CUADERNOS ETITC

Fundamentos de **Ciberseguridad**

Escuela Tecnológica
Instituto Técnico Central
Establecimiento Público de Educación Superior

Miguel Hernández Bejarano

Luis Eduardo Baquero Rey

CUADERNOS ETITC
© Junio 2025
ISBN DIGITAL 978-628-97163-0-6

CONSEJO DIRECTIVO
Dra. Adriana María López Jamboos
Delegada del Ministerio de Educación.
Hno. Edgar Figueroa Abrajim
Delegado del Sr. Presidente de la República.
Dr. Lukas Alberto Cruz Mora
Delegado del Sr. Gobernador de Cundinamarca.
Hno. Ariosto Ardila Silva
Rector.
Dr. Miguel Manrique Córdoba
Representante de los Exrectores.
Ing. Andrea García Rivas
Representante de los Docentes.
Ing. Henry Jinete Márquez
Representante de las Directivas Académicas.
Ing. Juan Miguel Santana Ortiz
Representante del Sector Productivo.
Ing. Walter Mauricio Useche Ruiz
Representante de los Egresados.
Julián David Vera Osorio
Representante de los Estudiantes.
Edgar Mauricio López Lizarazo
Secretario Técnico del Consejo Directivo.
Secretario General.

CONSEJO ACADÉMICO
Hno. Ariosto Ardila Silva
Rector.
Hno. Néstor Raúl Polanía González
Vicerrector Académico.
Dra. Luisa Marina Gómez Torres
Vicerrectora Investigación, Extensión y Transferencia.
Dr. Ariel Tovar Gómez
Vicerrector Administrativo y Financiero.
Ing. Carlos Alberto Cerón
Representante Áreas Académicas.
Ing. Ángela María García Mora
Decana Facultad de Procesos Industriales.
Ing. Héctor Ricardo Amaya Barbosa
Decano Facultad de Electromecánica.
Ing. Lady Fajardo Castellanos
Decana Facultad de Mecánica.
Ing. Henry Alberto Jinete Márquez
Decano Facultad de Mecatrónica.
Ing. María Nury Escobar Guzmán
Decana Facultad de Sistemas.
Ing. Alexander Sabogal Rueda
Representante de los Docentes.
Brayan Yesid Jurado Gutiérrez
Representante de los Estudiantes.
Ing. Wilson Ramiro Camargo Cardozo
Coordinador de los Programas de Especializaciones
Edgar Mauricio López Lizarazo
Secretario Técnico del Consejo Académico.
Secretario General.

CONSEJO EDITORIAL
Hno. Ariosto Ardila Silva
Rector.
Hno. Néstor Raúl Polanía González
Vicerrector Académico.
Dra. Luisa Marina Gómez Torres
Vicerrectora Investigación, Extensión y Transferencia
Adm. Ariel Tovar Gómez
Vicerrector Administrativo y Financiero
Ing. Ángela María García Mora
Decana designada por el Consejo Académico.
Ing. Jaime Alberto Páez Páez
Profesor designado por el Consejo Académico.
Prof. María Alejandra Millán Ramírez
Profesional responsable de publicaciones.

CUADERNOS ETITC
Dra. Luisa Marina Gómez Torres
Directora
María Alejandra Millán Ramírez
Editora
Elvira Rosa Aguilar Bustamante
Corrección de estilo
Poligrama
Diagramación

CUADERNOS ETITC es una publicación de la Escuela Tecnológica Instituto Técnico Central, dedicada a la difusión de sus prácticas académicas. Los contenidos publicados no reflejan necesariamente la posición de la Institución ni de la propia publicación. La Institución no se responsabiliza por las ideas y conceptos expresados por los autores de los trabajos publicados. Se autoriza la reproducción total o parcial del contenido, siempre que se cite la fuente y se respeten las normas sobre derechos de autor y propiedad intelectual.

CONTACTO
revistaletrasetitc@itc.edu.co
ESCUELA TECNOLÓGICA
INSTITUTO TÉCNICO CENTRAL

Contenido

Introducción **5**

1. Elementos de ciberseguridad 6

1.1 Ciberseguridad 6

1.2 Seguridad de la información 7

1.3 Los principios de la ciberseguridad 8

1.4 Tecnologías que apoyan la ciberseguridad 9

1.5 Tipos de ataques 11

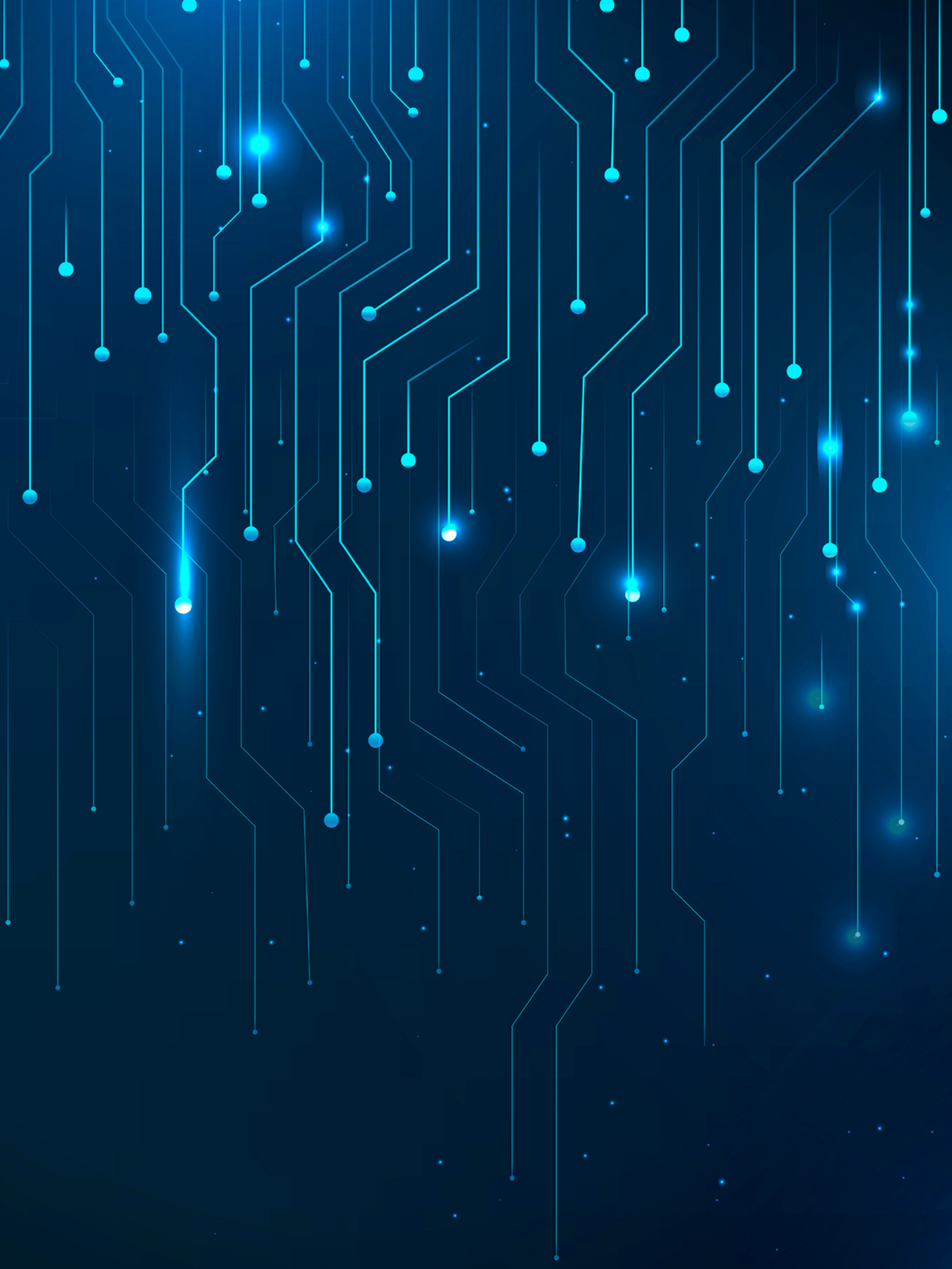
1.6 Grupos delictivos cibernéticos 14

1.7 Fraudes por computadoras 15

1.8 Falsificaciones informáticas 16

1.9 Actividades 18

Referencias **22**



Introducción

En la era digital contemporánea, la ciberseguridad se ha consolidado como un elemento esencial para salvaguardar la información y los sistemas de las organizaciones. La seguridad de la información abarca un conjunto de prácticas y tecnologías diseñadas para salvaguardar los datos contra accesos no autorizados, alteraciones y destrucción. A medida que las empresas y los individuos hacen uso cada vez más de la tecnología, la comprensión de los principios de la ciberseguridad se vuelve esencial para mitigar riesgos y proteger activos valiosos.

Los tipos de ataques cibernéticos son diversos y evolucionan constantemente, desde malware y phishing hasta ataques informáticos. Estos ataques no solo comprometen la integridad de la información, sino que también pueden tener repercusiones financieras y reputacionales significativas. Las organizaciones delincuenciales, que operan en la sombra de la web, aprovechan estas vulnerabilidades para llevar a cabo fraudes informáticos y otras actividades ilícitas, lo que subraya la exigencia de una supervisión continua y de estrategias de defensa robustas (Yirui et al., 2023).

Las amenazas cibernéticas son omnipresentes y pueden surgir de diversas fuentes, incluyendo actores maliciosos y errores humanos. Identificar y evaluar estos riesgos es crucial para desarrollar un enfoque proactivo en la ciberseguridad. Las organizaciones deben implementar políticas y procedimientos que no solo respondan a incidentes, sino que también prevengan su ocurrencia mediante la educación y la concienciación de los colaboradores de la organización acerca de las mejores prácticas de seguridad (Mohammed et al., 2024).

Para reforzar los temas abordados, se desarrollarán una serie de actividades prácticas que permitirán a los participantes aplicar los conceptos aprendidos. Estas actividades incluirán temas de ataques, y talleres sobre la identificación de vulnerabilidades. A través de este enfoque práctico, se busca no solo aumentar el conocimiento teórico, sino también fomentar habilidades prácticas que fortalezcan la capacidad de respuesta ante incidentes de ciberseguridad.

1. Elementos de ciberseguridad

1.1 Ciberseguridad

La ciberseguridad es un conjunto de tecnologías y métodos que buscan salvaguardar las redes de computadores, los sistemas conectados a la Internet, las aplicaciones de software y los datos frente a ataques, accesos no autorizados, cambios o daños (Macas, Wu, & Fuertes, 2022).

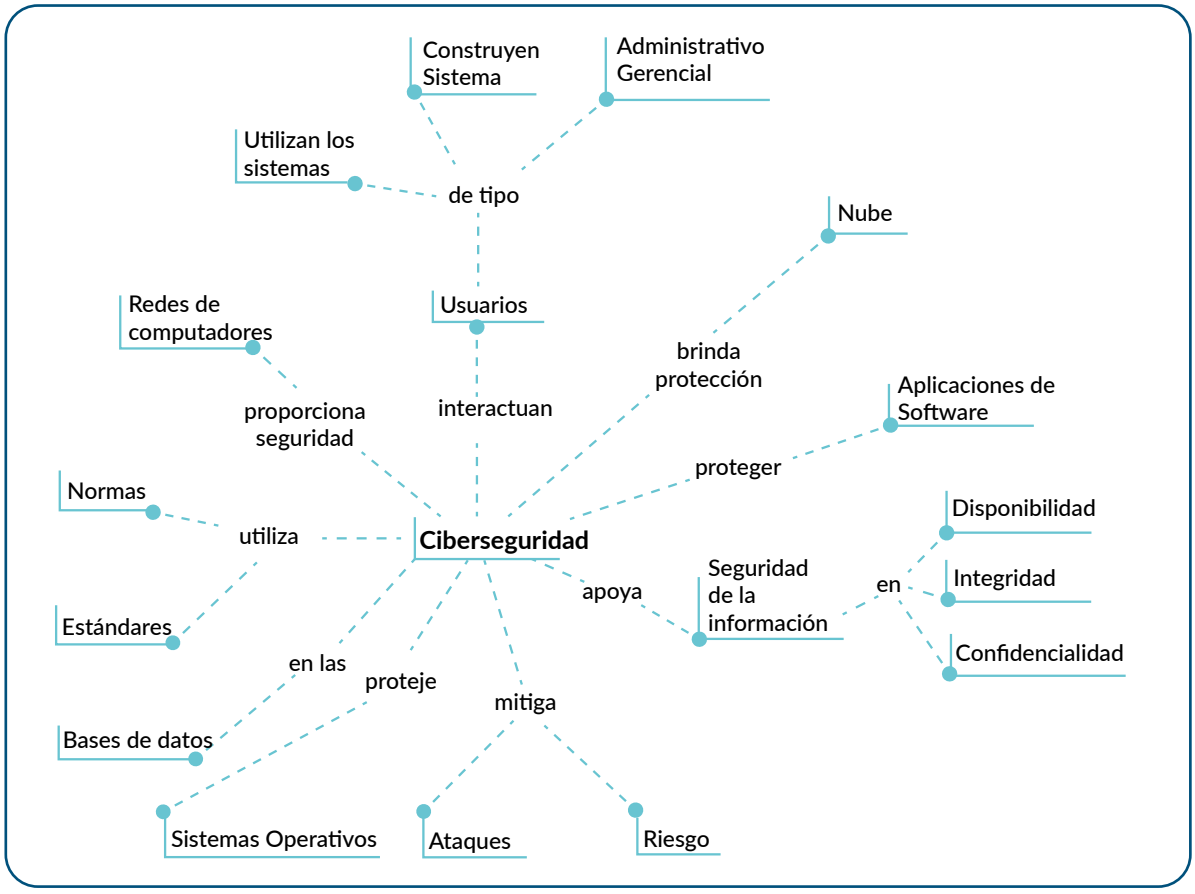
La ciberseguridad proporciona técnicas, estándares, políticas, configuraciones y recomendaciones para proteger los activos de los sistemas clásicos. Según los fundamentos de la tríada CIA (confidencialidad, integridad y disponibilidad) y las estructuras de dominio actuales utilizadas en los sistemas de infraestructura (Abushgra, 2023). Asimismo, la ciberseguridad es una forma de proteger los sistemas informáticos y las redes conectadas de ataques digitales, robos en línea y daños a los datos. Implica una combinación de tecnologías, procesos y políticas diseñadas para proteger los sistemas y evitar el acceso no autorizado a los datos, así como restaurar y recuperación de los sistemas en casos de un incidente de seguridad (Dwivedi et al., 2023).

En este sentido, la ciberseguridad propende por establecer medidas para evitar la ejecución de procesos no autorizados cuyos efectos pueden comprometer el sistema informático de una organización poniendo en riesgo la continuidad del negocio, en otra palabra se busca blindar las infraestructuras tecnológicas y de comunicación que respaldan las operaciones de una organización que hace uso de hardware y software.

En la Figura 1, se presenta un mapa conceptual en el contexto de la ciberseguridad esencial para proteger a todos los usuarios, desde los administrativos y creadores de sistemas hasta los usuarios finales. Las redes de computadores deben estar bien protegidas para evitar accesos no autorizados y ataques. La computación en la nube ofrece flexibilidad y escalabilidad, pero también requiere acciones de seguridad sólidas para resguardar la información almacenada. Los sistemas operativos y las bases de datos son objetivos frecuentes de ataques, por lo que es crucial mantenerlos actualizados y bien configurados.

Las aplicaciones de software deben desarrollarse teniendo en cuenta la seguridad, siguiendo normas y estándares reconocidos. La seguridad de la información consiste en salvaguardar los datos frente a riesgos y ataques mediante el uso de tecnologías avanzadas y buenas prácticas. Identificar y mitigar vulnerabilidades es una tarea continua para asegurar la integridad y confidencialidad de la información. Implementar políticas de seguridad y capacitar a los usuarios sobre las mejores prácticas es fundamental para crear un entorno digital seguro.

Figura 1. Contexto de la ciberseguridad



Nota. Mapa conceptual de ciberseguridad que visualiza las relaciones entre conceptos clave como ataques, usuarios, normas y estándares, facilitando la comprensión y gestión integral de la seguridad informática. Este enfoque ayuda a identificar y mitigar riesgos de manera efectiva. Fuente: propia.

1.2 Seguridad de la información

La seguridad de la información (SI) es un tema de actualidad a nivel mundial que afecta a todas las empresas. Consiste en un conjunto de estrategias diseñadas para proteger la información digital y no digital, y para detectar y prevenir incidentes. Se basa en los principios de confidencialidad, integridad y disponibilidad (Lundgren & Möller, 2019).

Cada organización adopta sus propias normativas de SI. Uno de los sistemas más adoptados se basa en la norma ISO 27001 (Ádám, Honfi & Bárkányi, 2024).

Para la Universidad Libre (Libre, 2023) se define como el conjunto de acciones preventivas y de respuesta del individuo, la entidad y las tecnologías, orientadas a salvaguardar la información y para garantizar que la seguridad la misma es gestionada correctamente, y dando, cumplimiento a las características de confidencialidad, integridad y disponibilidad de la información como un activo de la entidad.

En consecuencia, su ámbito de actuación abarca el análisis de riesgos, la seguridad del personal, la protección física y ambiental, la gestión de comunicaciones, el desarrollo y mantenimiento de sistemas, el control de accesos, la gestión de incidentes y la continuidad del negocio, entre otros de acuerdo con la ISO 27000 (Javier, 2012).

Es necesario recalcar que brindar un nivel de protección absoluto es inviable, incluso con un presupuesto ilimitado. El objetivo de un sistema de gestión de la seguridad de la información es, por lo tanto, asegurar que los riesgos asociados a la seguridad de la información sean identificados, asumidos, gestionados y reducidos por la organización de manera documentada, sistemática, estructurada, replicable, eficiente y ajustada a las variaciones en los riesgos, el entorno y las tecnologías (ISO-27000, 2023).

1.3 Los principios de la ciberseguridad

En un entorno cada vez más interrelacionado, en el que los datos han adquirido el estatus de un recurso de valor incalculable, la ciberseguridad ha adquirido una importancia crucial. Para las personas y las organizaciones, proteger sus datos y sistemas informáticos de las amenazas digitales es una necesidad imperiosa.

En este contexto, los principios de la ciberseguridad se erigen como pilares fundamentales para establecer estrategias de protección efectivas para resguardar los sistemas y la información de una organización frente a riesgos y agresiones cibernéticas. Estos principios, comúnmente conocidos como CIA, son:

Los principios de la ciberseguridad son fundamentales para proteger los sistemas e información de una empresa frente a amenazas y ataques cibernéticos. Estos principios son:

- **Confidencialidad:** Este principio se enfoca en preservar la confidencialidad de los datos, garantizando que únicamente las personas autorizadas tengan acceso a la información. La confidencialidad implica tomar medidas para evitar el acceso no autorizado a los datos, aunque es importante reconocer que no se puede garantizar una protección del 100% (Universitat Carlemany, 2024) (International Business Machines Corporation, IBM), (2022).
- **Integridad:** Este principio hace referencia a la salvaguarda de la información, contra cualquier tipo de modificación o corrupción no autorizada. La integridad ase-

gura que los datos se mantengan consistentes y precisos, y que los sistemas de la organización estén protegidos contra ataques e intrusiones. Esto incluye la protección de la información almacenada y su correcto funcionamiento sin intervención externa (IBM, 2022).

- **Disponibilidad:** Este principio se relaciona con la accesibilidad de la información y los sistemas de la organización. La disponibilidad garantiza que los datos y sistemas estén disponibles cuando se necesiten, evitando interrupciones en las operaciones de la organización. Esto implica implementar protocolos y procedimientos para minimizar el tiempo de inactividad del hardware y resolver problemas de software (IBM, 2022).
- **Autenticidad:** Aunque no se menciona explícitamente en las fuentes proporcionadas, la autenticidad es un principio crucial en la ciberseguridad. Este principio hace referencia a la verificación de la identidad de los usuarios y sistemas, con el fin de garantizar que únicamente las entidades autorizadas puedan acceder a los recursos e información. La autenticidad es fundamental para prevenir el acceso no autorizado y garantizar la seguridad de la información.

Además de estos principios básicos, existen otros aspectos importantes a considerar en la ciberseguridad, como el no repudio, que garantiza que las acciones realizadas en un sistema informático puedan ser asignadas a un usuario concreto (Shin et al., 2014).

La implementación de estos principios requiere un enfoque multidisciplinario que incluya la educación y sensibilización de los empleados, la definición y distribución de normas y procedimientos, la implementación de medidas de seguridad técnicas, y el cumplimiento de la legislación vigente (La Universidad Internacional de la Rioja), (2023). La ciberseguridad es esencial en la era digital contemporánea, donde los datos son el recurso más valioso y las amenazas cibernéticas son constantes. La no aplicación de estos principios puede resultar en pérdida de datos, crisis de reputación, pérdidas económicas y sanciones legales (UNIR, 2023).

En definitiva, los principios de la ciberseguridad constituyen la base para construir un mundo digital más seguro y confiable, donde la información se proteja y se utilice de manera responsable.

1.4 Tecnologías que apoyan la ciberseguridad

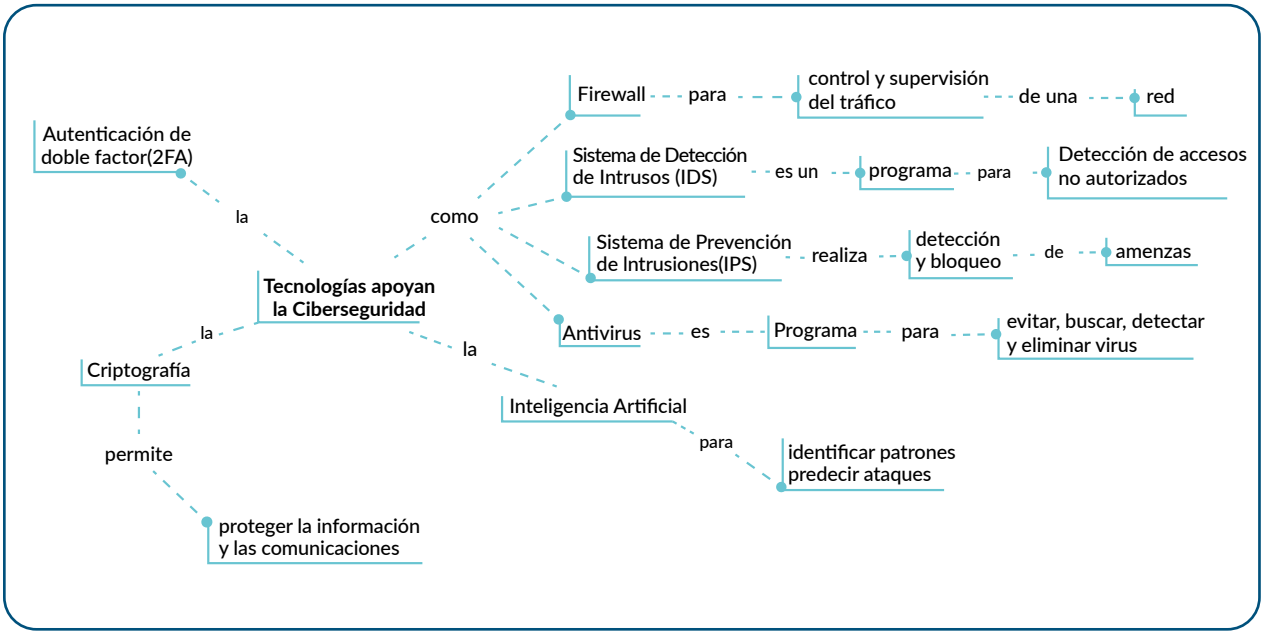
En la Figura 2 se presenta algunas tecnologías que apoyan la ciberseguridad como: Los firewalls funcionan como una barrera entre redes internas protegidas y redes externas no confiables, filtrando el tráfico según reglas de seguridad previamente establecidas. Los Sistemas de Detección de Intrusiones (IDS) y los Sistemas de Prevención de Intrusiones (IPS) complementan esta capa de seguridad al supervisar y analizar el tráfico de la red en busca de actividades sospechosas o dañinas. Mientras los IDS alertan sobre

posibles amenazas, los IPS pueden implementar medidas automáticas para bloquear los ataques en tiempo real, reforzando así la protección perimetral de la organización.

La autenticación de doble factor (2FA) implanta una capa extra de protección al exigir dos métodos de autenticación antes de otorgar acceso a sistemas o datos. Esto disminuye considerablemente el riesgo de acceso no autorizado, incluso en caso de que las credenciales de un usuario sean comprometidas (Zhenhua y Jun, 2024). La criptografía, por otro lado, protege la información mediante el cifrado de datos, asegurando que solo las partes autorizadas puedan descifrar y acceder a la información sensible. Estas tecnologías son esenciales para preservar la confidencialidad y la integridad de los datos en un entorno digital cada vez más amenazado (Vasile & Svasta, 2019).

Así mismo, la inteligencia artificial (IA) apoya la ciberseguridad mediante la identificación y mitigación de amenazas en tiempo real. Utiliza algoritmos avanzados para examinar grandes cantidades de datos, detectar comportamientos anómalos y anticipar posibles incidentes de seguridad. Esta capacidad proactiva permite a las organizaciones fortalecer sus defensas y mitigar riesgos de manera más eficiente (Calvin, 2024). A su vez, estas otras tecnologías serán abordadas con mayor profundidad en otro cuaderno.

Figura 2. Tecnologías que apoyan la ciberseguridad



Nota. Mapa conceptual de tecnologías que apoyan la ciberseguridad ilustra cómo herramientas como firewalls, sistemas de detección de intrusos, antivirus y soluciones de cifrado trabajan en conjunto para proteger la infraestructura digital. Este enfoque

facilita la identificación de brechas y la implementación de estrategias de defensa efectivas. Fuente: propia.

1.5 Tipos de ataques

Un ataque corresponde a una conexión válida que involucra herramientas, vulnerabilidades, eventos y resultados no autorizados, son los administradores de los sistemas quienes determinan que es lo que está autorizado y que no, mediante la definición de políticas de seguridad (Ortiz et al., 2016).

Un ataque informático es un acto constituido e intencionado por una o más personas agrupadas en organizaciones para causar daño o problemas a un sistema informático o red. Los ataques se pueden llevar a cabo en corporaciones o empresas, explotando vulnerabilidades o fallos en el software, hardware e incluso en los individuos que integran un entorno informático, con el fin de obtener un beneficio, generalmente económico, y generando un impacto adverso en la seguridad del sistema, algunos tipos de ataque según Fabián, (2013) algunos de estos pueden ser:

Interrupción: El ataque logra ocasionar una interrupción en la continuidad de un servicio, como la inaccesibilidad del servidor web, la desaparición del disco en red o su funcionamiento parcial.

Interceptación. El atacante ha conseguido infiltrarse en las comunicaciones de la entidad y ha replicado los datos que se encontraban en transmisión.

Modificación. El intruso ha logrado infiltrarse, pero en lugar de replicar la información, la está modificando para que llegue alterada al destino, generando una respuesta inusual. Por ejemplo, manipula los valores de una transacción financiera.

Fabricación. El atacante se finge el destinatario de la transmisión, lo que le permite acceder con libertad al contenido de la comunicación, este engaño con el fin de obtener información valiosa, etc.

En la Tabla 1 se puede evidenciar las técnicas ataque y una descripción de esta:

Tabla 1. Técnicas de ataques informáticos

Técnica de ataque	Descripción
Vishing	Se realizan llamadas telefónicas suplantando identidades para obtener información confidencial de las víctimas (Adam et al., 2023).
Whaling	Técnica de correo orientada a un perfil de usuario de banca online, como por ejemplo directivos de algunas organizaciones, a administradores de redes, a personas mayores (Sinkar & Rajabhushanam, 2021).
Phishing	El phishing sigue siendo un tipo rentable de engaño en la actualidad, en el que los estafadores ilegales también obtienen información confidencial de las víctimas. Los atacantes buscan acceder a servicios no autorizados, como los financieros, utilizando ingeniería social, malware y suplantación de identidad (Saraswat, Singh, & Solanki, 2022) (Higashino et al., 2019)
Ingeniería social	A diferencia de intentar descifrar la contraseña de la aplicación de una víctima mediante programas, algoritmos o técnicas de explotación avanzadas, los ataques de ingeniería social se centran en engañar a las víctimas para que entreguen sus datos a los piratas informáticos por sí mismas a partir de la manipulación psicológica de las víctimas para obtener información y acceder ilegalmente a sus equipos es una técnica central en muchos ciberataques, que ha evolucionado y mejorado con el tiempo (Salama et al., 2023) (Parthy & Rajendran, 2019).
Correos electrónicos fraudulentos	Los modelos de comunicación por correo electrónico se han utilizado durante mucho tiempo en la sociedad. Al observar quién se comunica con quién y con qué frecuencia, los investigadores han descubierto patrones interesantes que indican que el fraude se materializa al fingir que el correo proviene de una entidad bancaria, financiera, oficial, ONG o empresa (Lubarski & Morzy, 2012) (Al-Ghamdi & Alsubait, 2022).

Técnica de ataque	Descripción
Keyloggers	Keylogger es un programa espía que puede registrar las presiones de las teclas y los movimientos del ratón, junto con los movimientos del cursor para obtener información confidencial como usuario y las contraseñas (Singh y Singh, 2018) (Prasiddha, Namratha, y Mohana, 2023).
Smishing	Un mensaje de texto simula ser de un banco, informando problemas de validación o bloqueo de tarjeta, y pide al usuario acceder a un enlace web (Balim & Gunal, 2019).
Skimming	Se obtiene los datos registrados de la banda magnética y se copia en otra tarjeta (Jiang et al., 2021).
Troyanos Bancarios	Malware específicamente diseñado y desarrollado con el objeto de obtener información de acceso a la banca electrónica (Tjada et al., 2023).
Otras técnicas	Carta Nigeriana Correspondencias dirigidas a personas por correo que tienen como objetivo involucrar al destinatario en un esquema de fraude de pago por adelantado (Cukier et al., 2007). Ataques de fuerza bruta ocurre cuando los ciber atacante intentan acceder a su sitio web mediante prueba y error. Por lo general, se utiliza un software automatizado para adivinar información de inicio de sesión (Shah & Ayoade, 2023)

Nota. Tabla que presenta las técnicas de ataques informáticos incluyen el phishing, que engaña a los usuarios para que revelen información confidencial, y el malware, que se infiltra en sistemas para causar daños o robar datos. Ambas representan amenazas significativas para la seguridad digital. Fuente: propia.

En este sentido se hace necesario la concienciación del usuario en cuestiones de seguridad, el hacer uso contraseñas complejas, evitando el uso de información personal, e incorporando números o símbolos de puntuación en el medio o al final de la palabra. En algunos sistemas permiten visualizar la fortaleza de la contraseña elegida, así como cambiar la contraseña con frecuencia (un mes, una semana). Según el tipo de hardware

empleado, los ataques pueden demorar considerablemente, especialmente si previamente hemos modificado la clave, y no le es fácil obtener las credenciales.

1.6 Grupos delictivos cibernéticos

El crimen organizado en el entorno digital ejerce un impacto significativo tanto sobre los ciudadanos, como sobre las empresas y entidades del sector público, privado o mixto. Los ataques efectuados por los ciberdelincuentes tienen fines económicos directos mediante la obtención de credenciales o indirecto a través de extorsiones (CN-CERT, 2017).

El delito constituye una conducta humana (acción u omisión).

- Esta conducta debe ser contraria al ordenamiento jurídico y debe afectar o poner en riesgo un interés protegido por la ley.
- Debe ser atribuible a culpabilidad, ya sea por dolo (intención) o por culpa (negligencia), y una acción se considera atribuible cuando puede ser responsabilizada a una persona específica.
- La realización u omisión de dicha conducta debe estar sujeta a una sanción penal.

Algunas definiciones de delitos informáticos

- Se podría concebir el delito informático como cualquier conducta (acción u omisión) reprochable llevada a cabo por un ser humano, que cause un perjuicio a personas, sin que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor, aunque no perjudique de forma directa o indirecta a la víctima, tipificado por la Ley, que se realiza en el entorno informático y está sancionado con una pena.
- El escritor mexicano Julio Téllez Valdez sostiene que los crímenes informáticos son "a*ctitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y se tienen a las computadoras como instrumento o fin*"
- El jurista penal italiano, Carlos Sarzana, argumenta que los delitos informáticos son "*cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo*".
- El profesor Davara Rodríguez lo concibe como: "*la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevado a cabo utilizando un elemento informático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software.*"
- Finalmente, un conjunto de especialistas de la Organización para la Cooperación y el Desarrollo Económico (OCDE) en París, en 1983, definió el delito informático como "*cualquier acto ilegal, inmoral o no autorizado que implique el procesamiento automático de datos y/o su transmisión*".

Los tipos de delitos reconocidos por la Organización de las Naciones Unidades y que le han dado su carácter internacional, a fin de que los países los tomen en consideración para ser incorporados a sus distintas legislaciones penales correspondientes son:

1.7 Fraudes por computadoras

Fraudes llevados a cabo a través de la alteración de sistemas informáticos implican el uso de técnicas avanzadas para acceder ilegalmente a sistemas y datos. Los ciberdelincuentes emplean métodos como el phishing, malware y ataques de ingeniería social para engañar a los usuarios de computador y obtener información confidencial. En la tabla 2, se presentan algunos actos delictivos pueden tener graves consecuencias financieras y de privacidad para las personas y organizaciones afectadas.

Tabla 2. Tipos de fraude informático

Tipo de fraude	Descripción
Manipulación de los datos de entrada	Denominado como robo de datos, constituye el delito informático más prevalente, dado que es sencillo de ejecutar y complicado de detectar. No requiere conocimientos técnicos en informática, lo que permite que cualquier individuo pueda llevarlo a cabo (Gao et al., 2023).
La manipulación de programas	Este delito implica alterar los programas ya existentes en los sistemas informáticos o introducir nuevos programas o rutinas. Un enfoque habitual empleado por individuos con conocimientos avanzados en programación informática es el conocido como "*Caballo de Troya*" (Abinaya et al., 2018).
Manipulación de los datos de salida	Históricamente, estos fraudes se cometían utilizando tarjetas bancarias sustraídas. Sin embargo, en la actualidad, se emplean de manera generalizada equipos y software especializado para codificar datos electrónicos falsificados en las bandas magnéticas de tarjetas bancarias y de crédito (Guers, Chowdhury, y Rifat, 2022)

Nota. Tablas que presenta el fraude informático abarca técnicas como el robo de identidad, donde los delincuentes obtienen y usan datos personales sin autorización, y el fraude financiero, que implica manipular sistemas para desviar fondos o realizar transacciones no autorizadas.

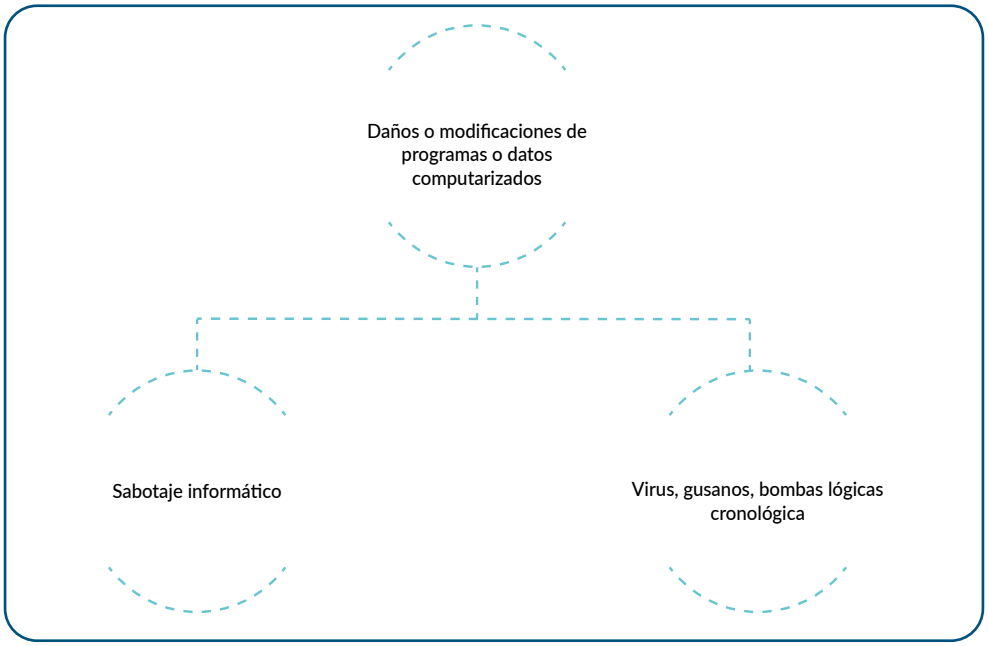
1.8 Falsificaciones informáticas

Como objetivo: Cuando se modifican los datos de los documentos almacenados electrónicamente.

Como herramientas: Las computadoras también pueden ser empleadas para la falsificación de documentos comerciales. Las fotocopiadoras de alta resolución pueden alterar documentos e incluso generar copias fraudulentas sin necesidad de un original. Los documentos falsificados que producen son de tal calidad que solo un especialista capacitado es capaz de distinguirlos de los auténticos (Nazli y Maghari, 2017).

Daños o modificaciones de programas o datos computarizados: Ataca la defensa informática de un sistema con autorización de la organización, notificado Informar a los administradores sobre las vulnerabilidades y fallos de seguridad detectados, ya que son accesibles para cualquier persona, como se presenta en la Figura 3.

Figura 3. Daños causados por programas



Nota. Fuente: propia

El término '*hacker'* se emplea comúnmente de manera generalizada para referirse a una persona que elude las medidas de seguridad de un sistema. En la Tabla 3 se presentan los tipos de atacantes.

Tabla 3. Tipo de atacantes

Tipo de Atacante	Descripción
Hacker	Compromete las medidas de seguridad cibernética de un sistema con autorización, notificando a los administradores sobre las debilidades de seguridad encontradas (Samtani y Chen, 2016)
Cracker	Generan ataques informáticos para sustraer información, interrumpir servicios y modificar datos.
Script kiddie	Los novatos en hacking y cracking llevan a cabo ataques encontrados en Internet sin tener una comprensión total de sus acciones ni de las repercusiones, lo que los convierte en una amenaza particularmente peligrosa (Arzheimer, 2017).
Programadores de malware	Con conocimiento y experiencia en programación explotan vulnerabilidades de software para crear programas de ataque (Sznaier Camps, Bohm Agostini, y Kaeli, 2019).
Sniffers	Experto Que tienen la capacidad de interceptar y examinar el flujo de datos de la red, el rendimiento de está, análisis de paquetes, en particular (Jovan et al., 2019).
Ciberterrorista	Intruso informático con intereses políticos y económicos de gran envergadura (Agubor et al., 2015).

Nota. Tabla que presenta Los tipos de atacantes incluyen los *hackers* éticos, que buscan vulnerabilidades para mejorar la seguridad, y los cibercriminales, que explotan las debilidades para obtener beneficios ilícitos. La tabla 4 detalla las motivaciones de la delincuencia informática. Fuente: propia.

Tabla 4. Motivación del atacante

Actor	Descripción
Cibervándalos y script kiddies	Evidenciar vulnerabilidades, piratería, diversión, retos (Farrah & Dacier, 2021).
Ciberactivismo	Ideologías, políticas, religiosas, entre otros (Vélez-Duarte et al., 2022).
Ciberyihadistas	Publicidad, reclutamiento, propaganda (Cameron et al., 2017)
Ciberterroristas	Alterar el normal desempeño social, amenazar e intimidar a una población, influir de decisiones sociopolíticas (Agubor et al., 2015)
Ciberdelincuentes	Buscan beneficios económicos de forma directa o indirecta (Miftari et al., 2022).
Estados	Espionaje, estrategias políticas, geopolítica (Baram & Sommer, 2019).

Nota. Tabla que visualiza motivos de los atacantes varían desde el lucro financiero, buscando ganancias económicas, hasta el activismo, donde se persiguen objetivos políticos o sociales a través de ciberataques los ciberatacantes Fuente: Ciberamenazas y Tendencias CCN-CERT IA-16/17. Fuente: propia.

1.9 Actividades

Completar la información en la Tabla 5, correspondiente a la función principal y el uso de las tecnologías de hardware que apoyan o ayudan a la ciberseguridad, registradas en la siguiente tabla. Es fundamental detallar cómo cada tecnología contribuye a la protección de la infraestructura digital y a la mitigación de riesgos, asegurando así una comprensión clara de su relevancia en el ámbito de la ciberseguridad.

Tabla 5. Tecnologías de hardware en ciberseguridad

Tecnología de Hardware	Función Principal	Ejemplo de Uso
Firewall	Filtrado de tráfico de red	Protección perimetral de redes
Sistema de Detección de Intrusos (IDS)		
Sistema de Prevención de Intrusos (IPS)		
Antivirus Hardware		
Dispositivos de Cifrado		
Hardware de Autenticación		
Routers Seguros		
Cámaras de Seguridad		
Controladores de Acceso		
Dispositivos de Respaldo		
Servidores de Seguridad		
Dispositivos de Red Privada Virtual (VPN)		
Hardware de Monitoreo de Red		
Dispositivos de Filtrado de Contenido		
Plataformas de Gestión de Seguridad		

Nota. Tabla que presenta el nombre de la tecnología de hardware, una descripción de la función y cuál es su uso principal. Fuente: propia.

Completar la información en la Tabla 6, correspondiente a la función principal y el uso de las tecnologías de hardware utilizadas en ciberseguridad, Es fundamental detallar cómo cada tecnología contribuye a la protección de la infraestructura digital y a la mitigación de riesgos, asegurando así una comprensión clara de su relevancia en el ámbito de la ciberseguridad.

Tabla 6. Software para la ciberseguridad

Tecnología de Software	Función Principal	Ejemplo de Uso
Antivirus	Detección y eliminación de malware	Protección de endpoints y servidores
Firewall de Aplicación		
Sistema de Detección de Intrusos (IDS)		
Sistema de Prevención de Intrusos (IPS)		
Software de Cifrado		
Gestores de Contraseñas		
Plataformas de Gestión de Seguridad		
Software de Monitoreo de Red		
Herramientas de Respuesta a Incidentes		
Sistemas de Autenticación Multifactor (MFA)		

Tecnología de Software	Función Principal	Ejemplo de Uso
Software de Análisis de Vulnerabilidades		
Plataformas de Seguridad en la Nube		
Herramientas de Filtrado de Contenido		
Sistemas de Gestión de Identidades y Accesos (IAM)		
Software de Backup y Recuperación		

Nota. Tabla que presenta el nombre de la aplicación de software, una descripción de la función y cual es su uso principal. Fuente: propia.

Completar la información registrada en la siguiente Tabla 7 de la función y tipo de ataque cibernético que previene

Tabla 7. Tecnologías de ciberseguridad para mitigar ataques

Tecnología	Función	Tipo de Ataque que Previene
Firewall	Filtrado de tráfico de red	Ataques de red (DDoS, intrusiones)
Sistema de Detección de Intrusos (IDS)		
Sistema de Prevención de Intrusos (IPS)	Bloqueo de amenazas en tiempo real	Intrusiones y ataques de malware
Antivirus		

Tecnología	Función	Tipo de Ataque que Previene
Cifrado de Datos		
Autenticación Multifactor (MFA)		
Gestores de Contraseñas		
Software de Análisis de Vulnerabilidades		
Plataformas de Seguridad en la Nube		
Herramientas de Respuesta a Incidentes		
Sistemas de Gestión de Identidades y Accesos (IAM)		
Dispositivos de Filtrado de Contenido	Bloqueo de contenido no deseado	Phishing y malware web

Nota. Tabla que permite asociar la tecnología que reduce el tipo de ataque. Fuente: propia.

Referencias

Abinaya E., Aishwarva K., Lordwin C. P. M., Kamatchi G. y Malarvizhi I.,"A Performance Aware Security Framework to Avoid Software Attacks on Internet of Things (IoT) Based Patient Monitoring System," 2018 International Conference on Current Trends towards Converging Technologies (ICCTCT), Coimbatore, India, 2018, pp. 1-6, doi: 10.1109/ICCTCT.2018.8550955

Abushgra, A. A. (2023). How Quantum Computing Impacts Cyber Security. 2023 Intelligent Methods, Systems, and Applications (IMSA), 74-79.

Adam W. A. Bin, Xuan, Tan I. Y., Lai C. S., Rahim N. T., Tham B. Y. Bin and H. Guo, "Vishing-Defender: An Advanced Vishing Defence System Against Vishing Attacks," 2023

IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), Singapore, 2023, pp. 1-8, doi: 10.1109/SOLI60636.2023.10425272

Agubor,C. K. Chukwudebe G. A. and Nosirl O. C.. (2015). Security challenges to telecommunication networks: An overview of threats and preventive strategies. 2015 International Conference on Cyberspace (CYBER-Abuja), 124-129.

Al-Ghamdi, N., y Alsubait, T. (2022). 2022 Fifth National Conference of Saudi Computers Colleges (NCCC). Digital Forensics and Machine Learning to Fraudulent Email Prediction, 99-106.

Arzheimer, K. (2017). Psephology and technology, or: the rise and rise of the script-Kiddie. Electoral Behaviour, 972.

Balim, C., y Gunal, E. S. (2019). Automatic Detection of Smishing Attacks by Machine Learning Methods. 2019 1st International Informatics and Software Engineering Conference (UBMYK), 1-3.

Baram, G., y Sommer, U. (2019). Covert or not Covert: National Strategies During Cyber Conflict. 2019 11th International Conference on Cyber Conflict (CyCon), 1-16.

Calvin, N. (2024). The Weaponization of Artificial Intelligence in Cybersecurity: A Systematic Review. Procedia Computer Science, 547-555.

Malin, Cameron and Gudaitis, Terry and Holt, Thomas and Kilger, Max (2017). 7 - Cyber Jihad and Deception: Virtual Enhancement and Shaping of the Terrorist Narrative. En Cameron et al., Deception in the Digital Age (págs. 183-205). Boston: Academic Press.

CN-CERT. (2017). Ciberamenazas y Tendencias. Madrid: Centro Criptologico Nacional.

W. L. Cukier, E. J. Nesselroth and S. Cody, (2007). Genre, Narrative and the "Nigerian Letter" in Electronic Mail. 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07), 70.

Dwivedi A., Saini G. K., Musa U. I. y Kunal (2023). Cybersecurity and Prevention in the Quantum Era. 2023 2nd International Conference for Innovation in Technology (INOCON), 1-6.

Fabián, R. B. (2013). Seguridad Informática. Madrid: McGraw Hill.

Farrah, D., y Dacier, M. (2021). Zero Conf Protocols and their numerous Man in the Middle (MITM) Attacks. 2021 IEEE Security and Privacy Workshops (SPW), 410-421.

Guers K., Chowdhury M. M. y Rifat N. (2022). Card Skimming: A Cybercrime by Hackers. 2022 IEEE International Conference on Electro Information Technology (eIT), 575-579.

Higashino M.,Kawato T., Ohmori M. y Kawamura T.. (2019). An Anti-phishing Training System for Security Awareness and Education Considering Prevention of Infor-

mation Leakage. 2019 5th International Conference on Information Management (ICIM), 82-86.

IBM. (16 de 10 de 2022). ¿Qué es la seguridad de TI? Obtenido de https://www.ibm.com/mx-es/topics/it-security

ISO-27000. (10 de 12 de 2023). ISO 27001. Obtenido de http://www.iso27000.es/sgsi.html

Javier, A. B. (2012). Seguridad de la Información Redes, Informáticas y Sistemas de Información. Madrid: Paraninfo.

Jiang M., Sakota D., Kosaka R. y Hijikata W.. (2021). Analysis of Plasma Skimming within a Hydrodynamic Bearing Gap for Designing Spiral Groove Bearings in Rotary Blood Pumps. 2021 43rd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC), 1213-1217.

Crnogorac J., Kovač J., Kočan E. y Vučinić M. (2019). d-Argus: a Distributed IEEE 802.15.4 Sniffer. 2019 27th Telecommunications Forum (TELFOR), 1-7.

Libre, U. (2023). Seguridad de la Información. Obtenido de http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/152-seguridad-de-la-informacion

Lubarski, P., y Morzy, M. (2012). Measuring the Importance of Users in a Social Network Based on Email Communication Patterns. 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, 86-90.

Lundgren, B., y Möller, N. (2019). Defining information security. Science and engineering ethics, 419-441.

Macas, M., Wu, C., y Fuertes, W. (2022). A survey on deep learning for cybersecurity: Progress, challenges, and opportunities. Computer Networks, 109032.

Miftari et al. (2022). Analysis of cybercriminals and where they fall on the spectrum of crime. 2022 International Conference on Data Analytics for Business and Industry (ICDABI), 287-291.

Mohammed Nasser A., Tariq A., Taher A., Karrar A., Rabiah A.y Mazin, A. M. (2024). Insider threat detection in cyber-physical systems: a systematic literature review. Computers and Electrical Engineering, 109489.

Nazli, M. N., y Maghari, A. Y. (2017). Comparación entre algoritmos de detección de falsificación de imágenes. 2017 8th International Conference on Information Technology (ICIT), 442-445.

Ortiz Bayona Zulima, G. P. (2016). Hacia una Taxonomía de Incidentes de Seguridad en Internet - Dialnet. Obtenido de https://dialnet.unirioja.es/descarga/articulo/4797163.pdf

Parthy, P. P., y Rajendran, G. (2019). Identification and prevention of social engineering attacks on an enterprise. 2019 International Carnahan Conference on Security Technology (ICCST), 1-5.

Prasiddha, B., Namratha, J., y Mohana, H. (2023). Cyber Security Testbed: Keyloggers and Data Visualization on Keyloggers - A Case Study. 2023 International Conference on Sustainable Communication Networks and Application (ICSCNA), 219-221.

Salama Salama R., Al-Turjman F., Bhatla S. y Yadav S. P. (2023). Social engineering attack types and prevention techniques- A survey. 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN), 817-820.

Samtani, S., y Chen, H. (2016). Using social network analysis to identify key hackers for keylogging tools in hacker forums. 2016 IEEE Conference on Intelligence and Security Informatics (ISI), 319-321.

Saraswat, P., Singh, S., y Solanki, M. (2022). Phishing Detection in E-mails using Machine Learning. 2022 2nd International Conference on Technological Advancements in Computational Sciences (ICTACS), 420-424.

Shah, P. G., y Ayoade, J. (2023). An Empricial Study of Brute Force Attack on Wordpress Website. 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), 659-662.

Shin W., Lee J. L., Park D. H. y Chang C. H. (2014). Design of authenticity evaluation metric for Android applications. 2014 Fourth International Conference on Digital Information and Communication Technology and its Applications (DICTAP), 275-278.

Singh, A. P., y Singh, V. (2018). Infringement of Prevention Technique against Keyloggers using Sift Attack. 2018 International Conference on Advanced Computation and Telecommunication (ICACAT), 1-4.

Sinkar, Y., y Rajabhushanam, C. (2021). GWOA Model For Data Protection. 2021 International Conference on Computer Communication and Informatics (ICCCI), 1-5.

Sznaier Camps G., Bohm Agostini N. and Kaeli D. (2019). 2019 18th IEEE International Conference On Machine Learning And Applications (ICMLA). Discovering Programmer Intention Behind Written Source Code, 432-437.

Tjada N., Cory N. y Cherie N. (2023). Web Injection and Banking Trojan Malware -A Systematic Literature Review. 2023 6th International Conference on Information and Computer Technologies (ICICT), 45-48.

UNIR. (01 de 04 de 2023). Los 4 principios de la seguridad informática y su implementación. Obtenido de https://unirfp.unir.net/revista/ingenieria-y-tecnologia/principios-seguridad-informatica/

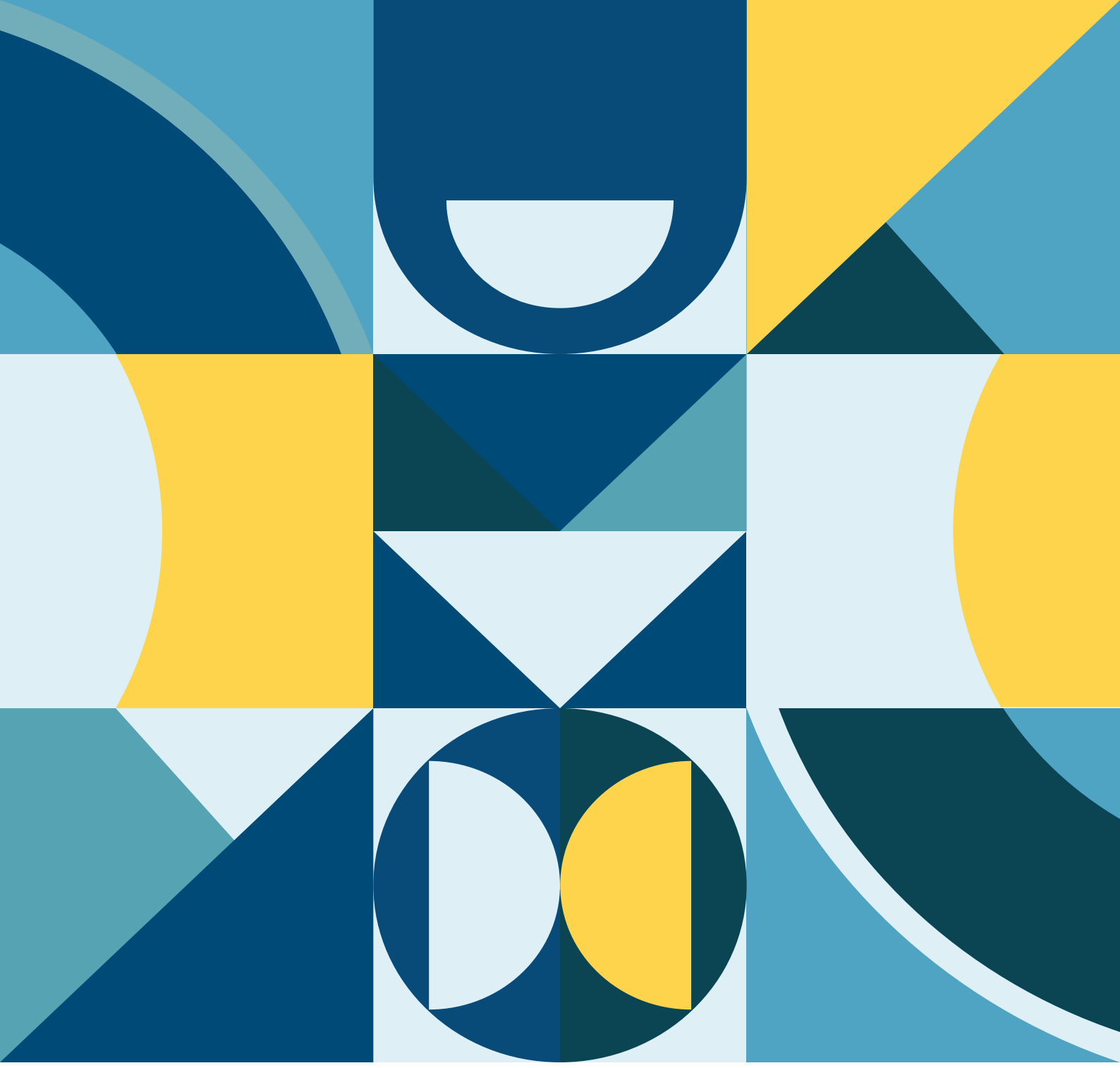
Universitat Carlemany. (25 de 02 de 2024). Qué es la seguridad informática: principios, tipos, ejemplos y más. Obtenido de https://www.universitatcarlemany.com/actualidad/blog/seguridad-informatica-que-es/

Vasile, D., y Svasta, P. M. (2019). Innovative Authentication Method for IoT Devices. 2019 22nd European Microelectronics and Packaging Conference & Exhibition (EMPC), 1-6.

Vélez-Duarte C. P., Calva-Cabrera D. y León-AlbercaCalva T. B. the last presidential elections in Ecuador. 2022 17th Iberian Conference on Information Systems and Technologies (CISTI), 1-6.

Yirui Z., Yong L., Yijia C. y Mingyu Y. (2023). Risk-based contingency analysis for power systems considering a combination of different types of cyber-attacks. Applied Energy, 121551.

Zhenhua, Y., y Jun, K. (2024). Cue-based two factor authentication. Computers & Security, 104068.



Escuela Tecnológica
Instituto Técnico Central
Establecimiento Público de Educación Superior