Curso de Fundamentos de la Ciberseguridad

Una introducción completa a la seguridad informática

DASSAEFD SÁNCHEZ JIMÉNEZ

Instituto Tecnológico Superior del Oriente del Estado de Hidalgo

Apan Hidalgo, México

Febrero 2025

Curso realizado en la plataforma Coursera.

Índice

1. Términos y conceptos clave de la ciberseguridad

Un analista de seguridad o analista de ciberseguridad se centra en supervisar las redes en busca de infracciones. También ayudan al desarrollo de estrategias para asegurar una organización y se dedican a investigar las tendencias de seguridad de la tecnología de la información, esto ayuda al analista a mantenerse a las nuevas amenazas potenciales.

Los analistas necesitan desarrollar conocimientos sobre los siguientes conceptos clave:

1.1. Cumplimiento normativo

Son estándares internos y regulaciones externas a lo cual permite que las organizaciones eviten multas y violaciones de la **SEGURIDAD**.

1.2. Marcos de seguridad

Directrices utilizadas para elaborar planes de ayuda para mitigar los riesgos y amenazas para los datos y la privacidad.

1.3. Controles de seguridad

Son diseñados para reducir el riesgo de seguridades específicas.

1.4. Postura de seguridad

Capacidad que tiene una organización para la gestionar su defensa de activos y datos crítico, reaccionar ante los cambios. Una postura de seguridad fuerte conlleva a que exista un menor riesgo para la organización.

1.5. Agente de amenaza

O también denominado atacante malicioso, cualquier persona o grupo que presenta un riesgo para la seguridad. Este riesgo puede estar relacionado con computadoras, aplicaciones, redes y datos.

1.6. Amenaza interna

Puede ser un empleado actual o antiguo, un proveedor externo o un socio de confianza que suponga un riesgo para la seguridad. En varias ocasiones una amenaza interna es accidental. Ejemplo, un empleado que haga clic accidentalmente en un enlace de correo electrónico malicioso se considera una amenaza accidental. O en algunas ocasiones el actor se involucra con datos no permitidos de maneta intencional.

1.7. Seguridad de red

Es aquella practica de mantener la infraestructura de red de una organización a salvo de accesos no autorizado. Esto incluye a los datos, servicios, sistemas y dispositivos que se almacenan en la red de la organización.

1.8. Seguridad de la nube

Es aquel proceso de garantizar que los activos almacenados en la nube estén correctamente configurados, o establecidos, y que el acceso a estos activos este limitado a los usuarios autorizados. La seguridad de la nube es un subcampo creciente de la ciberseguridad que se centra específicamente en la protección de los datos, las aplicaciones y la infraestructura en la nube.

1.9. Programación

Es un proceso que puede utilizar para crear un conjunto especifico de tareas o instrucciones para que una computadora se encargue de ejecutarlas. Las tareas pueden incluir:

- Automatización de tareas repetitivas (Ejemplo: buscar una lista de dominios maliciosos)
- Revisión del tráfico de web
- Alerta de actividades sospechosas

2. Competencias básicas para los profesionales de la ciberseguridad

2.1. Habilidades transferibles y técnicas de ciberseguridad

2.2. Comunicación

Un analista de ciberseguridad, necesitará comunicarse y colaborar con los demás. Comprender las preguntas o preocupaciones de los demás y comunicar la información con claridad a personas con conocimientos técnicos y no técnicos le ayudará a mitigar rápidamente los problemas de seguridad.

2.3. Colaboración

Identificar y resolver problemas de forma proactiva. Puede hacerlo reconociendo patrones de ataque y determinando después la solución más eficaz para minimizar el riesgo.

2.4. Gestionar el tiempo

Tener un gran sentido de la urgencia y priorizar las tareas adecuadamente es esencial en el campo de la ciberseguridad. Así, una gestión eficaz del tiempo le ayudará a minimizar los posibles daños y riesgos para los recursos y datos críticos.

2.5. Analista y Resolución de problemas

El analista de seguridad debe de tener habilidades técnicas como:

- Programación en varios lenguajes: Lenguajes como Python y SQL
- Administración de información y eventos de seguridad (SIEM): Se ocupa para analizar y entender las amenazas que existen.

- Información forense: Identificar, analizar y preservar la evidencia criminal dentro de redes, computadoras y dispositivos electrónicos.
- Sistemas de detección de intrusiones (IDS): Los analistas de ciberseguridad utilizan los IDS para monitorizar la actividad del sistema y las alertas de posibles intrusiones. Es importante familiarizarse con los IDS porque son una herramienta clave que toda organización utiliza para proteger los recursos y los datos.

3. La importancia de la ciberseguridad

La seguridad es esencial para garantizar la continuidad del negocio y la integridad ética de una organización. Existen tanto implicaciones legales como consideraciones morales en su mantenimiento. Una brecha de datos puede afectar la reputación de la organización y la vida de sus usuarios, clientes y consumidores. Mantener medidas de seguridad sólidas aumenta la confianza de los usuarios, lo que puede traducirse en crecimiento financiero y referencias comerciales.

Las organizaciones no son las únicas afectadas en una brecha de seguridad; también lo son los usuarios, clientes y proveedores. Proteger sus datos es clave para evitar la exposición de información personal identificable (PII), que incluye nombre, fecha de nacimiento, dirección, teléfono, correo electrónico y dirección IP.

Existe información personal identificable sensible (SPII), que requiere un manejo más estricto e incluye datos como números de seguridad social, información médica o financiera y datos biométricos. El robo de esta información puede ser aún más perjudicial.

Los datos PII y SPII son objetivos principales en una brecha de seguridad, lo que puede derivar en robo de identidad, donde los delincuentes utilizan información personal para cometer fraudes, principalmente con fines financieros.

La demanda de profesionales en seguridad sigue en aumento, ya que las empresas necesitan expertos que protejan datos, productos y personas, garantizando la confidencialidad, integridad y acceso seguro a la información. La Oficina de Estadísticas Laborales de EE.UU. estima que el crecimiento del sector superará el 30 % para 2030. Seguir aprendiendo permitirá contribuir a un entorno más seguro para organizaciones y personas.

4. Ataques comunes y su eficacia

Ataques como LoveLetter, tambien conocido como el virus ILOVEYOU, y el gusano Morris. Uno de los resultados fue la creacion de equipos de respuesta, que ahora se denominan conmumente “Equipos de respuesta ante incidentes de seguridad informatica (CSIRT).

4.1. Pishing

Es el uso de las comunicaciones digitales para engañar a las personas con el fin de que revelen datos sensibles o implementen software malicioso.

Algunos tipos mas comunes en la actualidad, son lo siguiente:

- Compromiso de correo electrónico empresarial (BEC): Un agente de amenaza envia un mensaje de correo electronico que parece proceder de una fuente conocida para realizar la solicitud de informacion.
- Spear pishing: Ataque malicioso por correo electronico dirigido a un usuario o gripo de usuarios especificos.

- Whaling: Forma de pishing dirigido. Los que atacan tienen como objetivo a ejecutivos de la empresa para obtener accesos a datos confidenciales.
- Vishing: El exploit de la comunicación electronica de voz para obtener informacion sensible o hacerse pasar por una fuente conocida.
- Smishing: Mensajes de texto para engañar a los usuarios, con el fin de obtner informacion sensible o hacerse pasar por una fuente conocida.

4.2. Software malicioso

Es un software diseñado para dañar dispositivos o redes. El objetivo principal del software malicioso es obtener dinero o, en algunos casos, una ventaja de inteligencia que pueda utilizarse contra una persona, una organización o territorio.

Algunos de estos software maliciosos en la actualidad son los siguientes:

- **Virus:** Código malicioso escrito para interferir en las operaciones de la computadora y causar daño a los datos y al software. Un virus debe ser iniciado por un usuario, que transmite el virus a traves de un archivo adjunto malicioso o de la descarga de un archivo.
- **Gusanos:** Software malicioso que puede duplicarse y propagarse por los sistemas por si mismo. A diferencia de un virus, un gusano no necesita ser descargado por un usuario. Este se propaga e infecta a varios dispositivos conectados a la misma red.
- **Ransomware:** Ataque malicioso en el que los agentes de amenazas encriptan los Datos de una organización y exigen un pago para restablecer la accesibilidad.
- **Software espía:** Software malicioso que se utiliza para recopilar y vender información sin consentimiento.

4.3. Ingeniería Social

Es una tecnica de manipulacion que explota el error humano para obtener informacion privada, accesibilidad u objetos de valor.

Algunos de los tipos más comunes de ataques de ingeniería social en la actualidad incluyen:

- Phishing en redes sociales: Un agente de amenaza recopila información detallada sobre su objetivo en los sitios de redes sociales. A continuación, inician un ataque.
- Ataque de “agujero de agua”: Un agente de amenaza ataca un sitio web visitado con frecuencia por un grupo específico de usuarios.
- USB baiting: Un agente de amenaza deja estratégicamente una memoria USB con software malicioso para que un empleado la encuentre e instale, con el fin de infectar una red sin saberlo.
- Ingeniería social física: Un agente de amenaza se hace pasar por un empleado, cliente o proveedor para obtener acceso no autorizado a un lugar físico.

La ingeniería social es eficaz porque aprovecha la confianza y el respeto a la autoridad. Su impacto aumenta con el uso de redes sociales, donde se exponen datos personales. Los ataques se basan en tácticas como: autoridad (haciéndose pasar por figuras de poder), intimidación

(presionando a la víctima), prueba social (simulando legitimidad), escasez (generando sensación de oportunidad limitada), familiaridad y confianza (creando vínculos emocionales) y urgencia (forzando decisiones rápidas).

A medida que evolucionan las amenazas, los profesionales de Seguridad deben adaptarse. El CISSP define ocho dominios para organizar este trabajo, ya que las brechas en uno pueden afectar a toda la organización. Comprender estos dominios ayuda a definir objetivos profesionales y roles dentro de una empresa.

5. Introducción a los ocho dominios de Seguridad CISSP, Parte 1

Este video presenta los primeros cuatro dominios:

- **Seguridad y gestión de riesgos:** Define metas de seguridad, mitiga riesgos y garantiza el cumplimiento de normativas como HIPAA.
- **Seguridad de los recursos:** Protege activos físicos y digitales, gestionando almacenamiento, mantenimiento y eliminación segura de datos.
- **Arquitectura e ingeniería de seguridad:** Optimiza la seguridad mediante herramientas y sistemas, como la correcta configuración de firewalls.
- **Seguridad de la red y las comunicaciones:** Administra y protege redes físicas e inalámbricas, evitando vulnerabilidades como el uso de accesos no seguros.

Mantener la seguridad es un esfuerzo de equipo. No es necesario ser experto en todos los dominios, pero conocerlos fortalece el desarrollo profesional en Seguridad.

6. Introducción a los ocho dominios de Seguridad CISSP, Parte 2

Este video presenta los últimos cuatro dominios de Seguridad del CISSP, esenciales para entender cómo los equipos trabajan juntos y cómo prepararse para roles en ciberseguridad.

- **Gestión de identidades y accesos:** Controla el acceso a recursos físicos y digitales, garantizando la seguridad mediante autenticación y permisos adecuados.
- **Evaluación y pruebas de Seguridad:** Realiza auditorías y pruebas de control para detectar riesgos, amenazas y vulnerabilidades.
- **Operaciones de Seguridad:** Implementa medidas preventivas e investiga incidentes, como la detección de dispositivos no autorizados en la red.
- **Seguridad del desarrollo de software:** Aplica prácticas de programación seguras para proteger aplicaciones y servicios desde su creación.

Con esto concluye la introducción a los ocho dominios de Seguridad. Se explorarán con más profundidad en el siguiente curso.

7. Tipos de ataque

- **Ataque de descifrado de contraseña:** Intento de obtener acceso a sistemas protegidos mediante técnicas como fuerza bruta y tablas rainbow. Relacionado con Seguridad de redes y comunicaciones.
- **Ataque de ingeniería social:** Explotación del error humano para obtener información o acceso. Incluye phishing, smishing, vishing, whaling, BEC, cebo USB, entre otros. Relacionado con Seguridad y Gestión de riesgos.
- **Ataque físico:** Afecta tanto a entornos digitales como físicos, incluyendo USBs maliciosos, clonación de tarjetas y robo de dispositivos. Relacionado con Seguridad de los recursos.
- **Inteligencia artificial antagónica:** Manipula la IA y el aprendizaje automático para realizar ataques más sofisticados. Relacionado con Seguridad de redes y comunicaciones, y Gestión de identidad y acceso.
- **Ataque a la cadena de suministro:** Compromete sistemas, software y hardware aprovechando vulnerabilidades en proveedores y terceros. Relacionado con Seguridad y Gestión de riesgos, Arquitectura de seguridad e ingeniería y Operaciones de seguridad.
- **Ataque criptográfico:** Compromete formas seguras de comunicación mediante técnicas como ataque de cumpleaños, colisión y degradación. Relacionado con Seguridad de redes y comunicaciones.

8. Comprender a los atacantes

8.1. Tipos de Actores de Amenaza en Ciberseguridad

En el mundo de la ciberseguridad, un actor de amenaza es cualquier persona o grupo que representa un riesgo para la seguridad de la información. Estos actores pueden tener diferentes motivaciones, intenciones y niveles de habilidad. A continuación, se presentan los tipos más comunes:

8.1.1. Amenaza Persistente Avanzada (APT)

Las APT (Advanced Persistent Threats) son grupos altamente organizados y con recursos que se infiltran en redes de grandes empresas o entidades gubernamentales con el objetivo de permanecer sin ser detectados durante largos periodos de tiempo.

Características:

- Son persistentes, lo que significa que pueden mantenerse dentro del sistema durante meses o años.
- Utilizan técnicas avanzadas para evadir la detección.
- Suelen estar respaldadas por Estados o grandes organizaciones criminales.

Motivaciones:

- Sabotaje: Dañar infraestructuras críticas, como la red eléctrica o los sistemas financieros de un país.
- Espionaje: Obtener acceso a secretos comerciales, patentes o información sensible de gobiernos y empresas.

8.1.2. Amenazas Internas

No todos los ataques vienen del exterior. Algunos de los riesgos más peligrosos provienen de personas con acceso autorizado a los sistemas de una organización.

Características:

- Puede ser un empleado, un ex-empleado, un contratista o cualquier persona con acceso a la red de la empresa.
- Generalmente, ya tienen acceso a datos críticos, lo que hace más difícil detectarlos.

Motivaciones:

- Sabotaje: Borrar o modificar información para dañar la empresa.
- Corrupción: Compartir datos confidenciales a cambio de dinero.
- Espionaje: Filtrar información estratégica a competidores o gobiernos extranjeros.
- Venganza: Empleados descontentos pueden filtrar información o realizar ataques internos.

8.1.3. Hacktivistas

Los hacktivistas son personas o grupos que utilizan la tecnología para promover una causa política, social o ideológica.

Características:

- Suelen atacar gobiernos, corporaciones o entidades que consideran "injustas".
- Sus acciones pueden incluir ataques de denegación de servicio (DDoS), filtraciones de datos o defacement (modificación de sitios web).

Motivaciones:

- Manifestaciones digitales: Protestar contra gobiernos o empresas.
- Propaganda: Difundir su ideología mediante ataques cibernéticos.
- Cambio social: Intentar exponer injusticias o corrupción a través del hackeo.
- Búsqueda de reconocimiento: Algunos lo hacen para ganar notoriedad o credibilidad en la comunidad hacker.

8.1.4. Tipos de Hackers

Los hackers pueden clasificarse en tres grandes categorías según su intención y el impacto de sus acciones:

Hackers Autorizados (Hackers Éticos o White Hat)

- Trabajan de manera legal para mejorar la seguridad de empresas y gobiernos.
- Siguen un código de ética y respetan la ley.
- Realizan pruebas de penetración para detectar vulnerabilidades antes de que los hackers maliciosos las aprovechen.

Hackers Semiautorizados (Gray Hat)

- Buscan vulnerabilidades, pero no siempre las reportan a los dueños del sistema.
- En ocasiones pueden explotar fallos para demostrar que existen, pero sin intención de dañar.

Hackers No Autorizados (Hackers Maliciosos o Black Hat)

- Son delincuentes informáticos que buscan explotar sistemas para obtener dinero, causar daños o robar información.
- Pueden vender datos personales, realizar ataques de ransomware o robar cuentas bancarias.

8.1.5. Otros Tipos de Hackers

Además de las categorías anteriores, existen otros tipos de hackers con diferentes motivaciones:

- Hackers novatos o no cualificados (Script Kiddies): Son principiantes que utilizan herramientas creadas por otros para atacar sistemas sin comprender realmente cómo funcionan.
- Hackers mercenarios: Trabajan por dinero y pueden ser contratados para actividades legales o ilegales.
- Hackers vigilantes: Actúan como "justicieros" en internet, atacando a hackers maliciosos o revelando información de criminales.

9. Introducción a los marcos y controles de Seguridad

Imagine que trabaja como analista de Seguridad y recibe múltiples alertas sobre actividades sospechosas en la red. Se da cuenta de que necesitará implementar medidas de Seguridad adicionales para evitar que estas alertas se conviertan en incidentes graves. Pero, ¿por dónde empezar?

Como analista, empezará por identificar los activos y riesgos críticos de su organización. A continuación, implementará los marcos y controles necesarios.

Los Marcos de seguridad son directrices que se utilizan para crear planes que ayuden a mitigar los riesgos y las amenazas a los datos y la privacidad. Marcos de seguridad proporcionan un enfoque estructurado para implementar un ciclo de vida de seguridad. El ciclo de vida de

la seguridad es un conjunto de políticas y normas en constante evolución que definen la forma en que una organización gestiona los riesgos, sigue las directrices establecidas y cumple con las leyes o el cumplimiento de las normativas.

Hay varios marcos de Seguridad que se pueden usar para administrar diferentes tipos de riesgos de cumplimiento normativo y organizacional. El propósito de los marcos de seguridad incluye proteger la información de identificación personal, conocida como PII, asegurar la información financiera, identificar las debilidades de seguridad, administrar los riesgos organizacionales y alinear la seguridad con los objetivos comerciales.

Los marcos tienen cuatro componentes principales y comprenderlos le permitirá gestionar mejor los riesgos potenciales. El primer componente principal es identificar y documentar los objetivos de Seguridad. Por ejemplo, una organización puede tener el objetivo de alinearse con el Reglamento General de Protección de Datos (GDPR). El RGPD es una ley de protección de datos establecida para conceder a los ciudadanos europeos un mayor control sobre sus datos personales. Es posible que se le pida a un analista de seguridad que identifique y documente las áreas en las que una organización no cumple con el GDPR.

El segundo componente principal es establecer directrices para lograr los objetivos de Seguridad. Por ejemplo, al implementar directrices para cumplir con el GDPR, es posible que su organización necesite desarrollar nuevas políticas sobre cómo gestionar las solicitudes de datos de los usuarios individuales.

El tercer componente central de los marcos de seguridad es la implementación de procesos de seguridad sólidos. En el caso del GDPR, un analista de Seguridad que trabaje para una empresa de redes sociales puede ayudar a diseñar procedimientos para garantizar que la organización cumpla con las solicitudes de datos de usuario verificadas. Un ejemplo de este tipo de solicitud es cuando un usuario intenta actualizar o eliminar la información de su perfil.

El último componente central de los marcos de Seguridad es el monitoreo y la comunicación de los resultados. Por ejemplo, puedes supervisar la red interna de tu organización e informar a tu gerente u oficial de cumplimiento normativo sobre un posible problema de Seguridad que afecte al GDPR.

Ahora que hemos presentado los cuatro componentes principales de los marcos de Seguridad, vamos a unirlos todos. Los marcos permiten a los analistas trabajar junto con otros miembros del equipo de Seguridad para documentar, implementar y usar las políticas y los procedimientos que se han creado. Es fundamental que un analista principiante comprenda este proceso, ya que afecta directamente al trabajo que realizan y a la forma en que colaboran con los demás. A continuación, analizaremos los controles de Seguridad.

Los Controles de seguridad son medidas de seguridad diseñadas para reducir los riesgos de seguridad específicos. Por ejemplo, es posible que su empresa tenga una directriz que obligue a todos los empleados a completar una formación sobre privacidad para reducir el riesgo de violaciones de datos. Como analista de Seguridad, puede utilizar una herramienta de software para asignar automáticamente y hacer un seguimiento de los empleados que han completado esta formación. Los Marcos de seguridad y los controles son vitales para administrar la seguridad de todos los tipos de organizaciones y garantizar que todos hagan su parte para mantener un nivel de riesgo bajo.

10. Diseño seguro

10.1. Tríada CID de la CIA

La tríada CID es un modelo fundamental en Seguridad de la Información que ayuda a gestionar el riesgo mediante tres principios clave:

Confidencialidad: Solo los usuarios autorizados pueden acceder a datos y recursos.
Implementación: Controles de acceso estrictos, autenticación y cifrado.

Integridad: Garantiza que los datos sean correctos, auténticos y confiables.
Implementación: Mecanismos de encriptación y protección contra manipulaciones.

Disponibilidad: Los datos deben estar accesibles para los usuarios autorizados.
Implementación: Sistemas de respaldo, redundancia y medidas contra ataques de denegación de servicio (DDoS).

10.2. Concepto de Recurso

Un recurso es cualquier elemento valioso para una organización, cuyo valor se determina por su costo o impacto.
Ejemplo: Una aplicación con datos sensibles (cuentas bancarias, Seguridad Social) requiere mayores controles que un sitio de noticias público.

10.3. Marco de Ciberseguridad del NIST (NIST CSF)

Desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU., este marco proporciona estándares, directrices y mejores prácticas para gestionar el riesgo de ciberseguridad.

Objetivo: Ayudar a los equipos de Seguridad a gestionar riesgos a corto y largo plazo.
Componentes clave:

- Identificar
- Proteger
- Detectar
- Responder
- Recuperarse

10.4. Actores de Amenazas

Los actores de amenazas pueden provenir de diversas fuentes, incluyendo:

- Empleados descontentos (riesgo interno)
- Hackers y atacantes externos
- Grupos patrocinados por estados o competidores

Para mitigar estos riesgos, se aplican principios como la disponibilidad controlada y el acceso basado en roles.

10.5. Importancia de la Diversidad en la Seguridad

Contar con un equipo diverso en Seguridad permite entender mejor las intenciones de los atacantes y mejorar la protección de la organización.

11. Controles, Marcos y Cumplimiento Normativo

11.1. Relación entre Controles, Marcos y Cumplimiento

Controles de seguridad: Salvaguardas que reducen riesgos específicos.
Marcos de seguridad: Directrices para mitigar amenazas y mejorar la protección.
Cumplimiento normativo: Adherencia a regulaciones y estándares internos y externos.

11.2. Marcos y Estándares Clave

- NIST CSF y NIST RMF: Frameworks del Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU. para gestionar riesgos.
- CIS Controls: Guías para fortalecer la seguridad informática.
- ISO: Normas internacionales para mejorar procesos y seguridad.

11.3. Principales Regulaciones

- GDPR: Protección de datos de ciudadanos de la UE.
- PCI DSS: Seguridad en el procesamiento de tarjetas de crédito.
- HIPAA: Protección de datos médicos en EE. UU.
- FedRAMP: Seguridad en la nube para agencias gubernamentales.
- FERC-NERC: Seguridad de la infraestructura eléctrica en EE. UU.
- SOC 1 y SOC 2: Auditorías de control organizacional y financiero.

11.4. Orden Ejecutiva 14028

Emitida en 2021 por el gobierno de EE. UU. para reforzar la ciberseguridad en infraestructuras críticas.
Consejo: Las regulaciones evolucionan constantemente; mantenerse actualizado es clave para la seguridad.

12. Ética en la ciberseguridad

Imparcialidad y Confidencialidad: Un profesional de seguridad debe actuar de manera imparcial, incluso si el incidente involucra a un amigo. Es crucial respetar las políticas y protocolos establecidos, garantizando la confidencialidad de los datos.

Responsabilidad en el Uso de Accesos: Los analistas de seguridad tienen un acceso privilegiado a la información. No deben abusar de este acceso, como en el caso de otorgarse un aumento sin justificación.

Principios Éticos:

- Confidencialidad: Mantener la información privada y segura. No se debe compartir información de acceso fuera de los canales oficiales.
- Protección de la Privacidad: Es importante proteger la información personal de accesos no autorizados, incluso si alguien, como un gerente, lo solicita de manera inapropiada.
- Cumplimiento de la Ley: Los profesionales deben seguir las leyes y regulaciones para garantizar la protección de los datos, evitando negligencias que puedan resultar en consecuencias legales.
- Evolución Constante de la Tecnología y la Seguridad: Los atacantes también evolucionan, por lo que los profesionales de seguridad deben seguir actualizándose y tomar decisiones éticas para mitigar los riesgos.

13. Conceptos éticos que guían las decisiones sobre ciberseguridad

13.1. Ética en la Seguridad Cibernética

La ética de la seguridad son reglas que ayudan a los profesionales a tomar decisiones correctas. Los expertos en seguridad deben ser imparciales, proteger los datos privados y seguir las leyes.

Contraataques: ¿Se deben hacer?

En EE.UU.: No se permite realizar contraataques. Las leyes prohíben hacerlo, y hacerlo puede empeorar la situación o causar más daños. Solo el personal del gobierno o militares pueden contraatacar.

Internacionalmente: Algunos países permiten los contraataques, pero solo si no empeoran el problema y son proporcionados. Sin embargo, las organizaciones prefieren no hacerlo porque hay muchos riesgos y no siempre está claro si es legal o no.

Principios Éticos Clave:

- Confidencialidad: Solo personas autorizadas deben acceder a los datos privados. Los profesionales deben proteger esa información.
- Protección de la Privacidad: Los datos personales deben protegerse para evitar que se usen de manera incorrecta. Esto incluye información como tu nombre, número de teléfono, o detalles bancarios.
- Cumplimiento de las Leyes: Los profesionales deben seguir las leyes sobre protección de datos, como la HIPAA (en EE.UU.), que protege la información de salud de los pacientes.

14. Herramientas para proteger operaciones B2B

Los analistas de seguridad utilizan diversas herramientas para proteger las operaciones **Business-to-Business (B2B)** (Negocio a negocio) y mitigar riesgos. Las herramientas clave incluyen:

- **Herramientas SIEM (Security Information and Event Management) - Gestión de Información y Eventos de Seguridad:**
  - Aplicaciones que recopilan y analizan datos de registro para monitorear las actividades críticas de una organización.
  - Permiten organizar y visualizar datos mediante paneles y generar alertas sobre amenazas y vulnerabilidades.
  - Se pueden alojar localmente (*on-premise*) o en la nube (*cloud*), según la experiencia del equipo.
- **Analizadores de protocolos de red (Packet Sniffers) - Rastreadores de paquetes:**
  - Capturan y analizan el tráfico de datos en una red para detectar actividad sospechosa o ataques.
  - Facilitan la investigación de incidentes y la detección de intrusiones.
- **Manuales de estrategias (Playbooks) - Libros de jugadas:**
  - **Cadena de custodia (Chain of Custody):** Documenta el control y la posesión de las pruebas durante una investigación para asegurar su integridad.
  - **Protección y preservación de evidencias (Evidence Protection and Preservation):** Define el orden para conservar datos volátiles y evitar su pérdida o manipulación.
    - La preservación adecuada implica hacer copias de los datos originales y trabajar sobre ellas.

Estas herramientas y estrategias son esenciales para la gestión de incidentes y la investigación forense, asegurando la integridad de los datos y el cumplimiento de los procedimientos de seguridad.

15. Herramientas para proteger operaciones B2B Parte 2

En el campo de la ciberseguridad, los analistas utilizan diversas herramientas para proteger las operaciones **Business-to-Business (B2B)** (Negocio a negocio) y mitigar riesgos. Las herramientas clave incluyen:

- **Programación:**
  - La programación permite crear instrucciones específicas para que una computadora ejecute tareas.
  - Los analistas de seguridad utilizan lenguajes como **Python** para automatizar tareas repetitivas y reducir errores humanos.
  - También utilizan **SQL (Structured Query Language) - Lenguaje de Consulta Estructurada** para interactuar con bases de datos y gestionar grandes volúmenes de información.
- **Sistemas operativos:**

- Los sistemas operativos (**OS**) como **Linux**, **macOS** y **Windows** gestionan la interacción entre el hardware y el usuario.
- Linux es un sistema operativo de **código abierto** que permite modificaciones por parte de la comunidad.
- La **interfaz de línea de comandos (CLI)** permite a los usuarios ejecutar comandos directamente para administrar sistemas.

- **Vulnerabilidades web:**
  - Una vulnerabilidad web es una falla en una aplicación web que puede ser explotada para permitir el acceso no autorizado o el robo de datos.
  - El proyecto **OWASP Top 10** enumera las vulnerabilidades más críticas para las aplicaciones web.
- **Software antivirus:**
  - Programa que previene, detecta y elimina software malicioso y virus.
  - Escanea la memoria del dispositivo para identificar patrones que indiquen amenazas potenciales.
- **Sistema de detección de intrusiones (IDS - Intrusion Detection System):**
  - Monitoriza la actividad del sistema y alerta sobre posibles intrusiones.
  - Analiza los paquetes de red para identificar intentos de acceso no autorizado o robos de datos.
- **Encriptación:**
  - Convierte datos legibles en texto cifrado para evitar accesos no autorizados.
  - El proceso transforma texto plano en texto cifrado seguro mediante algoritmos criptográficos.
  - La **codificación** se diferencia de la encriptación, ya que su propósito es permitir que diferentes sistemas compartan datos.
- **Pruebas de penetración (Pen Testing):**
  - Simulación de ataques para identificar vulnerabilidades en sistemas, redes, aplicaciones y procesos.
  - Evalúa amenazas externas e internas, identificando puntos débiles en la infraestructura de seguridad.

Las herramientas y procesos descritos permiten a los analistas de seguridad completar sus tareas de manera más eficiente y efectiva, ayudando a las organizaciones a protegerse de amenazas y vulnerabilidades.