Módulo 2: Fundamentos de seguridad computacional

Lección 2: Modelos de Ataque, Daños y Controles Iniciales

Objetivos de la Lección

Al finalizar la sesión, el estudiante podrá — con ejemplos concretos —

1. **Explicar** de forma específica las categorías de ataque (intercepción, modificación, fabricación e interrupción) y sus variantes técnicas.
2. **Analizar** los daños que dichos ataques provocan, distinguiendo entre la triada CIA y los impactos colaterales (vida, reputación, recursos).
3. **Seleccionar** controles físicos, técnicos y administrativos apropiados para prevenir, disuadir, desviar, mitigar, detectar y reportar incidentes, relacionándolos con políticas de privacidad, autenticidad, responsabilidad y confianza.

Introducción a la Lección

Cada incidente de ciberseguridad puede verse como una **cadena**: una **vulnerabilidad** abre la puerta; un **método de ataque** la atraviesa; se produce un **daño** concreto; y los **controles** interrumpen o amortiguan el proceso. Comprender el detalle de cada eslabón permite diseñar defensas **por capas** (***defence-in-depth***) en lugar de soluciones aisladas.

Desarrollo del Tema

Categorías de ataque: definiciones y ejemplos

En ciberseguridad distinguimos **cuatro grandes métodos de ataque** que describen *cómo* un adversario interfiere con un sistema (**Más información en:** https://www.baeldung.com/cs/security-interruption-interception-modification-fabrication?):

1. **Intercepción**
   Es la obtención no autorizada de información durante su almacenamiento o tránsito. El atacante *espía* sin modificar el contenido. Ejemplo clásico: un "sniffer" configurado en modo monitor, captura tráfico Wi-Fi abierto y extrae cookies de sesión, comprometiendo la **confidencialidad**. **Entiendase que un Sniffer** es una herramienta a nivel de software en el cual tiene como función el monitorizar y analizar el trafico de paquetes de una red. Los **sniffer** pueden realizar funciones como interceptación, registración y análisis de paquetes de datos que se transmiten entre dispositivos dentro de una red, permitiendo que administradores de sistemas y técnicos en ciberseguridad puedan examinar el contenido y estructura de estos paquetes, esto según Tarlogic Security(s.f.).
   a. **Flujo Simplificado**
      1. El atacante posiciona un sensor o sonda (sniffer, antena, microtap (**entiéndase con microtap** que este es un **dispositivo pequeño y discreto** que se coloca en una línea de comunicación (cable de red, línea telefónica, fibra) para **copiar o espiar el tráfico** sin interrumpirlo ni ser detectado fácilmente)).
      2. Captura pasivamente paquetes, señales o archivos.
      3. Reconstruye la información útil (cookies, credenciales, claves).
         - **Cookies** - Pequeños archivos de texto que un sitio web guarda en el navegador del usuario en el cual tienen como función el almacenar información para reconocer al usuario y recordar su actividad o preferencias.
   b. **Ejemplo Practico**

1. Un atacante configura una tarjeta Wi-Fi en modo monitor en un café y captura cookies de autenticación de usuarios que navegan sin HTTPS. Con ello secuestra sesiones de correo web, comprometiendo la **confidencialidad**.

2. **Modificación**

   Aquí el adversario altera datos legítimos — en reposo o en tránsito — para cambiar su significado o efecto. **Un ejemplo de Modificación** lo vemos en un ataque *Man-in-the-Middle* donde trata, según Lindemulder y Kosinski (2024), de un ataque en el que un ciber atacante roba información confidencial espiando las comunicaciones entre dos usuarios en línea, como por ejemplo un **usuario** y una **aplicación web (más información en: https://www.ibm.com/es-es/think/topics/man-in-the-middle)**. Para lo que es la **Modificación** el ataque MITM lo sería en que se puede reescribir un número de cuenta bancaria en una orden de transferencia violando así la **integridad** de los datos, aunque la víctima siga creyendo que todo es genuino.

   a. **Flujo simplificado**

      1. El atacante accede al flujo o archivo legítimo (p. ej., mediante ARP spoofing). **Entiedase** que **ARP Spoofing** es un ataque en redes locales donde un atacante envía mensajes falsos de ARP (Address Resolution Protocol) para asociar su dirección MAC con la IP de otro dispositivo (por ejemplo, el router o la víctima), esto con el objetivo de engañar a la red para que él tráfico que iba a un destino legítimo pase por él atacante.
      2. Edita el contenido (número de cuenta, comando, firmware).
      3. Reinyecta o almacena el dato modificado sin que el destinatario lo detecte.

   b. **Ejemplo práctico** e **imagen**

      1. Un *Man-in-the-Middle* en una red LAN corporativa reemplaza el IBAN (**International Bank Account Number**) en una orden de transferencia SWIFT. La víctima firma el pago, pero los fondos

llegan a la cuenta del atacante: se viola la **integridad** de la transacción.

2. La siguiente imagen muestra un ataque MITM

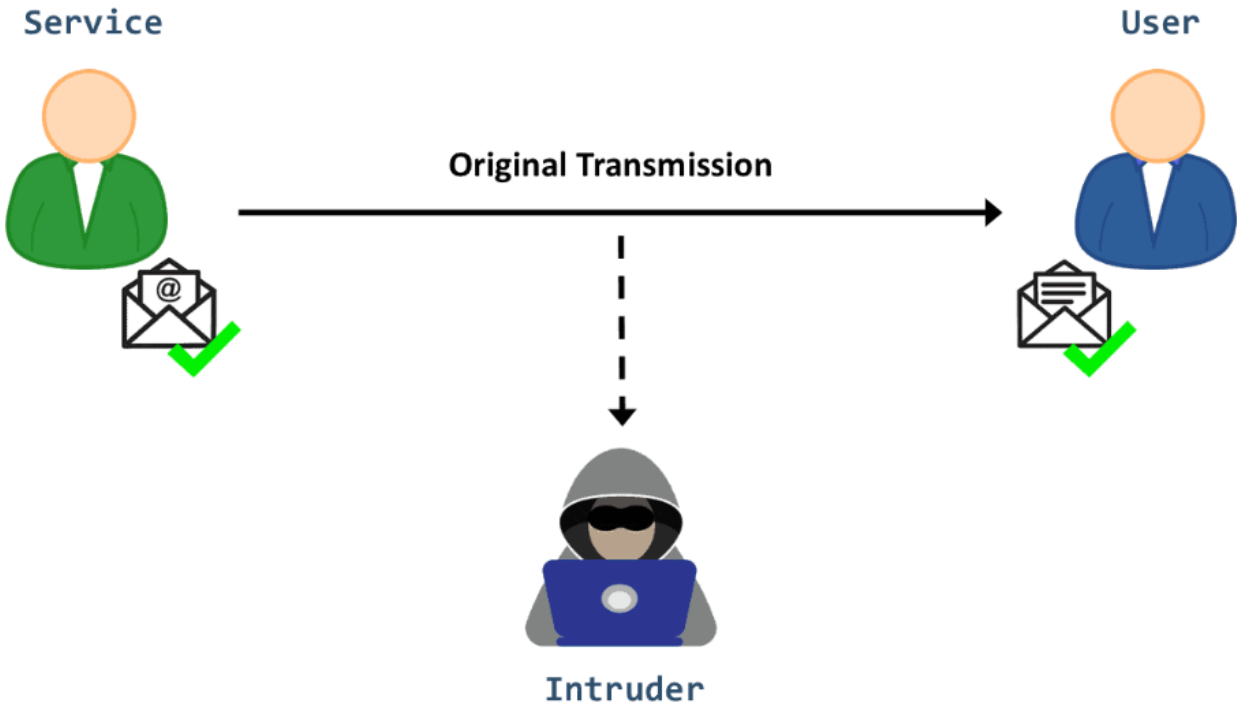

Imagen 1: *Ataque Man in th Middle*, Rhim y Simic (2023).

3. **Fabricación**

   Consiste en inyectar mensajes, paquetes o artefactos falsos que el sistema acepta como válidos, "**La falsificación ocurre cuando un intruso inyecta datos falsos o crea una pista falsa en el sistema**", Rhim y Simic (2023). Cuando un actor envía correos electrónicos falsificados con una factura apócrifa, hace que el ERP (**Enterprise Resource Planning**) cree datos que nunca fueron generados por la empresa, afectando simultáneamente **integridad** y **confidencialidad**.

   a. **Flujo simplificado**

      1. El adversario genera un objeto o mensaje apócrifo (phishing, paquete rogue, actualización falsa).

2. Lo introduce en el canal o repositorio de confianza (correo, DNS, gestor de software).
3. El sistema o usuario actúa sobre el objeto pensando que es legítimo.

b. Ejemplo práctico e imagen

1. Se envía por correo un archivo “Factura_abril.pdf.exe” firmado digitalmente con un certificado filtrado; al ejecutarlo, instala un *trojan* o troyano que extrae balances contables. Se comprometen **confidencialidad** e **integridad** simultáneamente. **Entiéndase que** un **Troyano** es un **Malware** que, bajo desconocimiento, podría descargarse en un ordenador aparentando ser un software o un programa legítimo.

2. Imagen del Metodo de Ataque de Fabricación

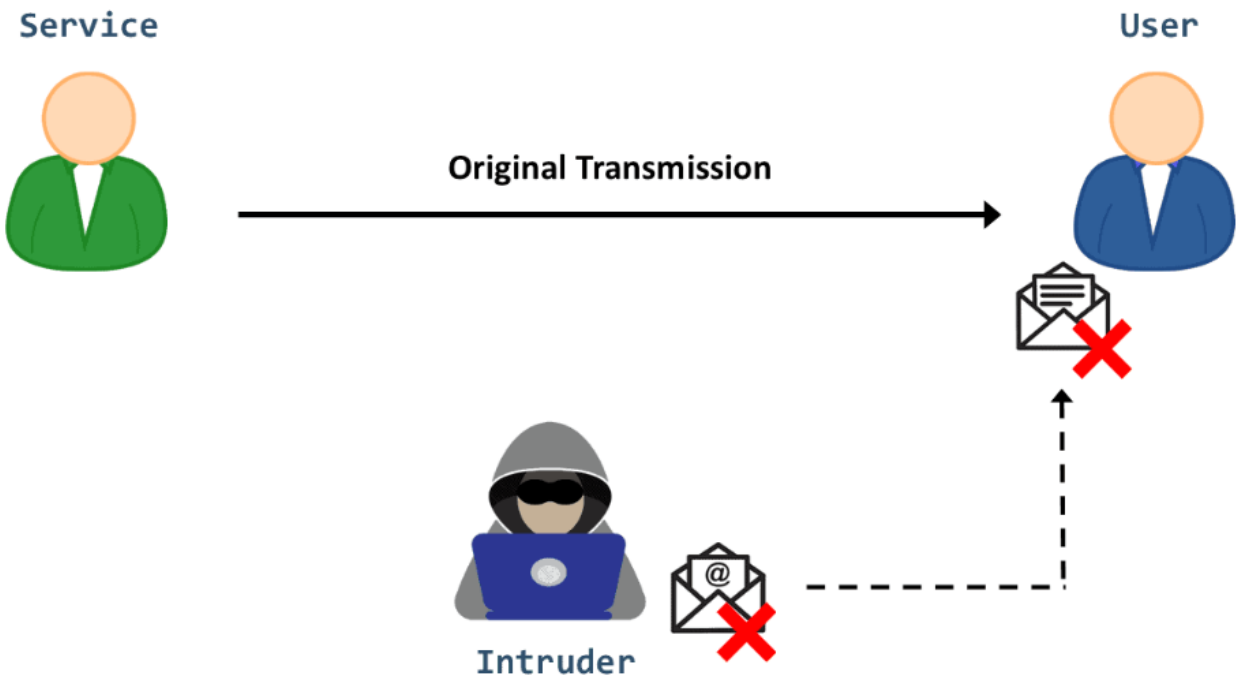

Imagen 2: Método de Ataque de Fabricación, Rhim y Simic (2023).

4. **Interrupción**

El objetivo es impedir el acceso legítimo a recursos o destruirlos. Este aparece

cuando un servicio de red o un activo del sistema se interrumpe o se destruye. Un *ransomware* que cifra el disco de un servidor crítico — o un DDoS de 22 Tbps que satura el ancho de banda de un CDN (**Content Delivery Network**) — degrada o anula la **disponibilidad** del servicio, con impacto directo en la continuidad de negocio. El **CDN** es una red de servidores distribuidos geográficamente que **acercan el contenido al usuario** (ej. videos, imágenes, páginas web) para mejorar velocidad y disponibilidad.

a. **Flujo simplificado**
    1. Identifica el recurso crítico (ancho de banda, disco, clave de cifrado).
    2. Lanza acción de agotamiento o destrucción (DDoS, ransomware, sabotaje físico).
    3. Mantiene la condición hasta que el servicio se degrada o cesa.

b. **Ejemplo práctico e imagen**
    1. Una botnet IoT envía 22 Tbps de tráfico a un CDN durante Black Friday; el portal de e-commerce queda fuera de línea ocho horas, generando pérdidas millonarias y afectando la **disponibilidad**.

    2. Imagen del método de ataque de Interrupción

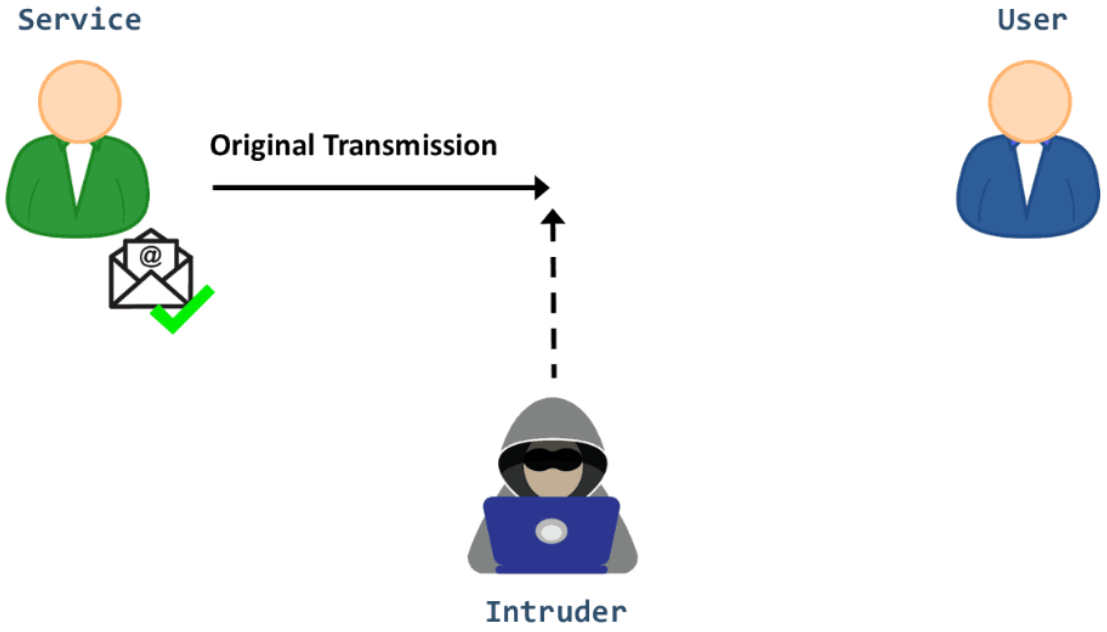

Imagen 3: Método de Ataque Interrupción, Rhim y Simic (2023).

Estos cuatro modelos son la lente a través de la cual analizaremos cualquier técnica listada en marcos como MITRE ATT&CK, pues toda táctica avanzada termina materializándose en al menos uno de estos mecanismos básicos. Dicho sea de paso que **MITTRE ATT&CK** es un **"catálogo mundial de técnicas de ataque"** usado por ciberseguridad para aprender, defender y simular ataques.

Perfil de perpetradores (Who)

Los **actores de amenaza** se distinguen por su nivel de recursos, motivaciones y métodos preferidos:

- **Script kiddies** operan con herramientas prefabricadas (Metasploit, Kali) y escasa comprensión del código. Buscan notoriedad rápida, atacan blancos aleatorios y suelen llevar a cabo *defacements* o escaneos de puertos masivos.
- **Ciberdelincuencia organizada** dispone de infraestructura de botnets, 0-days alquilados y modelos *ransomware-as-a-Service*. El grupo DarkSide, por ejemplo, comprometió Colonial Pipeline con fines puramente económicos, **más información en https://www.bbc.com/news/business-57050690**. En mayo de 2021 el grupo **DarkSide** comprometió a Colonial Pipeline (una de las mayores operadoras de oleoductos en EE.UU.), provocando **escasez de combustible** y pérdidas millonarias.
    - **0-days alquilados** - cuando grupos de ciberdelincuentes **pagan o arriendan el uso de un exploit 0-day** a desarrolladores o mercados clandestinos para usarlo en sus ataques. Entiéndase que un Zero Day es una vulnerabilidad desconocida por el fabricante y que aún **no tiene parche de seguridad.**
    - **Ransomware as a Service -** Los desarrolladores de ransomware crean la plataforma y **la alquilan o venden** a afiliados. Los afiliados lanzan

ataques, y las ganancias del rescate se **comparten** entre ambos. Básicamente un **Ransomware bajo Suscripción.**

- **Insiders** — empleados, contratistas o socios — combinan acceso legítimo con motivaciones que van desde la negligencia hasta la venganza. Un técnico de soporte que copia la base de datos de clientes a un USB y la vende en foros es un caso típico.
- **Hacktivistas** persiguen causas ideológicas; lanzan campañas de DDoS o publican filtraciones (#OpRussia 2022) para llamar la atención sobre un tema político o social.
    - **#OPRussia2022**
        - Fue una campaña de ciberataques y hacktivismo lanzada en 2022, poco después de la invasión de Rusia a Ucrania.
        - El hashtag #OpRussia ("Operation Russia") fue usado principalmente por colectivos de hacktivistas como Anonymous y grupos aliados.
- **APT de nación-estado** cuentan con presupuestos millonarios, tiempo y acceso a 0-days. Operaciones como *Stuxnet*o la intrusión en la cadena de suministro de SolarWinds ilustran su capacidad de ejecutar ataques dirigidos y persistentes contra infraestructuras estratégicas.

Conocer el perfil ayuda a anticipar tácticas: un script kiddie será disuadido por controles básicos (MFA, parches), mientras un APT requiere monitoreo avanzado y segmentación de red.

Perfil de perpetradores con nivel de recursos, herramientas y caso ilustrativo

Perfil	Nivel de recursos	Herramientas típicas	Caso ilustrativo
Script kiddie	Bajo	Metasploit, Kali Linux "out-of-the-box". (Kali Linux "out-of-	*Defacement* de un blog personal usando exploit "copy-paste".

Perfil	Nivel de recursos	Herramientas típicas	Caso ilustrativo
		the-box" = distribución que, al instalarla, ya trae todo el arsenal de ciberseguridad listo para usar.)	
Crimen organizado	Medio-alto	Botnets alquiladas (Mirai), kits de ransomware RaaS	*DarkSide* cifró Colonial Pipeline; motivación ↠ lucro.
Insider	Variable (pero con acceso)	USB Rubber Ducky (El **USB Rubber Ducky** es un **dispositivo de hacking físico** que se hace pasar por un teclado y **automatiza ataques** en cuestión de segundos.), privilegios nativos, credenciales compartidas	Técnico de soporte vende 70,000 registros de clientes.
Hacktivista	Bajo-medio	DDoS voluntario (LOIC), filtraciones, doxing	Anonymous lanzó operación #OpRussia 2022.
Nación-estado / APT	Muy alto	0-days, supply-chain, equipo dedicado	*Stuxnet* saboteó centrífugas Irán; *SolarWinds backdooreó* (insertaron o inyectaron una puerta trasera) el software de actualizaciones de la plataforma SolarWinds.

Concepto clave — **Kill Chain**: Reconocimiento → Armamento → Entrega → Explotación → Instalación → Control y C2 → Acción/Objetivo. Cada perfil recorre la cadena con distinta paciencia y recursos.

Explicación del Kill Chain

- **Kill Chain** - El término Kill Chain viene del ámbito militar y fue adaptado por Lockheed Martin para describir las fases de un ciberataque. La idea de este concepto es que un ataque no ocurre de golpe, sino que va poco a poco.
    - **Etapas del Kill Chain**
        1. **Reconocimiento (Reconnaissance):** El atacante investiga a la víctima → recopila datos de empleados, dominios, puertos abiertos, tecnologías usadas.
        2. **Armamento (Weaponization):** Crea o adapta la herramienta maliciosa (malware, exploit, phishing) lista para el ataque.
        3. **Entrega (Delivery):** Transfiere el ataque al objetivo (correo phishing, USB malicioso, descarga web, exploit remoto).
        4. **Explotación (Exploitation):** El malware/exploit aprovecha una vulnerabilidad (ej. ejecutar un RCE).
        5. **Instalación (Installation):** Se instala un backdoor, troyano o herramienta persistente en el sistema comprometido.
        6. **Control y C2 (Command & Control):** El atacante establece comunicación remota con la máquina comprometida para controlarla.
        7. **Acción/Objetivo (Actions on Objectives):** Se cumple la meta: robo de datos, cifrado (ransomware), espionaje, sabotaje.
- **Para más información: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html**

Motivos, causas y razones (MOM triad)

1. **Motivo (Why)**

- **Definición:** Responde al "¿por qué?" del atacante. **Razones** que impulsan el ataque.

- **Ejemplos**
  - **Financiero** → robo de tarjetas, ransomware, cripto-minería.
  - **Ideológico/político** → leaks, defacement, DoS.
  - **Competitivo/industrial** → espionaje, sabotaje.
  - **Venganza** → insider borra datos tras despido.

2. **Oportunidad (When/Where)**
   - **Definición:** Circunstancias o vulnerabilidades que permiten el ataque.
   - **Ejemplos:**
     - Ventanas de mantenimiento sin monitoreo.
     - Sistemas con fin de vida (Win XP en PLC).
     - Configuración por defecto (admin/admin).
3. **Método o Medios (How)**
   - **Definición:** Los Recursos y Herramientas disponibles para llevar a cabo el ataque.
   - **Ejemplos:**
     - Exploit 0-day, phishing, malware USB, dron con antena Wi-Fi para Evil-Twin.

- **Ejemplo completo** – Cadena MOM aplicada a *NotPetya 2017*:

  - ¿**De que trata este ejemplo**?
    - La "**Actualización contable M.E.Doc obligatoria en Ucrania**" fue el mecanismo usado para distribuir **NotPetya** en 2017 → un ataque de **supply chain** (cadena de suministro), porque los atacantes comprometieron el software de un proveedor confiable y lo usaron para propagar el malware.
  - **Cadena MOM**
    - **Motivo:** Desestabilización geopolítica.

- **Oportunidad:** Actualización contable *M.E.Doc* obligatoria en Ucrania.

- **Método:** Backdoor en paquete de software firmado digitalmente.

Daños potenciales (What)

a) Definiciones de conceptos claves:

1. **Confidencialidad**
   Propiedad que garantiza que la información solo sea accesible a sujetos, procesos o sistemas autorizados. Su violación supone la exposición, copia o inspección indebida de datos sensibles.
2. **Integridad**
   Cualidad que preserva la exactitud, veracidad y completitud de la información y de los sistemas que la procesan. Se vulnera cuando datos o configuraciones se alteran sin autorización, ya sea por acción maliciosa o por error.
3. **Disponibilidad**
   Condición de que la información, los servicios y los recursos asociados estén accesibles y utilizables por los usuarios legítimos cuando los necesiten. Se compromete mediante fallos de hardware, ataques DoS/DDoS, ransomware o desastres naturales.
4. **Vida/Salud**
   Impacto que un incidente de ciberseguridad puede tener sobre la integridad física de las personas—desde la interrupción de equipos médicos hasta el sabotaje de sistemas industriales capaces de provocar daños corporales o pérdida de vidas humanas.
5. **Reputación**
   Percepción pública y de los stakeholders (accionistas, clientes, socios) acerca de la fiabilidad y responsabilidad de una organización. Una

filtración de datos o un defacement visible puede erosionar la confianza, reducir la cuota de mercado y aumentar la desconfianza de inversores.

6. **Recursos/Dinero**
   Pérdidas económicas directas (robo de fondos, fraude, rescates pagados) e indirectas (costes de remediación, multas regulatorias, demandas legales, tiempo de inactividad). Incluye también la pérdida o degradación de activos tangibles y de infraestructura tecnológica.

b) **Tabla de ejemplos reales y métricas con consecuencias**

Categoría de daño	Ejemplos reales	Métricas / consecuencias
Confidencialidad	*Equifax 2017* – 147 M SSN filtradas.	Multa US $700 M + pérdida de confianza.
Integridad	*Stuxnet* alteró velocidades de centrifugado.	Destrucción física de 1 000+ centrífugas.
Disponibilidad	DDoS a DynDNS (2016) afectó Twitter, Netflix, GitHub.	Downtime de 11 h; pérdidas publicitarias.
Vida/Salud	*Ransomware* 2020 detuvo hospital Düsseldorf; una paciente trasladada falleció.	Impacto directo en vidas humanas.
Reputación	Campaña #DeleteWhatsApp tras política de datos 2021.	Éxodo de usuarios a Signal / Telegram.
Recursos/Dinero	*Bangladesh Bank Heist* – $81 M transferidos.	Costes legales, refor-mulación de procedimientos.

Herramientas de valoración — **CVSS 3.1** para impacto técnico, **OWASP Risk Rating** para negocio, **NIST SP 800-30 para** análisis organizacional.

Controles y contramedidas iniciales (How to respond?)

1. **Prevenir – eliminar la vulnerabilidad**
    - **El primer paso es evitar que el ataque tenga lugar eliminando las debilidades que pueden ser explotadas.**
    - **Ejemplos:**
        i. **Físico:** implementar cerraduras biométricas o jaulas Faraday para racks de servidores, reduciendo accesos no autorizados o interferencias.
        ii. **Técnico:** aplicar parcheo regular de sistemas, deshabilitar macros en Office mediante políticas de grupo (GPO) y actualizar configuraciones seguras.
        iii. **Administrativo:** políticas como la segregación de funciones (ej. en contabilidad bajo SOX), evitando que una sola persona tenga control total sobre procesos críticos.
2. **Disuadir – elevar el coste/temor del atacante**
    - **Aquí el objetivo es hacer que el atacante lo piense dos veces porque el riesgo o esfuerzo aumenta.**
    - **Ejemplos:**
        i. Cámaras CCTV visibles envían un mensaje claro de vigilancia.
        ii. Marcas de agua en documentos sensibles dificultan su filtración sin rastro.

iii. Cláusulas legales severas en contratos advierten de sanciones si se cometen actos maliciosos.

3. **Desviar – dirigir al atacante lejos de activos reales**
    - **Consiste en engañar al atacante y redirigirlo a sistemas falsos.**
    - **Ejemplos:**
        i. Honeynets o honeypots: entornos falsos que imitan sistemas productivos para atraer al atacante. Al interactuar con estas trampas, el atacante revela sus TTPs (Tácticas, Técnicas y Procedimientos).
        ii. Trampas con datos “XOR-Encoded” que parecen legítimos, pero realmente solo registran la actividad del atacante.
4. **Mitigar – reducir la severidad del impacto**
    - **Si el ataque ocurre, se busca limitar los daños y permitir la recuperación rápida.**
    - **Ejemplos:**
        i. Backups offline (air-gapped): copias desconectadas de la red, que no pueden ser cifradas por ransomware.
        ii. Redundancia geográfica: sistemas duplicados en ubicaciones distintas que mantienen la operación.
        iii. Limitación de privilegios: aplicar *least privilege* (**Principio de mínimo privilegio**), de modo que incluso si una cuenta se compromete, el daño sea mínimo.
5. **Detectar – reconocer el evento anómalo**
    - **Se trata de identificar lo antes posible que algo no va bien.**

- **Ejemplos:**

    i. **IDS/IPS (Intrusion Detection/Prevention Systems):** monitorean el tráfico buscando patrones conocidos o anómalos.

    ii. **EDR (Endpoint Detection and Response):** detecta actividad sospechosa en dispositivos finales.

    iii. **UEBA (User and Entity Behavior Analytics):** analiza patrones de comportamiento para encontrar anomalías como accesos inusuales.

6. **Reportar – comunicar rápidamente**

    - **Una vez detectado el incidente, la comunicación ágil es vital para contenerlo y cumplir con regulaciones.**

    - **Ejemplos:**

        i. **SIEM (Security Information and Event Management):** centraliza logs y eventos para correlación.

        ii. **SOAR (Security Orchestration, Automation and Response):** automatiza la creación de tickets (ej. en JIRA) y notificaciones inmediatas al CISO.

        iii. **Canales de notificación legal:** por ejemplo, GDPR exige reportar incidentes de datos en ≤ 72 horas.

Otros conceptos clave

Concepto	Descripción operativa	Ejemplo concreto
Privacidad	Minimizar recolección y empleo de PII; aplicar “Privacy by Design”.	Mascarar campos de SSN salvo 4 dígitos en interfaz CSR.
Autenticidad	Garantizar que algo/ alguien es quien dice ser.	Certificados X.509 para API; FIDO2 tokens para VPN.
Responsabilidad	Atribución clara de acciones (accountability).	Logs firmados con Hashicorp Vault; SIEM retiene 400 días.
No-repudio	Imposibilidad de negar la autoría de una transacción.	Firma digital de facturas (Factura-e) con sello de tiempo.
Auditabilidad	Capacidad de reconstruir eventos.	Syslog central + WORM storage para evidencia forense.
Políticas y confianza	Documentos que establecen nivel de confianza y controles aceptados.	Declaración de aplicabilidad ISO 27001; política Zero-Trust adoptada por CIO.

Relación con Otros Conceptos

- **Vulnerabilidad** → **Ataque** → **Daño** enlaza con el **Análisis de Riesgos**.
- Los controles listados se profundizarán en **Autenticación, Control de Acceso y Criptografía** (Módulo 3).
- Los principios de **privacidad y auditabilidad** sirven de base a los temas **ético-legal y gobernanza** (Módulo 7).

Resumen de la Lección

Analizamos en detalle los métodos de ataque (intercepción, modificación, fabricación, interrupción), los perfiles y motivos que los impulsan, y los daños que acarrean sobre CIA, vidas humanas, reputación y finanzas. Vinculamos cada daño con controles iniciales—físicos, técnicos y administrativos—clasificados por su función (prevenir, disuadir, desviar, mitigar, detectar, reportar). Finalmente, integramos conceptos transversales de privacidad, autenticidad, responsabilidad, no-repudio y auditabilidad dentro de un marco de políticas y confianza, cimentando la defensa en profundidad.

Actividad de la Lección

Diagrama Bow-Tie enriquecido (120 min, inicio en clase, cierre en casa)

1. Seleccione uno de estos entornos: sistema SCADA, app FinTech móvil, red universitaria.
2. Elabore un *bow-tie* con:
    - Vulnerabilidad raíz.
    - Cuatro ataques (I, M, F, Int.) conectados a ella.
    - Daños CIA + colaterales en el lado derecho.
    - Controles clasificados (P, D, De, M, Det, Rep) en cada brazo.
3. Añada etiquetas de **perfil del perpetrador** y **motivo** sobre cada ataque.
4. Adjunte una tabla que muestre la relación **Ataque ↔ Control ↔ Principio (privacidad, no-repudio, etc.)**.
   Entrega: PDF con diagrama + tabla; 10 min de exposición la próxima clase.

Referencias Adicionales

- Baeldung. (s. f.). *Security: Interruption, Interception, Modification, and Fabrication*. Baeldung. Recuperado el 15 de septiembre de 2025, de https://www.baeldung.com/cs/security-interruption-interception-modification-fabrication

- IBM. (s. f.). *Ataque de intermediario (Man-in-the-Middle, MITM)*. IBM Think. Recuperado el 15 de septiembre de 2025, de https://www.ibm.com/es-es/think/topics/man-in-the-middle

- Fortinet. (s. f.). *Caballo de Troya (troyano)*. Cyberglossary de Fortinet. Recuperado el 15 de septiembre de 2025, de https://www.fortinet.com/lat/resources/cyberglossary/trojan-horse-virus

- Lockheed Martin. (s. f.). *Cyber Kill Chain®*. Lockheed Martin. Recuperado el 15 de septiembre de 2025, de https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

- Pfleeger, C. P., Pfleeger, S. L., & Coles-Kemp, L. (2023). *Security in Computing* (6.ª ed.).
- Stallings, W., & Brown, L. (2017). *Computer Security: Principles and Practice* (4.ª ed.).
- Bishop, M. (2018). *Computer Security: Art and Science* (2.ª ed.).
- MITRE ATT&CK Navigator (2025).
- NIST SP 800-53 Rev. 5 – *Security & Privacy Controls*.
- ENISA. *Threat Landscape 2024*.

- Tarlogic Security. (s. f.). *¿Qué es sniffer?* Recuperado el 12 de septiembre de 2025, de https://www.tarlogic.com/es/glosario-ciberseguridad/sniffer/