Introducción a la Ciberseguridad.

Principios CIA. Historia, actores de amenazas.

1. Objetivos de la sesión

- Definir ciberseguridad y diferenciarla de seguridad informática tradicional.
- Explicar los principios CIA (Confidencialidad, Integridad, Disponibilidad) y sus extensiones (Autenticidad, No repudio, Trazabilidad).
- Reconstruir hitos históricos clave que dieron forma a la disciplina de la ciberseguridad.
- Clasificar actores de amenazas según motivación, recursos y método de operación.
- Identificar fuentes académicas abiertas (DOAJ, SciELO, RedALyC) para investigación en ciberseguridad.

2. Pregunta

- *¿Alguna vez te hackearon, perdiste una cuenta o sufriste un intento de phishing?*
- *¿Que es una IP, Mascara, Direccion de Red, DNS?*
- *¿Que son los puertos de red? Ejemplos*
- *¿Que es el modelo OSI y TCP/IP?*
- *¿Que son puertos?*
- *¿Como funciona un firewall?*

Seguridad Informática vs. Ciberseguridad

Definiciones simples

Concepto	**Definición**
Seguridad Informática	Protección de la **información** y los **sistemas informáticos** dentro de un perímetro definido (empresa, institución, data center).
Ciberseguridad	Protección de activos digitales en un entorno **interconectado**, que incluye redes, nube, dispositivos móviles, IoT y la propia interacción humana en el ciberespacio.

La diferencia fundamental: el perímetro

> **Seguridad Informática** piensa: *"¿Cómo protejo lo que está dentro de mis cuatro paredes?"*
>
> **Ciberseguridad** piensa: *"¿Cómo protejo todo lo que está conectado a Internet, incluyendo lo que sale de mis cuatro paredes?"*

Analogía

Imagina una **universidad**:

	Seguridad Informática	**Ciberseguridad**
Enfoque	Proteger los servidores del campus, las computadoras del laboratorio, los archivos del rector.	Proteger también el campus virtual, el correo en la nube, las laptops de los profesores cuando trabajan desde casa, las cámaras de seguridad conectadas a Wi-Fi, y los datos que fluyen por Internet.
Pregunta clave	*"¿Está seguro el edificio?"*	*"¿Está seguro el edificio, la información que viaja por las carreteras, y las casas desde donde se conectan?"*

Diferencias detalladas

Aspecto	**Seguridad Informática**	**Ciberseguridad**
Alcance	Local, interno, on-premise.	Global, distribuido, híbrido (local + nube + móvil).
Vectores de ataque	USB, acceso físico, malware en red interna.	Phishing, ransomware por email, ataques a la cadena de suministro, IoT comprometido, deepfakes (Contenido en video, audio o imagen creado con inteligencia artificial que imita con gran realismo el rostro, el cuerpo o la voz de una persona).
Tecnologías	Antivirus, firewall de perímetro, backups locales, control de acceso físico.	Zero Trust (Confianza Cero), SIEM (Gestión de Información y Eventos de Seguridad - logs), SOAR (Orquestación, Automatización y Respuesta de Seguridad -automatiza respuesta), EDR/XDR

Aspecto	Seguridad Informática	Ciberseguridad
		(Detección y Respuesta en Puntos Finales / Extendida), cifrado end-to-end, inteligencia de amenazas (Threat Intelligence).
Enfoque del atacante	Romper la seguridad del edificio/servidor.	Romper la confianza entre sistemas interconectados, explotar el factor humano.
Dimensión humana	Importante, pero secundaria.	**Crucial.** El 74% de las brechas involucra el factor humano (Verizon DBIR 2024).
Marco legal	Políticas internas, normas de la organización.	GDPR, NIS2, leyes de ciberseguridad nacional, ciberdelito internacional.
Velocidad de cambio	Relativamente estable.	Evoluciona diariamente (nuevas amenazas, IA generativa, supply chain).

Tecnologías Ciberseguridad

- Zero Trust (Confianza Cero) : Es un modelo de seguridad bajo la premisa **"nunca confiar, siempre verificar"**. Por defecto, no se confía en ningún usuario o dispositivo, esté dentro o fuera de la red de la empresa. Exige autenticar y autorizar cada acceso de forma continua.
- SIEM (Gestión de Información y Eventos de Seguridad) : Es un software central que **reúne y analiza los registros (logs)** de toda la infraestructura informática (servidores, redes, bases de datos). Su función principal es detectar actividades sospechosas en tiempo real y generar alertas para los analistas.
- SOAR (Orquestación, Automatización y Respuesta de Seguridad) : Es una plataforma que va un paso más allá del SIEM. No solo centraliza alertas, sino que **automatiza la respuesta ante incidentes** mediante reglas predefinidas (*playbooks*). Por ejemplo, puede bloquear automáticamente un usuario sospechoso sin intervención humana.
- **EDR / XDR (Detección y Respuesta en Puntos Finales / Extendida)**
  - **EDR (Endpoint Detection and Response):** Protege los **dispositivos finales** (computadoras, servidores, celulares) monitoreándolos activamente para bloquear amenazas avanzadas como el ransomware.
  - **XDR (Extended Detection and Response):** Es la evolución del EDR. Amplía esa misma capacidad de detección uniendo los datos de los dispositivos con los de la **red, la nube y los correos** en una sola plataforma.

- Cifrado End-to-End (De Extremo a Extremo) : Es un sistema de comunicación donde **solo los usuarios que se comunican pueden leer los mensajes**. Los datos se encriptan en el dispositivo del emisor y solo se desencriptan en el del receptor. Ni los proveedores de internet ni las aplicaciones (como WhatsApp) pueden ver el contenido.
- Inteligencia de Amenazas (Threat Intelligence) : Es la recolección y análisis de información sobre **ataques cibernéticos existentes o emergentes**. Ayuda a las organizaciones a entender quiénes son los atacantes, qué herramientas usan y cómo operan, permitiendo preparar las defensas antes de ser atacados.

Ejemplos prácticos

Escenario: Un hospital.

Situación	**¿Es Seguridad Informática o Ciberseguridad?**
Un empleado roba una base de datos desde una PC del hospital.	**Seguridad Informática** (insider, control de acceso interno).
Un ransomware llega por email al médico, se propaga por la red y cifra historias clínicas.	**Ciberseguridad** (vector externo, red interconectada, email como vector).
Las cámaras de seguridad del hospital son hackeadas desde Internet porque tenían contraseña por defecto.	**Ciberseguridad** (IoT expuesto, ataque remoto).
El hospital hace backups en cinta y los guarda en una bóveda física.	**Seguridad Informática** (protección física de activos).

¿Cómo se relacionan?

La Seguridad Informática es el antecedente. La Ciberseguridad es la evolución.

```
Seguridad Informática (años 80-90)
        ↓
        + Internet masivo
        + Dispositivos móviles
        + Cloud Computing
        + IoT
        + Trabajo remoto
        + Ciberdelito organizado
        ↓
    Ciberseguridad (actualidad)
```

Toda Ciberseguridad incluye Seguridad Informática, pero no toda Seguridad Informática es Ciberseguridad.

Para recordar

"La Seguridad Informática protege la computadora. La Ciberseguridad protege a la persona que usa la computadora, en cualquier lugar, desde cualquier dispositivo, contra cualquier amenaza que venga de Internet."

Pregunta

"¿Una empresa que tiene su data center físico bien protegido con antivirus y firewall, pero permite a sus empleados acceder a correo corporativo desde celulares personales sin MFA (Multi-Factor Authentication), tiene Seguridad Informática o Ciberseguridad?"

3 ¿Qué es la ciberseguridad?

Conceptos clave a:

Ciberseguridad es el conjunto de prácticas, tecnologías y procesos diseñados para proteger redes, dispositivos, programas y datos de ataques, daños o accesos no autorizados.

- **Diferencia clave:** Seguridad Informática vs. Ciberseguridad.
    - *Seguridad Informática:* enfoque tradicional, protección de infraestructura TI interna.
    - *Ciberseguridad:* enfoque amplio, incluye entornos conectados, nube, IoT, dispositivos móviles, cadena de suministro y dimensión geopolítica.
- **Dimensiones de la ciberseguridad:**
    - Técnica (firewalls, criptografía, pentesting (simulación controlada de un ciberataque autorizada para encontrar fallos de seguridad en sistemas, redes o aplicaciones antes de que los delincuentes los dañen)).
    - Humana (concienciación, ingeniería social).
    - Organizacional (políticas, gobernanza, cumplimiento).
    - Legal (normativas, ciberdelito).

3.1 Principios CIA y extensiones

Principio	**Definición**	**Ejemplo práctico**	**Falla famosa**
Confidentiality	Solo usuarios autorizados acceden a la información.	Cifrado de disco, VPN	Filtración de datos de Equifax (2017)
Integrity	La información no es alterada de forma no autorizada.	Hash SHA-256, firmas digitales	Ataque NotPetya (2017)
Availability – Disponibilidad	Los sistemas están accesibles cuando se necesitan.	Backups, redundancia, DDoS mitigation	Ataque DDoS a Dyn (2016)

Extensiones del modelo CIA:

- **Autenticidad:** Asegurar que quien envía o recibe información es realmente quien dice ser.
    - Cuando inicias sesión en el banco, no basta con que la información viaje cifrada (confidencialidad). El banco debe verificar que eres tú — ya sea con contraseña, huella dactilar o token. Si un atacante roba tu sesión pero el sistema no valida tu identidad, la confidencialidad no sirve de nada.
- **No repudio:** Evitar que alguien niegue haber realizado una acción o haber enviado/recibido un mensaje.
    - Firmas un contrato digital con tu firma electrónica certificada. Meses después no puedes decir "yo no firmé eso" porque la firma digital está vinculada irrefutablemente a tu clave privada. Lo mismo ocurre cuando el banco te envía un comprobante de transferencia: ellos no pueden negar que la hicieron.
- **Trazabilidad:** Capacidad de reconstruir el historial completo de quién accedió a qué recurso, qué hizo y en qué momento.
    - Un estudiante modifica una nota en el sistema académico. Sin trazabilidad, no hay forma de saber quién fue. Con trazabilidad (logs de auditoría), el sistema registra: "Usuario 20151234 accedió al módulo de notas el 05/08/2026 a las 14:32, cambió la nota de 3.2 a 4.5 desde la IP 192.168.1.45".

Ejercicio :

> *Caso:* Un hospital utiliza un sistema de historias clínicas electrónicas. Un ransomware - *tipo de software malicioso (malware) que secuestra los datos o sistemas de una víctima, bloqueando su acceso mediante cifrado, para luego exigir el pago de un rescate económico a cambio de la clave de liberación* - bloquea el acceso. Un médico imprime historias en papel porque no puede acceder al sistema. Mientras tanto, un atacante publica 10,000 historias en la dark web. Además, se descubre que un administrador borró registros de auditoría.
>
> *Pregunta :* ¿Qué principios del CIA se violaron en cada escenario? ¿Qué principios extendidos aplican?

3.2 Historia de la ciberseguridad

Línea de tiempo interactiva (hitos clave):

Año	Evento	Impacto en la disciplina
1960s	ARPANET, primeros conceptos de red	Origen de la interconexión
1971	Creeper (primer malware)	Creado en 1971 por el ingeniero Bob Thomas en la red ARPANET (la predecesora de Internet). No fue diseñado

Año	Evento	Impacto en la disciplina
		con intenciones dañinas, sino como un experimento científico para comprobar si un programa podía replicarse y moverse por sí solo entre computadoras.
1983	Película *WarGames* + Computer Fraud and Abuse Act (EE.UU.)	Conciencia pública y primeras leyes
1988	Morris Worm	Su creador fue Robert Tappan Morris, un estudiante de posgrado de la Universidad de Cornell, quien paradójicamente quería medir el tamaño de la red en ese momento. El código contenía un error de diseño que provocó el colapso de aproximadamente el 10% de las computadoras conectadas a Internet (unas 6,000 de las 60,000 existentes). Primer gran ataque a Internet; nace el CERT/CC (Computer Emergency Response Team Coordination Center o Centro de Coordinación del Equipo de Respuesta a Emergencias Informáticas)
1990s	Aparición de firewalls comerciales, antivirus, cifrado SSL	Comercialización de la seguridad
2000	ILOVEYOU, Code Red	ILOVEYOU: Llegaba por correo electrónico con el asunto "ILOVEYOU" y un archivo adjunto engañoso llamado LOVE-LETTER-FOR-YOU.TXT.vbs. El virus borraba fotos y archivos de música, y se autoenviaba en segundos a todos los contactos de la libreta de direcciones de Microsoft Outlook de la víctima. Code Red : Explotaba una vulnerabilidad de desbordamiento de búfer (buffer overflow) en los servidores web que utilizaban el software Microsoft IIS. Estaba programado para que, al llegar el día 20 del mes, todos los servidores infectados lanzaran un ataque masivo simultáneo contra la dirección IP de la Casa Blanca (whitehouse.gov), logrando saturar y tumbar su sitio web. • Que es DDoS (Distributed Denial of Service - Denegación de Servicio Distribuido)
2007	Ataques a Estonia (primer ciberataque a nivel país)	Considerados históricamente como la primera ciberguerra del mundo o el primer ciberataque a escala nacional. Durante 22 días, el país báltico —que ya era uno de los más digitalizados del planeta— sufrió una ofensiva digital masiva que paralizó su infraestructura pública y privada, redefiniendo la ciberseguridad global y el papel de la OTAN. El conflicto comenzó tras la decisión del gobierno estonio de trasladar una estatua de bronce de la era soviética (el

Año	Evento	Impacto en la disciplina
		Soldado de Bronce de Tallin) desde el centro de la capital a un cementerio militar. Esto enfureció a la minoría rusa local y al gobierno de Moscú, desatando protestas en las calles y, casi de inmediato, el ataque informático. • En Colombia ocurre?
2010	Stuxnet	Ciberarma; ataque a infraestructura crítica (OT Operational Technology - Tecnología de Operación /ICS Industrial Control Systems - Sistemas de Control Industrial). Obtuvieron acceso a PLC y SCADA permitiendo el acceso a sensores y actuadores – compuertas de agua, valvulas, interruptores-. • Que paso en Venezuela en Marzo de 2019 y Enero de 2026? – Buscar ciberataque venezuela sistema electrico 2019 2026
2013	Snowden / NSA	En junio de 2013, el excontratista de la Agencia de Seguridad Nacional de EE. UU. (NSA), Edward Snowden, filtró miles de documentos clasificados a la prensa mundial. Esta filtración reveló la existencia de una red global de vigilancia. Las revelaciones forzaron a la industria tecnológica a adoptar el cifrado de extremo a extremo de forma masiva e impulsó la creación de regulaciones de privacidad estrictas a nivel global, sirviendo como catalizador directo para el nacimiento del GDPR (Reglamento General de Protección de Datos) en Europa. Ademas destruyó la confianza entre las empresas tecnológicas estadounidenses y sus clientes internacionales • Debate sobre privacidad vs. vigilancia
2017	WannaCry, NotPetya	Ransomware global; afectó hospitales, empresas, gobiernos. WannaCry: Lanzado en mayo de 2017, fue un ataque de ransomware masivo que infectó a más de 300,000 computadoras en 150 países en cuestión de horas. Aprovechaba la vulnerabilidad EternalBlue en el protocolo de red de Windows (SMB). No necesitaba que el usuario abriera ningún correo; si una computadora estaba conectada a la red sin actualizar, se infectaba sola. NotPetya: Lanzado en junio de 2017, comenzó disfrazado como un ataque de ransomware tradicional, pero en realidad era un wiper: un ciberarma diseñada

Año	Evento	Impacto en la disciplina
		exclusivamente para destruir datos de forma irreversible. Una vez dentro de una red, utilizaba EternalBlue para saltar de computadora en computadora en segundos. A diferencia de WannaCry, NotPetya cifraba el Master Boot Record (MBR) del disco duro de tal forma que la computadora nunca más podía arrancar, haciendo imposible recuperar los datos incluso si se pagaba el rescate.
2020+	Ataques a cadena de suministro (SolarWinds), Log4j, IA generativa	Ciberseguridad como cadena de confianza; nuevos vectores. Realizar la siguiente lectura.

3.3 Lectura:

La seguridad informática moderna ha dejado de enfocarse únicamente en el perímetro de una empresa para centrarse en los elementos externos que utiliza: el software de terceros, las librerías de código abierto y, más recientemente, las herramientas basadas en Inteligencia Artificial.

SolarWinds (Ataque a la cadena de suministro, 2020)

Descubierto a finales de 2020 por la empresa de ciberseguridad FireEye, el ataque a **SolarWinds** es el ejemplo más sofisticado de un **Supply Chain Attack** (Ataque a la cadena de suministro). En lugar de atacar directamente a un objetivo protegido, los hackers envenenaron el software que ese objetivo utilizaba.

- **El mecanismo (SUNBURST):** El grupo de espionaje ruso conocido como APT29 (o *Cozy Bear*) logró infiltrarse en los sistemas de desarrollo de SolarWinds. Allí, introdujeron una puerta trasera en una actualización legítima de su plataforma de monitoreo de redes, llamada **Orion**.
- **El Caballo de Troya:** Alrededor de 18,000 organizaciones (incluyendo ministerios clave del gobierno de EE. UU., agencias de inteligencia y grandes empresas de tecnología) descargaron e instalaron la actualización oficial firmada digitalmente, sin saber que contenía el código malicioso.
- **El Impacto:** Los atacantes seleccionaron quirúrgicamente a un grupo de víctimas de alto perfil para espiar sus redes durante meses, marcando un antes y un después en cómo el mundo evalúa la confianza en el software comercial.

Log4j / Log4Shell (Vulnerabilidad en código abierto, 2021)

En diciembre de 2021 se descubrió **Log4Shell**, una vulnerabilidad crítica en **Log4j**, una librería de código abierto basada en Java que se utiliza en millones de servidores y aplicaciones de todo el mundo para registrar eventos (hacer "logs").

- **Gravedad Máxima (CVSS 10/10):** Permitía la Ejecución Remota de Código (RCE). Un atacante solo tenía que enviar una cadena de texto simple (por ejemplo, a través del chat de un juego o un cuadro de búsqueda) para que el servidor ejecutara comandos maliciosos de forma automática.
- **El Caos en Internet:** Dado que Log4j estaba profundamente oculto dentro de productos de gigantes como Apple, Minecraft, Amazon, Twitter y millones de servidores corporativos, la superficie de ataque fue masiva. Las empresas pasaron semanas rastreando si sus sistemas utilizaban internamente la librería para poder aplicar el parche de emergencia.

3.4 El Impacto de la IA Generativa en la Ciberseguridad

A partir de 2023, la explosión de la Inteligencia Artificial Generativa cambió drásticamente las reglas del juego tanto para los atacantes (ofensiva) como para los defensores (defensiva).

Del lado de los atacantes (Malware y Phishing avanzado)

- **Phishing hiperrealista:** La IA permite redactar correos de ingeniería social perfectos, sin faltas de ortografía y adaptados al tono de una empresa real, eliminando las señales de alerta tradicionales.
- **Vishing y Deepfakes:** Herramientas de clonación de voz y video por IA permiten realizar estafas telefónicas simulando ser el CEO de una empresa o un familiar en problemas.
- **Generación de código malicioso:** Aunque los modelos comerciales tienen restricciones, los atacantes usan técnicas de *jailbreaking* (o modelos de IA clandestinos en la Dark Web como FraudGPT) para escribir scripts de hackeo, mutar malware de forma automática y encontrar vulnerabilidades en minutos.

Del lado de los defensores (Ciberseguridad automatizada)

- **Detección a velocidad de máquina:** Los sistemas de detección y respuesta (EDR Endpoint Detection and Response - Detección y Respuesta en Endpoints /XDR Extended Detection and Response - Detección y Respuesta Extendida) utilizan modelos de lenguaje e IA para analizar miles de millones de eventos en tiempo real, identificando comportamientos anómalos mucho antes que un analista humano. XDR Es la evolución natural del EDR. El problema del EDR es que es "ciego" fuera de las computadoras. XDR rompe esa limitación unificando la seguridad de toda la empresa en una sola plataforma.
- **Asistentes de seguridad:** Herramientas de IA ayudan a los ingenieros a auditar millones de líneas de código en busca de fallos (como Log4j) y a redactar parches o reportes de incidentes en segundos.

Pregunta de debate:

- *¿La ciberseguridad es más difícil hoy que en los 90, o solo es diferente?*
- *¿Que herramienta de seguridad implementarías en la Universidad?*

3.5 Actores de amenazas

Taxonomía de actores:

Tipo	Motivación	Ejemplos
Script Kiddies	Fama, diversión	Personas con poco o ningún conocimiento técnico que usan herramientas de hacking creadas por otros. No entienden cómo funcionan por dentro; solo aprietan botones. Un estudiante descarga LOIC (herramienta de DDoS), mete la IP de un servidor de un videojuego que no le gustó, y lo tumba por 20 minutos. No sabe programar, pero la herramienta hace el trabajo.
Hacktivistas	Ideología política/social	Hackers que usan sus habilidades para promover una causa política, social o ideológica. Mezclan "hacker" + "activista". Anonymous, LulzSec (hackeaba "por las risas" y por denunciar la mala seguridad de grandes empresas)
Criminales organizados	Económica	Grupos estructurados que operan como verdaderas empresas delictivas, pero en el ciberespacio. Tienen divisiones de trabajo: unos infectan, otros cobran, otros lavan dinero. Grupos de ransomware (REvil, LockBit)
Insiders	Venganza, económica, negligencia	Personas dentro de la organización (empleados, contratistas, socios) que abusan de su acceso legítimo para causar daño o robar información. Empleados descontentos, errores humanos
APT (Amenazas Persistentes Avanzadas)	Espionaje, sabotaje	Grupos de hackers altamente sofisticados, bien financiados y organizados, generalmente ligados a gobiernos o instituciones estatales. La palabra clave es "Persistente": no entran, roban y salen. Se quedan meses o años dentro de la red, espiando silenciosamente. APT28 (Fancy Bear- Rusia), APT41 (China), Lazarus Group (Corea del Norte)
Estados-nación	Geopolítica, militar	No son hackers individuales, sino programas oficiales de ciberoperaciones dirigidos por gobiernos. Pueden usar unidades militares, agencias de inteligencia, o contratar grupos APT como "subcontratistas". Operaciones de ciberinteligencia estatal

Estudio de caso:

Caso: Ataque a Colonial Pipeline (2021)

- Grupo: DarkSide (ransomware-as-a-service).

- Vector: Contraseña comprometida de VPN (sin MFA Multi-Factor Authentication - Autenticación Multifactor).
- Impacto: Paralización del mayor oleoducto de EE.UU., escasez de combustible, pago de ~$4.4M en bitcoin (parte recuperado).
- Lección: La seguridad no es solo técnica; es cadena de confianza y gestión de identidades.

Actividad: En grupos de 3-4, clasificar al actor del caso según la taxonomía y proponer qué principio CIA se vio más afectado.

4. MFA

Es un método de seguridad que exige **dos o más factores** para verificar tu identidad. Se clasifican así:

Factor	¿Qué es?	Ejemplo
1. Algo que sabes	Información que solo tú conoces	Contraseña, PIN
2. Algo que tienes	Un objeto físico o digital que posees	Celular, token, tarjeta
3. Algo que eres	Una característica biológica tuya	Huella dactilar, rostro, iris

---

¿Cómo funciona en la práctica?

Escenario	¿Es MFA?	¿Por qué?
Solo contraseña	❌ No	Un solo factor (algo que sabes)
Contraseña + código SMS	✅ Sí	Dos factores (sabes + tienes el celular)
Contraseña + app autenticadora (Google Authenticator, Microsoft Authenticator)	✅ Sí	Dos factores
Contraseña + huella dactilar	✅ Sí	Dos factores (sabes + eres)
Contraseña + pregunta de seguridad ("¿nombre de tu primera mascota?")	❌ No	Ambos son "algo que sabes" — sigue siendo un solo factor

5.1 Filtración de datos de Equifax (2017)

¿Qué pasó?

Equifax, una de las tres grandes agencias de crédito de EE.UU., sufrió una filtración masiva que expuso los datos personales de **147 millones de personas** (aproximadamente la mitad de la población adulta de ese país).

Datos comprometidos

- Nombres completos
- Números de Seguro Social (equivalente a cédula/DNI)
- Fechas de nacimiento
- Direcciones
- Números de licencias de conducir
- Datos de tarjetas de crédito (~200,000 registros)

¿Cómo ocurrió?

- Los atacantes explotaron una vulnerabilidad conocida en **Apache Struts** (CVE-2017-5638), un framework Java para aplicaciones web.
- **El parche de seguridad estaba disponible desde marzo de 2017**, pero el equipo de Equifax no lo aplicó.
- Los atacantes tuvieron acceso no autorizado a los sistemas durante **varios meses** (de mayo a julio de 2017) antes de ser detectados.

Principio CIA violado

> **Confidencialidad** — La información privada de millones de personas fue accedida y extraída por actores no autorizados.

Lección clave

- **La gestión de parches es crítica.** Tener tecnología de seguridad avanzada no sirve si no se aplican las actualizaciones básicas.
- **El tiempo de detección importa.** Los atacantes estuvieron meses dentro del sistema sin ser detectados (mala monitorización y logging).
- **La responsabilidad legal:** Equifax tuvo que pagar más de **$700 millones** en compensaciones y multas.

5.2. Ataque NotPetya (2017)

¿Qué pasó?

NotPetya fue un malware destructivo que se propagó globalmente en junio de 2017, afectando principalmente a Ucrania pero extendiéndose a empresas multinacionales. Aunque se disfrazó como ransomware (exigía un rescate de $300 en Bitcoin), en realidad era un **wiper** (limpiador): su objetivo real era destruir datos, no obtener dinero.

Empresas afectadas destacadas

- Maersk (naviera danesa, líder mundial)
- Merck (farmacéutica)
- FedEx (subsidiaria TNT Express)
- Reckitt Benckiser (fabricante de productos de consumo)
- Sistemas gubernamentales de Ucrania

¿Cómo ocurrió?

- Vector inicial: Software contable ucraniano **M.E.Doc**, muy utilizado por empresas en Ucrania. Los atacantes comprometieron los servidores de actualización del software e inyectaron el malware.
- Mecanismo de propagación: Exploit **EternalBlue** (misma herramienta robada de la NSA que usó WannaCry) + herramientas de credenciales (Mimikatz) para moverse lateralmente en redes Windows.
- Una vez en el sistema, cifraba el **Master File Table (MFT)** del disco duro, haciendo imposible el arranque del sistema operativo.

Principio CIA violado

> **Integridad** — El malware destruyó la estructura de archivos de los sistemas infectados. Los datos no fueron "robados" sino **corrompidos e inaccesibles**.
>
> También afectó **Disponibilidad**, ya que paralizó operaciones críticas (Maersk estuvo 2 semanas sin poder operar sus terminales de contenedores).

Lección clave

- **No todo ransomware busca dinero.** NotPetya fue probablemente un ciberataque patrocinado por estado (Rusia) contra Ucrania que se salió de control.

- **La cadena de suministro es un vector crítico.** Comprometer un software legítimo y popular es extremadamente efectivo.
- **Los costos fueron devastadores:** Se estiman **más de $10,000 millones** en daños globales, convirtiéndolo en el ciberataque más costoso de la historia hasta esa fecha.

5.3. Ataque DDoS a Dyn (2016)

¿Qué pasó?

El 21 de octubre de 2016, **Dyn** (uno de los mayores proveedores de DNS del mundo) sufrió un ataque de Denegación de Servicio Distribuido (DDoS) masivo que provocó la caída de cientos de sitios web y servicios populares en EE.UU. y Europa.

Servicios afectados

- Twitter
- Netflix
- Spotify
- Reddit
- CNN
- The New York Times
- Airbnb
- GitHub

¿Cómo ocurrió?

- Tipo de ataque: **DDoS** (Distributed Denial of Service) — saturar servidores con tráfico malicioso hasta dejarlos inoperativos.
- Escalón: **Aproximadamente 1.2 Tbps** de tráfico (un récord en ese momento).
- **El arma: Mirai**, un malware que infecta dispositivos IoT (cámaras de seguridad, routers domésticos, DVRs) con contraseñas por defecto o débiles.
- Estos dispositivos IoT comprometidos formaron una **botnet** (red de "zombies") que lanzó el ataque coordinado contra los servidores DNS de Dyn.

Principio CIA violado

> **Disponibilidad** — Los servicios no estaban disponibles para millones de usuarios legítimos. No hubo robo de datos ni corrupción, simplemente **negación del servicio**.

Lección clave

- **El Internet de las Cosas (IoT) es un vector de ataque masivo.** Dispositivos baratos con seguridad deficiente pueden ser reclutados en botnets.
- **La seguridad por defecto importa.** Mirai funcionó porque miles de dispositivos tenían contraseñas como "admin/admin" o "123456".
- **La centralización es un riesgo:** Al atacar un solo proveedor de DNS (Dyn - empresa estadounidense que proveía servicios de DNS), se derribó una parte significativa de Internet.
- **Dyn fue adquirida poco después** por Oracle, en parte debido a la necesidad de mayor infraestructura resiliente.

Tabla comparativa

Caso	Año	Tipo de ataque	Vector	Principio CIA	Actor probable	Costo estimado
Equifax	2017	Filtración de datos	Vulnerabilidad sin parchear (Apache Struts)	**Confidencialidad**	Criminales / APT	$700M+ en multas
NotPetya	2017	Wiper disfrazado de ransomware	Cadena de suministro (M.E.Doc) + EternalBlue	**Integridad** (y Disponibilidad)	Estado-nación (Rusia)	$10,000M+
Dyn DDoS	2016	DDoS masivo	Botnet Mirai (IoT comprometidos)	**Disponibilidad**	Hacktivistas / criminales	Millones en pérdidas operativas

Preguntas para debate

1. **¿Cuál de los tres casos consideras más grave y por qué?** (Robo de identidad vs. destrucción de datos vs. paralización de servicios)
2. **¿Podría haberse evitado el ataque a Equifax?** ¿Qué proceso de seguridad falló?
3. **¿Por qué NotPetya se considera un ataque geopolítico y no criminal común?**
4. **¿Tienes dispositivos IoT en casa?** ¿Cambiaste las contraseñas por defecto?

Respuesta Pregunta:

Pregunta

> *"¿Una empresa que tiene su data center físico bien protegido con antivirus y firewall, pero permite a sus empleados acceder a correo corporativo desde celulares personales sin MFA (Multi-Factor Authentication), tiene Seguridad Informática o Ciberseguridad?"*

Respuesta correcta: Tiene Seguridad Informática, pero **carece de Ciberseguridad** porque no protege el perímetro extendido (dispositivos móviles, acceso remoto).