciales riesgos de seguridad y así se habilitan los equipos de protección para darle prioridad a las alertas según el grado de las amenazas.

Características:

- **Visibilidad centralizada:** la plataforma brinda una visión conjunta de los sucesos de seguridad tanto en contextos locales como en la nube, adecuando a los equipos de seguridad la supervisión de acciones desde un solo panel.
- **Capacidades de integración extensas:** QRadar, con más de 700 integraciones prediseñadas, tiene la capacidad de conectarse sin dificultades con herramientas de seguridad y fuentes de datos ya existentes.
- **Identificación sofisticada de amenazas:** tanto la inteligencia artificial como el aprendizaje automático potencian la priorización de alertas y la correlación de sucesos.

- Verifique la fiabilidad de IBMQRadar SIEM y sus propuestas revisando las valoraciones en Gartner Peer Insights.

- **Administrador de seguridad empresarial de Trellix:** es una solución de código abierto SIEM destinada a identificar, reaccionar y administrar amenazas de seguridad; incorporando múltiples tareas de seguridad en una plataforma unificada; ofrece una visión completa de los sistemas, redes, aplicaciones y ambientes de nube.

Características:

- **Vigilancia de amenazas:** trellix fusiona información de amenazas externas y de reputación con la actividad interna del sistema, proporcionando una perspectiva integral del escenario de seguridad.
- **Monitoreo y análisis:** la plataforma facilita la vigilancia constante de las acciones, lo que posibilita a los equipos de seguridad darle prioridad, indagar y reaccionar de manera rápida a posibles amenazas.
- **Manejo automatizado del cumplimiento:** se alinea con múltiples normativas y marcos internacionales como GDPR, HIPAA y otros, al automatizar las labores de cumplimiento, disminuyendo así el trabajo manual necesario para las auditorías.

- **Rapid7 InsightIDR:** es una solución SIEM de nube propia que combina habilidades de detección y reacción ante incidentes con análisis sofisticados para detectar posibles amenazas.

Características:

- **Evaluación de la conducta del usuario (UBA):** InsightIDR utiliza UBA para definir pautas para el comportamiento habitual del usuario, facilitando la identificación de irregularidades como cuentas en riesgo o desplazamiento lateral en la red.
- **Tecnología de engaño:** engloba herramientas de engaño, como honeypots y honey users, creadas para captar la atención de los atacantes y revelar sus estrategias al inicio de la cadena de ataques.
- **Respuesta de seguridad automatizada:** la solución proporciona procesos de trabajo automatizados para la reducción de incidentes, facilitando a los equipos de seguridad la adopción de medidas inmediatas, como la cuarentena de los puntos finales infectados o la suspensión de las cuentas de usuario afectadas.
- Investiga los comentarios y las evaluaciones para adquirir más detalles sobre las habilidades de Rapid7 InsightIDR.

- **Microsoft Sentinel:** es una solución SIEM de código abierto creada para ofrecer análisis de seguridad e identificación de amenazas en todo el escenario digital de una organización. Previamente denominada Azure Sentinel, emplea inteligencia artificial y automatización para optimizar las operaciones de seguridad, proporcionando a las entidades la administración y reacción ante las amenazas de ciberseguridad.

Características:

- **Detección activa de amenazas:** la plataforma ofrece instrumentos para la identificación proactiva de amenazas, facilitando a los analistas de seguridad la búsqueda de señales de compromiso en sus fuentes de información antes de que se implementen las alertas.
- **Incorporación de inteligencia sobre amenazas:** fusiona las fuentes de inteligencia con relación a las amenazas de Microsoft y simultáneamente brinda a los usuarios la posibilidad de incluir sus propios recursos de inteligencia sobre amenazas.
- **Conectores de información:** Microsoft Sentinel proporciona una extensa variedad de conectores de datos integrados que simplifican la unificación de información de seguridad de diferentes fuentes, al igual que productos de Microsoft, servicios de terceros y ambientes de nube.

- **Google Chronicle SIEM:** proporciona a las entidades habilidades avanzadas para la identificación, estudio y reacción frente a amenazas. Aplica la robusta infraestructura de Google para examinar grandes volúmenes de datos de telemetría de seguridad, suministrando a los equipos de seguridad incrementar su eficacia operacional para luchar contra las amenazas informáticas.

Características:

- **Motor de detección:** automatiza la búsqueda de problemas de seguridad en la información proporcionada. Los usuarios tienen la posibilidad de configurar normas para poner en marcha alertas cuando se detectan posibles amenazas, lo que acelera el proceso de reacción ante incidentes.
- **Análisis avanzado:** el instrumento examina en tiempo real los datos de seguridad a través del aprendizaje automático. Esta habilidad posibilita a las organizaciones identificar con rapidez indicadores de riesgo (IoC) y reaccionar ante posibles amenazas antes de que se intensifiquen.
- **Manejo y normalización de información:** Google Chronicle tiene la capacidad de ingerir una extensa gama de tipos de telemetría de seguridad mediante diversos procedimientos, que incluyen reenvíos livianos y API de gestión.

- **McAfee ESM:** McAfee Enterprise Security Manager (ESM) es un software SIEM de código abierto que asiste en la identificación, investigación y reacción ante amenazas de seguridad. Incorpora análisis sofisticados, correlación de sucesos en tiempo real y extensas habilidades de integración para ofrecer datos valiosos para las operaciones de seguridad.

Características:

- **Manejo y evaluación de registros:** la solución comprende McAfee Enterprise Log Manager, automatiza la recolección y evaluación de registros de cualquier tipo.
- **Inteligencia acerca de amenazas a nivel mundial:** McAfee ESM se fusiona con la Inteligencia de Amenazas Globales de McAfee (GTI), potenciando su habilidad para identificar amenazas y vulnerabilidades importantes.
- **Motor de correlación avanzado:** emplea un potente motor de correlación que examina sucesos de seguridad en lapso real. Esta característica facilita el rápido reconocimiento de posibles amenazas al vincular información de diversas fuentes, y posibilita a los equipos de seguridad proporcionar prioridad a los incidentes.

- **Splunk:** Enterprise Security (ES), es una solución creada para asistir a las organizaciones en la identificación, investigación y reacción ante amenazas de seguridad en tiempo real. Ofrece una visibilidad completa de los sucesos de seguridad en diversos contextos.

Características:

- **Paneles íntegros:** Splunk ES ofrece paneles a medida que brindan datos acerca de indicadores de seguridad, patrones de incidentes y desempeño del sistema.
- **Detección avanzada de amenazas:** el programa emplea aprendizaje automático y análisis del comportamiento del usuario (UBA) para identificar irregularidades y posibles amenazas, estableciendo así los fundamentos para el comportamiento habitual.

- **Análisis de datos en tiempo real:** posibilita la supervisión y el estudio constante de datos de seguridad provenientes de una variedad de fuentes, capacita a los equipos de seguridad para detectar y reaccionar ante las amenazas a medida que suceden.

Características importantes en una plataforma SIEM basada en la nube incluyen:

- **Análisis de seguridad histórico y en tiempo real:** para llevar a cabo este proceso, un motor de detección debe examinar directamente en el instante de la

ingesta y no posteriormente mediante una indexación alta. Las normas de detección y análisis se implementan de manera constante en los datos en tiempo real, facilitando así la detección instantánea de amenazas e irregularidades. Para el estudio histórico, el motor de detección necesita analizar eficazmente los datos anteriores para identificar amenazas incorporadas. Los trabajos programados tienen la capacidad de procesar y examinar automáticamente la información antigua a intervalos regulares para una revisión sistemática de los registros y eventos históricos.

- **Ingesta y retención de registros rentables:** la implementación de métodos de automatización para la ingesta optimiza la administración y la visualización de los registros. La conservación de registros debe estar separada de la indexación, para alcanzar una rentabilidad superior.

- **Lenguaje de consulta avanzado:** lenguaje de consulta sencillo e intuitivo asiste en la recuperación, filtrado y análisis de datos de registros y sucesos; posibilitando efectuar búsquedas de datos concretos y simplifica la detección de patrones o irregularidades.

- **SOAR:** grupo de recursos y servicios creados para potenciar la posición de seguridad en una entidad a través de la automatización y coordinación de las respuestas ante amenazas cibernéticas; uniendo instrumentos y sistemas de seguridad, tanto internos como externos, con el objetivo de consolidar procedimientos.

  La automatización se emplea para labores repetitivas y que demandan gran cantidad de tiempo, así como para la implementación manual de estrategias que solucionan incidentes concretos, con respuestas que posibilitan llevar a cabo unas acciones más rápidas y exactas para los incidentes de seguridad.

- **UEBA:** solución de ciberseguridad que utiliza aprendizaje automático, análisis estadístico, de comportamiento para detectar actividades inusuales y potencialmente dañinas dentro de la red de una organización. Incorpora líneas de base de comportamiento, detección de anomalías y aprendizaje automático; se integra con otras herramientas de seguridad y se centra en la detección de amenazas internas.

- **Paneles de control:** la plataforma necesita contar con interfaces visuales que incorporen, representen y organicen datos y métricas de seguridad, entregando a los equipos de seguridad supervisar, examinar y reaccionar con rapidez a los sucesos y tendencias de seguridad en todo su ambiente.

6.2.3.3 Firewall

Es una herramienta de protección de red que supervisa el tráfico de red entrante y saliente, determinando si autoriza o impide cierto tráfico de acuerdo a un conjunto de normas de seguridad establecidas.

Entre los diferentes tipos de firewalls encontramos:

- **Cortafuegos proxy:** un cortafuegos proxy actúa como un enlace entre una red con otra para una determinada aplicación, los servidores proxy pueden ofrecer funciones extra, como el almacenamiento en caché de contenido y la seguridad, al prevenir conexiones directas desde el exterior de la red, no obstante, esto puede impactar en las capacidades de rendimiento y las aplicaciones que pueden acoger.

- **Cortafuegos con inspección de estado:** actualmente, un cortafuegos de revisión de estado, también conocido como un firewall "tradicional", permite o bloquea el tráfico basándose en el estado, el puerto y el protocolo, donde se vigila toda la actividad desde el inicio de una conexión hasta su finalización. Las decisiones de filtrado se apoyan en las normas establecidas por el administrador, en el contexto al que hace referencia al empleo de datos de conexiones previas y paquetes que forman parte de la misma conexión.

- **Firewall de gestión unificada de amenazas (UTM):** un aparato UTM generalmente fusiona, de manera adaptable, las capacidades de un cortafuegos de control de estado con las de prevención de intrusiones y antivirus, puede incorporar servicios extras y frecuentemente administración en la nube, los UTM se enfocan en la sencillez y facilidad de manejo.

- **Cortafuegos de próxima generación (NGFW):** los cortafuegos han progresado más allá de la propia filtración de paquetes y la revisión de estado. La mayoría de las empresas están poniendo en marcha firewall de vanguardia para neutralizar amenazas contemporáneas, como malware sofisticado y ataques a la capa de aplicación.

De acuerdo con Gartner, Inc., un cortafuegos de futura generación debe contar con:

- Gestión de acceso fundamentada en inteligencia con revisión del estado.
- Sistema integrado para prevenir intrusiones (IPS).
- Detección y bloqueo de aplicaciones peligrosas.
- Rutas de actualización para incluir fuentes de información futuras.
- Técnicas para abordar las amenazas de seguridad en evolución.
- Métodos para enfrentar las amenazas de seguridad que son de constante cambio.

- Filtrado de URL en función de la geolocalización y la reputación.

- **NGFW centrado en amenazas:** estos cortafuegos incorporan todas las funcionalidades de un NGFW convencional, proveen detección y solución de amenazas sofisticadas, mediante un NGFW centrado en amenazas y así:

  - Determina qué activos tienen un mayor riesgo con un entendimiento total del contexto.
  - Responde con rapidez a los ataques a través de una automatización de seguridad inteligente que define políticas y mejora sus defensas de manera ágil.
  - Detecta con mayor precisión la actividad evasiva o sospechosa vinculada a los incidentes de la red y puntos finales.
  - Disminuye significativamente el ciclo desde la detección hasta la limpieza retrospectiva de seguridad que monitorea de manera constante la actividad y comportamiento sospechosos incluso tras la inspección inicial.
  - Facilita la gestión y disminuye la complejidad mediante políticas conjuntas que resguarden durante todo el proceso de ataque.

- **Cortafuegos virtual:** se suele poner en marcha un firewall virtual en una nube privada (VMware ESXi, Microsoft Hyper-V, KVM) o pública (Amazon Web Services o AWS, Microsoft Azure, Google Cloud Platform o GCP, Oracle Cloud Infrastructure o OCI) con el objetivo de monitorear y salvaguardar el tráfico en redes físicas y virtuales. Un cortafuegos virtual es un elemento esencial en las redes de software definidas (SDN).

- **Firewall nativo de la nube:** los cortafuegos originarios de la nube están actualizando el método para salvaguardar las aplicaciones y la infraestructura de gran volumen de trabajo y ofrecen que las operaciones de red y los equipos maniobren a velocidades rápidas.

Beneficios de los cortafuegos locales de la nube:

- Seguridad flexible y eficaz
- Capacidad para múltiples inquilinos
- Equilibrio de carga inteligente

Diferencia entre Firewall y Antivirus

El cortafuegos y el antivirus son dos elementos de seguridad informática distintos, aunque vinculados, que se encargan de resguardar los sistemas y redes informáticas de distintas amenazas.

Este sistema de seguridad es un mecanismo de protección tecnológica encargado de prevenir la entrada de conexiones no autorizadas a nuestra red. En cambio, el antivirus es un software diseñado para identificar y erradicar los virus que podrían interferir con el funcionamiento de nuestros aparatos.

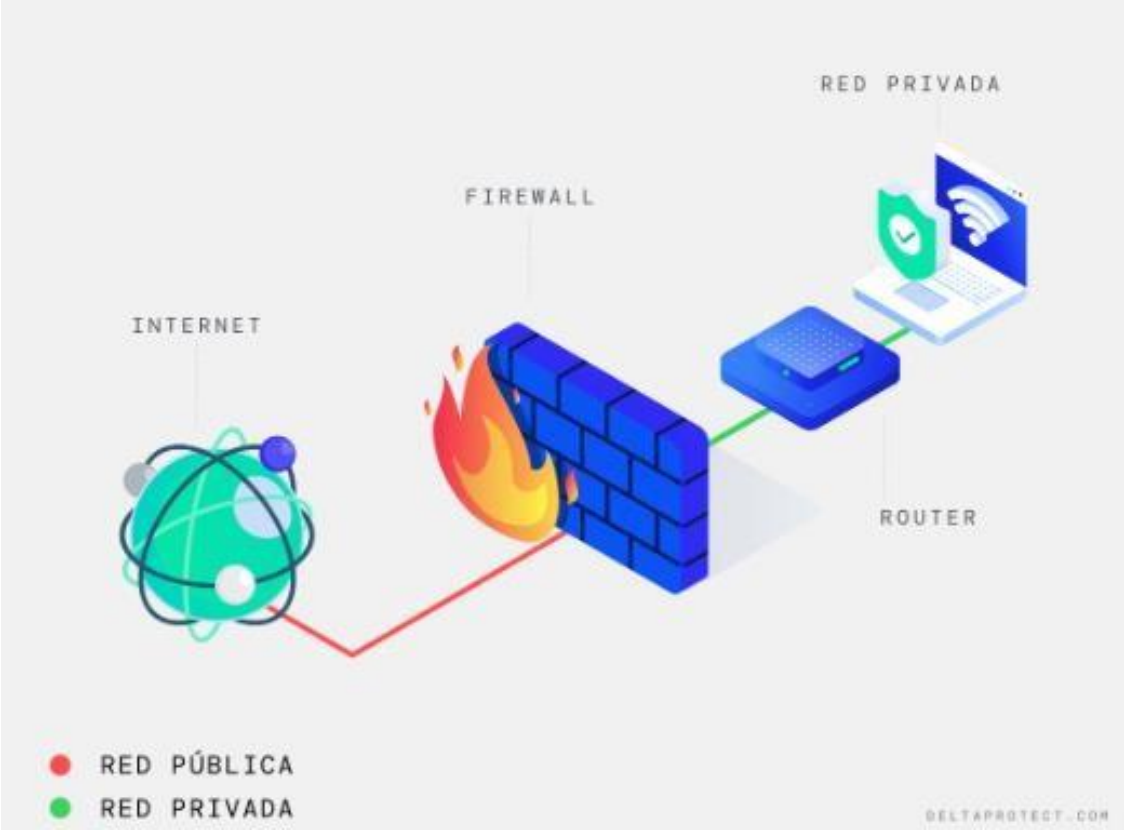
¿Quiénes deberían utilizar un Firewall?

Aquellos que deseen resguardar su red de computadoras de accesos no permitidos deberían emplear un cortafuegos, dado que son un dispositivo que contribuye a salvaguardar las redes de computadoras de ataques informáticos, el hurto de información, el malware y el sabotaje.

Usuarios que deberían usar un firewall:

- **Instituciones educativas:** los colegios, universidades y otras entidades educativas manejan una gran cantidad de datos delicados, incluida la información personal de los estudiantes.
- **Todo usuario que haga uso de Wi-Fi público:** debe tener un cortafuegos al acceder a diferentes sitios públicos: cafeterías, aeropuertos, entre otros, para resguardarse de posibles riesgos de seguridad.
- **Usuarios del hogar:** las personas que cuenten con una computadora, tableta o móvil vinculado a Internet en su hogar deben emplear un firewall, de esta manera contribuye a salvaguardar los dispositivos y la información personal frente a potenciales amenazas en línea.
- **Instituciones financieras:** bancos, compañías de seguros y otras instituciones financieras manejan información altamente confidencial y sensible.
- **Hospitales y centros de salud:** las entidades sanitarias gestionan registros médicos privados e información de los pacientes, con la utilización de un firewall se salvaguarda la información y previene el acceso indebido.
- **Organizaciones y empresas:** las compañías de cualquier tamaño, junto con entidades gubernamentales y no lucrativas, necesitan emplear un firewall para resguardar sus redes, sistemas de computación frente a accesos no permitidos, ataques malintencionados y robo de información.

Figura 14. Estructura del Firewall



Fuente: Gómez, JA. Delta Protect. (2022, 7 de septiembre). Firewall: Qué es, cómo funciona y para qué sirve. [Consultado: 12 de enero de 2025]. Disponible en: https://www.deltaprotect.com/blog/que-es-un-firewall

¿Cómo funcionan los firewalls?

Un cortafuegos determina qué tráfico de red es permitido y cuál es visto como peligroso. En esencia, distingue el tráfico positivo del negativo, o el seguro del no confiable, pero resulta beneficioso comprender la estructura de las redes basadas en la web.

El propósito de los cortafuegos es salvaguardar las redes privadas y los dispositivos de punto de conexión que las componen, denominados hosts de red, que son equipos que establecen "comunicación" con más host dentro de la red, también transmiten y reciben tráfico entre las redes internas, así como entre las redes externas.

Las computadoras y otros equipos de punto de conexión hacen uso de redes para conectarse a Internet y establecer comunicación entre sí. No obstante, el Internet se ha dividido en subredes debido a razones de seguridad y privacidad.

Los siguientes son los segmentos de subredes fundamentales:

- **Redes públicas externas:** generalmente relacionadas con el Internet público o mundial o con diversas extranet.
- **Redes privadas internas:** incluyen redes de vivienda, intranets corporativas y "cerradas".
- **Redes de perímetro:** aluden a las redes fronterizas formadas por hosts bastión, ordenadores host especializados con seguridad reforzada que están listos para resistir ataques externos.

  Como un enlace entre redes internas y externas, se pueden emplear para albergar cualquier servicio externo proporcionado por la red interna (como servidores para páginas web, correo electrónico, FTP, VoIP, entre otros), tienen mayor seguridad que las redes externas, pero menos que las redes internas, y no siempre se encuentran en las básicas, como las redes de vivienda, pero suelen emplearse en las intranets de empresas o a nivel nacional.

Las puertas de enlace de filtrado: son puertas especializadas situadas en una red con el objetivo de segmentarla, se les denomina como firewalls domésticos a nivel de red, se tienen los dos modelos de segmentación más habituales que son el cortafuegos de host filtrado y el cortafuegos de subred filtrado.

- **Cortafuegos de usuarios filtrados:** utilizan un solo enrutador de filtrado entre las redes internas y externas; que constituyen las dos redes secundarias de este modelo.
- **Cortafuegos de subred filtrados:** emplean dos enrutadores de filtrado. Uno denominado enrutador de acceso entre la red exterior y la perimetral y otro enrutador de choque entre la perimetral y la red interna, generando tres subredes correspondientes.

Tanto las máquinas de host como el perímetro de red pueden ser el hogar de un cortafuegos para ello se sitúa entre una computadora y su conexión con la red privada.

- **Los firewalls de red:** se refiere al empleo de uno o varios cortafuegos entre las redes externas y las redes internas privadas, controlan el flujo de datos entrantes y salientes; distinguen las redes públicas externas (como el Internet mundial) de

las redes internas, como las redes de wifi en el hogar y las intranets de empresas o gobiernos; los cortafuegos de red pueden presentarse en cualquiera de los siguientes tipos: hardware exclusivo, software y virtual.

- **Los firewalls de host** o "Firewalls de software": necesitan firewalls en dispositivos individuales de usuario y otros puntos de conexión de red privados para establecer barreras entre los dispositivos dentro de la red, a estos equipos o host son el objeto de una regulación personalizada del tráfico desde y hacia aplicaciones específicas de la computadora; los cortafuegos de host pueden funcionar en equipos locales, como un servicio del sistema operativo o una aplicación de seguridad para el punto de conexión.

  Los cortafuegos de host pueden tener un acceso más detallado al tráfico web, el filtrado basado en HTTP y otros protocolos de red, facilitando la gestión del contenido que el equipo recibe, en vez de un firewall de red requiere una configuración ante una amplia variedad de conexiones, mientras que un firewall de host puede personalizarse para adaptarse a las necesidades del equipo, son ideales para un sistema de seguridad de varias capas.

La **filtración del tráfico a través de un cortafuegos** emplea normas previamente establecidas o aprendidas de manera dinámica para permitir y rechazar los intentos de conexión. estableciendo la manera en que el cortafuegos controla el tráfico web a través de la red privada y los equipos de computación privados. Todos los cortafuegos pueden efectuar el filtrado a través de un acoplamiento de lo siguiente:

- **Origen**: sitio desde el cual se busca establecer la conexión.
- **Destino**: sitio al que se busca enviar la conexión.
- **Contenido**: datos que la conexión está tratando de transmitir.
- **Protocolos del paquete**: el "lenguaje" empleado para comunicar el mensaje durante el intento de establecer la conexión. Dentro de los protocolos de red que los hosts utilizan para "comunicarse", los TCP/IP son los más utilizados para la comunicación a través de Internet y entre intranets o subredes.
- **Protocolos de aplicaciones**: entre los más ocupados encuentran HTTP, Telnet, FTP, DNS y SSH.

Cómo activar y desactivar un firewall

Según el sistema operativo usado, se aplican las instrucciones siguientes:

- En **Windows**, ingresen al Panel de control y elija la opción de 'Sistema y seguridad’. Luego, seleccionen 'Firewall de Windows' y seleccionen 'Activar o desactivar Firewall de Windows'.

- En **macOS**, vaya a la sección de Preferencias del Sistema y elija 'Seguridad y privacidad', después elija la sección 'Firewall' y haga clic en 'Activar Firewall' o 'Desactivar Firewall'.
  En **Linux**, inicien la terminal y ejecuten el comando 'sudo ufw enable' para ejecutar el cortafuegos, para desactivarlo se repiten los mismos procedimientos, pero digitando 'sudo ufw disable'.

6.2.3.4 Wireshark

Herramienta para el estudio del tráfico de red que posibilita, en su papel de analizador de protocolos estándar, proporcionar sus funciones de manera gratuita a empresas, individuos y estudiantes, con el fin de examinar los paquetes de información que se desplazan en una red.

Es perfecta para:

- Adquirir conocimientos sobre el tráfico,
- Identificar potenciales inconvenientes de seguridad.
- Analizar paquetes de código abierto y gratuito que examina su red para identificar problemas de desempeño y seguridad,
- Proporciona una superioridad frente a los piratas informáticos.
- El software para Windows tiene la capacidad de examinar el flujo de red de redes inalámbricas, Ethernet, VLAN y Bluetooth. Adicionalmente, todas estas capacidades no están restringidas a Windows. También se puede descargar Wireshark para Mac.

- **¿Qué tipo de herramienta es Wireshark?**

  En una red doméstica o laboral, numerosas vulnerabilidades se ocultan y pueden llevar a perder clientes, labores y datos personales. Al capturar y examinar paquetes, puedes comprender el estado de salud y seguridad de toda tu red. El seguimiento de paquetes también es un método que los cibercriminales emplean para descubrir y aprovechar fallos en la red.

  Wireshark es un programa de software para analizar protocolos de red de código abierto. Opera capturando paquetes de una red, aunque ésta puede ser de su casa, trabajo o conexión a Internet. Un paquete se refiere a una unidad de datos para una red Ethernet o WiFi. Una vez que los paquetes son capturados, Wireshark examina cada uno de ellos.

- **¿Es ilegal utilizar Wireshark y para qué se emplea?**

El programa se beneficia de la asistencia de una comunidad de especialistas que lo expanden de manera constante para proporcionar más funcionalidades. No obstante, es ilícito hacer uso del programa para monitorear redes sobre las que no se cuenta con permiso.

Wireshark se emplea en los siguientes casos:

- Capturar y examinar la información táctica. Lo realiza mediante el uso de las más recientes características, funcionalidades y procedimientos. En realidad, de acuerdo con la compañía, es uno de los analizadores de protocolos de red más empleados a nivel global. El software de código abierto se encuentra accesible de manera gratuita, tanto para uso individual como para empresas.
- Facilita que los usuarios modifiquen algunas secciones de las aplicaciones. Los programadores tienen la capacidad de efectuar análisis y ensayos en diversos tipos de redes, disectores y firmas. Además, se puede almacenar de manera sencilla toda la información recolectada en la plataforma, permitiendo que otras aplicaciones que utilicen o examinen el tráfico de la red puedan acceder con facilidad a esta interpretación de datos.
- Wireshark puede ser una alternativa adecuada para monitorear todos los elementos de tu red y resolver cualquier inconveniente de rendimiento o seguridad que el software pueda identificar.

- **Características**

- Los usuarios tienen la posibilidad de utilizar los filtros ofrecidos por Wireshark, para añadir o eliminar entradas de su búsqueda y ajustar la sección de filtros para enfocarse en datos concretos.
- En el panel de control se descarga esta herramienta, la barra de expresiones facilita la obtención de los resultados esperados al comparar ciertos paquetes. Evita el proceso de búsqueda manual que habría requerido explorar diversos marcos para localizar una entrada específica.
- El software también le ofrece la posibilidad de añadir colores a los paquetes, permitiéndole rastrearlos cada vez que se abre Wireshark.
- Ofrece a los usuarios datos exhaustivos que comprenden respuestas HTTP y peticiones. Al seleccionar el menú que se encuentra en la sección de estadísticas, se puede visualizar un árbol con datos jerárquicos que presenta el tráfico entre dos puntos o direcciones IP y protocolos.
- Se ha reservado la sección llamada Información de expertos para registrar todos los inconvenientes que se presenten en tu red. Claro que todos los registros no

representan necesariamente problemas, se pueden emplear para rastrear cualquier irregularidad que se detecte.

- Wireshark y todas sus funciones son bastante confiables y están respaldadas por una comunidad de usuarios que actualizan el programa constantemente.
- La aplicación ofrece a los diferentes usuarios análisis de VoIP y les facilite utilizar formatos de captura de lectura o escritura.
- El software también admite la función de cifrado y toda la información se exporta a un dispositivo local en un documento CSV, XML, PostScript o de texto.
- Su potencial no está restringido a las redes WiFi o Ethernet. Disponible para examinar el flujo de red de VLAN, USB y aparatos Bluetooth.

6.2.3.5 OpenVAS

Escáner gratuito de vulnerabilidades que ayuda a identificar problemas en sistemas y redes. Es útil para realizar auditorías de seguridad y aprender sobre la gestión de vulnerabilidades. Puede detectar problemas de diferentes calibres, tanto de bajo riesgo para usuarios, como vulnerabilidades más graves en equipos en dispositivos en red. Desde 2009 y en código abierto, lo desarrolló la empresa Greenbone Networks bajo la Licencia Pública General de GNU (GNU GPL) y fue avanzado a medida según iban siendo sus necesidades, así como con su API.

> "OpenVAS es un escáner de vulnerabilidades con todas las funciones. Sus capacidades incluyen pruebas autenticadas y no autenticadas, varios protocolos industriales y de Internet de alto y bajo nivel, ajuste del rendimiento para escaneos a gran escala y un potente lenguaje de programación interno para implementar cualquier tipo de prueba de vulnerabilidad"[25]

- **Para qué sirve Open VAS**
  Este scanner cuenta con diversas funciones posibles, entre las que se encuentran:

  - Pruebas autenticadas y no autenticadas.
  - Dispone de protocolos industriales y de Internet de nivel superior e inferior.
  - Modificaciones de rendimiento personalizadas para investigaciones de gran envergadura.
  - Creado en un robusto lenguaje de programación interno.

[25] GREENBONE OPEN VAS. Open Vulnerability Assessment Scanner. [Consultado: 12 de enero de 2024]. Disponible en: https://www.openvas.org/

- **Características principales de OpenVAS**

    - Amplia y precisa documentación.
    - Opción desde línea de comandos y en formato gráfico con una interfaz llena de utilidades y datos relevantes, con la capacidad de generar informes de utilidad.
    - Proporciona numerosos tutoriales, respaldo en la exploración de vulnerabilidades, tanto a través de su sitio web, o de otros foros como RedditExtensa y definida documentación.
    - Posibilidad desde línea de comandos y en modo gráfico con una interfaz con utilidades y repleta de datos de interés, capaz de sacar informes de utilidad.
    - Facilita la ejecución de escaneos en varios nodos al mismo tiempo, revelar vulnerabilidades detectadas en servicios y aplicaciones instaladas.
    - La herramienta proporciona una interfaz visual mediante el Greenbone Security Assistant (GSA), simplificando la administración y la visualización de los resultados de los escaneos.
    - Interfaz Web: incluye una interfaz gráfica a través del Greenbone Security Assistant (GSA), suministra la gestión y visualización de los resultados de los escaneos.
    - Compatibilidad multiplataforma: OpenVAS es compatible con varios sistemas operativos y reconocer su uso en diferentes entornos informáticos16.
    - Utiliza una base de datos con más de 47,000 pruebas de vulnerabilidad (NVTs) que se actualizan regularmente.
    - Informes detallados: ofrece reportes en múltiples formatos, incluyendo XML y HTML, facilitar la interpretación de los resultados.

6.2.3.6 Nmap

Aplicación de código abierto ampliamente empleada en Linux para la exploración de redes y la auditoría de red. Es particularmente beneficioso para gestores de red y expertos en ciberseguridad.

> "Nmap es la abreviatura de Network Mapper. Es una herramienta de línea de comandos de Linux de código abierto que se utiliza para escanear direcciones IP y puertos en una red y para detectar aplicaciones instaladas. Nmap permite a los administradores de red encontrar qué dispositivos se están ejecutando en su red, descubrir puertos y servicios abiertos y detectar vulnerabilidades"[26]

[26] SHIVANANDHA, Manos. Traductor: BlackeyeB. Qué es Nmap y cómo usarlo: Un tutorial para la mejor herramienta de escaneo de todos los tiempos. . [Consultado: 23 de enero de 2024]. Disponible en: https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos/

- ¿Para qué sirve Nmap?: es útil para el mapa de puertos de una red, dispone de diversas características que facilitan la adquisición de numerosa información adicional como:

    - Mapear una red.
    - Determina equipos que están vinculados a una red.
    - Identificar servicios en funcionamiento.
    - Conoce varios servicios que operan en la red, como servidores de correo electrónico o servidores web.
    - Ofrece detalles sobre la categoría de aplicaciones y sus ediciones.
    - Lleva a cabo una completa auditoría de seguridad de la red.
    - Analizar una red para detectar el sistema operativo que están utilizando los diferentes equipos que se conectan a la red.

- Características de Nmap

    - Exploración de redes: facilita la identificación de dispositivos en funcionamiento en una red y la recopilación de datos específicos sobre éstos.
    - Escaneo de puertos: identifica puertos abiertos y los servicios que operan.
    - Halla información sobre el sistema operativo que se ejecuta en los dispositivos y provee planificar de enfoques adicionales durante las pruebas de penetración.
    - Capacidad para reconocer rápidamente todos los dispositivos, en redes únicas o múltiples: servidores, enrutadores, conmutadores, dispositivos móviles, etc.
    - Identifica versiones de los servicios que están corriendo en los puertos abiertos.
    - Ayuda a identificar los servicios que se ejecutan en un sistema, incluidos los servidores web, los servidores DNS y otras aplicaciones comunes.
    - Nmap tiene una interfaz gráfica de usuario llamada Zenmap. Ayuda a desarrollar mapeos visuales de una red para un mejor servicio y generación de informes.
    - Durante la auditoría de seguridad y el escaneo de vulnerabilidades, Nmap puede atacar sistemas usando scripts existentes del motor de scripting de Nmap.
    - Incluye una base de datos de scripts y ser ocupados para realizar tareas específicas como detección de vulnerabilidades.

6.2.3.7 Zenmap

Interfaz gráfica oficial del escáner de seguridad Nmap, diseñada para facilitar su uso tanto a principiantes como a usuarios avanzados. Es una aplicación multiplataforma, disponible para sistemas operativos como Linux, Windows, Mac OS X y BSD, y es gratuita y de código abierto.

> "Zenmap como la interfaz gráfica de usuario oficial de Nmap, que permite usar el programa de manera práctica, cómoda, clara y más organizada. Esta interfaz es ideal para expertos y principiantes, aunque también depende del gusto y hay quienes prefieren su uso directamente en la consola. No obstante, la intefaz gráfica de Nmap, Zenmap, facilita visualmente la ejecución de aplicaciones de escaneo de puertos de uso común y hace más cómodo el uso de este programa"[27]

- Usos comunes de Zenmap por administradores de red y profesionales de ciberseguridad:

  Descubrir Hosts y servicios: identificar los dispositivos activos en una red y los que están disponibles.
  - Auditorías de seguridad: realizar análisis para detectar vulnerabilidades en la infraestructura de red.
  - Monitoreo continuo: facilitar el seguimiento de cambios en la red mediante escaneos regulares.

- Características principales de Zenmap

  - Interfaz gráfica: Zenmap proporciona una interfaz intuitiva que aprueba a los usuarios visualizar los resultados de los escaneos de forma interactiva, en lugar de depender únicamente de la línea de comandos.
  - Creación de comandos: incluye un asistente que crea comandos de Nmap de manera interactiva y facilita la configuración de escaneos sin necesidad de recordar sintaxis complejas.
  - Comparación de resultados: los escaneos pueden guardarse y compararse, de esta forma facilita a los administradores identificar cambios en la red a lo largo del tiempo.
  - Mapas topológicos: Zenmap puede generar mapas topológicos que visualizan la conectividad entre los hosts descubiertos en una red y ayuda a entender mejor la estructura de la red.

[27] KEEPCODING. ¿Qué es Zenmap?. [Consultado: 14 de enero de 2024]. Disponible en: https://keepcoding.io/blog/que-es-zenmap-ciberseguridad/

6.2.3.8 Acunetix Online (Gratuito y sin restricciones)

Es una solución de seguridad de aplicaciones web todo en uno, totalmente automatizada para acceder a realizar escaneos de aplicaciones web de caja negra, caja gris (IAST), del lado del cliente y fuera de banda.

- El escáner utiliza una interfaz web y el motor está disponible tanto para Windows como para Linux y próximamente Mac.
- Acunetix aprovecha dos tecnologías únicas que lo ayudan a descubrir más vulnerabilidades: AcuMonitor y AcuSensor que sirve de apoyo para encontrar la vulnerabilidad en el código fuente.

- Etapas fundamentales en las que opera Acunetix
  - Crear y configurar un objetivo
  - (Crawling) Rastreo y escaneo
  - Informes y remediación
  - Manejo de vulnerabilidades -> Issue Tracker

- Características:

  - Escaneo exhaustivo de vulnerabilidades: Acunetix puede detectar más de 45,000 vulnerabilidades web, incluyendo inyecciones SQL, Cross-Site Scripting (XSS), y configuraciones incorrectas. Su capacidad para analizar aplicaciones complejas, autenticadas y basadas en tecnologías como HTML5 y JavaScript lo hace ideal para entornos modernos.
  - Tecnologías avanzadas: DeepScan: permite el rastreo de aplicaciones de una sola página (SPA) que utilizan AJAX, mejorando la detección en aplicaciones dinámicas.
  - AcuSensor: combina análisis de caja negra con retroalimentación del código fuente, para ayudar a identificar vulnerabilidades directamente en el código.
  - Interfaz amigable y eficiente: la interfaz web de Acunetix está diseñada para facilitar el uso e iniciar escaneos con pocos clics. Además, proporciona informes detallados y personalizables que ayudan a los equipos a comprender y remediar las vulnerabilidades encontradas.
  - Monitoreo continuo: ofrece la opción de realizar escaneos programados y monitoreo continuo, permitiendo a las organizaciones estar al tanto de nuevas vulnerabilidades en tiempo real.
  - Informes personalizables: los informes generados pueden adaptarse a diferentes audiencias, incluyendo informes ejecutivos y técnicos, lo que facilita la comunicación sobre el estado de seguridad a los interesados.

- Integración con DevOps: se integra fácilmente con herramientas y flujos de trabajo existentes en entornos DevOps, para incorporar pruebas de seguridad en el ciclo de desarrollo y reducir el riesgo de introducir vulnerabilidades en producción.
- Grabación de secuencias de inicio de sesión: concede escanear áreas protegidas por contraseña y formularios complejos, asegurando que todas las partes del sitio web sean evaluadas adecuadamente.

6.2.3.9 OWASP ZAP

En linux (gratis) nos muestra vulnerabilidades, soluciones, riesgos encontrados y especifica si el riesgo es alto, bajo o medio.

OWASP ZAP (Zed Attack Proxy) es una herramienta de seguridad de aplicaciones web de código abierto. Desarrollada por la comunidad de OWASP (Open Web Application Security Project), ZAP proporciona a los profesionales de seguridad y ejecutores una forma poderosa de detectar y resolver vulnerabilidades en sus aplicaciones web.

> "OWASP ZAP (Zed Attack Proxy) es el escáner web de vulnerabilidades más utilizado en todo el mundo, es completamente gratuito y de código abierto, por lo que podrás adaptarlo a tus necesidades. Este programa es mantenido activamente por una comunidad internacional de voluntarios, los cuales trabajan para ir mejorando la herramienta poco a poco y también incorporando nuevas características"[28]

En esencia, ZAP es lo que se conoce como un "proxy de intermediario". Se encuentra entre el navegador del probador y la aplicación web para que pueda interceptar e inspeccionar los mensajes enviados entre el navegador y la aplicación web, modificar el contenido si es necesario y reenviar esos paquetes al destino

- ZAP usos: opera en dos modos principales:

  - Modo activo: a través de la ejecución de pruebas intrusivas enviando solicitudes modificadas a la aplicación para identificar vulnerabilidades.
  - Modo pasivo: monitorea el tráfico sin alterarlo, registrando información sobre posibles debilidades sin riesgo de afectar la aplicación

- Características destacadas

[28] HERNANDEZ, Alonso Mikel. Escaneo de vulnerabilidades automático con Owasp Zap. [Consultado: 12 de enero de 2024]. Disponible en: https://academy.seguridadcero.com.pe/blog/escaneo-vulnerabilidades-autom%C3%A1tico-OWASP-ZAP

- Intercepción de tráfico: ZAP actúa como un proxy que permite a los usuarios interceptar y modificar el tráfico HTTP/HTTPS entre el navegador y la aplicación web. Esta capacidad es decisiva para identificar vulnerabilidades que podrían no ser evidentes a simple vista.
- Escaneo automatizado y pasivo: se centra en analizar el tráfico sin alterarlo, siendo útil para obtener una visión general del estado de seguridad de la aplicación.
- Fuzzing: ZAP incluye funcionalidades de fuzzing, evita datos aleatorios a la aplicación para descubrir posibles vulnerabilidades que podrían ser explotadas por atacantes. Así, se puede encontrar fallos que no son fácilmente detectables mediante escaneos convencionales.
- Scripting personalizado: se puede crear y ejecutar scripts personalizados para automatizar pruebas específicas o manipular solicitudes y respuestas; permitiendo mayor flexibilidad y adaptabilidad en las pruebas de seguridad.
- Gestión de contextos: ZAP define contextos que agrupan características específicas de la aplicación web, como mecanismos de autenticación y gestión de sesiones; facilitando la organización y ejecución de pruebas más precisas.
- Marketplace de extensiones: proporciona a los usuarios añadir nuevas funcionalidades a través de un marketplace, mejorando constantemente la herramienta con contribuciones de la comunidad.

6.2.3.10 Antivirus de seguridad para Móviles

Son plataformas de seguridad que proporciona protección multicapa en tiempo real para dispositivos móviles. Utiliza tecnologías avanzadas basadas en la nube y aprendizaje automático para detectar y neutralizar amenazas antes de que puedan causar daño. Esta herramienta no solo protege contra el malware, sino que previene el acceso no autorizado a datos sensibles y consiente la gestión remota de dispositivos en caso de pérdida o robo.

- **Tecnología usada para proteger:**

  - El dispositivo del spyware y el malware en vínculos maliciosos con la función Antiphishing para poder usar el teléfono sin preocuparte.
  - Las actividades bancarias con herramientas de protección de pagos en línea, como navegación segura*, Mensajería segura* y un antivirus* avanzado.
  - El teléfono con la función ¿En dónde está mi dispositivo?* para que se pueda bloquear, saber dónde está y fotografiar al ladrón, todo de forma remota, si se pierde o alguien lo roba.
  - Controla la información personal y decidir dónde, cuándo y con quién la comparte.
  - Protege tu actividad en Internet, las contraseñas, almacena datos personales en una bóveda privada y aumenta la privacidad.

- **Las características principales de la seguridad móvil son:**

    - Analiza el dispositivo en tiempo real para detectar amenazas.
    - Realiza análisis antivirus para detectar, neutralizar virus y otras amenazas.
    - Actualiza constantemente sus bases de datos para anticiparse a amenazas emergentes.
    - Borra y restablece de forma remota el dispositivo a los valores predeterminados de fábrica.
    - Controla las aplicaciones que se instalan en el dispositivo.
    - Se protegen los pagos que se realizan en el dispositivo.
    - Protege la cámara web del dispositivo.
    - Permite localizar el dispositivo y tomar una foto del ladrón.
    - Ofrece protección segura para la navegación en el dispositivo.

6.2.3.11 Antivirus Gratuitos

Es una buena opción si se busca una herramienta gratuita o si ya se está familiarizado con su interfaz. Free Antivirus es un software que protege contra una amplia gama de amenazas, desde virus y malware hasta phishing y ransomware.

Características:

- Protección efectiva contra amenazas como virus, malware, spyware y phishing.
- Es ligero y no ralentiza tu dispositivo.
- Reciben actualizaciones frecuentes para combatir las amenazas más recientes
- Se puede combinar con Windows defender para mejorar significativamente la protección general del equipo.
- Resguarda dispositivos con Windows, Mac, Android e iOS.
- Protección contra ransomware, evita accesos no autorizados a archivos personales.
- Navegación segura, bloquea sitios web maliciosos y descargas peligrosas.

Desventaja:

- Limitaciones: Algunas funciones avanzadas requieren compra separada.

Para finalizar puedo afirmar que la creciente integración de la tecnología en la vida cotidiana transformó la forma en que los jóvenes interactúan con el mundo, pero también ha planteado serios desafíos en términos de seguridad y bienestar. La implementación de herramientas parentales se presenta como una estrategia crucial para proteger a los estudiantes de los peligros que acechan en la red, como el ciberacoso, el acceso a contenido inapropiado y la exposición a los ciberdelincuentes en línea. Sin embargo, estas herramientas deben complementarse con una capacitación integral y continúa dirigida a docentes, padres y estudiantes, es fundamental que los educadores reciban formación sobre cómo abordar temas de seguridad digital en la institución educativa, así mismo, los alumnos necesitan desarrollar habilidades críticas para navegar de manera segura y responsable en internet. En síntesis, la educación y la concienciación son pilares fundamentales para la seguridad de los estudiantes al usar la red internet.

6.3 PROPONER BUENAS PRÁCTICAS DE CIBERSEGURIDAD DE LA INFORMACIÓN PARA QUE SIRVA DE GUÍA A LOS DOCENTES, PADRES DE FAMILIA Y EL ENTORNO ESTUDIANTIL

Para alcanzar una educación de alta calidad, es esencial potenciar la función de los padres como formadores y actores activos en el proceso educativo de sus hijos. La familia constituye el entorno natural para el crecimiento de los niños, según lo sugiere la Convención de los Derechos del Niño de la ONU. Entonces debe interpretarse como la entidad en la que todos sus miembros contribuyen directamente a la educación de los niños y niñas, asumiendo una responsabilidad social para el bienestar y la sociedad.

6.3.1 Buenas prácticas de ciberseguridad a los docentes

La protección de la información en el contexto educativo es valiosa, teniendo en cuenta que los distintos centros educativos recolectan grandes volúmenes de datos. Es importante destacar que no solo me refiero a las notas y referencias personales, como la edad, dirección, género, condiciones o competencias de cada uno de sus alumnos, sino también datos del núcleo familiar. Siendo fundamental implementar buenas prácticas para salvaguardar tanto al personal docente y a los estudiantes.

Tabla 11. Buenas Prácticas Tecnológicas

Práctica Recomendadas	
• Obtener políticas de contraseña	
• Conseguir duplicados de la labor cotidiana, ya sea en la nube (en línea) o en un disco duro externo (en línea).	
• Usar el correo laboral en lugar del personal.	
• Emplear herramientas seguras orientadas a la seguridad de la información.	
• Evitar descargar ficheros adjuntos que sean sitios web dudosos.	
• Mantener equipos personales actualizados y configurados correctamente para prevenir que sean vulnerados.	
• Concientizar a los estudiantes sobre los peligros al usar las redes sociales y suministrar información privada o personal.	

Fuente: MARSH MCLENNAN. Guía de buenas prácticas de ciberseguridad. [Consultado: 15 de enero de 2024]. Disponible en: https://www.marsh.com/es/services/cyber-risk/insights/good-cybersecurity-practices.html

Figura 15. Responsabilidad proactiva

Fuente: González, D. (18,febrero,2022). [imagen]. La responsabilidad proactiva en materia de protección de datos. Laworatory.[Consultado: 10 noviembre,2023]. Disponible en: https://laworatory.com/blog/responsabilidad-proactiva-proteccion-datos/

6.3.1.1 Capacitación a los docentes

El objetivo principal de la formación a los profesores es actuar como mediadores de información y fomentar una conducta en línea responsable y segura entre los estudiantes. Por lo tanto, los diversos programas de formación continua para profesores en ciberseguridad son de carácter fundamental para salvaguardar la información, sino que también implementen medidas para guiar a los jóvenes acerca de la relevancia de la seguridad en internet.

Al implementar estas tácticas en forma constante, los docentes pueden aportar a la construcción de un ambiente educativo más seguro y resistente ante las amenazas

tecnológicas, se vuelven un elemento indispensable para salvaguardar la integridad y seguridad de los menores de edad, al utilizar la tecnología.

La formación en ciberseguridad para docentes se basa en el conocimiento de los distintos ataques a individuos y dispositivos vulnerables, así como en cómo evitarlos. Estar al día de manera constante le facilita el aprendizaje de las diversas herramientas que resguardan los datos y las páginas web; que incluyen claves seguras, información biométrica, autenticación de dos factores y cortafuegos, entre otros.

6.3.1.2 Manejo de conceptos básicos en Ciberseguridad

El profesional realiza actualizaciones constantes sobre temas de ciberseguridad, entre los que se pueden destacar:

- Distintos prototipos de ataques cibernéticos: ataques de ingeniería social, malware, inyección de SQL, bots malintencionados y riesgos físicos a datos, dispositivos y redes.
- Herramientas para salvaguardar información, aparatos y redes, tales como: claves seguras, datos biométricos, autenticación de dos factores (2FA), programas antivirus, cortafuegos y otros.
- Métodos de ciberseguridad: la desinfección de accesos, protocolos de seguridad adecuadamente estructurados, sistemas de regulación de acceso a datos y redes.

6.3.1.3 Temas de la capacitación docente

Los procesos de formación para el docente, profesor o instructor, ya sea de manera individual o grupal dentro del marco de las instituciones educativas en forma presencial o en línea, se transformaría en una excelente opción para mantenerse al día y a la vez profundizar en los siguientes aspectos:

- Comprender la interpretación de términos que definen ataques informáticos comunes, como phishing, pharming, blagging.
- Valorar la seguridad de las claves.
- Reconocer las protecciones que la Ley brinda a los usuarios frente al uso no autorizado de aparatos informáticos.
- Clasificar las clases de malware.
- Obtener entendimiento sobre el funcionamiento del programa antivirus.
- Describir las diversas clases de ciberataques y la manera en que pueden mitigar.

- Entender los procedimientos utilizados para proteger una red.

6.3.1.4 Estrategias en la capacitación docente

Es fundamental que los profesores reciban formación constante en ciberseguridad para no solo salvaguardar su información, sino también para guiar a los estudiantes sobre la importancia de la seguridad en internet. Cuando los educadores implementan estas estrategias, pueden aportar a la construcción de un ambiente educativo más seguro y resistente ante las amenazas del ciberespacio.

Hay que tener presente las siguientes estrategias:

- **Asistencia a seminarios y lecciones sobre ciberseguridad:** a través de programas proporcionados por entidades educativas o plataformas de capacitación, tratando asuntos como la detección de riesgos, la solución a incidentes y las mejores prácticas para la seguridad en internet.
- **Aprovechamiento de recursos en línea:** ofrecen información reciente sobre ciberseguridad. Blogs, webinars y páginas web especializadas brindan artículos y orientación de los últimos ataques cibernéticos y la manera de evitarlos.
- **Ejecución de protocolos definidos:** las entidades educativas deben definir reglas de uso seguro para las plataformas digitales y las videoconferencias.
- **Fomentar la responsabilidad:** es imprescindible que los docentes fomenten una cultura de protección digital en el salón de clases. Ejecutar sesiones informativas breves de la ciberseguridad al comienzo de las clases o enviar mensualmente correos electrónicos con sugerencias sobre buenas prácticas en ciberseguridad.
- **Actualización constante del software:** los docentes tienen que mantener actualizados todos los sistemas y aplicaciones usando parches de seguridad regularmente para protegerse contra vulnerabilidades conocidas.
- **Colaboración con expertos:** establecer vínculos con profesionales en ciberseguridad puede ser beneficioso porque pueden ofrecer capacitación específica, realizar auditorías de seguridad y ayudar a implementar medidas adecuadas para proteger la infraestructura digital de la institución.
- **Participación en comunidades educativas:** mediante foros o grupos donde se discutan temas de ciberseguridad y compartir experiencias con otros educadores puede enriquecer el conocimiento colectivo sobre cómo enfrentar los desafíos digitales.

6.3.2 Buenas prácticas de ciberseguridad a los padres de familia

En lo que respecta a los padres de familia, son ellos los responsables de fomentar un entorno de cordialidad en el hogar, educar con el ejemplo, que fomente la creación de confianza con sus hijos e hijas, se transformen en el primer respaldo y asistencia; demostrando interés por su actividad digital para que así puedan interactuar con ellos en este campo y no recurrir a la prohibición como primera medida, sin antes haber descubierto y examinado todo lo que consideramos apropiado; más bien promover desde una edad temprana, prácticas que instruyan acerca de los riesgos al utilizar internet.

Por esta razón, los padres y las personas encargadas de los menores de edad, reflexionen y se comprometan a actuar como guardianes de sus hijos e hijas, mediante el control parental correspondiente. Mantener una comunicación constante con sus hijos menores de edad para que denuncien ante las diversas instituciones gubernamentales y estén pendientes y acompañándolos en este proceso de problemas o delitos digitales, es esencial mantenerse actualizado sobre las nuevas plataformas y contenidos para adolescentes, con el fin de asesorar y dirigir su actividad hacia lo que sea apropiado.

6.3.2.1 Prácticas de Ciberseguridad

Tener conocimiento sobre las actuales amenazas cibernéticas facilitará a todo el personal de las entidades evitar ataques, en caso de producirse alguno.

Tabla 12. Prácticas de ciberseguridad en padres de familia

Prácticas
• Identificar con quiénes sus hijos establecen interacción tanto en el ámbito virtual como en el mundo real.
• Informar a los menores de edad de comunicarse con la Policía y al sitio de redes sociales, si por alguna razón se sintieran amenazados.
• Dar a conocer a los jóvenes menores de edad de los grados mencionados, que cualquier dato que publiquen o suban a internet (fotos, mensajes, etc), no puede ser borrada, incluso si han pasado apenas segundos del evento efectuado, ya que ésta permanecerá inalterable.
• La clave es disminuir el tiempo de empleo de los dispositivos, que tengan como: móvil, tablet y consolas, utilizando una app de control parental.
• Denunciar que existen adultos que aparentan ser niños o niñas con el objetivo de engañarlos y capturar imágenes o videos de los menores de edad en situaciones comprometidas que posteriormente pueden emplear para amenazarlos**.**
• Instruir a sus hijos sobre la moda de ser populares, acumular seguidores y numerosos likes y aunque es un comportamiento común en el ámbito digital, representa un riesgo.
• El diálogo frecuente entre padres e hijos(as), permite informar de los riesgos a los que se pueden ver involucrados como son el sexting, el Ciberbullying, las apuestas online, el consumo de pornografía, el contenido hiperviolento, entre otros.

Fuente: MALWAREBYTES. Consejos de Seguridad en Internet para Niños, Adolescentes. y Padres. .[Consultado: 10 noviembre,2023]. Disponible en: https://www.malwarebytes.com/es/cybersecurity/basics/internet-safety-tips-for-kids

6.3.2.2 Capacitación a padres de familia

Es fundamental formar de manera constante a los padres y madres en términos de ciberseguridad en las diversas actividades programadas con el propósito de salvaguardar a sus hijos, promover sus competencias digitales, guías parentales, herramientas apropiadas y establecer una comunicación eficaz sobre los peligros presentes en la red.

- **Temas de capacitación para padres de familia.**
    - **Protección de los hijos:** los niños, niñas y adolescentes se encuentran cada vez más vulnerables a peligros en internet, como el acoso cibernético y el acceso a contenido inadecuado. Los padres educados en ciberseguridad implementan estrategias de seguridad y control sobre la actividad digital de sus hijos, contribuyendo a evitar situaciones de riesgo.
    - **Fomentar una comunicación abierta:** la capacitación en ciberseguridad contribuye a los padres a crear un ambiente donde se pueda hablar abiertamente sobre los riesgos en línea, ayuda a los menores a sentirse cómodos al compartir sus dudas y experiencias, siendo fundamental para su seguridad.
    - **Formación en buenas prácticas:** los progenitores y tutores pueden instruir a sus hijos acerca de fraudes en internet, la relevancia de establecer contraseñas seguras, evitar el compartir datos personales.
    - **Implementación de herramientas de control parental:** los padres formados tienen la capacidad de poner en marcha instrumentos como filtros de control parental y definir restricciones temporales en la utilización de aparatos. Estas acciones contribuyen a controlar el acceso a la red y a salvaguardar a los menores de edad de contenido no apropiado.

- **Estrategias de la capacitación a padres de familia.**

A continuación, se presentan algunas estrategias efectivas para llevar a cabo esta capacitación:

- **Conversaciones y seminarios informativos:** programar sesiones de enseñanza en las que especialistas en ciberseguridad puedan explicar los peligros vinculados con el uso de Internet y proporcionar sugerencias útiles. En estas sesiones, se pueden tratar asuntos como la privacidad en internet y la administración de la identidad digital requeridas para simplificar estas exposiciones.
- **Cursos en línea:** ofrecer cursos gratuitos que los padres de familia pueden realizar a su propio ritmo. Plataformas como el Ministerio de Educación y CISCO han lanzado iniciativas que incluyen cursos sobre fundamentos de ciberseguridad y seguridad en la nube.
- **Promover el diálogo familiar:** propiciar un entorno en el que se discutan de manera franca las experiencias en línea. Es imprescindible que los padres hagan preguntas frecuentes a sus hijos referente a sus actividades digitales

para que puedan detectar posibles dificultades y de esta manera, proporcionar la guía requerida.

- **Implementación de herramientas de seguridad:** capacitar a los padres sobre el uso de software de seguridad, incluyendo funciones de control parental para monitorear la actividad en línea y establecer límites.
- **Creación de pactos familiares:** promover la elaboración conjunta de acuerdos, cumplimiento de normas relacionados con el uso de dispositivos y redes sociales.
- **Sensibilización sobre privacidad:** educar a los padres sobre la importancia de configurar adecuadamente las opciones de privacidad en las plataformas que utilizan sus hijos; al gestionar su información personal y cómo interactúan con otros usuarios.

6.3.3 Buenas prácticas de ciberseguridad para los adolescentes del entorno estudiantil

Se busca que, con estas prácticas de ciberseguridad, los menores de edad de los grados 9º.10º y 11º, hagan efectivos sus derechos, en el entorno digital, por lo siguiente:

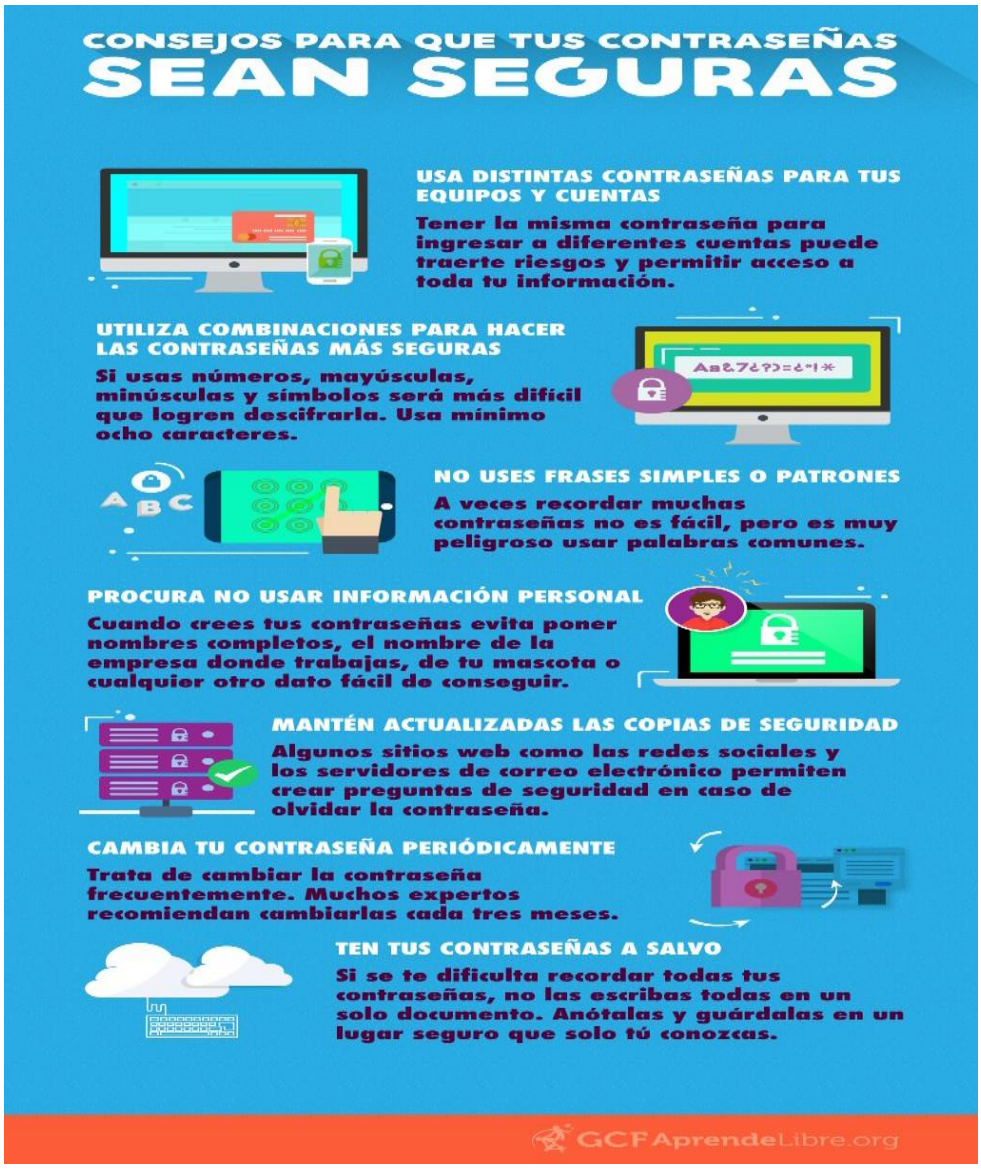
- La utilización de la tecnología es más frutífera si se realiza con fundamentos éticos y responsables.
- Insistir en que es un delito simular o falsear la identidad de otra persona.
- Entender que no es apropiado subir imágenes y vídeos a su sitio web, ni tampoco reenviar imágenes o videos que ha subido otra persona.
- Emplear un lenguaje adecuado en las diversas conversaciones.

Tabla 13. Prácticas de ciberseguridad para los adolescentes

RECOMENDACIONES
• Evitar la interacción con mensajes o correspondencia sospechosa; especialmente aquellos que son más atractivos y pueden conducir a enlaces que llevan a sitios fraudulentos. • Difundir o compartir falsedades, mofas o imágenes íntimas o de su vida personal y familiar. • No compartir las contraseñas, con sus amigos o colegas. • Acceso ilegal a bases de datos personales y destrucción de los mismos. • Evitar el diálogo con personas ajenas en línea. Si alguien desconocido trata de entrar en contacto; es necesario que el menor de edad notifique a un adulto de inmediato. • Rehúse suplantar identidad y proporcionar información que no es propia. • Escoja crear claves seguras y únicas para su cuenta, para ello es importante hacerse asesorar de sus padres. • Hay que recordar en no guardar sus contraseñas física o virtualmente, en un lugar al cual otros tienen acceso. Emplee contraseñas seguras con mayúsculas, minúsculas, números y símbolos. Posteriormente cambiarlas después de 30, 60 o 90 días.

Fuente: MALWAREBYTES. Consejos de Seguridad en Internet para Niños, Adolescentes. y Padres. .[Consultado: 12 noviembre,2023]. Disponible en: https://www.malwarebytes.com/es/cybersecurity/basics/internet-safety-tips-for-kids

Figura 16. Manejo de Contraseñas Seguras



Fuente: GCFGLOBAL.org. Seguridad en internet. ¿Cómo crear una contraseña segura? [Consultado el 10, noviembre, 2023]. Disponible en: https://edu.gcfglobal.org/es/seguridad-en-internet/como-crear-una-contrasena-segura/1/

6.3.3.1 Capacitación a los estudiantes en ciberseguridad

La formación continua, constante y adaptable al mundo digital en ciberseguridad no solo proporciona a los alumnos competencias técnicas, sino que también fomenta la cultura de seguridad en los centros educativos. Así, les facilita obtener las herramientas requeridas para desplazarse de forma segura en un mundo interconectado, salvaguardando su información y promoviendo un uso consciente de la tecnología. Los estudiantes aprenden a proteger su información personal, reconocer riesgos cibernéticos y responder de forma anticipada ante circunstancias inusuales, lo que resulta esencial en un ambiente tecnológico cada vez más complicado.

Para alcanzar este objetivo, es esencial que sea una regla en los centros educativos, incorporar la ciberseguridad en los currículos desde una edad temprana Impartir conocimientos acerca de la privacidad en internet, la protección de los datos y el comportamiento apropiado en el ambiente digital. Se hace necesario establecer programas de formación constante que mantengan a los niños y jóvenes al tanto de las amenazas más recientes y las mejores prácticas, para llevar a cabo:

- Estrategias educativas: la capacitación a los menores de edad se imparte a través de los siguientes parámetros y la orientación de todos los estamentos de educación y de hogar.
- Educación Práctica: clases interactivas donde los estudiantes pueden practicar técnicas de seguridad.
- Concientización: programas que abordan vulnerabilidades comunes como phishing, malware y gestión de contraseñas
- Recursos Online: plataformas como edX ofrecen cursos accesibles que cubren desde fundamentos hasta temas avanzados en ciberseguridad.

Contenidos de capacitación a estudiantes: en la siguiente tabla se propone unas temáticas y acciones que se pretende lograr con los estudiantes de los colegios.

Tabla 14. Temas de capacitación en ciberseguridad para estudiantes

TEMAS	SUBTEMAS	SE PRETENDE
HABILIDADES TÉCNICAS DIGITALES Y CIBERSEGURIDAD	Programación y desarrollo Web.	Formación encaminada a proteger su información personal, identificar amenazas cibernéticas y actuar ante situaciones sospechosas.
	Uso responsable de la Tecnología:	Educación sobre ética digital. Uso adecuado de las redes sociales y privacidad en línea.
JUEGOS INTERACTIVOS.	Riesgos en juegos en línea:.	Discusión sobre los peligros asociados con los videojuegos, incluyendo el grooming y el acoso, así como la importancia de reportar comportamientos inapropiados.
	Control parental:	Trabajo en Equipo: uso seguro de videojuegos. Información para que los padres pueden utilizar herramientas de control parental para supervisar la actividad en línea de sus hijos.
PROTECCIÓN DE LA INFORMACIÓN PERSONAL	Privacidad y compartir información:	Enseñar a los jóvenes a evitar divulgar datos personales, es decir, direcciones, números telefónicos o imágenes personales, en plataformas sociales y redes digitales.
	Robo de identidad:	Capacitación sobre cómo protegerse contra el robo de identidad y la importancia de mantener seguros sus datos personales.
RECONOCIMIENTO Y PREVENCIÓN DE ESTAFAS .	Phishing y estafas Online:	Actividades de capacitación para detectar correos electrónicos y mensajes sospechosos que buscan sustraer datos personales o financieros.
	Ofertas demasiado buenas para ser verdaderas:	Enseñar a los estudiantes a ser escépticos ante ofertas que parecen demasiado atractivas, ya que a menudo son estafas.
SEGURIDAD DE LA INFORMACIÓN PERSONAL .	Privacidad en redes sociales:	Instruir para mantener la privacidad y no compartir información personal sensible.
	Gestión de contraseñas:	Educar sobre la creación de contraseñas seguras y la importancia de no compartirlas.
COMPORTAMIENTOS SEGUROS EN LÍNEA .	Interacciones con desconocidos:	Implementar tareas prácticas en las que los alumnos realicen interacciones en línea y debatan sobre qué conductas son seguras y cuáles no.
	Juegos interactivos:	Utilizar juegos que enseñen a los niños y niñas a reconocer comportamientos seguros y peligrosos en internet.

Fuente: Líderes en Seguridad de la Información, Ethical Hacking y Seguridad en la Nube. Ciberseguridad en el sector de la educación. [Consultado el 15, noviembre, 2023]. Disponible en: https://www.cloudseguro.co/ciberseguridad-para-colegios-y-universidades/

6.3.4 Medidas de Protección Contra Amenazas Cibernéticas

En un ambiente donde las amenazas son constantes y cambian rápidamente, es imprescindible establecer estrategias de protección sólidas. Descripción de algunas tácticas fundamentales:

- Contraseñas fuertes

Las contraseñas deben ser complejas y aleatorias, evitando información personal como fechas de nacimiento o nombres familiares: incluir una combinación de letras mayúsculas, minúsculas, números y caracteres especiales aumenta significativamente la seguridad.

- Validación de dos elementos (2FA)

El sistema de doble factor de verificación ofrece una capa adicional de protección, requiriendo no solo una contraseña, solicita un segundo factor de verificación, que se fundamenta en un código enviado al dispositivo móvil.

- Actualización de Software

Actualización de programas informáticos. Es esencial mantener actualizado tanto el software como los sistemas operativos para reducir las brechas de seguridad. Generalmente, las actualizaciones incluyen mejoras que corrigen las vulnerabilidades identificadas en versiones anteriores.

- Seguridad perimetral

Es importante invertir recursos en cortafuegos, VPN (Redes Privadas Virtuales) y normativas de acceso estrictas para proteger el entorno digital de la compañía. Estas herramientas ayudan a prevenir ingresos no autorizados y a proteger la infraestructura interna.

- Uso de software de seguridad

Los antivirus, antimalware y programas antispam son esenciales para detectar y neutralizar amenazas antes de que puedan causar daño. Asegurarse de que estos programas estén actualizados y debidamente licenciados.

- Copias de respaldo

Tener respaldos constantes de todos los datos esenciales facilita una pronta recuperación en caso de un ataque. Garantizando la continuidad de la empresa y reduce el efecto de cualquier suceso de seguridad.

6.3.5 Netiqueta

Tener presente que los consejos de ciberseguridad no deben quedar en el papel, que es necesario vivenciarlo y para ello, en Tecnología se hace énfasis en la Netiqueta, referente a las normas de comportamiento que los usuarios de los servicios online establecen voluntariamente, para que exista excelente comunicación, colaboración en los diferentes servicios que se presta.

> La netiqueta comprende las normas de etiqueta en la red, lo que se debe que hacer y lo que no en la comunicación en línea. Son recomendaciones de comportamiento que se refieren a la cortesía en línea y las reglas informales del ciberespacio, un canal de comunicación más complejo al existir el cara a cara en contadas ocasiones (aunque cada vez son más frecuentes las conexiones como las videoconferencias) y conectar frecuentemente a usuarios desconocidos. La palabra netiqueta es un acrónimo coloquial del inglés «network etiquette», etiqueta de la red, un conjunto de convenciones sociales que facilitan la interacción a través de las redes, y que incluyen desde chats y correos eléctricos a blogs y foros.[29]

[29] ARIMETRICS. Netiqueta. (17 Febrero, 2022)).[sitio web].[Consultado: 25, noviembre, 2023]. Disponible en: https://www.arimetrics.com/glosario-digital/netiqueta

Figura 17. Recomendaciones Generales de Netiqueta

Fuente: UPCT.es Universidad Politécnica de Cartagena. Netiqueta. (s/f). [Consultado: 2, septiembre, 2023]. Disponible en: https://www.bib.upct.es/imagenes/final-Recomendaciones_generales_002.png

Figura 18. Netiqueta en redes sociales

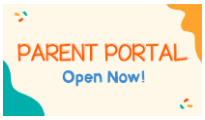
Fuente: Netiqueta. (s/f). Gobiernodecanarias.org. [imagen].[Consultado: 22, noviembre, 2023]. Disponible en: https://www3.gobiernodecanarias.org/medusa/contenidosdigitales/FormacionTIC/cdtic2014/03co/33_netiqueta.html

- Es primordial invertir en la educación desde la infancia y mantener el proceso para que los jóvenes utilicen las herramientas digitales de forma segura y consciente.
- La prevención a nivel familiar, la educación emocional y la comunicación son recursos eficaces para evitar la violencia, las repercusiones en su integridad física, mental y ética.
- Cuando se chatea con desconocidos, no hay que emplear la cámara web porque pueden estar grabando y ser utilizada para futuras extorsiones. Tener en cuenta que la imagen es un componente de la identidad digital y depende de cada uno el cuidado y protección.
- Cuando se juega online, se recomienda evitar escribir el nombre completo o usuario. En lugar de ello se puede hacer uso de sobrenombres; con el propósito de que desconocidos puedan ingresar a la información personal.
- Es importante realizar la denuncia penal, ésta es la mejor forma de contribuir para que el abusador no perjudique a toda una sociedad.
- Entonces se genera justicia social para la víctima y para los demás porque los abusadores agreden no sólo aún chico o chica; sino a varios.
- Una forma útil es guardar las pruebas del acoso como: conversaciones, diálogos, fotografías, mensajes, imágenes y almacenar esta información. Posteriormente todos estos datos son útiles para una futura investigación.
- Tener presente en revisar los dispositivos de los menores de edad: computadora, tableta o teléfono celular; lo productivo de esta acción es evitar el virus. Además, la reducción de las listas de contactos de las redes sociales y el reemplazo de claves de acceso son urgente.
- Analizar en conjunto el tipo de delito porque es diferente si se encontró con el acosador en línea o éste ya se realizó personalmente.

6.3.6 Plataformas Útiles Para Estudiantes

En la siguiente tabla pueden encontrar algunas plataformas útiles para estudiantes y que deben conocer no sólo el núcleo familiar sino también el núcleo académico.

Tabla 15. Plataformas Prácticas Para Estudiantes

PLATAFORMAS	EXPLICACIÓN	CARACTERÍSTICAS
FACEBOOK PARENTS PORTAL 	Web en la que recopilarán recursos para padres y madres.	• Red social que nació en el año de 1977. • Ayuda a mejorar la comunicación entre padres e hijos en lo que se refiere a seguridad online. • Disponible: facebook.com/safety/parents. • Presenta información para que hijos e hijas naveguen por Internet de forma segura. • Contiene vídeos y está traducido a 55 idiomas.
CANVAS 	Plataforma de diseño gráfico en línea, contenidos y cursos online. Creada en 2008 por dos estudiantes de posgrado.	• Crea fácilmente contenidos y cursos online. • Los afiches, las imágenes para redes sociales, las infografías, las presentaciones y hasta los videos se pueden crear. • Estimula la creatividad de los estudiantes. • Fomentar nuevas formas de pensar para generar una solución única y original. • Interfaz gráfica moderna y visualmente atractiva. • Adaptable a diferentes dispositivos.
GOOGLE CLASSROOM 	Herramienta insignia de Google para el aprendizaje online.	• Permite gestionar y crear las clases. • Asigna tareas. • Herramienta que es ideal para participar en entornos colaborativos. • Se necesita contar con una cuenta de Gmail.
EDMODO 	Plataforma digital, que funciona de forma similar a una red social.	• Puede ser utilizada por docentes, alumnos y padres de familia. • Permite compartir contenidos, textos, vídeos en las clases virtuales. • Plataforma educativa fundada en 2008. • Se puede gestionar actividades y las evaluaciones de forma fácil y ágil.
ENIALLY 	Herramienta online que permite la creación de contenido interactivo y animado.	• Da vida a las imágenes, a las tablas, a los gráficos y en unos pocos minutos. • El contenido se perfecciona con espectaculares efectos visuales. • Admite la creación de infografías, presentaciones, mapas mentales, certificados, entre otros. • En este nuevo aprendizaje niños, niñas y jóvenes son los protagonistas. • Integración con plataformas como Dropbox, Google Maps, Youtube, etc.

Fuente: GENIALLYBLOCK. Mejores plataformas educativas online para la formación y el aprendizaje.].[Consultado: 24, noviembre, 2023]. Disponible en: https://blog.genially.com/plataformas-educativas-online/

6.3.7 Estrategias de Ciberseguridad Propuestas al Gobierno Para Los Estudiantes de Colegios

Teniendo en cuenta que el gobierno tiene compromiso de establecer aspectos relacionados con la ciberseguridad y protección de la información, debido a que los estudiantes de entidades educativas son víctimas por los diferentes ciberdelincuentes.

Se necesita implementar políticas efectivas que protejan a estudiantes de edad escolar en el ámbito de la ciberseguridad, que les garanticen un entorno digital seguro, donde ellos puedan explorar, aprender en internet sin riesgos y fomentar la creación de programas de formación en ciberseguridad.

Se consideran las siguientes propuestas para analizar, revisar e implementar:

- Mediante ciertos medios de comunicación convencionales o digitales, fomentar una sensibilización pública acerca de la ciberseguridad entre los ciudadanos y dentro de las instituciones educativas.
- Presentar y llevar a cabo proyectos de ciberseguridad en los que participen instituciones educativas de carácter público y privado.
- Aplicación de estrategias de seguridad en las instituciones educativas como el cifrado de datos y la verificación basada en múltiples factores.
- Diseñar y ejecutar un plan de seguridad informática, que contemple: objetivos, prioridades y responsables.
- Formación constante al personal de diversas instituciones o empresas en temas de ciberseguridad por parte de personal especializado; mediante prácticas y seminarios relacionados con el tema de ciberseguridad para los colegios.
- Crear y exponer planes de protección a corto y largo plazo ante ataques informáticos u otros eventos que puedan poner en riesgo la seguridad de los jóvenes.
- Contar con becas que faciliten la formación de personal y especialistas en Ciberseguridad.
- Implementar tecnologías asociadas en esta estrategia con la Inteligencia Artificial (IA).
- Establecer un sistema de monitoreo con los equipos más avanzados y personal cualificado para detectar y reaccionar de manera rápida ante las amenazas cibernéticas.
- Gestionar y garantizar el Internet de las cosas (IoT) en aparatos vinculados con esta tecnología.

7 CONCLUSIONES

Se puntualizó en que los grupos más vulnerables ante los riesgos y amenazas que existen en el ciberespacio son los menores edad como: ciberacoso, grooming, sexting, phishing, malware, el robo de identidad o la suplantación que perjudicaron en forma negativa su desarrollo físico, emocional y social; incidiendo en su reputación, autoestima y confianza.

Se enfatizó en que los datos son esenciales en educación porque facilitan la toma de decisiones en momentos oportunos, en forma personalizada se podrá monitorear el progreso estudiantil, fomentar la mejora continua e impulsar la innovación y la transformación significativa de la experiencia educativa.

Al estar expuestos y en contacto con diferentes distracciones como: televisión, videojuegos, computadoras, teléfonos inteligentes y otras pantallas; incluyendo el acceso a redes sociales y videos.

Las principales tácticas de phishing encierran el uso de ingeniería social, sitios web fraudulentos, ataques por correo electrónico y redes sociales, técnicas más específicas como el “catphishing” y empleo de cuentas de LinkedIn comprometidas.

A través de diferentes imágenes y argumentos se señaló sobre las diferentes recomendaciones en los casos de grooming y phishing con el propósito de proteger a los menores de edad de los riesgos y peligros, al interactuar con otros, al subir o buscar contenido, fotos o brindar información personal.

Se justificó los peligros y riesgos a los que están expuestos los menores de edad de los grados 9º, 10º, y 11º, de Básica Secundaria, quienes en diferentes situaciones se exponen más fácilmente a las amenazas del mundo digital porque accedieron a sitios web como: youtube, videojuegos y redes sociales, sin supervisión de padres de familia o personas a cargo.

Se reiteró que los profesores, los padres de familia y los estudiantes, de acuerdo con su rol y contexto continúen contribuyendo en la construcción de las buenas prácticas de ciberseguridad para lograr una sana cultura digital, en forma responsable y segura.

Se hizo hincapié en protegerse de estos ataques, los jóvenes deben ser conscientes de las técnicas de manipulación utilizadas por los ciberdelincuentes y tomar medidas para evitar compartir información confidencial, credenciales de usuario o contraseñas, no responder a correos electrónicos sospechosos ni proporcionar información personal a desconocidos.

Se determinó que, en los menores de edad, la ingeniería social presenta una gama de técnicas como: la carnada, vishing, phising, manipulación cara a cara, farming, entre otros que buscan con el engaño y a través de diferentes métodos como llamadas extrañas, solicitudes de amistad, adquirir contraseñas, datos personales, accesos no autorizados

o hacerse pasar por algún amigo y todo con un solo fin, ganarse la confianza y atacar la seguridad informática.

Se verificó y comprobó los diferentes proyectos de ley establecidos por la justicia colombianas, orientados a velar por la integridad de los menores de edad, que están encaminados a regular el acceso a redes sociales y plataformas digitales, con el objetivo de protegerlos de conductas perjudiciales al estar conectados en línea.

Se enfatizó en la temática relacionada con las diferentes plataformas que son útiles para estudiantes, padres de familia y docente; complementando la formación en ciberseguridad.

8 RECOMENDACIONES

Capacitar a docentes y padres de familia en protección de datos para supervisar en línea las actividades de los menores de edad, pero también para poder orientar a los jóvenes en los peligros inherentes de la navegación en línea y estar preparados en la problemática de los delitos informáticos en todas sus modalidades.

Establecer en el entorno familiar y educativo, unas normas de seguridad en línea, con el objetivo de garantizar su protección y tranquilidad y también es fundamental el apoyo de las entidades gubernamentales, para que entre todos se genere el respeto de la identidad y cultura digital, construyendo así, las buenas prácticas de ciberseguridad.

Invertir en la educación desde que son niños y niñas y continuar el proceso en los adolescentes, para el uso responsable y seguro de herramientas digitales porque es necesario una mejor educación, en la cual los forjadores del conocimiento sean docentes comprometidos tanto académica, humana y espiritual, es decir, con bases sólidas para orientar a los colombianos del presente y del futuro.

Orientar a los estudiantes de los grados 9º, 10º y 11º, en temas relacionados con la seguridad en las redes sociales, los peligros en línea que pueden perjudicar la integridad emocional y física; pero es urgente saber identificar el contenido apto para los menores de edad porque el peligro no está en la propia red como tecnología, sino en el uso que cada usuario le proporcione, o en las buenas o malas intenciones.

Es fundamental designar un grupo responsable, con los profesionales pertinentes para la creación de un canal, en el cual se dé a conocer los incidentes de ciberviolencia, ciberbullying e ingeniería social; con el único propósito de que los menores de edad y padres de familia logren informarse sin restricciones sobre las diferentes situaciones, los peligros a los que están expuestos y aplicar las medidas necesarias para su protección y seguridad.

Colaboración entre autoridades de infancia y adolescencia y proveedores de servicios para revelar y notificar en forma inmediata situaciones de ciberviolencia y ciberbullying; buscando alternativas inmediatas para la protección de los menores de edad.

BIBLIOGRAFÍA

AGUILAR, Mariana. Riesgos de ciberseguridad. qué son, ejemplos y cómo prevenirlos. [sitio web]. [Consultado 12 mayo de 2024]. Disponible en: https://www.deltaprotect.com/blog/riesgos-de-ciberseguridad-ejemplos-y-prevencion

ARIMETRICS. Glosario digital. (s/f). Una guía completa del concepto, tipos, amenazas y estrategias. [sitio web]. [Consultado 12 abril de 2023]. Disponible en: https://www.arimetrics.com/glosario-digital

BITSO BLOG Colombia, (2023, 30 de octubre). Tipos de Riesgos de Ciberseguridad más Comunes [sitio web].[Consultado 10 diciembre de 2024]. Disponible en: https://blog.bitso.com/es-co/seguridad-co/tipos-de-riesgos-de-ciberseguridad

CHACON, Paola. Ciberbullying: ONU reveló los altos índices de este delito que se presentan en Colombia. [sitio web]. [Consultado 8 marzo de 2023]. Disponible en: https://www.infobae.com/colombia/2023/03/08/ciberbullying-onu-revelo-los-altos-indices-de-este-delito-que-se-presentan-en-colombia/

CIBERSEGURIDAD. (s/f). Infosecuritymexico.com, [sitio web]. [Consultado 12 abril de 2023]. Disponible en: https://www.infosecuritymexico.com/es/ciberseguridad.html

CISCO.com, ¿Qué es un firewall? (23 de septiembre de 2021). [sitio web]. [Consultado 12 enero de 2025]. Disponible en: https://www.cisco.com/c/en_ca/products/security/firewalls/what-is-a-firewall.html

COLOMBIA.com, Consejos de Seguridad Informática Para Niños y Jóvenes. [sitio web]. Disponible en: https://www.colombia.com/tecnologia/informatica/sdi/57401/consejos-de-seguridad-informatica-para-ninos-y-jovenes

DATADOG Centro de Conocimiento. ¿Qué es un SIEM? [sitio web]. Cómo funciona y casos de uso. [Consultado 10 enero de 2025]. Disponible en: https://www.datadoghq.com/knowledge-center/siem/

DAYTONA. Cloud, Conceptos Generales de la protección de datos personales y la importancia de la seguridad de la información. [sitio web]. [Consultado 12 abril de 2023]. Disponible en: https://daytona.cloud/proteccion-de-datos-personales.html

DE GODADDY, (26 de julio 2024). Firewall: Qué es, cómo funciona y su importancia en la seguridad informática. [sitio web]. [Consultado 15 enero de 2025]. Disponible en: https://www.godaddy.com/resources/latam/seguridad/firewall-que-es-como-protege-red

DIDÁCTICA. (2023, 13 de septiembre). Protección de datos y privacidad en la educación en línea [en línea]. [Consultado 14 diciembre de 2024]. Disponible en:

https://asociaciondidactica.es/como-garantizar-proteccion-datos-y-privacidad-en-educacion-en-linea/

DOCUSIGN. Seguridad Digital y Ciberseguridad: ¡aprende todo sobre estos conceptos! (3 marzo 2020). [sitio web]. [Consultado 12 abril de 2023]. Disponible en: https://www.docusign.mx/blog/seguridad-digital-y-ciberseguridad

FUNDACION SAVE THE CHILDREN. Qué es, Cómo Detectarlo y Prevenirlo 1 de Julio de 2019. [sitio web]. [Consultado 18 junio de 2023]. Disponible en: https://www.savethechildren.es/actualidad/grooming-que-es-como-detectarlo-y-prevenirlo

GOV. Cómo prevenir los riesgos en el entorno digital: 10 recomendaciones en el Día del Internet Seguro. (10 de febrero de 2020). [sitio web]. [Consultado 22 junio de 2023]. Disponible en: https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/125836:Como-prevenir-los-riesgos-en-el-entorno-digital-10-recomendaciones-en-el-Dia-del-Internet-Seguro

GOV.CO. Ley 2489 de 2025 Congreso de la República. [sitio web]. [Consultado 12 septiembre de 2025]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=260756

IBM. ¿Qué es el phising? Informando a niños y jóvenes sobre los riesgos en Internet. (24 de septiembre de 2021). [sitio web]. [Consultado 26 junio de 2023]. Disponible en: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/182632:En-TIC-Confio+-una-decada-informando-a-ninos-y-jovenes-sobre-los-riesgos-en-Internet

IBM. ¿Qué es el Ransomware? [sitio web]. [Consultado 26 junio de 2023]. Disponible en: https://www.ibm.com/es-es/topics/ransomware

INSTITUTO FEDERAL DE COMUNICACIONES. Guía para prevenir el Pharming. [sitio web]. Disponible en: https://ciberseguridad.ift.org.mx/files/guias_y_estudios/guia_prevenir_pharming_vf1.pdfP

LATAM.KASPERSKY, ¿Qué es un firewall? Funcionamiento de los firewalls y tipos de firewalls. [sitio web]. [Consultado 14 enero de 2025]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/firewall?srsltid=AfmBOooWAYQk5DudYzgKqEFdlinUMESdlbevl4NcNo53DB5oTa88RdqW

LISA Institute. Guía práctica de control parental: consejos, ventajas y herramientas para prevenir los riesgos de Internet para tus hijos. [sitio web]. Disponible en: https://www.lisainstitute.com/blogs/blog/guia-practica-control-parental-hijos-consejos-ventajas-herramientas-riesgos

MICROSOFT.com, ¿Qué es SIEM? (s/f). [sitio web]. [Consultado 11 enero de 2025]. Disponible en: https://www.microsoft.com/es-co/security/business/security-101/what-is-siem

MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. MINTIC Le dice no al acoso escolar y reafirma su compromiso para prevenir el bullying. [sitio web]. Disponible en: https://mintic.gov.co/chicassteam/801/w3-article-210272

MINTIC Colombia. ¡Pilas con los datos personales en la vida digital! (2020). [sitio web]. [Consultado 12 junio de 2024]. Disponible en: https://www.mintic.gov.co/portal/inicio/Sala-de- prensa/Noticias/125647:Pilas-con-los-datos-personales-en-la-vida-digital

M, Omar Antonio. Los 10 Mejores Filtros del Contenido de Internet | Filtrado Web que Funciona al. [sitio web]. Disponible en: https://famisafe.wondershare.com/es/internet-filter/best-internet-content-filters

PECH, Xenia. ¿Es adictiva la tecnología? [sitio web]. [Consultado 29 noviembre de 2023]. Disponible en: https://blog.laminasyaceros.com/blog/es-adictiva-la-tecnolog%C3%Ada

Programa educativo Foro Nativos Digitales. Redes Sociales y Adolescentes. Secretaría General de Educación. Consejería de Educación y Empleo. [sitio web]. Disponible en: https://emtic.educarex.es/nativosdigitales_materiales/pildoras_familias/rrssyadolescentes/suplantacin_de_identidad.html

RANSOMWARE. (2018). Malware bytes. [sitio web]. [Consultado 30 noviembre de 2023]. Disponible en: https://es.malwarebytes.com/ransomware/

RIOS HERNANDEZ, Neftalí. LUZARDO BRICEÑO, Marianela. ¿riesgoso o inofensivo?: validación de una escala de sexting con estudiantes de secundaria. en Colombia. . [sitio web]. Disponible en: https://revistacriminalidad.policia.gov.co:8000/index.php/revcriminalidad/article/view/369/703#toc

SEMANA. Lanzan estrategia para prevenir el 'Grooming', el 'Sexting' y el ciberacoso en Bogotá: este año ya van 214 capturados. Bogotá. [sitio web]. [Consultado 20 septiembre de 2023]. Disponible en: https://www.semana.com/nacion/bogota/articulo/lanzan-estrategia-para-prevenir-el-grooming-el-sexting-y-el-ciberacoso-en-bogota-este-ano-ya-van-214-capturados/202324/

SENTINELONE, Las 9 mejores herramientas SIEM de código abierto para 2025. (25 de noviembre de 2024). [sitio web]. [Consultado 12 enero de 2025]. Disponible en: https://www.sentinelone.com/cybersecurity-101/data-and-ai/open-source-siem-tools/

TUS ABOGADOS & CONTADORES. Acciones que son consideradas un delito informático en Colombia. [sitio web]. [Consultado 12 junio de 2024]. Disponible en: https://tusabogadosycontadores.co/blog/acciones-que-son-consideradas-un-delito-informatico-en-colombia/

UNIR. La Universidad en Internet. ¿Qué es la seguridad informática y cuáles son sus tipos? (15 / 06 / 2021). [sitio web]. [Consultado 13 junio de 2024]. Disponible en: https://ecuador.unir.net/actualidad-unir/que-es-seguridad-informatica/

UNIR Revista, ¿Qué son los Sistemas de Gestión de Eventos e Información de Seguridad? [sitio web]. [Consultado 12 enero de 2025]. Disponible en: https://www.unir.net/revista/ingenieria/siem-gestores-eventos-seguridad/

Anexo A. Video Socialización de la opción de Grado II

https://drive.google.com/file/d/1pRpeQ190QaZhrlwO9jdoZhOB1_AmvfNt/view?usp=sharing