Amenazas digitales, ingeniería social y ética en ciberseguridad

Breve descripción:

Ese componente formativo establece las bases para comprender las amenazas digitales, la ingeniería social y la ética en ciberseguridad. Aborda tipos de ataques, vulnerabilidades, estrategias de manipulación, medidas preventivas y normativas éticas, proporcionando herramientas clave para la gestión de incidentes y la protección de la información en entornos digitales.

Abril 2025

Tabla de contenido

Introducción

Este componente formativo permite comprender las amenazas digitales, la ingeniería social y la ética en ciberseguridad, proporcionando un enfoque integral sobre los riesgos que afectan la seguridad de la información. A través del análisis de ataques informáticos, vulnerabilidades y estrategias de manipulación, se busca desarrollar habilidades para la prevención, detección y gestión de incidentes. Además, se abordan principios éticos y normativas que regulan la ciberseguridad, promoviendo buenas prácticas en entornos digitales. Para comprender la importancia del contenido y los temas abordados, se recomienda acceder al siguiente video.

Video 1. Amenazas digitales, ingeniería social y ética en ciberseguridad

Enlace de reproducción del video

Síntesis del video: Amenazas digitales, ingeniería social y ética en ciberseguridad
En este componente formativo se abordan los principales riesgos que afectan la seguridad digital en la actualidad. A medida que la tecnología avanza, también lo hacen las amenazas cibernéticas, y conocer su funcionamiento es clave para proteger la información personal y organizacional. El recorrido inicia con una mirada a los ataques informáticos más frecuentes y su impacto en redes y sistemas. Se continúa con el análisis de las vulnerabilidades más comunes y las formas en que los delincuentes logran explotarlas. Un tema fundamental es la ingeniería social, una práctica que aprovecha la manipulación psicológica para engañar a los usuarios. A través de ejemplos concretos se aprende a identificar estas estrategias y evitar caer en ellas. La formación también incorpora herramientas de prevención, medidas de seguridad y prácticas recomendadas para fortalecer los sistemas informáticos desde el primer nivel de defensa. Además, se profundiza en el papel de la ética dentro del entorno digital, resaltando los principios que orientan el comportamiento responsable frente a los datos, la privacidad y los derechos de los usuarios. El componente finaliza con la importancia de los reportes y la gestión adecuada de incidentes, promoviendo una cultura de alerta, respuesta y colaboración.

Este conocimiento permite desarrollar una visión crítica y comprometida frente a la ciberseguridad, entendiendo que proteger la información es responsabilidad de todos.

1. Ataques y amenazas informáticas

Los ataques y amenazas informáticas representan una de las principales preocupaciones en el mundo digital actual. A medida que dependemos cada vez más de la tecnología para realizar tareas cotidianas, desde la gestión de información personal hasta operaciones comerciales críticas, los ciberdelincuentes han encontrado nuevas formas de explotar vulnerabilidades en sistemas y redes. Estos ataques pueden adoptar diversas formas, como virus, malware, ransomware, phishing, entre otros, y tienen como objetivo desde el robo de datos hasta la interrupción de servicios esenciales.

Las consecuencias de estos eventos pueden ser devastadoras, afectando no solo a las personas y empresas a nivel económico, sino también en términos de reputación, privacidad y confianza. A esto se suma el hecho de que muchas amenazas están diseñadas para evadir los sistemas de detección tradicionales, lo que incrementa el nivel de riesgo y la complejidad de las respuestas requeridas.

El aumento de la sofisticación de las amenazas informáticas ha puesto de manifiesto la necesidad urgente de fortalecer las estrategias de ciberseguridad, tanto a nivel individual como organizacional. Entender las amenazas, sus características y métodos de propagación es el primer paso para anticiparse a ellas y reducir su impacto. Este conocimiento permite desarrollar políticas de protección más eficaces y fomentar una cultura digital consciente, resiliente y preparada ante cualquier intento de ataque.

1.1. Tipos de ataques cibernéticos

Los ataques cibernéticos son acciones maliciosas dirigidas a sistemas, redes o dispositivos con el fin de robar información, interrumpir servicios o causar daños. Para

ejecutarlos, los ciberdelincuentes emplean diversas técnicas, siendo el malware una de las herramientas más utilizadas. Comprender los distintos tipos de ataques y cómo se propagan permite tomar decisiones más efectivas para prevenirlos, contenerlos y eliminarlos.

A. Ataques mediante software malicioso (malware)

El malware es cualquier software diseñado con fines dañinos como robar información, evadir controles o comprometer sistemas. Existen múltiples variantes:

- ✓ **Spyware**: diseñado para espiar al usuario, recopila información sobre su actividad, contraseñas y datos confidenciales, como credenciales bancarias. Suele instalarse junto a programas legítimos o mediante troyanos.
- ✓ **Adware**: muestra anuncios no deseados en el navegador o en el sistema. Aunque en algunos casos no es dañino, interfiere con la experiencia del usuario y puede abrir la puerta a otros tipos de malware.
- ✓ **Puerta trasera** (backdoor): permite el acceso remoto a un sistema sin autorización, evitando los mecanismos de seguridad. Actúa de forma silenciosa, facilitando el control total por parte del atacante.
- ✓ **Ransomware**: bloquea el acceso a los datos o al sistema mediante cifrado, exigiendo un pago (rescate) para liberarlos. Se propaga principalmente a través de correos electrónicos de phishing o vulnerabilidades en el sistema. Un ejemplo es WannaCry, que afectó a miles de dispositivos en todo el mundo en cuestión de horas.

- ✓ **Scareware**: utiliza mensajes alarmantes para inducir al usuario a instalar programas falsos de "protección". Generalmente se manifiesta como ventanas emergentes que advierten sobre infecciones inexistentes.
- ✓ **Virus**: se adhiere a archivos ejecutables y necesita la intervención del usuario para activarse. Puede replicarse, mutar y propagarse a través de dispositivos extraíbles, redes compartidas o correo electrónico.
- ✓ **Troyanos**: se presentan como software legítimo, pero ejecutan acciones maliciosas sin el conocimiento del usuario. No se replican por sí solos, y frecuentemente se ocultan en archivos multimedia o juegos.
- ✓ **Gusanos**: se replican automáticamente para propagarse por redes sin necesidad de intervención humana ni programa anfitrión. Son altamente destructivos y pueden afectar a miles de dispositivos en poco tiempo. Un ejemplo es el gusano Code Red, que en 2001 infectó más de 300.000 servidores en 19 horas.

B. Ataques pasivos

Son técnicas de espionaje digital donde el atacante intercepta información sin modificarla ni alterar el sistema, lo que dificulta su detección. No generan daños directos ni cambios en los datos, pero permiten recopilar información confidencial al operar de forma silenciosa. Entre los más comunes se encuentran el sniffing, que captura paquetes de datos transmitidos por la red; el eavesdropping o escucha clandestina, que intercepta comunicaciones como llamadas VoIP o correos electrónicos; y el análisis de tráfico, que estudia patrones de comunicación para deducir relaciones o horarios de uso entre los usuarios.

C. Ataques masivos

Son ataques a gran escala dirigidos a múltiples usuarios o sistemas simultáneamente, con el objetivo de saturar infraestructuras o causar daños significativos. Afectan a muchas víctimas al mismo tiempo, son altamente visibles y disruptivos, y suelen valerse de automatización o redes distribuidas, como los bots. Entre los más comunes se encuentran:

- ✓ **Ataques DDoS**: colapsan servidores mediante millones de solicitudes simultáneas.
- ✓ **Phishing masivo**: correos electrónicos enviados en masa para engañar a numerosos usuarios.
- ✓ **Ransomware a gran escala**: infecciones simultáneas de múltiples dispositivos, como el caso WannaCry.

1.2. Impacto de las amenazas en sistemas y redes

Las amenazas cibernéticas pueden tener consecuencias graves en los sistemas informáticos y redes, afectando tanto a nivel técnico como operativo, financiero y reputacional. A continuación, se presentan los principales impactos:

- ✓ **Pérdida de confidencialidad**: las amenazas como el spyware o los ataques pasivos pueden exponer información confidencial, como datos personales, credenciales de acceso, secretos comerciales o información financiera.
- ✓ **Pérdida de integridad**: el malware puede alterar datos críticos o introducir modificaciones no autorizadas, afectando la precisión, consistencia y fiabilidad de la información almacenada en los sistemas.

- ✓ **Pérdida de disponibilidad**: ataques como el ransomware o los ataques DDoS pueden dejar fuera de servicio plataformas, servidores o servicios completos, impidiendo el acceso legítimo a los recursos.
- ✓ **Daños económicos**: las organizaciones pueden enfrentar altos costos derivados de la recuperación de sistemas, pérdida de ingresos, multas legales por incumplimientos normativos y contratación de servicios de ciberseguridad.
- ✓ **Pérdida de reputación**: una violación de seguridad puede dañar la imagen de una empresa, disminuir la confianza de los usuarios o clientes y afectar relaciones comerciales.
- ✓ **Interrupción de operaciones**: los sistemas infectados o comprometidos pueden provocar la paralización de procesos productivos, logísticos o administrativos, afectando la continuidad del negocio.
- ✓ **Uso indebido de recursos**: algunos tipos de malware, como los gusanos o troyanos, utilizan los recursos del sistema para actividades maliciosas, como enviar spam, realizar ataques a otros equipos o minar criptomonedas sin autorización.
- ✓ **Exposición legal y regulatoria**: cuando se compromete información sensible o personal, se pueden generar responsabilidades legales por el incumplimiento de leyes de protección de datos.

La prevención, detección oportuna y respuesta adecuada frente a las amenazas son fundamentales para mitigar estos impactos y garantizar la seguridad de los sistemas y redes.

2. Vulnerabilidades en ciberseguridad

En ciberseguridad las vulnerabilidades representan puntos débiles o fallos en los sistemas, redes o procedimientos que pueden ser aprovechados por atacantes para comprometer la integridad, confidencialidad o disponibilidad de la información. Estas pueden originarse en diferentes capas tecnológicas, desde errores humanos hasta deficiencias técnicas en software o hardware. Comprenderlas y mitigarlas es fundamental para establecer una postura de seguridad efectiva.

2.1. Tipos de vulnerabilidades

Las vulnerabilidades pueden clasificarse según su origen o naturaleza. A continuación, se describen algunas de las más comunes y críticas:

Tabla 1. Tipos de vulnerabilidades

Vulnerabilidad	Descripción	Riesgo asociado
Contraseñas débiles o por defecto	Uso de contraseñas simples como “123456” o no cambiar las credenciales predeterminadas.	Acceso no autorizado por ataques de fuerza bruta o uso de credenciales conocidas.
software sin actualizar	Aplicaciones o sistemas con parches de seguridad pendientes.	Exploits conocidos que pueden ser utilizados fácilmente por atacantes.

Vulnerabilidad	Descripción	Riesgo asociado
Inyección SQL	Inclusión de comandos SQL maliciosos en formularios o URLs vulnerables.	Robo, modificación o eliminación de datos en bases de datos.
Mala configuración de seguridad	Servicios mal configurados, como permisos excesivos o falta de autenticación en servidores.	Exposición de información sensible o acceso total al sistema.
Falta de cifrado	Transmisión de datos en texto plano (ej. HTTP en lugar de HTTPS).	Interceptación y robo de datos sensibles por parte de atacantes.
Ingeniería social	Engaños dirigidos a los usuarios para obtener información confidencial (phishing, vishing, etc.).	Acceso indebido mediante el uso de credenciales o instalación de malware.

Estas vulnerabilidades representan puntos críticos dentro de cualquier infraestructura tecnológica, ya que pueden ser aprovechadas por actores maliciosos para obtener acceso no autorizado, comprometer la integridad de los datos o interrumpir servicios esenciales. Aunque muchas de ellas pueden parecer simples o fácilmente evitables, su presencia suele deberse a la falta de actualización constante, la

ausencia de políticas de seguridad claras o la poca conciencia de los usuarios frente a los riesgos digitales. Identificar y gestionar estas debilidades de manera proactiva es esencial para reducir la superficie de ataque y fortalecer la seguridad global del entorno informático.

2.2. Métodos de explotación de vulnerabilidades

Los atacantes aprovechan las vulnerabilidades identificadas mediante diversas técnicas que les permiten comprometer sistemas, robar datos o interrumpir servicios. Estas técnicas pueden clasificarse según el tipo de fallo que se explota:

- ✓ **Explotación de vulnerabilidades de software**: errores como desbordamientos de búfer, ejecución remota de código o inyecciones permiten comprometer sistemas. Estas fallas son comunes cuando se carece de prácticas seguras de desarrollo o se usan librerías obsoletas.
- ✓ **Ataques a nivel de red**: protocolos sin cifrado, servicios expuestos o la falta de autenticación pueden facilitar ataques como sniffing o man-in-the-middle, comprometiendo la confidencialidad de la información.
- ✓ **Explotación de configuraciones incorrectas**: sistemas mal configurados pueden ser descubiertos y manipulados fácilmente. Ejemplos incluyen bases de datos sin contraseña o interfaces de administración expuestas a internet.
- ✓ **Ingeniería social**: se basa en manipular a los usuarios para obtener acceso a sistemas. Ataques como el phishing, el vishing o el baiting son métodos habituales de entrada, especialmente cuando no existe formación en ciberseguridad.

Para reducir el riesgo de explotación de vulnerabilidades, se recomienda implementar las siguientes acciones preventivas:

- ✓ Aplicar parches y actualizaciones de seguridad de forma constante.
- ✓ Configurar correctamente los servicios y sistemas según buenas prácticas.
- ✓ Implementar el principio de mínimo privilegio en el control de accesos.
- ✓ Usar protocolos seguros (como HTTPS, SSH) para proteger la transmisión de datos.
- ✓ Capacitar continuamente a los usuarios para prevenir ataques de ingeniería social.
- ✓ Auditar y monitorear continuamente la infraestructura para identificar vulnerabilidades.

Ataques y vulnerabilidades

A continuación, se presenta un video sobre ataques y vulnerabilidades en ciberseguridad. Este recurso audiovisual permite reforzar los conocimientos adquiridos mediante ejemplos prácticos y un lenguaje claro: Acceda al video a través del siguiente enlace: https://www.youtube.com/watch?v=au8EXjh-0jw&ab_channel=EcosistemadeRecursosEducativosDigitalesSENA

3. Ingeniería social

La ingeniería social consiste en engañar o influenciar a las personas para que realicen determinadas acciones o revelen información sensible. Los atacantes que emplean estas técnicas suelen aprovechar la buena voluntad, la falta de conocimiento o los puntos débiles emocionales o psicológicos de los usuarios. En lugar de vulnerar un

sistema directamente, manipulan a las personas para que, sin darse cuenta, les otorguen acceso o información valiosa.

Un ejemplo común es cuando un atacante se hace pasar por una figura de autoridad y contacta a un empleado con un supuesto problema urgente. Durante la conversación, puede emplear halagos, amenazas sutiles o referencias a personas influyentes para presionar al usuario y lograr su objetivo.

A continuación, se presenta un video sobre la ingeniería social, en el cual se explican los principios básicos de esta técnica de manipulación, sus principales métodos de ejecución y los riesgos que representa para la seguridad de la información.

Acceda al video a través del siguiente enlace: https://www.youtube.com/watch?v=5FeJVcZerS0&ab_channel=EcosistemadeRecursosEducativosDigitalesSENA

3.1. Técnicas de ingeniería social

Las técnicas utilizadas en ingeniería social son diversas y se adaptan al contexto y al perfil de la víctima. Algunas de las más comunes incluyen:

- ✓ **Phishing**: envío de correos electrónicos fraudulentos que aparentan ser legítimos para obtener credenciales o instalar malware.
- ✓ **Vishing (voice phishing)**: uso de llamadas telefónicas en las que el atacante finge ser un representante de soporte técnico o una entidad bancaria.
- ✓ **Smishing (SMS phishing)**: envío de mensajes de texto con enlaces maliciosos o solicitudes de información personal.

- ✓ **Pretexting**: creación de una historia falsa (pretexto) para obtener información confidencial, como un supuesto auditor que solicita datos de acceso.
- ✓ **Baiting**: utilización de cebos físicos o digitales (como memorias USB infectadas o enlaces de descarga atractivos) para que el usuario acceda a malware.
- ✓ **Shoulder surfing**: observación directa de credenciales o datos personales mientras la víctima los ingresa, en lugares públicos o laborales.

3.2. Ejemplos de ataques basados en manipulación psicológica

Los ataques de ingeniería social utilizan estrategias psicológicas para inducir a las personas a actuar en contra de sus propios intereses o de la seguridad de su organización. Estos ataques se basan en la confianza, la urgencia, el miedo o la curiosidad, y son diseñados cuidadosamente para explotar comportamientos humanos predecibles. A diferencia de los ataques puramente técnicos, su eficacia radica en la capacidad del atacante para generar una falsa sensación de legitimidad o necesidad.

Conocer ejemplos reales y comunes de este tipo de ataques es fundamental para desarrollar una actitud crítica y alerta frente a posibles intentos de manipulación. La prevención empieza por identificar patrones de comportamiento sospechosos y comprender cómo se ejecutan estas tácticas en diferentes entornos, tanto digitales como presenciales. A continuación, se presentan los ejemplos más frecuentes utilizados por los atacantes:

- ✓ **Correo falso de soporte técnico**: un usuario recibe un mensaje urgente que solicita verificar su cuenta en un enlace que imita la página oficial de la empresa. Al ingresar sus datos, estos son capturados por el atacante.

- ✓ **Llamada del "jefe" en emergencia**: el atacante simula ser el gerente general que necesita urgentemente una clave de acceso o el envío de información confidencial. La presión del tono y la autoridad percibida suelen hacer que el empleado coopere.
- ✓ **USB abandonada en el estacionamiento**: un empleado encuentra una memoria USB etiquetada como "nómina confidencial" y la conecta a su equipo por curiosidad. El dispositivo instala un malware de acceso remoto.
- ✓ **Mensaje SMS con enlace de rastreo falso**: el usuario recibe un mensaje sobre un paquete pendiente. Al hacer clic en el enlace, se descarga un programa malicioso.

4. Técnicas de prevención

En un mundo digital plagado de amenazas invisibles, prevenir los ataques es tan importante como detectarlos. La ingeniería social, al explotar el comportamiento humano, requiere medidas de protección que involucren tanto la tecnología como la conciencia de los usuarios. Para explicar la importancia de la prevención, se puede imaginar una ciudad virtual llamada "Fortaleza de Datos", donde sus habitantes (trabajadores digitales) enfrentan a diario intentos de engaño disfrazados de correos urgentes, llamadas sospechosas o promesas engañosas. Esta narrativa sirve como metáfora para destacar que la primera línea de defensa en ciberseguridad no es un software ni un dispositivo, sino el criterio informado de cada persona.

El Consejo de Ciberseguridad de esta ciudad virtual entrenó a sus ciudadanos con cinco técnicas clave de defensa. Estas estrategias prácticas ayudan a detectar y evitar los ataques más comunes basados en manipulación psicológica.

a) Piensa antes de hacer clic

Evitar abrir enlaces o archivos adjuntos de remitentes desconocidos es una práctica fundamental. Verificar cuidadosamente la dirección del remitente antes de actuar puede evitar caer en trampas como correos falsos que simulan provenir de entidades legítimas.

b) Verifica siempre la identidad

Ante solicitudes sospechosas, especialmente si hay urgencia, se debe confirmar la identidad del remitente por otro canal confiable. Esto aplica tanto a correos como a llamadas o mensajes instantáneos.

c) No compartas más de la cuenta

La información aparentemente inofensiva en redes sociales puede ser utilizada para diseñar ataques personalizados. Se recomienda limitar lo que se publica, especialmente si está relacionado con la vida laboral o contraseñas indirectas.

d) Duda de lo urgente y lo emocional

Los atacantes suelen crear una sensación de urgencia o manipular emociones para forzar decisiones rápidas. Tomarse un momento para reflexionar y verificar siempre la información ayuda a evitar errores.

e) Capacitación constante

La formación periódica del personal en temas de ciberseguridad y la realización de simulacros refuerzan la cultura de prevención. Los métodos de ingeniería social evolucionan, por lo que el conocimiento actualizado es una herramienta crítica.

Estas prácticas no solo reducen el riesgo de ataques, sino que también fortalecen el papel del usuario como parte activa de la seguridad organizacional.

4.1. Medidas de seguridad y buenas prácticas

Para enfrentar los ataques de ingeniería social y otras amenazas cibernéticas, es fundamental adoptar una serie de medidas preventivas que complementen las buenas prácticas de los usuarios. Estas acciones deben implementarse tanto a nivel personal como organizacional y enfocarse en reducir los riesgos desde distintos frentes. Entre las medidas más efectivas se encuentran:

- ✓ Verificar siempre la identidad de quienes solicitan información confidencial.
- ✓ No hacer clic en enlaces ni descargar archivos de correos electrónicos sospechosos.
- ✓ Aplicar autenticación en dos pasos (2FA) para añadir una capa extra de protección a las cuentas.
- ✓ Limitar la información publicada en redes sociales, especialmente si puede ser usada para suplantaciones.
- ✓ Fomentar una cultura de ciberseguridad a través de capacitaciones, campañas de concientización y simulacros.

- ✓ Establecer protocolos claros de respuesta ante incidentes, de modo que los empleados sepan cómo actuar si identifican un posible ataque.

Estas prácticas deben integrarse en el comportamiento diario de los usuarios, ya que la ingeniería social se basa en errores humanos más que en fallas técnicas.

4.2. Herramientas de protección en ciberseguridad

Además de las buenas prácticas, existen herramientas tecnológicas que ayudan a prevenir los ataques y fortalecer la seguridad de la información. Estas soluciones están diseñadas para proteger tanto los dispositivos como los datos, mediante mecanismos de autenticación, encriptación, detección y control de accesos. Algunas de las herramientas más utilizadas incluyen:

- ✓ **Autenticación en dos pasos (2FA)**: añade una verificación adicional para acceder a cuentas. Herramientas como Google Authenticator, Microsoft Authenticator, Duo Security o Authy ofrecen opciones seguras. Incluso existen soluciones físicas como YubiKey.
- ✓ **Firewalls**: dispositivos que filtran el tráfico de red para bloquear accesos no autorizados. Ejemplos: Cisco ASA, Fortinet FortiGate y Palo Alto Networks.
- ✓ **Sistemas de detección y prevención de intrusiones (IDS/IPS)**: detectan actividades sospechosas en la red. Ejemplos: Snort, Suricata y Cisco Firepower.
- ✓ **VPN (Red Privada Virtual)**: cifran la conexión a internet para proteger la información transmitida. Ejemplos: Cisco AnyConnect y Netgear VPN Router.

- ✓ **Dispositivos de autenticación física**: tarjetas inteligentes (como CAC) o dispositivos biométricos (lectores de huellas o reconocimiento facial) que permiten el acceso seguro a sistemas críticos.
- ✓ **Almacenamiento cifrado**: protege archivos confidenciales con soluciones como Kingston IronKey o Apricorn Aegis Secure.

Estas herramientas deben integrarse en una estrategia de seguridad integral, complementada con políticas claras, monitoreo constante y educación continua del personal.

5. Ética en ciberseguridad

La ética en ciberseguridad se refiere al conjunto de principios y normas morales que orientan el comportamiento de los profesionales, usuarios y organizaciones en el ámbito de la seguridad digital. Este campo exige un compromiso responsable con la protección de la información, el respeto por la privacidad, la transparencia y la legalidad en el uso de tecnologías.

5.1. Principios éticos en la seguridad de la información

Entre los desafíos más frecuentes en este ámbito se encuentran situaciones complejas que ponen a prueba la integridad ética de los profesionales y las organizaciones encargadas de la seguridad digital. Estos desafíos surgen por el acelerado avance tecnológico, la creciente dependencia de los sistemas informáticos y la necesidad de equilibrar la innovación con el respeto a los derechos fundamentales. A continuación, se detallan algunos de los más relevantes:

- ✓ **Privacidad de los datos personales**: el acceso, almacenamiento y uso de información privada sin consentimiento plantea dilemas importantes.

Empresas, gobiernos o ciberdelincuentes pueden vulnerar la privacidad, lo que exige establecer límites claros sobre el tratamiento de los datos y garantizar la protección de la información sensible.

- ✓ **Hacking ético vs. hacking malicioso**: distinguir entre el uso legítimo de técnicas de hacking para fortalecer la seguridad y el uso con fines ilícitos es crucial. El hacking ético se realiza con autorización y persigue prevenir riesgos, mientras que el hacking malicioso busca dañar, espiar o robar.
- ✓ **Vigilancia masiva**: la recopilación de datos a gran escala por parte de gobiernos o corporaciones, con fines de control o seguridad, puede derivar en prácticas invasivas. Este tipo de vigilancia debe estar regulada para no vulnerar derechos fundamentales como la privacidad o la libertad de expresión.
- ✓ **Uso de inteligencia artificial en ciberseguridad**: las decisiones automatizadas que se aplican a la seguridad digital pueden reproducir o amplificar sesgos si los algoritmos no están bien diseñados o auditados. Esto plantea el desafío de garantizar transparencia, equidad y control humano en el uso de la IA.

Para enfrentar estos desafíos, se promueven principios como:

- ✓ Confidencialidad: proteger la información contra accesos no autorizados.
- ✓ Integridad: asegurar que los datos no sean modificados sin autorización.
- ✓ Transparencia: comunicar de manera clara cómo se recopila, usa y protege la información.
- ✓ Responsabilidad: asumir las consecuencias de las decisiones tomadas en entornos digitales.

- ✓ Legalidad: actuar conforme a las leyes vigentes en materia de ciberseguridad.

También surgen dilemas éticos que implican tomar decisiones complejas:

- ✓ ¿Es aceptable vulnerar sistemas para denunciar injusticias (hacktivismo)?
- ✓ ¿Debe reportarse una vulnerabilidad a la empresa o hacerla pública?
- ✓ ¿Es ético que los gobiernos accedan a datos personales para prevenir delitos?
- ✓ ¿Se justifica el uso de malware con fines de defensa nacional?

El hackeo ético representa una respuesta a estos dilemas, al permitir pruebas controladas de seguridad bajo autorización formal, con el objetivo de fortalecer los sistemas informáticos.

A continuación, se presenta un video sobre metodologías del hacking ético. El video complementa los principios éticos abordados, resaltando la importancia del consentimiento, la legalidad y la responsabilidad en el ejercicio profesional de la seguridad digital.

Acceda al video a través del siguiente enlace: https://www.youtube.com/watch?v=r3S8tscj-bg&ab_channel=EcosistemadeRecursosEducativosDigitalesSENA

5.2. Legislación y normativas éticas aplicadas

El ejercicio ético de la ciberseguridad no solo se basa en valores, sino también en normativas y leyes que regulan el manejo de la información digital y establecen responsabilidades legales.

Algunas de las principales normativas y marcos éticos a nivel internacional y nacional incluyen:

- ✓ **Ley 1581 de 2012 (Colombia)**: regula la protección de datos personales.
- ✓ **Ley 1273 de 2009 (Colombia)**: crea nuevos tipos penales relacionados con delitos informáticos y la protección de la información.
- ✓ **Reglamento General de Protección de Datos (GDPR – Unión Europea)**: establece normas estrictas para el tratamiento de datos personales y su transferencia internacional.
- ✓ **ISO/IEC 27001**: norma internacional sobre gestión de la seguridad de la información.
- ✓ **Código de Ética de (ISC)²**: organización global que promueve estándares éticos en profesionales de seguridad informática.
- ✓ **Principios de Budapest (Convenio sobre Ciberdelincuencia)**: primer tratado internacional que busca armonizar legislaciones y fortalecer la cooperación contra delitos informáticos.

Estas leyes y normas exigen a las organizaciones implementar controles técnicos y administrativos para prevenir abusos, garantizar la privacidad y promover un entorno digital seguro y justo para todos los usuarios.

6. Reportes y gestión de incidentes en ciberseguridad

La gestión de incidentes de ciberseguridad implica la identificación, análisis, reporte y respuesta ante eventos que comprometen la confidencialidad, integridad o disponibilidad de los sistemas informáticos. En este proceso, los reportes juegan un papel fundamental al documentar de manera estructurada los hallazgos, riesgos y acciones recomendadas para mitigar amenazas y fortalecer la postura de seguridad de la organización.

6.1. Mecanismos de denuncia y respuesta a incidentes

Un reporte en ciberseguridad es un documento técnico que describe incidentes detectados, vulnerabilidades identificadas o resultados de auditorías de seguridad. Su propósito es informar a los responsables sobre eventos relevantes que podrían afectar la infraestructura tecnológica y proporcionar la base para tomar decisiones correctivas o preventivas.

Un buen reporte debe incluir los siguientes elementos esenciales:

1) **Título y fecha**

Identifica el tipo de reporte (incidente, auditoría o vulnerabilidad) y la fecha de elaboración.

2) **Descripción del incidente o hallazgo**

Explica de forma clara qué ocurrió, cómo fue descubierto y en qué contexto.

3) **Impacto y nivel de riesgo**

Evalúa las posibles consecuencias para la organización (pérdida de datos, interrupción del servicio o filtración de información).

4) **Evidencia**

Incluye registros del sistema (logs), capturas de pantalla, pruebas de explotación u otra documentación que respalde los hallazgos.

5) **Análisis técnico**

Describe las causas del incidente, técnicas utilizadas por los atacantes (si aplica), y detalles técnicos sobre cómo se explotó la vulnerabilidad.

6) **Recomendaciones**

Proporciona medidas de remediación, parches sugeridos o cambios en la configuración para prevenir futuros incidentes.

7) **Conclusión**

Resume los hallazgos e indica los próximos pasos o responsables de la implementación de las soluciones.

Un reporte de ciberseguridad es una tarea fundamental para documentar incidentes, vulnerabilidades o hallazgos técnicos que puedan comprometer la integridad, confidencialidad o disponibilidad de los sistemas informáticos. A continuación, se describen los pasos esenciales para su elaboración:

a) **Recolección de información**: este paso consiste en recopilar todos los datos relacionados con el incidente, incluyendo registros de actividad (logs), archivos del sistema, reportes de monitoreo, mensajes de error y testimonios de usuarios involucrados. Cuanta más información se reúna, mayor será la claridad del análisis posterior.

b) **Identificación y delimitación del incidente**: es fundamental definir con precisión qué ocurrió, cuándo y en qué parte del sistema. Esto implica determinar si se trata de una intrusión, una fuga de datos, una infección por malware, una falla interna o un intento de acceso no autorizado, y delimitar su alcance.

c) **Análisis del impacto y evaluación del riesgo**: se debe examinar cómo ha afectado el incidente a la organización, tanto desde el punto de vista técnico como operativo. Esto incluye evaluar la pérdida de datos, la afectación al servicio, el daño reputacional y el posible incumplimiento normativo.

d) **Documentación clara de hallazgos**: en esta etapa se redacta el contenido del informe con lenguaje técnico preciso pero comprensible para los responsables de la seguridad o la gerencia. Deben incluirse detalles sobre las evidencias recopiladas, patrones detectados, comportamiento del atacante (si aplica), vectores de ataque y vulnerabilidades explotadas.

e) **Elaboración de recomendaciones y medidas correctivas**: con base en el análisis, se sugieren soluciones para resolver el incidente y acciones preventivas para evitar su repetición. Estas pueden incluir parches de seguridad, actualizaciones de software, refuerzo de políticas de acceso o capacitación del personal.

f) **Presentación del reporte a los responsables**: finalmente, el informe debe entregarse a las áreas correspondientes (como el equipo de TI, el CSIRT o la alta dirección) para su evaluación y toma de decisiones. En algunos casos, también se puede compartir con entidades externas como autoridades legales o CERT nacionales, si la magnitud del incidente lo requiere.

Un reporte bien estructurado y oportuno no solo permite atender un incidente de forma eficaz, sino que también se convierte en un recurso valioso para fortalecer la estrategia de la organización. Con el fin de poner en práctica lo aprendido, se presenta el siguiente ejemplo de reporte de ciberseguridad:

a) **Título**: informe sobre vulnerabilidad de acceso en el servidor web.
b) **Fecha**: 30 de marzo de 2025.
c) **Descripción**: durante una auditoría rutinaria de seguridad, se identificó una vulnerabilidad crítica de inyección SQL en el módulo de autenticación del servidor web institucional. Esta vulnerabilidad permite a un usuario malintencionado manipular las consultas enviadas a la base de datos a través de los campos de entrada del formulario de inicio de sesión.
d) **Impacto**: la explotación de esta vulnerabilidad podría permitir la ejecución de comandos arbitrarios en la base de datos, lo que comprometería la integridad, disponibilidad y confidencialidad de la información almacenada. Además, podría permitir el acceso no autorizado a credenciales de usuarios y a datos sensibles de la organización.
e) **Evidencia**: se adjuntan capturas de pantalla que evidencian la ejecución exitosa de pruebas de inyección SQL en el formulario de autenticación, así como los registros (logs) del servidor que muestran los errores generados como resultado de las consultas manipuladas.
f) **Análisis técnico**: se comprobó que el sistema no aplica mecanismos adecuados de validación ni sanitización de los datos ingresados por los usuarios. Esto permite que comandos SQL maliciosos sean interpretados

directamente por el motor de base de datos. La falta de uso de sentencias preparadas y de una arquitectura segura aumenta el riesgo de este tipo de ataques.

g) **Recomendaciones:**

- ✓ Implementar validaciones estrictas del lado del servidor para todas las entradas de usuario.
- ✓ Utilizar consultas parametrizadas o sentencias preparadas para evitar la manipulación de comandos SQL.
- ✓ Actualizar las versiones del framework y del sistema de gestión de bases de datos utilizados.
- ✓ Realizar pruebas de penetración periódicas para detectar vulnerabilidades similares.

h) **Conclusión**: se recomienda aplicar de manera inmediata las medidas correctivas sugeridas y realizar una revisión completa del código del sistema web para prevenir otras posibles vulnerabilidades. También se sugiere fortalecer los controles de desarrollo seguro dentro del ciclo de vida del software.

6.2. Entidades encargadas de la gestión de reportes

La gestión efectiva de incidentes de ciberseguridad requiere la participación de entidades especializadas que centralicen, analicen y coordinen las respuestas ante amenazas. Estas organizaciones, tanto a nivel nacional como internacional, ofrecen canales para reportar incidentes, divulgar vulnerabilidades y emitir alertas de seguridad. A continuación, se describen algunas de las principales entidades encargadas de esta labor:

En Colombia:

- ✓ **ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia)**: dependiente del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), ColCERT es el equipo nacional encargado de coordinar la respuesta a incidentes de ciberseguridad. Recibe reportes, analiza amenazas y emite boletines de alerta. Sitio web: https://colcert.gov.co
- ✓ **CSIRT de entidades estatales y privadas**: muchas organizaciones públicas y privadas cuentan con su propio CSIRT (Computer Security Incident Response Team), equipos especializados en recibir, analizar y mitigar incidentes dentro de sus redes.
- ✓ **Policía Nacional - Centro Cibernético Policial (CCP)**: encargado de recibir denuncias sobre delitos informáticos. Ofrece canales como el CAI Virtual y el portal de denuncias en línea. Sitio web: https://caivirtual.policia.gov.co
- ✓ **Fiscalía General de la Nación**: investiga y judicializa los delitos informáticos reportados por ciudadanos, empresas o instituciones del Estado.

A nivel internacional:

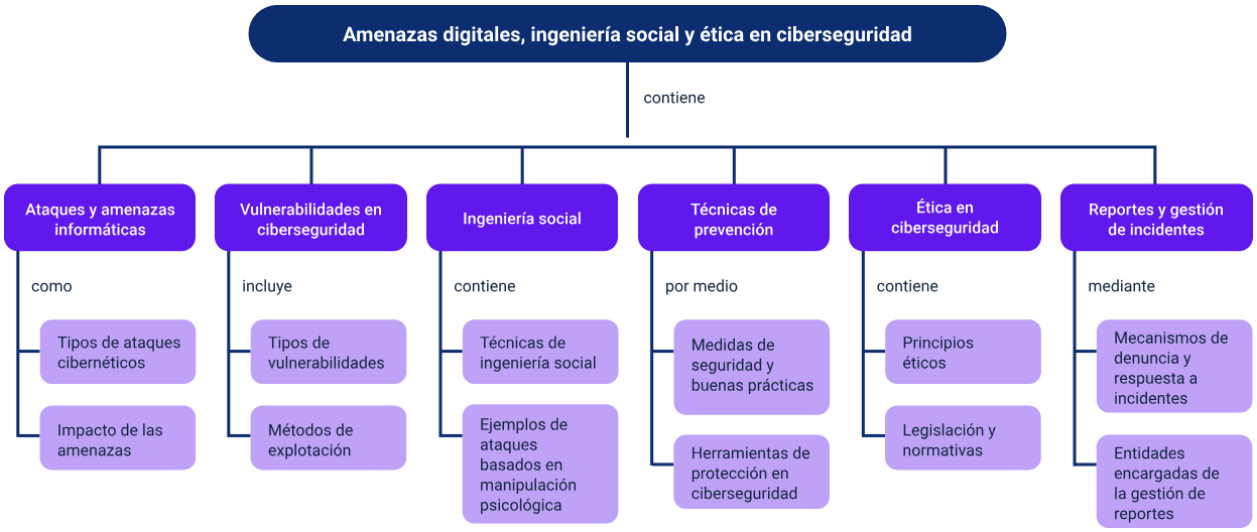
- ✓ **CERT/CC (Carnegie Mellon University - EE.UU.)**: uno de los primeros equipos de respuesta a incidentes en el mundo. Publica alertas, coordina respuestas a amenazas globales y mantiene una base de datos de vulnerabilidades.

- ✓ **FIRST (Forum of Incident Response and Security Teams)**: red global de equipos de respuesta que promueve la cooperación internacional en la gestión de incidentes. Incluye miembros en más de 90 países.
- ✓ **ENISA (Agencia de la Unión Europea para la Ciberseguridad)**: coordina esfuerzos en Europa para mejorar las capacidades de ciberseguridad, proporciona herramientas de gestión de riesgos y fomenta la colaboración entre países.
- ✓ **INTERPOL – Cybercrime Directorate**: apoya la lucha contra el cibercrimen a nivel internacional, facilitando la cooperación entre cuerpos policiales de distintos países.

Estas entidades proporcionan mecanismos formales de reporte, así como recursos educativos, boletines de seguridad y directrices para la prevención de incidentes. Conocerlas y saber cómo contactarlas es fundamental para fortalecer las capacidades de respuesta en ciberseguridad tanto a nivel organizacional como nacional.

Síntesis

Este componente formativo aborda los principales aspectos de la ciberseguridad, comenzando con el análisis de los tipos de ataques cibernéticos y el impacto que generan en sistemas y redes informáticas. A continuación, se profundiza en las vulnerabilidades más comunes, así como en los métodos empleados para su explotación. También se examina la ingeniería social, destacando sus técnicas y ejemplos de manipulación psicológica utilizadas por los atacantes. Se presentan diversas estrategias de prevención, incluyendo buenas prácticas y herramientas de protección. Además, se reflexiona sobre los principios éticos que deben guiar el actuar en entornos digitales, junto con las normativas legales que regulan esta materia. Finalmente, se estudia el proceso de elaboración de reportes de incidentes y la actuación de las entidades responsables de gestionar y responder ante estos eventos.



Material Complementario

Tema	Referencia	Tipo de material	Enlace del recurso
Ataques y amenazas informáticas	Correa, C. A. P., & Díaz, H. P. (2007). Las amenazas informáticas: Peligro latente para las organizaciones actuales. Revista Gerencia Tecnológica Informática, 6(16), 85–97.	Revista	https://core.ac.uk/download/pdf/230227206.pdf
Ataques y amenazas informáticas	ESET Latinoamérica. (2023). Tendencias en ciberseguridad para el 2024.	Articulo	https://web-assets.esetstatic.com/wls/es/articulos/reportes/cybersecurity-trends-2024-es.pdf
Ingeniería social	Pérez, J. (2023). Ataques basados en ingeniería social en Colombia: buenas prácticas y recomendaciones. Revista Tecnología en Marcha, 24(49), 120-130.	Articulo	https://www.scielo.sa.cr/pdf/is/v24n49/2215-2458-is-24-49-120.pdf
Ética en ciberseguridad	Ecosistema de Recursos Educativos Digitales. (2022,	Video	https://www.youtube.com/watch?v=b4X4Rh4eNyU

Tema	Referencia	Tipo de material	Enlace del recurso
	abril 27). ¿En qué se diferencian los hackers éticos de los hackers maliciosos? [Video]. YouTube.		
Reportes y gestión de incidentes en ciberseguridad	Sabillón, R., Serra-Ruiz, J., & Cano, J. (2019). Auditorías en ciberseguridad: Un modelo de aplicación general para instituciones académicas. Revista Ibérica de Sistemas e Tecnologías de Informação, (32), 45–58.	Articulo	https://scielo.pt/pdf/rist/n32/n32a04.pdf

Glosario

Ataque de phishing: técnica de ingeniería social que busca engañar a los usuarios para que revelen información confidencial, como credenciales de acceso o datos financieros, a través de correos electrónicos fraudulentos o sitios web falsos.

Ataque de ransomware: tipo de amenaza informática en la que un malware cifra los archivos del usuario o sistema y exige un rescate para su liberación.

Cifrado: técnica de seguridad que convierte información en un formato ilegible para protegerla de accesos no autorizados. Solo puede ser descifrada con una clave específica.

Código malicioso (malware): programas diseñados para dañar, alterar o acceder de forma no autorizada a sistemas informáticos, incluyendo virus, troyanos, gusanos y spyware.

Doble autenticación: método de seguridad que requiere dos formas de verificación antes de conceder acceso a un sistema, como una contraseña y un código enviado al móvil.

Firewall: sistema de seguridad que controla el tráfico de red entrante y saliente según reglas predefinidas, protegiendo los dispositivos contra accesos no autorizados.

Gusano: tipo de malware que se replica automáticamente en un sistema sin necesidad de intervención humana, propagándose a través de redes y causando daños.

Malware: software malicioso diseñado para infiltrarse, dañar o comprometer la seguridad de un sistema informático sin el consentimiento del usuario.

Privacidad digital: derecho y práctica de proteger la información personal y los datos de los usuarios en entornos digitales, evitando el acceso no autorizado y el uso indebido de la información.

Puerta trasera: método de acceso oculto en un sistema que permite el control remoto sin el conocimiento del usuario, a menudo explotado por atacantes.

Riesgo informático: probabilidad de que una vulnerabilidad sea explotada por una amenaza, causando daño o afectación a un sistema, red o información.

Spyware: tipo de software malicioso que recopila información del usuario sin su consentimiento y la transmite a un tercero.

VPN (Red Privada Virtual): tecnología que crea una conexión segura y cifrada entre un dispositivo y una red, protegiendo la privacidad y evitando la interceptación de datos.

Referencias bibliográficas

Arango Gómez, O. (s.f.). El ABC de la seguridad informática: Guía práctica para entender la seguridad digital. Instituto Tecnológico Metropolitano. https://repositorio.itm.edu.co/bitstream/handle/20.500.12622/5901/El%20ABC%20de%20la%20seguridad%20inform%C3%A1tica%20gu%C3%ADa%20pr%C3%A1ctica%20para%20entender%20la%20seguridad%20digital.pdf

Ecosistema de Recursos Educativos Digitales. (2022). Ataques y vulnerabilidades [Video]. YouTube. https://www.youtube.com/watch?v=au8EXjh-0jw

Ecosistema de Recursos Educativos Digitales. (2022). La ingeniería social [Video]. YouTube. https://www.youtube.com/watch?v=5FeJVcZerS0

Ecosistema de Recursos Educativos Digitales. (2022). Metodologías del Hacking ético [Video]. YouTube. https://www.youtube.com/watch?v=r3S8tscj-bg

Guaña-Moya, J. (2023). La importancia de la seguridad informática en la educación digital: Retos y soluciones. RECIMUNDO, 7(1), 609–616. https://doi.org/10.26820/recimundo/7.(1).enero.2023.609-616

Instituto Valenciano de Ciberseguridad y Telemática. (2021). Ciberseguridad: El reto del siglo XXI. https://invaci.es/wp-content/uploads/2021/08/CIBERSEGURIDAD-EL-RETO-DEL-SIGLO-XXI.pdf

Paya-Santos, C., & Luque-Juárez, J. M. (2021). El sistema de inteligencia criminal ante las nuevas amenazas y oportunidades del ciberespacio. Revista Científica General José María Córdova, 19(36), 1121–1136. https://doi.org/10.21830/19006586.855

Tejena-Macías, M. A. (2018). Análisis de riesgos en seguridad de la información. Polo del Conocimiento, 3(4), 230. https://doi.org/10.23857/pc.v3i4.809

Créditos

Nombre	Cargo	Centro de Formación y Regional
Milady Tatiana Villamil Castellanos	Responsable Ecosistema de Recursos Educativos Digitales (RED)	Dirección General
Diana Rocío Possos Beltrán	Responsable de línea de producción	Centro de Comercio y Servicios - Regional Tolima
Javier Eduardo Díaz Machuca	Experto temático	Centro de Comercio y Servicios - Regional Tolima
Viviana Esperanza Herrera Quiñonez	Evaluadora instruccional	Centro de Comercio y Servicios - Regional Tolima
Oscar Ivan Uribe Ortiz	Diseñador web	Centro de Comercio y Servicios - Regional Tolima
Juan Daniel Polanco Muñoz	Diseñador web	Centro de Comercio y Servicios - Regional Tolima
Sebastian Trujillo Afanador	Desarrollador Fullstack	Centro de Comercio y Servicios - Regional Tolima
Ernesto Navarro Jaimes	Animador y productor audiovisual	Centro de Comercio y Servicios - Regional Tolima
Jorge Eduardo Rueda Peña	Evaluador de contenidos inclusivos y accesibles	Centro de Comercio y Servicios - Regional Tolima

Nombre	Cargo	Centro de Formación y Regional
Jorge Bustos Gómez	Validador y vinculador de recursos educativos digitales	Centro de Comercio y Servicios - Regional Tolima