EXPOSICIÓN: CIBERATAQUES MÁS FRECUENTES Y SU ANÁLISIS

1. Clasificación de los ciberataques más conocidos:
Tras una investigación conjunta, se identificaron los tipos de ciberataques más frecuentes:

- **Ransomware**: El más relevante, por su impacto en **gobiernos, hospitales y empresas**, ya que **secuestra y cifra datos** para luego exigir un **rescate**.
- **Phishing**: Técnica de **engaño** para robar información confidencial. A pesar de ser antigua, sigue siendo muy efectiva.
- **DDoS (Denegación de Servicio Distribuida)**: Saturación de servidores mediante múltiples solicitudes simultáneas, afectando la **disponibilidad**.
- **Malware**: Propagación de **software malicioso** para dañar, borrar o controlar sistemas.
- **Hacktivismo**: Ataques con **motivaciones políticas o sociales**, que se analizarán con mayor profundidad más adelante.

2. Fuentes de información consultadas:

- Se usaron recursos como **Google, Google Académico y bases de datos en línea**.
- Los resultados están detallados en los **anexos del informe**.

3. Datos recopilados:

Los tipos de ciberataques identificados incluyeron: **ransomware, filtración de datos, DDoS, acceso no autorizado, robo de criptomonedas**, entre otros. En el año 2022, el **ransomware** lideró en frecuencia con **26 registros**.

✅ **Respuestas estructuradas a las preguntas del informe:**

1. **¿Cuántos de esos ataques tuvieron como vector inicial la ingeniería social (por ejemplo, phishing)?**

al menos tres ataques tuvieron como vector inicial la ingeniería social:

- **Gobierno de Costa Rica:** acceso inicial por **phishing o credenciales comprometidas**.
- **Conflicto Rusia-Ucrania:** se menciona el **phishing dirigido** como técnica de acceso inicial.

- **Generalidades del MITRE ATT&CK:** uso de correos institucionales falsificados (ingeniería social).

📌 **Total: 3 ataques identificados con phishing como vector inicial.**

Vector de Ingeniería Social	***Descripción Técnica***	***Casos Reales Relevantes***
Phishing tradicional (Email genérico)	Correos masivos con enlaces o archivos maliciosos, haciéndose pasar por empresas conocidas.	- **Gobierno de Costa Rica (2022)**: acceso inicial sospechado vía phishing. - **Sony Pictures (2014)**: spear phishing inicial previo al ataque de Corea del Norte.
Spear Phishing	Phishing personalizado usando datos reales del objetivo (nombre, cargo, temas específicos).	- **Hackeo a John Podesta (2016)**: spear phishing dirigido al jefe de campaña de Hillary Clinton. - **Rusia-Ucrania (2022)**: ataques dirigidos a personal militar.
Whaling (Phishing a ejecutivos)	Variante de spear phishing dirigida a altos ejecutivos ("peces gordos") para fraudes financieros.	- **Crelan Bank (2016)**: ataque tipo whaling robó más de €70 millones mediante suplantación de CEO.
Business Email Compromise (BEC)	El atacante suplanta una cuenta empresarial legítima para desviar pagos o obtener datos.	- **Toyota Boshoku (2019)**: pérdida de $37 millones por redireccionamiento de pagos mediante BEC. - **Facebook y Google (2013–2015)**: engaño de $100M con facturas falsas.
Vishing (Phishing por voz)	Llamadas telefónicas que simulan ser de entidades confiables (bancos, soporte técnico).	- **Twitter Hack (2020)**: se usó ingeniería social vía llamadas para engañar a empleados y tomar control de cuentas verificadas.
Smishing (Phishing por SMS)	Mensajes de texto con enlaces maliciosos o solicitudes de datos personales.	- **Campañas bancarias falsas en España (2021)**: SMS falsos que llevaban a sitios clonados de bancos para robar credenciales.
Deepfake o voz sintética	Uso de inteligencia artificial para crear audio/video falso de personas reales.	- **Caso de CEO en Reino Unido (2019)**: deepfake de voz suplantó a directivo

		alemán para autorizar transferencia de €220K.
Uso de credenciales comprometidas	Uso de datos filtrados o comprados en dark web para ingresar sin levantar sospechas.	- **LinkedIn Data Leak (2021)**: millones de credenciales fueron filtradas y usadas en campañas posteriores. - **Costa Rica (2022)**: posible uso de este vector.
Pretexting	Engaño que involucra un "pretexto" o historia falsa para obtener acceso o datos.	- **Target (2013)**: atacantes se hicieron pasar por empleados de un proveedor para infiltrar sistemas de HVAC y luego robar datos de tarjetas.
Quid pro quo (intercambio fraudulento)	El atacante ofrece un servicio falso (actualización, soporte, etc.) a cambio de acceso.	- Casos frecuentes en **call centers falsos de soporte técnico** simulando ser de Microsoft para controlar PCs remotamente.
Uso de instaladores o actualizaciones falsas	Ofrecen actualizaciones de software o antivirus falsos que instalan malware.	- **Ucrania (2022)**: instaladores falsos utilizados como vector de entrada en ministerios clave.
Correos institucionales falsificados	Suplantación de cuentas reales para generar confianza y lograr acceso interno.	- **APT29 (Cozy Bear, 2020)**: usó correos falsos para acceder a organizaciones vinculadas a la vacuna del COVID-19.

2. ¿Cuántos tipos de vectores iniciales de ataque han sido identificados?

✅ **Resumen del análisis del informe sobre ciberataques (2022)**

Vector de Ataque	*Descripción*	*Canal principal*
Phishing tradicional	Correos masivos con enlaces o archivos maliciosos, simulando ser de empresas legítimas.	Email
Spear phishing	Variante dirigida de phishing que usa información personalizada del objetivo para mayor eficacia.	Email, mensajería interna

Whaling	Spear phishing dirigido específicamente a altos ejecutivos o directivos de una organización.	Email corporativo
Business Email Compromise (BEC)	Suplantación de cuentas reales de empresas para desviar pagos o recolectar información sensible.	Email empresarial
Vishing	Llamadas telefónicas donde el atacante se hace pasar por una entidad legítima (banco, soporte).	Teléfono (voz)
Smishing	Envío de SMS con enlaces maliciosos o solicitudes de datos bajo apariencia de mensajes legítimos.	Mensajes de texto (SMS)
Deepfake o voz sintética	Uso de audio o video generado por IA para imitar a personas reales y engañar al receptor.	Audio/Video
Uso de credenciales comprometidas	Utilización de usuarios y contraseñas obtenidos previamente (por filtraciones o compras).	Web, VPN, email, RDP
Pretexting	El atacante finge una identidad o situación para obtener datos o acceso (ej. auditor, técnico).	Teléfono, email
Quid pro quo (intercambio fraudulento)	El atacante ofrece un beneficio falso (soporte, premio) a cambio de acceso o datos confidenciales.	Teléfono, email
Instaladores o actualizaciones falsas	Se ofrecen supuestas actualizaciones de software que en realidad instalan malware.	Web, USB, email
Correos institucionales falsificados	Correos que aparentan provenir de instituciones o personas confiables (usando nombres reales).	Email

---

🤳 Vectores de ataque inicial identificados

Se clasificaron principalmente en:

1. **Phishing (ingeniería social)**
2. **Credenciales comprometidas**
3. **Explotación de vulnerabilidades no parchadas**
4. **Uso de software legítimo para fines maliciosos (Living Off the Land – LOLbins)**
5. **Medios físicos (USB infectados u otros dispositivos)**
6. **Actualizaciones o correos oficiales falsificados**

🦹 Grupos atacantes y su origen

En el análisis, se identificaron grupos cibercriminales conocidos:

- **Conti** (origen: Rusia)
- **Lazarus Group** (Corea del Norte)
- **Guacamaya** (Latinoamérica, activismo)
- **APT28 / Fancy Bear** (Rusia)
- **Killnet** (Rusia)

🔎 **Observación importante**: Se concluyó que **Rusia fue el país con mayor cantidad de ataques atribuidos**, al menos en los reportes analizados (posiblemente más de 15 de los 55 incidentes).

🔥 Tipo de ciberataques más comunes

- **Ransomware**: el más frecuente y de mayor impacto económico.
- **Phishing**: ampliamente utilizado por su efectividad.
- **DDoS (Denegación de Servicio)**: usado en ataques a infraestructuras críticas.
- **Malware genérico** y **robo de datos** también fueron destacados.

📌 Errores identificados y recomendaciones

- Faltan **referencias específicas por cada incidente** reportado.

- La ficha técnica por ataque debe incluir: vector inicial, impacto, grupo atacante, país de origen y fuente o reporte verificado.
- No debe asumirse información basada en creencias o "lo que se dice", sino en fuentes académicas, técnicas o reportes especializados (como MITRE, ENISA, CSIRT, etc.)

📜 **Palabras clave y definiciones**

TÉRMINO	DEFINICIÓN
PHISHING	Técnica de engaño para obtener información sensible, generalmente por correo.
RANSOMWARE	Malware que cifra archivos y exige un pago para liberarlos.
DDOS	Ataque que satura un servidor con múltiples solicitudes hasta bloquearlo.
VECTOR DE ATAQUE	Punto de entrada inicial del atacante en un sistema o red.
APT (AMENAZA PERSISTENTE AVANZADA)	Grupo altamente organizado con recursos para mantener acceso prolongado en un sistema.
MITRE ATT&CK	Marco de referencia que clasifica tácticas, técnicas y procedimientos de ataque.
LIVING OFF THE LAND (LOLBINS)	Uso de herramientas legítimas del sistema con fines maliciosos.

📜 **Sobre el volumen y criticidad de los ataques**

- **Periodo analizado**: 1995 a 2025 (según la base CVE).
- **Número total de incidentes identificados en 2022**: de 0 a 40 casos, con varios saltos y vacíos de numeración (por ejemplo, entre los casos 5 y 21 no hay registros completos).
- **Sobre los niveles de criticidad**: no se indicó cuántos ataques fueron clasificados como **críticos, medios o bajos**. Esto debe ser abordado si se desea comprender la **potencialidad del impacto** y priorización de riesgos.

🛡️ **Resumen general: Empresas certificadoras y certificaciones en ciberseguridad**

¿Qué es una certificación en ciberseguridad?
Una **certificación** es una credencial oficial que valida los **conocimientos teóricos y habilidades prácticas** de un profesional en el ámbito de la seguridad informática. Se obtiene tras superar exámenes (teóricos, prácticos o ambos) avalados por instituciones reconocidas.

🔑 **Características principales:**

- **Validación de competencias**: se demuestra mediante pruebas.

- **Periodo de validez**: puede ser temporal (1-3 años) o indefinido.
- **Especialización**: según el área (redes, ofensiva, gobernanza, etc.).
- **Valor profesional**: aumenta la empleabilidad, el salario y la competitividad.

🏢 Principales empresas certificadoras destacadas

✅ CREST

- Origen: Reino Unido.
- Enfocada en: Seguridad ofensiva (penetration testing).
- Reconocida por: Gobiernos y el sector financiero.
- Enfoque: Pruebas rigurosas prácticas.
- Certificación estrella: CREST CRT.

✅ Hack The Box (HTB)

- Enfoque: Plataforma gamificada.
- Método: Aprendizaje práctico mediante retos reales.
- Reconocida por: Empresas tecnológicas y comunidades técnicas.
- Ideal para: Formación práctica desde niveles básicos hasta avanzados.

✅ ISACA

- Enfoque: Gobierno TI, auditoría, cumplimiento normativo.
- Certificaciones clave: CISA, CISM, CRISC.
- Presencia: Más de 165,000 miembros en 180 países.
- Ideal para: Gestión de riesgos, gobernanza TI, roles ejecutivos.

✅ Offensive Security (OffSec)

- Producto destacado: Kali Linux (Pentesting).
- Certificación principal: OSCP (Offensive Security Certified Professional).
- Reconocida por: Su examen práctico de 24 horas.
- Enfoque: Habilidades ofensivas en escenarios reales.

✅ SANS Institute

- Ofrece más de 85 cursos avanzados.

- Áreas: Seguridad, análisis forense, respuesta a incidentes.
- Certificaciones GIAC: altísima valoración global.
- Instructores: Profesionales activos en la industria.

🧠 **Palabras clave y definiciones**

Palabra clave	***Definición***
Certificación	Acreditación oficial que valida habilidades y conocimientos técnicos.
Ciberseguridad	Disciplina que protege sistemas y redes frente a ataques digitales.
Pentesting	Pruebas de penetración para evaluar vulnerabilidades de un sistema.
Phishing	Técnica de engaño para obtener credenciales o información sensible.
Ransomware	Tipo de malware que secuestra datos y exige un rescate para liberarlos.
Ingeniería social	Manipulación psicológica para engañar y obtener información confidencial.
Mitre ATT&CK	Marco que categoriza tácticas y técnicas utilizadas en ataques reales.
Indicador de Compromiso (IoC)	Señal o evidencia de que una red o sistema ha sido comprometido.

Cada certificación mencionada debe tener una **URL o fuente** donde se pueda verificar:

- Costos
- Duración
- Nivel de dificultad
- Validez
- Enfoque técnico (ofensivo, defensivo, gestión)

👉 Por ejemplo: si se menciona que **Cisco** adquirió **Sourcefire** o que su programa **Security** tiene especialidades, **debe indicarse** la fuente exacta de la página de Cisco donde aparece esa información.

EMPRESA / CERTIFICACIÓN	💰 COSTOS	⏳ DURACIÓN	🎯 DIFICULTAD	🌐 VALIDEZ	🛡️ ENFOQUE TÉCNICO	🤝 ADQUISICIONES / PROGRAMAS	🎓 ESPECIALIDADES
🟦 **CISCO SYSTEMS**	$300 – $1,200	3 – 6 meses	Intermedio – Alto	Muy alta	Defensivo / Gestión técnica	Adquirió **Sourcefire**, empresa de detección de intrusos (IDS/IPS).	Seguridad de redes, monitoreo, infraestructura
▪ **CCNA SECURITY**	~$300	3 meses	Intermedio	Global	Seguridad de red	Incluido en su programa **Networking Academy**	Redes seguras, dispositivos Cisco
▪ **CYBEROPS ASSOCIATE**	~$400	3–4 meses	Intermedio	Global	Operaciones de seguridad	–	Análisis de eventos, SOC, SIEM
▪ **CCNP SECURITY**	~$1,200	5–6 meses	Alto	Alta	Infraestructura defensiva	–	Arquitectura de seguridad avanzada
----------	----------	----------	----------	----------	----------	----------	----------
🟨 **COMPTIA**	$150 – $400	1 – 3 meses	Básico – Intermedio	Muy alta	Defensivo / Gestión básica	Programa **Career Pathways** y **Stackable Certs**	Formación básica en TI y ciberseguridad
▪ **A+**	~$250	1–2 meses	Básico	Global	Soporte técnico	–	Hardware, software, solución de problemas
▪ **NETWORK+**	~$300	2–3 meses	Básico – Medio	Alta	Redes	–	Routing, switching, redes LAN/WAN
▪ **SECURITY+**	~$370	2–3 meses	Intermedio	Alta	Seguridad general	–	Criptografía, amenazas, controles de acceso

▪ **LINUX+**	~$350	2–3 meses	Intermedio	Alta	Sistemas operativos	–	Administración de sistemas Linux
----------	----------	----------	----------	----------	----------	----------	----------
🟥 **EC-COUNCIL**	$500 – $1,200	3 – 6 meses	Alto	Muy alta	Ofensivo / Gestión	Creador de la plataforma **iClass** y laboratorio **CyberQ**	Pentesting, auditorías, ciberataques simulados
▪ **CEH (ETHICAL HACKER)**	~$1,200	4–6 meses	Alto	Reconocimiento global	Hacking ético	–	Pruebas de penetración, hacking ético
▪ **ECSA / CISSM**	$600 – $1,000	3–4 meses	Alto	Muy valoradas	Auditoría / gestión	–	Riesgo, seguridad organizacional, cumplimiento
----------	----------	----------	----------	----------	----------	----------	----------
🟩 **(ISC)²**	$599 – $749	4 – 8 meses	Alto – Experto	Estándar global	Gestión / Defensa estratégica	Sin adquisiciones, pero con la iniciativa **One Million Certified in Cybersecurity**	Liderazgo, gobernanza, compliance, riesgo
▪ **CISSP**	$749	6–8 meses	Muy alto	La más valorada	Gestión avanzada	–	Seguridad organizacional, legalidad, criptografía
▪ **CCSP / CSSLP / SSCP**	$599 – $650	4–6 meses	Alto	Alta	Nube, desarrollo seguro	–	DevSecOps, cloud security, operaciones seguras

---

2. 🏅 ¿Qué significa que una certificación sea “estándar de oro”?

El término "**estándar de oro**" se refiere a que esa certificación es:

- Altamente reconocida a **nivel internacional**
- Considerada una **referencia o base** para otros programas similares
- Usualmente **requerida en puestos de alto nivel** o especializada en el área

📌 Ejemplo:

- **CISSP (de ISC²)** es llamado el "estándar de oro" en seguridad porque es una de las certificaciones más completas y exigidas para **puestos de liderazgo en seguridad informática**.
- En contraste, otras certificaciones pueden ser más técnicas, básicas o de nicho.

📌 **En el contexto de ciberseguridad, esto implica que:**

1. ✅ **Es altamente reconocida** a nivel global por empleadores, gobiernos y organizaciones.
2. 🧠 **Demuestra un dominio profundo** de conocimientos y habilidades clave del área.
3. 🎓 **Es exigente en su obtención**, tanto en estudio como en experiencia previa (no es una certificación básica).
4. 🔐 **Cumple con estándares internacionales** (como ISO/IEC 17024 u otros marcos de calidad profesional).
5. 💼 **Es requisito común** para cargos de alto nivel (como CISO, auditor líder, arquitecto de seguridad, etc.).
6. 🏛️ **Aporta credibilidad y confianza** al profesional ante terceros, proyectos críticos o evaluaciones.

📍 **Ejemplos de certificaciones consideradas "estándar de oro":**

- **CISSP (de (ISC)²)** en gestión de seguridad de la información.
- **CEH (de EC-Council)** en hacking ético ofensivo (aunque algunos la discuten frente a OSCP).
- **PMP (Project Management Professional)** en gestión de proyectos (en su propio dominio).
- **CPA / CFA** en contabilidad o finanzas (como paralelos en otras disciplinas).

---

3. 🗺️ ¿Existe un mapa de certificaciones?

Sí. Existen **mapas de ruta** de certificaciones que agrupan las credenciales por áreas como:

- Seguridad ofensiva (pentesting, hacking ético)
- Seguridad defensiva (gestión de incidentes, monitoreo)
- Gobernanza (auditoría, cumplimiento)
- Infraestructura (redes, arquitectura)

Por ejemplo:

- Cisco tiene rutas como **Security Operations**, **Architecture Security**, etc.
- CompTIA separa sus certificaciones por niveles: **Core**, **Infrastructure**, **Cybersecurity**, etc.

🟨 Pero si en el informe se menciona que hay "más de 400 certificaciones" o "tantas organizaciones", es indispensable **presentar esa base en anexos numerados**, bien detallada y con referencias claras (por ejemplo: número total, agrupación por tipo, por fabricante).

¡Sí! 📍 **Existen varios mapas de certificaciones en ciberseguridad**, conocidos como **"Cybersecurity Certification Roadmaps"**. Estos mapas organizan visualmente las certificaciones por:

- 🧩 **Nivel de dificultad** (básico, intermedio, avanzado, experto)
- 💼 **Roles profesionales** (analista SOC, auditor, CISO, pentester, etc.)
- 🔧 **Áreas de enfoque** (defensivo, ofensivo, nube, forense, gestión, etc.)
- 🎓 **Progresión formativa** (de principiante a experto)

🗺️ **Ejemplo de estructura típica de un mapa de certificaciones:**

🔷 **Nivel básico / entrada (Entry-Level)**

- CompTIA ITF+
- CompTIA A+
- Cisco IT Essentials
- Microsoft Fundamentals (AZ-900)

🔷 **Nivel intermedio (Associate-Level)**

- CompTIA Security+
- Cisco CyberOps Associate
- Microsoft Security, Compliance & Identity
- EC-Council CND

🔷 **Nivel avanzado (Professional-Level)**

- CEH (EC-Council)
- CompTIA CySA+
- Cisco CCNP Security
- (ISC)² SSCP

🔷 **Nivel experto (Expert-Level)**

- CISSP ((ISC)²)
- OSCP (Offensive Security)
- CISM / CISA (ISACA)
- CCSP ((ISC)²) – en nube
- GIAC / GSEC (SANS Institute)

📦 **Recursos donde puedes ver o descargar mapas actualizados:**

1. 📎 **(ISC)² Career Pathways**: en su sitio oficial
2. 📎 **CompTIA Cybersecurity Career Pathway Map**
3. 📎 **SANS Institute Roadmap**
4. 📎 **Infografías de CyberSeek (EE. UU.)**: muy visual y por roles
5. 📎 **Redes de LinkedIn o GitHub**: comunidad de ciberseguridad suele compartir infografías útiles.

Se mencionan certificaciones como HTB o CSA sin validar su respaldo en la industria.

🧠 1. HTB – Hack The Box Certifications

🔍 ¿Qué es Hack The Box (HTB)?

Es una plataforma reconocida mundialmente para practicar *penetration testing* (pruebas de intrusión) y habilidades ofensivas en entornos simulados.

🎓 Certificaciones HTB destacadas:

CERTIFICACIÓN HTB	ENFOQUE PRINCIPAL	NIVEL	RECONOCIMIENTO
HTB CPTS *(CERTIFIED PENETRATION TESTING SPECIALIST)*	Pentesting, explotación, reportes	Intermedio	Aceptada en el entorno ofensivo
HTB CPTL *(CERTIFIED PENETRATION TESTING LEADER)*	Gestión de equipos de Red Team	Avanzado	En crecimiento

💡 Estas certificaciones son **prácticas al 100%**, con laboratorios reales (tipo *OSCP*) y son especialmente valoradas en **roles ofensivos técnicos**, como **Red Team, pentester y bug bounty**.

🛡️ 2. CSA – Certified SOC Analyst (de EC-Council)

🔍 ¿Qué es CSA?

Es una certificación de **EC-Council** enfocada en formar **analistas SOC de nivel 1**, es decir, personal que monitorea, detecta y responde a amenazas de seguridad en tiempo real.

🎓 Detalles clave:

CARACTERÍSTICA	DETALLE
NOMBRE COMPLETO	*Certified SOC Analyst (CSA)*
ENFOQUE	Defensa, monitoreo de seguridad, SIEM, respuesta inicial
NIVEL	Básico – Intermedio
DURACIÓN SUGERIDA	2–3 meses
REQUISITOS	Conocimientos básicos en redes y seguridad
IDEAL PARA	Ingreso a centros SOC, roles de seguridad blue team

📌 Aunque el nombre **CSA** puede confundirse con otras certificaciones, en este contexto se refiere a la de **EC-Council**.

✅ **Comparativa rápida**

CERTIFICACIÓN	TIPO	ENFOQUE TÉCNICO	NIVEL	IDEAL PARA
HTB CPTS	Privada / práctica	Ofensivo – hacking	Intermedio	Pentesters, Red Team
CSA (EC-COUNCIL)	Profesional	Defensivo – SOC	Básico – intermedio	Analistas SOC, monitoreo

- Se confunden certificaciones con el mismo acrónimo pero distinto origen (por ejemplo: SISA vs CISA).

🔍 **1. CISA – Certified Information Systems Auditor**

CARACTERÍSTICA	DETALLE
🏢 **ENTIDAD EMISORA**	**ISACA** (Information Systems Audit and Control Association)
🎯 **ENFOQUE PRINCIPAL**	Auditoría, control, aseguramiento y gestión de sistemas de información
🧠 **PERFIL OBJETIVO**	Auditores de TI, consultores de riesgo, gestores de cumplimiento
💼 **ÁREAS CUBIERTAS**	- Auditoría de sistemas - Gobierno de TI - Seguridad y control interno - Gestión de riesgos
🎓 **REQUISITOS**	5 años de experiencia profesional en auditoría, control o seguridad de TI (con exenciones)
🌎 **RECONOCIMIENTO**	Muy alto a nivel global – estándar en auditoría y compliance

📌 CISA es una **certificación profesional formal** altamente reconocida por gobiernos, Big Four, y grandes empresas.

🔧 2. SISA – Secure Information Sharing Architecture / o SISA Infosec (empresa)

Aquí hay dos sentidos posibles de SISA, dependiendo del contexto:

a) ✅ SISA como empresa: SISA Infosec

CARACTERÍSTICA	DETALLE
🏢 **ENTIDAD**	**SISA Information Security Pvt. Ltd.** (India)
🛡️ **ESPECIALIDAD**	Consultoría en **PCI DSS, pagos seguros, protección de datos**
🎓 **CERTIFICACIONES**	Ofrecen certificaciones como **CISP** (Certified Information Security Professional)
🔎 **RECONOCIMIENTO**	Regionalmente reconocida en Asia y por empresas en el rubro de pagos

b) 🔄 SISA como término técnico (menos común)

- En algunos contextos, **SISA** se refiere a *Secure Information Sharing Architecture*, un marco conceptual para **compartir datos de forma segura entre organizaciones**.
- No es una certificación en sí, sino un **modelo técnico o marco de referencia** usado en entornos gubernamentales o militares.

🧠 Resumen comparativo

Característica	*CISA (ISACA)*	*SISA (empresa o arquitectura)*
Tipo	Certificación profesional	Empresa / Marco de seguridad
Enfoque	Auditoría de sistemas, cumplimiento	Seguridad en pagos, PCI DSS, intercambio de información
Nivel de reconocimiento	Muy alto, global	Regional (Asia / sector financiero)
Certificación asociada	Certified Information Systems Auditor (CISA)	Certified Information Security Professional (CISP - SISA)

Ausencia de Evidencia en el Mercado Laboral: No se revisaron portales de empleo (como LinkedIn, Bumeran, Computrabajo) para validar cuáles certificaciones realmente son solicitadas. No se muestran tendencias de demanda.

Puedes usar capturas o gráficos de:

- LinkedIn o Indeed: cantidad de ofertas que mencionan **CISSP**, **Security+**, **OSCP**, etc.
- Comparativa: certificaciones más solicitadas vs. menos relevantes.

Mapa de Certificaciones en Ciberseguridad – Por Área de Especialización

Área	*Certificaciones Ejemplo*
Seguridad ofensiva (Red Team)	- **OSCP** (Offensive Security Certified Professional) - **CEH** (Certified Ethical Hacker – EC-Council) - **PNPT** (Practical Network Penetration Tester) - **HTB CPTS** (Hack The Box) - **eJPT** (eLearnSecurity Junior Penetration Tester)
Seguridad defensiva (Blue Team)	- **CompTIA Security+** - **Blue Team Level 1 (BTL1)** - **Cisco CyberOps Associate** - **CompTIA CySA+** (Cybersecurity Analyst) - **GCDA** (GIAC Certified Detection Analyst)
Gestión / Gobierno / Liderazgo	- **CISSP** (Certified Information Systems Security Professional – ISC^2) - **CISM** (Certified Information Security Manager – ISACA) - **CRISC** (Certified in Risk and Information Systems Control – ISACA)
Auditoría / Cumplimiento	- **CISA** (Certified Information Systems Auditor – ISACA) - **ISO 27001 Lead Auditor** (varias entidades) - **CGEIT** (Certified in Governance of Enterprise IT – ISACA)
Seguridad en la nube	- **CCSK** (Certificate of Cloud Security Knowledge – CSA) - **CCSP** (Certified Cloud Security Professional – ISC^2) - **AWS Security Specialty** - **AZ-500** (Microsoft Azure Security Engineer) - **Google Cloud Professional Cloud Security Engineer**
Análisis forense / respuesta a incidentes	- **CHFI** (Computer Hacking Forensic Investigator – EC-Council) - **GCFA** (GIAC Certified Forensic Analyst)

	- **GCIH** (GIAC Certified Incident Handler) - **CFR** (CyberSec First Responder)
💻 ***Administración de sistemas / generalista***	- **CompTIA A+** - **CompTIA Network+** - **CompTIA Linux+** - **Microsoft MTA Security Fundamentals**
💼 ***Formación técnica inicial / básica***	- **CompTIA ITF+** (Fundamentos de TI) - **Google IT Support Certificate** - **Cisco IT Essentials** - **ISC² Certified in Cybersecurity (CC)**

🧭 **Clasificación por niveles (transversal):**

🔷 NIVEL	📘 CERTIFICACIONES EJEMPLO
🟢 **BÁSICO**	ITF+, A+, Network+, eJPT, ISC² CC, Security+
🟡 **INTERMEDIO**	CEH, CySA+, CCSK, CHFI, Cisco CyberOps, AZ-500
🔴 **AVANZADO**	OSCP, PNPT, CISSP, CISM, CCSP, GCFA, CISA
⚫ **EXPERTO / LIDERAZGO**	CRISC, CGEIT, CISO-level, ISO 27001 Lead Auditor, GSE (GIAC Security Expert)

🛡️ **Introducción al Panorama de Ciberataques en 2024**

Hola. Para comenzar con nuestra presentación, queríamos mostrar algunos datos relevantes sobre los ciberataques ocurridos en el año 2024. Se trata de un panorama bastante complejo y diverso, con cifras altas reportadas por diversas fuentes internacionales.

En primer lugar, encontramos reportes anuales de Microsoft, donde se estima que se producen alrededor de 300 millones de ataques cibernéticos al año. Sin embargo, en 2024, algunas cifras incluso superaron eso: por ejemplo, la empresa **Stormous** reportó más de 280 millones de incidentes globales.

Por otro lado, plataformas como **Statista** —un servicio alemán especializado en datos estadísticos— indicaron que, solo en el primer trimestre de 2024, se detectaron cerca de 3,000 amenazas tipo ransomware en sectores críticos. Además, el **mapa de amenazas de CheckPoint**

(herramienta que el profesor nos mostró en clase) llegó a registrar más de 10 millones de intentos de ataque por día a nivel mundial.

En el caso de Perú, el medio *El Comercio* reportó que, solo en 2024, se habían registrado cerca de 1 millón de ciberataques, afectando tanto a instituciones públicas como privadas.

Como puede notarse, obtener una cifra exacta es difícil, ya que depende de la fuente y del método de detección. Por eso, en nuestro análisis nos basamos en datos consolidados y reportes oficiales.

🧩 Caso Interval International – Ciberataque Relevante de 2024

Uno de los casos más sonados de 2024 fue el ataque contra la empresa **Interval International**, una reconocida compañía que opera a nivel global en el sector turístico. El ciberataque fue altamente relevante a nivel nacional e internacional, debido a la magnitud de los datos comprometidos.

Este ataque fue perpetrado por un grupo conocido como **PATCH**, el cual exigió un rescate de **4 millones de dólares** para no divulgar la información robada. En total, se vieron comprometidos **3.7 millones de registros**, correspondientes a alrededor de **3 millones de clientes**. Entre los datos filtrados estaban nombres, direcciones, documentos de identidad, contraseñas cifradas y datos financieros.

El impacto económico estimado fue de **alrededor de 1,700 millones de dólares** en pérdidas potenciales. Aunque no se ha confirmado oficialmente, todo indica que el acceso se obtuvo mediante un tercero con permisos privilegiados, lo que abre la posibilidad de que haya sido un **ataque interno o facilitado por un "insider"** (empleado con malas intenciones).

La empresa confirmó el incidente y señaló que estaba trabajando en colaboración con autoridades para mitigar el impacto y fortalecer sus medidas de ciberseguridad. Este ataque evidenció la urgencia de proteger la infraestructura digital, especialmente en empresas que manejan grandes volúmenes de datos personales y financieros.

🛡️ Caso 2: National FortiLuckham (Estados Unidos, 2024)

Continuando con los casos relevantes de ciberataques en el año 2024, presentamos el incidente ocurrido en la empresa **National FortiLuckham**, una subsidiaria de una entidad mayor dedicada al manejo de grandes volúmenes de datos públicos y privados en Estados Unidos.

🔍 Contexto y naturaleza de la empresa

National FortiLuckham tiene como función principal la **recolección, verificación y almacenamiento masivo de datos** personales para diversos fines legales, especialmente en procesos de verificación de antecedentes judiciales y administrativos.

📆 Cronología del ataque

- **Inicio de amenazas:** Se identificaron intentos de intrusión desde finales del año 2023.
- **Fecha de confirmación del ataque:** 8 de abril de 2024.
- **Grupo atacante:** Se sospecha de un colectivo denominado **"The Point"**, el cual operó utilizando tácticas de **ingeniería social** para infiltrarse en la infraestructura de la organización.
- **Petición de rescate:** El grupo exigió **5 millones de dólares** para no divulgar los datos robados.

🧨 Datos comprometidos

Se estima que fueron filtrados **más de 3 mil millones de registros** con información personal altamente sensible, entre ellos:

- Nombres completos
- Direcciones
- Correos electrónicos
- Números de seguridad social
- Información financiera
- Credenciales electrónicas

Además, al menos **35 millones de registros** ya fueron liberados públicamente en foros y redes clandestinas.

⚠️ Consecuencias del ataque

- **Riesgo de suplantación de identidad:** El acceso a información personal permite la creación de cuentas falsas, fraudes bancarios y manipulación de registros oficiales.
- **Daño reputacional:** La empresa sufrió una pérdida severa de confianza por parte de sus clientes y entidades colaboradoras.
- **Impacto político:** El ataque generó tensiones internas y cuestionamientos sobre la gestión de datos por parte de FortiLuckham, lo cual derivó en cambios en la directiva, incluyendo la salida de su director general, **Adriano Lanzarote**, en octubre de 2024.

💥 ¿Quién es "The Point"?

A pesar del nombre que hace referencia al Departamento de Defensa, **"The Point" no es una institución oficial de EE. UU.**, sino un grupo **de ciberatacantes especializado en filtración de datos masivos y extorsión digital**. Es considerado un **actor de amenaza avanzado**, con operaciones dirigidas a sectores gubernamentales y corporativos.

Intervención del docente (versión mejorada):

¿Se trata de intentos de ataque? ¿Son ataques confirmados y documentados? ¿Cuál es la fuente y qué metodología se ha seguido para validarlos?

1️⃣ ¿Qué es un intento de ataque?

Un **intento de ataque** es cualquier **actividad sospechosa o maliciosa detectada por sistemas de seguridad** (como firewalls, SIEM, IDS/IPS), que **indica que un actor externo ha intentado vulnerar un sistema**, sin importar si tuvo éxito o no.

📌 Ejemplos:

- Un escaneo de puertos desde una IP externa.
- Un correo con un archivo adjunto malicioso que no fue abierto.
- Un intento de inicio de sesión fallido con credenciales incorrectas múltiples veces.

🧠 Importante: **No todos los intentos son exitosos**, pero **deben ser monitoreados**, ya que pueden formar parte de una campaña más grande.

2️⃣ ¿Qué son ataques confirmados y documentados?

Un **ataque confirmado** es un evento en el que **se ha comprobado que un atacante logró vulnerar al menos una capa de seguridad**, generando consecuencias reales: acceso no autorizado, fuga de información, cifrado de datos, etc.

📋 "Documentado" significa que el evento ha sido:

- Investigado formalmente por un equipo técnico (SOC, CSIRT).
- Registrado en un informe o base de datos (interna o pública).
- Atribuido y clasificado bajo algún marco como **MITRE ATT&CK**, CVE, o normativas legales.

✅ Requiere **evidencia técnica forense** que respalde la intrusión.

3️⃣¿Qué metodología se sigue para validarlos?

Para diferenciar intentos de ataques de ataques confirmados, se aplica una **metodología de análisis de incidentes**, que incluye:

🛠️ **Fases comunes de validación:**

FASE	ACCIÓN CLAVE
1. DETECCIÓN INICIAL	Alertas de sistemas de seguridad (SIEM, IDS/IPS, antivirus, EDR)
2. CLASIFICACIÓN/TRIAGE	Se evalúa la alerta: ¿falso positivo o actividad anómala real?
3. RECOLECCIÓN DE EVIDENCIAS	Logs, capturas de tráfico, análisis de archivos, snapshots de sistema
4. ANÁLISIS TÉCNICO	Uso de herramientas forenses y frameworks como MITRE ATT&CK para entender el comportamiento
5. CONFIRMACIÓN	Se valida si hubo impacto real (acceso, ejecución, fuga de datos, cifrado, sabotaje, etc.)
6. DOCUMENTACIÓN	Redacción de informe, creación de tickets o reportes para gerencia y respuesta técnica
7. REMEDIACIÓN Y CIERRE	Aislamiento, contención, eliminación del malware, recuperación, lecciones aprendidas

---

📚 **Metodologías o marcos usados:**

- **MITRE ATT&CK**: para mapear tácticas y técnicas del adversario.
- **NIST 800-61**: guía de respuesta a incidentes de seguridad informática.
- **SANS Incident Handling Process**: enfoque en detección, análisis, contención, erradicación y recuperación.
- **ISO/IEC 27035**: estándar internacional de gestión de incidentes de seguridad.

✅ **Ejemplo práctico:**

🔔 **Alerta SIEM:** múltiples intentos fallidos de login desde una IP rusa.
🧪 Se analiza el tráfico ➤ no hubo acceso ➤ **es un intento de ataque**.

Luego, en otro sistema, se detecta acceso con cuenta comprometida y extracción de datos ➤ **ataque confirmado**.

Se documenta, se analiza con MITRE y se emite informe ➤ **ataque documentado y validado**.

Comprendo. Pero lo que se esperaba del informe no era simplemente enlistar cifras brutas, sino **seleccionar ataques relevantes, documentados y con información suficiente para analizarlos**. Esto incluye:

- Una descripción del ataque
- Cómo fue ejecutado
- Cómo se detectó o fue anunciado
- Cuáles fueron sus consecuencias o impactos

Además, hay otras fuentes oficiales como la OEA, el ENISA o el *Verizon DBIR*, que ofrecen **informes anuales con datos desagregados por tipo de ataque, vector inicial, sector afectado, y porcentaje de impacto**. Ustedes pudieron haber contrastado y enriquecido la información de *H-EDU* con estas otras fuentes, para lograr un análisis más sólido y confiable.

El objetivo era comprender los **patrones y tendencias** de ciberataques en 2024, no solo cuantificarlos. Por eso, en su informe también deberían indicar **cuántos de esos ataques fueron publicados, documentados en medios oficiales o especializados**, y qué grado de profundidad informativa tienen.

📊 Panorama General de Ciberataques en 2024

🔷 Tipos de Ataques y Vectores Iniciales

Según diversos informes de ciberseguridad, los vectores de ataque más comunes en 2024 fueron:

- **Explotación de vulnerabilidades**: 33%
- **Robo de credenciales**: 16%
- **Phishing por correo electrónico**: 14%
- **Compromiso web**: 9%
- **Vectores desconocidos**: 34%

En ataques de ransomware, los vectores iniciales más comunes fueron:blog.ehcgroup.io

- **Fuerza bruta (RDP, contraseñas predeterminadas)**: 26%
- **Credenciales robadas**: 21%
- **Explotación de vulnerabilidades**: 21%
- **Compromiso previo**: 15%
- **Compromiso de terceros**: 10%

🔷 Sectores Más Afectados

Los sectores que sufrieron el mayor número de ciberataques en América Latina y el Caribe fueron:global.ptsecurity.com

- **Instituciones gubernamentales**: 21%
- **Organizaciones financieras**: 13%
- **Comercio minorista**: 11%
- **Educación**: 9%

Además, el sector manufacturero fue el más afectado globalmente por ataques de ransomware en el primer trimestre de 2024, representando el 29% de los ataques publicados.Secureframe

🔷 Impacto de los Ataques

Los ciberataques exitosos a organizaciones provocaron con mayor frecuencia:global.ptsecurity.com+1Cadena SER+1

- **Filtraciones de datos**: 53%
- **Interrupciones del negocio**: 35%

Más de la mitad del volumen total de datos robados a las organizaciones consistió en:global.ptsecurity.com

- **Datos personales**: 32%
- **Credenciales de cuentas**: 21%

En el sector sanitario, los ataques de ransomware alcanzaron un récord en 2024, con un aumento en el tiempo de recuperación y un costo medio de recuperación de 2,57 millones de dólares.Cadena SER

📜 Casos Relevantes de Ciberataques en 2024

1️⃣ Generalitat de Cataluña

- **Descripción**: En 2024, la Generalitat de Cataluña enfrentó un total de 6.900 millones de ciberataques, de los cuales 3.372 fueron exitosos y provocaron daños, en su mayoría leves.El País
- **Ejecución**: Los ataques más comunes incluyeron filtraciones de credenciales y ataques de phishing, especialmente a través de SMS.El País
- **Detección**: La mayoría de los ataques exitosos fueron detectados en etapas tempranas, lo que supuso una reducción del 30% en incidentes graves respecto al año anterior.El País

- **Consecuencias**: Las universidades fueron las más afectadas debido al uso de dispositivos personales por parte de estudiantes sin la protección necesaria.El País

2️⃣ Banco do Brasil

- **Descripción**: En marzo de 2024, el Banco do Brasil sufrió un ciberataque significativo que comprometió la seguridad de los datos financieros de los usuarios.
- **Ejecución**: El ataque se centró en empleados del banco, quienes, al ser víctimas de ingeniería social, facilitaron la introducción de scripts maliciosos en los sistemas internos.
- **Detección**: El incidente fue identificado tras observar actividades anómalas en los sistemas internos.
- **Consecuencias**: El ataque resaltó las vulnerabilidades derivadas del error humano y subrayó la necesidad de una capacitación continua del personal en protocolos de ciberseguridad.

3️⃣ Operación Triangulación

- **Descripción**: Descubierta por Kaspersky, esta operación utilizó una cadena de cuatro vulnerabilidades de día cero para espiar dispositivos iOS, afectando a miles de víctimas, incluyendo organizaciones gubernamentales y diplomáticas.
- **Ejecución**: La infección se iniciaba mediante un iMessage especialmente diseñado que, sin interacción del usuario, ejecutaba código malicioso.
- **Detección**: El ataque fue identificado por Kaspersky al analizar comportamientos anómalos en dispositivos iOS.
- **Consecuencias**: El ataque llevó a varias organizaciones gubernamentales a prohibir el uso de dispositivos Apple para fines oficiales debido a preocupaciones de seguridad.

4️⃣ Repsol en España

- **Descripción**: En septiembre de 2024, Repsol sufrió un ciberataque que comprometió datos personales de clientes de electricidad y gas en España.
- **Ejecución**: El acceso no autorizado a los datos fue consecuencia de un incidente con uno de sus proveedores tecnológicos.
- **Detección**: La empresa detectó el acceso no autorizado el 10 de septiembre y notificó a los clientes afectados mediante correo electrónico.
- **Consecuencias**: Los datos comprometidos incluyeron nombres, apellidos, DNI, domicilios y datos de contacto, aunque no se vieron afectados datos financieros ni contraseñas.

5️⃣ Ayuntamiento de Toledo

- **Descripción**: En marzo de 2024, la página web oficial del Ayuntamiento de Toledo fue hackeada por un grupo de activistas rusos, impidiendo el acceso a la web y la sede electrónica del Ayuntamiento.
- **Ejecución**: El ataque consistió en una denegación de servicio que afectó también a otras instituciones y empresas en España.
- **Detección**: El incidente fue detectado a primera hora de la mañana, y los técnicos lograron recuperar parcialmente el servicio antes del mediodía.
- **Consecuencias**: Aunque no se comprometieron datos personales ni se accedió a información sensible, el ataque provocó la interrupción temporal de servicios electrónicos.

📈 Patrones y Tendencias Observadas

- **Aumento de ataques con IA**: Los ciberataques han alcanzado cifras históricas con pérdidas que suman 10.000 millones de euros, doblando las del año anterior. La inteligencia artificial ha jugado un rol crucial al hacer los ataques más precisos y personalizados.El País
- **Incremento de ataques a infraestructuras críticas**: Los 'hackers' se han cebado contra las empresas e infraestructuras críticas, siendo el sector del transporte el más afectado por ataques de ciberseguridad, seguido del financiero, TI y la energía.El País
- **Mayor impacto en el sector sanitario**: Los ataques de ransomware a organizaciones sanitarias han alcanzado un récord en 2024, con un aumento en el tiempo de recuperación y un costo medio de recuperación de 2,57 millones de dólares.Cadena SER

📚 Publicación y Documentación de los Ataques

Los ataques mencionados han sido ampliamente documentados y publicados en medios oficiales y especializados, incluyendo informes de empresas de ciberseguridad como Kaspersky y Sophos, así como en medios de comunicación como El País y Cadena SER.

🧠 PALABRAS CLAVE Y SIGNIFICADOS

TÉRMINO	DEFINICIÓN
RANSOMWARE	Software malicioso que cifra datos y exige un rescate para liberarlos.

PHISHING	Engaño por correo o mensajes para robar credenciales o datos personales.
DOS / DDOS	Ataques de denegación de servicio que saturan un servidor.
APT (AMENAZA PERSISTENTE AVANZADA)	Grupo especializado que ejecuta ataques prolongados, sigilosos y dirigidos.
INSIDER	Persona interna a una organización que facilita un ataque.
VECTOR DE ATAQUE	Método por el cual un atacante accede al sistema o red.
MITIGACIÓN	Acciones para reducir el impacto de un incidente.
EXFILTRACIÓN	Robo y extracción de datos sin autorización.
INGENIERÍA SOCIAL	Técnica de manipulación psicológica para obtener información o acceso.
CVE (COMMON VULNERABILITIES AND EXPOSURES)	Registro de vulnerabilidades públicas.
BACKDOOR	Acceso oculto a un sistema sin que el usuario lo sepa.

🔷 **Principales tipos de ciberataques identificados:**

- **Ransomware:** El más frecuente, afecta a gobiernos, empresas e instituciones educativas; encripta la información y exige rescate.
- **Phishing:** Utiliza técnicas de engaño como correos o mensajes falsos para robar credenciales.
- **DDoS:** Saturación de servicios mediante múltiples solicitudes simultáneas para interrumpir su funcionamiento.
- **Filtración de datos:** Robo de información confidencial, como ocurrió con Interbank y otras entidades.
- **Malware especializado y backdoors:** Utilizados para comprometer infraestructuras críticas, como en el caso de SolarWinds (2020).
- **Ingeniería social:** Empleada para engañar a empleados o proveedores y obtener acceso inicial.

🔷 **Casos destacados:**

1. **Gobierno de Costa Rica (2022):** Ataque con ransomware por el grupo Conti, con un impacto económico de hasta 30 millones de dólares diarios.
2. **Interbank (2024):** Exposición de información de 3.7 millones de clientes. Se filtraron direcciones, DNIs y contraseñas.
3. **National Public Data Leak (2024):** Robo de 3 mil millones de registros públicos mediante ingeniería social.

4. **SolarWinds (2020):** Puerta trasera en software Orion, comprometiendo agencias gubernamentales de EE.UU.

5. **Phishing bancario y aplicaciones espía:** Falsas apps móviles captaban datos sensibles y se desinstalaban automáticamente.

6. **Ataques DDoS a servicios financieros, telecomunicaciones y plataformas de entretenimiento (2020–2024):** Se mitigaron con servicios como Akamai y AWS Shield.

🔷 **Impacto de los ciberataques:**

- **Económico:** Millones de dólares en pérdidas, gastos en recuperación y mejoras en ciberdefensa.
- **Social:** Interrupción de servicios críticos (banca, salud, energía), pérdida de confianza en entidades.
- **Político:** Ciberataques como herramientas de guerra híbrida (ej. conflicto Rusia-Ucrania).
- **Reputacional:** Daño a la imagen institucional y pérdida de alianzas estratégicas.

🔷 **Medidas de mitigación observadas:**

- Fortalecimiento de defensas perimetrales.
- Monitoreo continuo con inteligencia artificial.
- Alianzas internacionales en ciberseguridad.
- Migración a servicios en la nube con protección DDoS.
- Aplicación de parches y segmentación de red.

📘 **Palabras Clave y Significados**

TÉRMINO	DEFINICIÓN
RANSOMWARE	Tipo de malware que encripta archivos y exige un pago (rescate) para liberarlos.
PHISHING	Técnica de ingeniería social que simula mensajes legítimos para robar información confidencial.
DDOS (DENEGACIÓN DE SERVICIO)	Ataque que satura un sistema o red con tráfico excesivo para interrumpir su funcionamiento.
VECTOR DE ATAQUE INICIAL	Punto de entrada que usa un atacante para iniciar la intrusión (ej. phishing, credenciales robadas, vulnerabilidades).
BACKDOOR	Puerta trasera insertada en software o sistemas para acceso no autorizado posterior.
INGENIERÍA SOCIAL	Manipulación psicológica de personas para obtener acceso a sistemas o información.

CIBERDEFENSA PERIMETRAL	Conjunto de herramientas y estrategias que protegen los accesos externos de una red.
MITIGACIÓN	Acciones para contener o reducir el impacto de un ciberataque.
APT (AMENAZA PERSISTENTE AVANZADA)	Ataques sofisticados y prolongados en el tiempo realizados por grupos bien financiados y organizados.
ANÁLISIS FORENSE DIGITAL	Investigación técnica para identificar, contener y reconstruir incidentes de ciberseguridad.

🔷 Principales Tipos de Ataques

Según el análisis de los casos recopilados, se identificaron como vectores de ataque más frecuentes los siguientes:

- **Phishing**: Representó el mayor porcentaje de ataques, especialmente mediante correos electrónicos y plataformas de mensajería.
- **Intrusión remota no autorizada**: Como segundo vector más frecuente, se presentaron casos donde los atacantes lograron vulnerar accesos utilizando exploits o credenciales filtradas.

🔷 Puertos más expuestos

En el análisis técnico, se identificaron como **los puertos más vulnerables y frecuentemente atacados** los siguientes:

1. Puerto 23 – Telnet

- **Servicio**: Telnet (*TELecommunication NETwork*)
- **Función principal**: Permite acceso remoto a un sistema o dispositivo a través de línea de comandos.
- **Protocolo**: TCP
- **Uso típico**: Administración remota de routers, switches, y servidores antiguos.
- ⚠️ **Problema de seguridad**: Transmite todo **en texto plano**, incluidas contraseñas. Hoy está considerado **inseguro** y ha sido reemplazado por **SSH (puerto 22)**.

🔌 **2. Puerto 5555 – Varios usos**

- **Servicio común**: Android Debug Bridge (**ADB**) en modo TCP/IP.
- **Uso principal**: Comunicación remota con dispositivos Android para desarrollo o pruebas.
- **Protocolo**: TCP
- **Otros posibles usos**:
    - Algunos backdoors/malware abren este puerto para acceso remoto.

- Algunos routers o servicios personalizados lo usan como puerto de administración.

- ⚠️ **Riesgo**: Si ADB está habilitado en una red sin seguridad, puede permitir el **control total del dispositivo**.

🔌 **3. Puerto 2323 – Alternativa de Telnet**

- **Servicio**: Telnet alternativo o personalizado
- **Uso**: Algunos dispositivos (especialmente IoT o routers) usan este puerto como **Telnet secundario** para evitar conflictos o como backdoor.
- **Protocolo**: TCP
- **Ejemplo**: Algunos malware como **Mirai** lo usan para explotar dispositivos mal configurados.

Estos puertos fueron comúnmente explotados para lanzar ataques automatizados y tomar control de dispositivos expuestos.

🔷 **Impacto regional: América Latina**

Durante el análisis regional, **Perú** destacó como uno de los países más afectados por ataques de **ingeniería social**, representando el **31.96% del total de ataques de este tipo** en la región. A Perú le siguió **México**, con un 16.44%, y otros países con porcentajes menores.

Este resultado refleja una alarmante vulnerabilidad en el entorno digital peruano, especialmente en contextos donde el teletrabajo y el uso intensivo de tecnologías se incrementó a raíz de la pandemia.

🔷 **Conclusiones Generales**

- El contexto de la **pandemia por COVID-19** expuso a muchas organizaciones a amenazas para las que no estaban preparadas, tanto por falta de infraestructura como por carencias en cultura digital.
- El **phishing** y la **ingeniería social** fueron las técnicas más utilizadas, aprovechándose del desconocimiento y la confianza de los usuarios.
- Grupos avanzados de amenazas persistentes (APT), como **Hydra**, **Cobra** o **Artusa**, fueron responsables de múltiples incidentes, usando tácticas sofisticadas como ataques tipo **DDoS**, malware encubierto, y vulnerabilidades en aplicaciones móviles.

✅ ¿Cómo se interpreta la matriz MITRE ATT&CK en el caso SolarWinds?

La **matriz MITRE ATT&CK** permite identificar y clasificar las **tácticas** y **técnicas** que utilizan los grupos de amenazas persistentes avanzadas (APT) para comprometer un sistema. En el caso de **SolarWinds (2020)**, la matriz fue empleada para describir cada una de las fases del ataque perpetrado por el grupo UNC2452, presuntamente vinculado al APT29 de origen ruso.

- Cada **táctica** representa una etapa en la cadena de ataque: desde el acceso inicial hasta la exfiltración de datos.
- Las **técnicas** detallan cómo se logró esa etapa. Por ejemplo, uso de credenciales comprometidas, ejecución remota, evasión de defensas, persistencia, etc.
- Los **cuadros en azul** dentro de la matriz representan técnicas utilizadas por el grupo UNC2452, pero **no confirmadas al 100%**.
- Los **cuadros en rojo** señalan aquellas **confirmadas por Microsoft** y otras entidades como pasos concretos en el ataque.

Esta matriz sirve como herramienta de análisis forense y también como guía para **mejorar la defensa proactiva** ante amenazas similares.

MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) es un **marco de conocimiento global** que:

- 📌 Documenta **cómo actúan los atacantes en el mundo real**.
- 🔍 Ayuda a **detectar, prevenir y responder** a amenazas cibernéticas.
- 💡 Está basado en incidentes reales y observado por defensores, analistas SOC y red teams

---

🔍 ¿Qué es un ataque a la cadena de suministro?

Un **ataque a la cadena de suministro** ocurre cuando los ciberdelincuentes no atacan directamente a la víctima final (por ejemplo, una institución del gobierno o empresa privada), sino que comprometen a uno de sus **proveedores tecnológicos**.

En el caso de SolarWinds:

- El software **Orion** de SolarWinds era utilizado por múltiples organizaciones del mundo para monitorear redes.
- Los atacantes **inyectaron una puerta trasera (backdoor)** en una actualización oficial del software Orion, la cual fue distribuida automáticamente a los clientes de SolarWinds.

- Como los clientes **confiaban en la legitimidad** de la actualización, esta se instaló sin sospechas, permitiendo a los atacantes ingresar sin levantar alertas.

💡 Este tipo de ataque es **especialmente peligroso**, ya que compromete **decenas o cientos de organizaciones** desde un solo punto vulnerable (el proveedor).

Un **ataque a la cadena de suministro** (*Supply Chain Attack*) es una forma avanzada de ciberataque en la que el objetivo **no es atacar directamente a la víctima final**, sino **comprometer a uno de sus proveedores, socios o terceros** que tienen acceso privilegiado o confianza dentro del ecosistema.

Un ataque a la cadena de suministro es una táctica donde los ciberatacantes comprometen software, hardware, servicios o procesos de terceros para infiltrarse en una organización objetivo.

🔄 ¿Cómo funciona?

El atacante:

1. Identifica una **parte débil** de la cadena (un proveedor de software, un proveedor de servicios, una biblioteca de código, etc.).
2. **Infecta** esa parte (por ejemplo, con malware dentro de una actualización legítima).
3. Cuando el cliente final instala o usa ese producto, el atacante **gana acceso indirecto** al sistema.

💥 Riesgos de usar productos de terceros en ciberseguridad

En los ataques recientes, especialmente los analizados en 2020 como el caso de **SolarWinds** o **FireEye**, los atacantes no atacaron directamente a las instituciones finales (como bancos o gobiernos), sino que **comprometieron productos de terceros** utilizados por esas instituciones.

🔁 ¿Cómo funciona este tipo de ataque?

1. **El atacante compromete el software de un proveedor confiable.**
   - Ejemplo: SolarWinds Orion, FireEye.
2. **Ese software infectado se distribuye normalmente a través de actualizaciones.**
3. **Las organizaciones lo instalan sin sospechar**, ya que confían plenamente en su proveedor.
4. **El atacante obtiene acceso** a las redes de múltiples clientes desde ese punto.

🧠 **Reflexión clave:** El ataque no apunta al proveedor (SolarWinds, FireEye) como víctima principal, sino a sus **clientes finales**.

🧨 ¿Por qué es tan grave?

- **Es masivo**: Una sola brecha en un proveedor puede afectar a **miles de clientes**.
- **Es sigiloso**: Las actualizaciones se instalan automáticamente. No levantan sospechas.
- **Es costoso**: Afecta infraestructuras críticas, bancos, instituciones estatales y privadas.

🔍 Ejemplo práctico explicado

"Es como si confiáramos en nuestro antivirus, y un día esa actualización trae un virus oculto. En vez de protegernos, se convierte en la **puerta de entrada del ataque**."

Lo mismo ocurrió con **FireEye**, una empresa dedicada a seguridad informática. Su producto fue usado para atacar a sus propios clientes del sector financiero y estatal en EE.UU.

📊 Duda frecuente: ¿Son todos los ataques detectados, ataques confirmados?

No necesariamente. En los reportes:

- **"Detecciones" ≠ "ataques exitosos"**.
- Muchos son **intentos bloqueados**, no intrusiones confirmadas.
- Ejemplo: En el caso del *phishing*, puede haber miles de correos maliciosos enviados, pero solo un porcentaje logra que un usuario haga clic y comprometa su sistema.

📌 Por eso, al analizar tablas o anexos con cifras, se debe aclarar si son:

- **Intentos**
- **Amenazas detectadas**
- **Ataques confirmados (exitosos)**

🟡 **Ataque detectado**	🟢 **Ataque confirmado**
Es una alerta o indicio generado por herramientas de seguridad (SIEM, antivirus, IDS, etc.).	Es un evento que ha sido **verificado técnicamente** como real.
Puede incluir falsos positivos (actividad legítima mal interpretada).	Tiene **evidencia concreta** de que hubo una acción maliciosa exitosa.

Requiere análisis posterior para confirmar si es real.	Ya ha pasado por análisis, validación y documentación.
Ejemplo: intento de login sospechoso desde una IP rara.	Ejemplo: acceso real a datos sensibles por un actor no autorizado.

📘 PALABRAS CLAVE Y SIGNIFICADOS

Término	*Significado*
Ransomware	Tipo de malware que encripta datos y exige rescate económico para liberarlos.
Phishing	Técnica de ingeniería social que engaña al usuario para obtener credenciales o datos sensibles.
DDoS	Ataque que sobrecarga un servidor mediante múltiples solicitudes simultáneas, inutilizando el servicio.
Cadena de suministro	Conjunto de proveedores de software/servicios usados por una organización. Se vuelve un blanco indirecto en ataques cibernéticos.
APT (Amenaza Persistente Avanzada)	Grupos altamente organizados que realizan ciberataques dirigidos a largo plazo, con sofisticación y evasión.
MITRE ATT&CK	Marco que describe tácticas y técnicas usadas por atacantes en fases de un ciberataque.
Acceso inicial	Primer punto de entrada que usa un atacante (ej: phishing, vulnerabilidad no parchada).
Movimiento lateral	Técnica usada por atacantes para moverse entre sistemas dentro de una red comprometida.
CVE	Identificador único para una vulnerabilidad conocida (Common Vulnerabilities and Exposures).
Exfiltración	Robo y extracción de datos de forma encubierta.
Impacto reputacional	Daño a la imagen de una entidad tras un ciberataque, afectando confianza pública o relaciones comerciales.
Zero-Day	Vulnerabilidad explotada antes de ser descubierta o parchada oficialmente.

🧠 Informe mejorado: Incidentes de ciberseguridad vinculados a dispositivos Apple y entorno corporativo Myrne (2023)

📌 Descubrimiento sobre malware en dispositivos Apple

El investigador **Patrick Wardle**, presidente de la organización especializada en seguridad de dispositivos, reportó en 2023 la detección de **21 nuevas familias de malware dirigidas a sistemas macOS**, lo que representa un aumento de más del 50% respecto al año 2022.

Este crecimiento evidencia el **creciente interés de los ciberatacantes por vulnerar sistemas Apple**, especialmente por el auge de dispositivos como los **smartwatches** y el uso extendido de **Macs en entornos corporativos y hospitalarios**.

🔎 **Principales amenazas identificadas:**

- **Tipo de malware más común**: *Infostealers*, cuyo objetivo es robar contraseñas, cookies, información financiera y credenciales.
- **Malware específicos detectados**: *Atomic Stealer*, *BlackTail*, *Pollen Rebel*, *MetaStealer*, *MacStealer*, entre otros.
- **Grupos APT activos (Amenazas Persistentes Avanzadas)**: Se registró una actividad significativa de grupos APT vinculados a Corea del Norte. Algunos de los malware utilizados incluyen *Reindeer*, *RustBucket* y *CloudMensis*.
- **Otras amenazas relevantes**: *Spectra* (instala puertas traseras mediante plataformas legítimas), *DazzleSpy* (aprovecha vulnerabilidades en macOS), y otros desarrollos altamente sofisticados que apuntan a vulnerabilidades en Word y navegadores web.

Este escenario confirma que **el ecosistema macOS ya no es inmune a los ciberataques**, y que incluso grupos APT han comenzado a **diversificar sus herramientas para vulnerar estos entornos**. Se recomienda a usuarios y organizaciones mantener sistemas actualizados, aplicar protección avanzada, y monitorear constantemente el comportamiento de los dispositivos.

🧩 **Caso 2: Ataque informático al entorno corporativo de MITRE Corporation**

Organización afectada: *MITRE Corporation*, una entidad sin fines de lucro que colabora con agencias gubernamentales de EE.UU. en investigación, ciberseguridad y desarrollo tecnológico (como el proyecto *ATT&CK*).

🗓️ **Detalles del incidente:**

- **Fecha de inicio**: 31 de diciembre de 2023.
- **Método de ataque**: Aprovechamiento de una vulnerabilidad *zero-day* en dispositivos de red conectados a su entorno de experimentación.
- **Acceso inicial**: Se obtuvo mediante credenciales comprometidas y el uso de una vulnerabilidad crítica.
- **Herramientas utilizadas**: Se implementó malware personalizado, como *BEELINE* y *Bvp47*, para la persistencia y el movimiento lateral dentro de la red.

🔥 **Impacto:**

- El ataque comprometió la red de pruebas utilizada por MITRE para simulaciones de ciberseguridad, aunque **no se reportó robo de datos sensibles**.
- A pesar de las medidas de mitigación implementadas, **el ataque logró permanecer sin ser detectado por varias semanas** entre febrero y marzo de 2024.

- Se atribuye el ataque al **grupo APT29**, también conocido como *Cozy Bear*, vinculado al gobierno ruso, según el informe técnico publicado por **Palo Alto Networks**.

⚠️ **Riesgo global:**

El incidente puso en evidencia la **vulnerabilidad incluso de instituciones altamente protegidas**, lo cual alertó a agencias como **CISA** (Cybersecurity and Infrastructure Security Agency) sobre la necesidad de reforzar medidas ante futuras amenazas en infraestructuras críticas.

🔐 Incidentes de Ciberseguridad – Grupo Setem / STONE9950 y Ataques a Infraestructura Crítica (2023)

🛡️ Incidente 3: Ataque masivo liderado por el grupo Setem (también conocido como STONE9950)

Este ciberataque fue ejecutado por el **grupo Setem**, también identificado en campañas previas bajo los nombres *Anterior* y *GotAnyway*. En otros reportes de inteligencia, también ha sido catalogado como **Storm-9950**, y clasificado como parte del grupo de amenazas persistentes avanzadas (APT) conocido como *Spawn Servement 0150*.

📌 **Modus operandi del grupo atacante:**

- Explotación de **vulnerabilidades de día cero** en software ampliamente utilizado.
- Robo masivo de datos confidenciales.
- Extorsión a las víctimas: exigencia de pagos económicos a cambio de no divulgar la información robada.

📉 **Impacto y consecuencias:**

- Aunque aún no se ha determinado con precisión el volumen total de datos comprometidos, **se estima que más de 2,600 organizaciones y más de 3 millones de personas fueron afectadas**.
- Se reportaron **pérdidas económicas considerables**, así como un daño reputacional severo para las instituciones comprometidas.
- Actualmente se mantienen **investigaciones activas en múltiples países** para esclarecer el origen exacto y alcance del ataque.

⚠️ Incidente 4: Ataque a infraestructura crítica en los Países Bajos (abril - mayo 2023)

El cuarto caso relevante corresponde a un **ataque dirigido contra una planta energética holandesa**, en un contexto de alta dependencia tecnológica por las condiciones climáticas invernales de la región.

💥 Detalles del ataque:

- **Fecha del primer ataque**: 25 de abril de 2023.
- **Vulnerabilidad explotada**: Una falla crítica identificada como **CVE-2023-287**, presente en el firewall empresarial **SonicWall**.
- **Tipo de acceso**: El exploit permitía **control remoto no autenticado** de los dispositivos afectados.
- **Canal comprometido**: Utilización del **puerto UDP 500**, explotando debilidades en el protocolo de seguridad **IPsec/IKE (Internet Key Exchange)**.

🛠️ Métodos y ejecución:

- Los atacantes realizaron escaneos de red que les permitieron detectar dispositivos vulnerables y recopilar información filtrada de **más de 1,000 proveedores**.
- Se obtuvieron credenciales internas y configuraciones mediante técnicas de *brute force* y explotación de software de control operativo (OT).
- **Segundo ataque**: Registrado el **22 de mayo de 2023**, utilizando la misma vulnerabilidad no parcheada.
- Los atacantes accedieron a la **red SCADA** de la planta, reconfigurando usuarios y sistemas desde dentro.

🔍 Consecuencias:

- Comprometieron sistemas clave que controlaban la **distribución energética nacional**.
- El uso de **herramientas privadas** y redes internas permitió escalar el ataque y **poner en riesgo el suministro eléctrico nacional**.

🛡️ Incidente 5: Nuevas vulnerabilidades críticas en dispositivos de seguridad CISA – Dinamarca y Norteamérica (2023)

El **descubrimiento final** se realizó el **24 de mayo de 2023**, cuando la empresa **CISA** reveló **dos vulnerabilidades críticas** en sus modelos de dispositivos de seguridad:

- **CVE-2023-3309**
- **CVE-2023-3310**

Estas fallas permitían la explotación remota de dispositivos **a través de puertos físicos y redes expuestas**, sin necesidad de autenticación previa. Esto implicaba que **diversos proveedores** —incluidas cámaras de vigilancia y dispositivos conectados— podían ser vulnerados sin conocimiento de las organizaciones que los utilizaban.

📍 **Contexto geográfico:**

- Afectó principalmente a empresas e infraestructuras de **Canadá**, **Estados Unidos** y **Hong Kong**.
- El incidente fue reportado inicialmente el **25 de abril de 2023**, pero **la exposición completa** y el alcance real de las vulnerabilidades no se conocieron hasta mayo.

💣 **Impacto técnico:**

- Se comprometieron **sistemas de control industrial** en **22 organizaciones** de alto perfil.
- **11 de estas infraestructuras** fueron desconectadas de emergencia como medida preventiva.
- A pesar de la gravedad, **no se interrumpió el suministro eléctrico**, gracias a una **respuesta inmediata** de los equipos de ciberseguridad.

🛠️ **Respuesta y mitigación:**

- Implementación urgente de **parches de seguridad** y **auditorías técnicas completas**.
- Coordinación efectiva con proveedores tecnológicos para el **refuerzo de la defensa perimetral**.
- Esta respuesta fue considerada ejemplar por medios internacionales, que titularon:

"Dinamarca enfrenta su mayor incidente de ciberseguridad industrial hasta la fecha."

🦹 **Incidente 6: Infiltración en T-Mobile – Estados Unidos (febrero a mayo 2023)**

Entre el **24 de febrero y el 30 de mayo de 2023**, **T-Mobile USA** fue víctima de un ciberataque que permitió accesos **no autorizados a sus servidores**. El atacante logró evadir los controles internos del sistema de autenticación y obtener información sensible de millones de clientes.

📂 **Datos comprometidos:**

- Nombres completos
- Direcciones físicas
- Correos electrónicos
- Números de seguridad social

- Información financiera parcial

⚠️ **Método de ataque:**

- **Exfiltración silenciosa de datos** mediante técnicas de evasión avanzadas.
- Se sospecha que el punto de entrada fue una **API mal configurada**, lo que permitió a los atacantes acceder sin detección durante semanas.

📉 **Consecuencias:**

- Se estima una pérdida de **confianza significativa** por parte de los usuarios.
- T-Mobile enfrenta **varias investigaciones federales** y demandas colectivas en Estados Unidos.
- Se cuestionó la robustez de sus sistemas de ciberseguridad, especialmente en la sede de **Hong Kong**, que también fue comprometida.

Estos casos demuestran que, aunque muchas organizaciones tienen protocolos establecidos, **las vulnerabilidades en hardware y software de terceros siguen siendo el eslabón más débil**. Asimismo, recalcan la importancia de:

- Mantener **sistemas actualizados**
- Realizar **auditorías periódicas**
- Implementar **estrategias de detección temprana** y respuesta rápida

🔍 ¿Qué es una vulnerabilidad de día cero (zero-day vulnerability)?

Una **vulnerabilidad de día cero** se refiere a una falla de seguridad en un sistema, software o aplicación que **aún no ha sido descubierta ni por el fabricante ni por los desarrolladores responsables**. Dado que **no existe parche o solución disponible en el momento en que se detecta o explota**, se considera especialmente peligrosa.

🔶 **"Día cero"** alude al hecho de que los responsables de la seguridad tienen *cero días* para resolver el problema desde que se hace público o comienza a ser explotado.

Una **vulnerabilidad de día cero (zero-day vulnerability)** es una **falla de seguridad desconocida por el proveedor del software o hardware** al momento en que es descubierta por un atacante. Una **vulnerabilidad de día cero** es una debilidad en un sistema, aplicación o componente que aún **no ha sido parcheada ni publicada** oficialmente por el fabricante, y por tanto **no hay defensa conocida** contra ella en ese momento.

🕓 ¿Por qué se llama “día cero”?

- Porque el desarrollador tiene exactamente **“cero días” de conocimiento** y **cero días de ventaja** para solucionarla desde que se hace pública o comienza a explotarse.
- El ataque que explota esta vulnerabilidad se llama **“exploit de día cero” (zero-day exploit)**.

💥 ¿Por qué es tan crítica?

Porque los atacantes —como ciberdelincuentes o grupos APT (amenazas persistentes avanzadas)— pueden **aprovechar esa vulnerabilidad sin que nadie lo sepa**, logrando:

- Acceso no autorizado a sistemas
- Robo de información sensible
- Instalación de malware sin ser detectados
- Daño a la infraestructura antes de que siquiera se reconozca el fallo

🧠 Ejemplo real:

Uno de los casos más conocidos es el exploit **EternalBlue**, una vulnerabilidad de día cero en el protocolo SMB (Server Message Block, puerto 445 de Windows), que fue utilizada por el ransomware **WannaCry**. Antes de que Microsoft pudiera lanzar un parche, cientos de miles de equipos en todo el mundo ya habían sido afectados.

Otro caso se relaciona con software de Adobe que fue aprovechado por atacantes para espiar a través de vulnerabilidades desconocidas en ese momento.

🎯 Aclaración importante:

Cuando un informe menciona "vulnerabilidad día cero", **no se refiere a que los atacantes ya tuvieran acceso desde el primer día** por tener credenciales previas. Más bien, **se trata de una brecha técnica que el fabricante ni siquiera sabía que existía**, y por lo tanto, no se ha corregido.

🧠 Pregunta técnica: ¿Qué servicio se ejecuta comúnmente en el puerto UDP 500?

El **puerto UDP 500** es utilizado principalmente por el protocolo **IKE (Internet Key Exchange)**, que forma parte del protocolo de seguridad **IPsec (Internet Protocol Security)**. Este protocolo es fundamental para el establecimiento de **VPNs (Virtual Private Networks)**, ya que permite el intercambio de claves y la negociación segura de los parámetros criptográficos entre dos puntos.

🔷 **Uso común**: configuraciones de VPN corporativas y dispositivos de red como firewalls, routers o appliances de seguridad.

El **puerto UDP 500** se utiliza **comúnmente por el protocolo IKE (Internet Key Exchange)**, que es parte esencial del establecimiento de **VPNs basadas en IPsec**.

📌 **Detalles técnicos:**

Parámetro	Valor
🧠 **Protocolo**	IKE (Internet Key Exchange), versiones IKEv1 e IKEv2
🔒 **Uso**	Intercambio seguro de claves y establecimiento de túneles VPN
📦 **Transporte**	UDP
🌐 **Puerto**	**UDP 500**

🔧 **¿Para qué se usa IKE en UDP 500?**

- Para negociar y establecer **canales cifrados seguros entre dos puntos**.
- Se usa en protocolos como:
    - **IPsec VPNs**
    - **Site-to-Site VPN**
    - **Remote Access VPN**

⚠️ **Consideraciones de seguridad:**

- Este puerto es **frecuente objetivo de escaneo** por parte de atacantes que buscan vulnerabilidades en servicios de VPN mal configurados.
- Las versiones antiguas de IKE (como IKEv1) tienen **vulnerabilidades conocidas** (ej. ataques de fuerza bruta y DoS).

🛡️ **Caso mencionado: Explotación de vulnerabilidades en dispositivos CISA**

El ataque mencionado en el informe aprovechó precisamente una vulnerabilidad crítica en **dispositivos de seguridad que ejecutaban servicios VPN**. Al no requerirse autenticación para acceder por el puerto UDP 500, los atacantes lograron el **acceso no autorizado al sistema**, controlando dispositivos industriales sin que los administradores lo detectaran a tiempo.

🔐 ¿Qué tipo de persistencia se utilizó en los ataques analizados?

La **persistencia** en ciberseguridad se refiere a los métodos utilizados por un atacante para **mantener el acceso a un sistema comprometido**, incluso después de reinicios o intentos de eliminación. En los casos presentados, los mecanismos de persistencia identificados o inferidos incluyen:

- ✅ **Uso de credenciales comprometidas**: permitió mantener acceso prolongado a redes internas.
- ✅ **Malware personalizado**: algunos ataques implantaron software malicioso diseñado para ejecutarse automáticamente al iniciar el sistema o a través de tareas programadas.
- ✅ **Backdoors** (puertas traseras): creadas dentro de software de terceros (caso típico de cadena de suministro), permitieron a los atacantes reingresar al sistema sin levantar sospechas.
- ✅ **Modificaciones de configuraciones internas**: en los sistemas industriales atacados, se identificó la creación de usuarios falsos o cambios en políticas de red que facilitaron la permanencia dentro del entorno comprometido.

🔐 **Persistencia** es una fase crítica en los ciberataques, donde el atacante busca **mantener el acceso al sistema comprometido**, incluso después de reinicios o cambios. En los ataques analizados en 2024, se identificaron varios **métodos de persistencia** usados, según el tipo de ataque y objetivo.

📝 Conclusión para futuras presentaciones o informes

Cuando se mencionen términos técnicos como **vulnerabilidad de día cero, puerto UDP 500, IKE/IPsec, o persistencia**, es clave que:

1. Se incluya una **explicación sencilla y técnica a la vez**.
2. Se especifique el **impacto real** (por ejemplo, qué permitió esa persistencia).
3. Se respalde con una **referencia clara y directa** (no solo la web principal, sino la URL del informe o publicación técnica específica).

📌 ¿Cuál ha sido el vector inicial de acceso más comúnmente utilizado en este año?

Durante este año, el **vector de ataque más frecuente** ha sido el **uso de credenciales comprometidas**, es decir, contraseñas filtradas o robadas, generalmente obtenidas a través de técnicas de **phishing**, ingeniería social o bases de datos expuestas en la dark web.

Esto se evidenció en varios casos analizados en el informe. A continuación se detallan los principales:

🛑 Caso 1 – Infraestructura crítica en Dinamarca

- **Vector inicial**: *Credenciales comprometidas*.
- **Acceso**: A través del puerto UDP 500 (IPSec VPN), sin requerir autenticación en ciertos modelos de firewall.
- **Resultado**: Los atacantes lograron acceso directo a la red industrial sin levantar sospechas iniciales.

🛑 Caso 2 – Corporación MITRE

- **Vector inicial**: *Vulnerabilidad de día cero (Zero-Day)*.
- **Método**: Explotación de software sin parche disponible.
- **Resultado**: Acceso persistente y silencioso a sistemas de alto valor en investigación.

🛑 Caso 3 – Grupo Stone9950

- **Vector inicial**: *Campañas de phishing y explotación de vulnerabilidades*.
- **Método**: Ingreso mediante técnicas mixtas, incluyendo descarga de malware personalizado.
- **Resultado**: Más de 2,600 organizaciones afectadas y robo masivo de datos.

🛑 Caso 4 – Ataque a usuarios de Apple (macOS)

- **Vector inicial**: *Ingeniería social y aplicaciones maliciosas*.
- **Método**: Instalación de software espía que aparentaba ser legítimo.
- **Resultado**: Robo de contraseñas, cookies, tokens y accesos remotos no autorizados.

🔎 Conclusión:

La **ingeniería social** sigue siendo el punto de entrada más explotado por los atacantes, aprovechando que la parte más vulnerable de cualquier sistema sigue siendo **el usuario**. En varios de los casos, incluso cuando se utilizaron técnicas avanzadas como vulnerabilidades de día cero o

malware personalizado, el ataque comenzaba muchas veces con un engaño al usuario o una credencial comprometida.

Caso 1: Ciberataque a la aseguradora CNA Financial (Estados Unidos)

En marzo de 2021, la aseguradora CNA Financial, una de las más grandes de Estados Unidos, sufrió un sofisticado ataque de ransomware que afectó gravemente su infraestructura tecnológica. El ataque ocurrió el 21 de marzo y fue atribuido al grupo de ransomware vinculado a la organización rusa de hackers Evil Corp. Se utilizó una nueva variante llamada *Phoenix CryptoLocker*, derivada del ransomware *Hades*.

Los atacantes lograron acceder a la red de CNA a través de una explotación de vulnerabilidades, cifrando más de 15,000 dispositivos, incluyendo equipos de empleados en trabajo remoto. Como resultado, CNA tuvo que suspender temporalmente sus operaciones. Originalmente, los atacantes exigieron USD 60 millones, pero tras negociaciones, se pagó un rescate de USD 40 millones para recuperar el acceso a los sistemas.

La empresa no anunció inicialmente el incidente. Fue el medio *BleepingComputer* quien reportó la caída de los servicios online. Posteriormente, *ComputerWeekly* confirmó el ataque. CNA implementó medidas de mitigación como el aislamiento de sistemas comprometidos, implementación de herramientas forenses avanzadas, y refuerzo de la seguridad en sus redes.

Caso 2: Ataque a Colonial Pipeline (Estados Unidos)

El 7 de mayo de 2021, Colonial Pipeline, la empresa responsable de distribuir el 45% del combustible en la costa este de Estados Unidos, fue víctima de un ataque de ransomware que obligó al cierre total de sus operaciones. El ataque fue atribuido al grupo *DarkSide*, quienes demandaron un rescate a cambio del restablecimiento de los sistemas.

Colonial Pipeline pagó aproximadamente USD 4.4 millones en bitcoins para recuperar el control de sus sistemas. Este ataque tuvo un impacto masivo, afectando el suministro energético, provocando escasez de combustible, alzas de precios y generando alarma nacional.

La respuesta incluyó la colaboración del FBI y agencias de seguridad cibernética, así como la implementación de medidas de recuperación para restablecer la operación de los sistemas. Este caso marcó un punto de inflexión sobre la vulnerabilidad de las infraestructuras críticas frente a ciberataques.

Caso 2: Ciberataque a Colonial Pipeline (Estados Unidos)

El 7 de mayo de 2021, la empresa **Colonial Pipeline**, encargada del 45% del suministro de combustible en la costa este de Estados Unidos, fue víctima de un ciberataque con **ransomware**

atribuido al grupo criminal **DarkSide**. Este incidente forzó el cierre completo de sus operaciones durante varios días.

¿Cómo se realizó el ataque?

El acceso inicial se produjo a través de una **VPN comprometida** perteneciente a un empleado de la compañía. A través de esta puerta de entrada, los atacantes accedieron a la red interna e instalaron el ransomware, cifrando sistemas críticos.

DarkSide operaba bajo un modelo de *Ransomware-as-a-Service (RaaS)*, en el que desarrolladores proveen herramientas de ataque a afiliados a cambio de una parte del rescate. La empresa pagó **4.4 millones de dólares en bitcoins**, aunque el **FBI logró recuperar aproximadamente 2.3 millones**, gracias a la trazabilidad del monedero digital utilizado.

Impacto

- Suspensión de todas las operaciones logísticas.
- Desabastecimiento de combustibles en múltiples estados.
- Aumento de precios en las estaciones de servicio.
- Afectación de la infraestructura energética crítica.

Colonial Pipeline reconoció el ataque días después del incidente, y el caso fue confirmado y seguido por el FBI. La imagen pública de la empresa se vio fuertemente afectada, y se evidenció la fragilidad de infraestructuras esenciales frente a ciberamenazas.

Caso 3: Ataque al proveedor Kaseya – Fin de semana del 4 de julio (2021)

El **2 de julio de 2021**, el grupo **REvil** lanzó un ataque de ransomware aprovechando una vulnerabilidad de **día cero** en los sistemas de **Kaseya**, una empresa de software de gestión de infraestructura IT utilizada por proveedores de servicios administrados (MSP).

Detalles del ataque:

Se explotaron tres vulnerabilidades:

1. **Bypass de autenticación** que permitía acceso sin credenciales válidas.
2. **Ejecución remota de código (RCE)** mediante la interfaz web.
3. **Carga de archivos maliciosos**, lo que facilitó la instalación del ransomware.

El ataque afectó directamente a **60 MSPs**, quienes a su vez brindaban servicios a más de **1500 clientes**. Uno de los casos más conocidos fue el de la cadena de supermercados **Coop (Suecia)**, que tuvo que cerrar temporalmente más de **800 tiendas** debido a la caída de sus sistemas de punto de venta.

El grupo REvil exigió un **rescate de 70 millones de dólares en bitcoins** para liberar la clave maestra de descifrado. La empresa Kaseya, días después, lanzó un parche de seguridad y anunció que habían obtenido una herramienta universal de descifrado, aunque no se aclaró si se pagó el rescate.

Consecuencias:

- Paralización temporal de miles de empresas a nivel global.
- Pérdidas económicas significativas para sectores como retail, logística y servicios TI.
- Reputación comprometida de Kaseya y de sus clientes.

Análisis Final y Tipología de Ataques Informáticos en 2021

Durante el año 2021, los **ataques de tipo ransomware** fueron los más frecuentes y dañinos, como lo evidencian tres de los seis casos analizados: el ataque a la aseguradora **CNA Financial**, el caso del proveedor **Kaseya**, y el incidente crítico con **Colonial Pipeline**. Todos estos comparten características comunes:

- Infiltración mediante vulnerabilidades o accesos no autorizados.
- Cifrado de información clave para exigir rescates millonarios.
- Interrupción grave de operaciones esenciales.

El caso de **Colonial Pipeline** fue especialmente emblemático, ya que generó el pago de **4.4 millones de dólares** en rescate y una crisis de abastecimiento de combustible en varios estados de EE. UU., destacándose como el incidente con mayor impacto económico y mediático del año.

En cuanto a la **explotación de vulnerabilidades**, los ataques patrocinados por actores estatales (por ejemplo, los atribuidos a **grupos iraníes** según informes conjuntos del Reino Unido, Estados Unidos, Australia y la CISA) utilizaron vulnerabilidades de **día cero** en plataformas como **Microsoft Exchange** y sistemas de **Fortinet**, representando una amenaza persistente para múltiples sectores estratégicos.

Respecto a **fugas de datos**, el caso de **Twitch (propiedad de Amazon)** es uno de los más relevantes, ya que se filtraron datos sensibles de creadores de contenido, así como partes del código fuente del servicio, revelando fallas en la protección de datos y control interno.

Sobre los **ataques a la identidad**, se presentó un caso en el que se suplantó al **FBI** mediante el uso de servidores legítimos vulnerados, desde los cuales se enviaron correos falsos en campañas avanzadas de **phishing**.

Finalmente, en lo referente a **infraestructura crítica**, casos como el ataque al **oleoducto Colonial Pipeline** y otros dirigidos al sector salud (como el ataque a un hospital infantil) dejaron en

evidencia que los ciberataques hoy pueden poner en riesgo no solo datos, sino **servicios vitales para la sociedad**.

Conclusión General

Se reportaron y analizaron **seis incidentes clave** del año 2021, seleccionados por su alto impacto, cobertura mediática y valor analítico. Aunque existen muchos más eventos documentados, se priorizaron los más significativos para efectos del informe.

Según datos del año 2021:

- En **América Latina**, el 29% de los ciberataques correspondieron a **ransomware cifrado**.
- El **bloqueo de servicios esenciales** fue una de las consecuencias más comunes.
- El vector inicial más utilizado fue la **comprometida interacción humana**, mediante técnicas como **phishing**, seguido por **explotación de vulnerabilidades no parchadas**.

Este análisis demuestra la urgente necesidad de adoptar **medidas preventivas, formación continua** y **parches de seguridad oportunos** en todos los niveles organizacionales.

Justificación del enfoque y resumen del análisis

Nuestro informe se centró deliberadamente en **seis casos emblemáticos** de ciberataques ocurridos en el año 2021. Sabemos que existen **cientos de incidentes documentados** a lo largo del año; sin embargo, el objetivo de este trabajo no fue listar la totalidad, sino **comprender en profundidad el funcionamiento de los ataques más representativos** en sus diversas etapas: acceso inicial, persistencia, impacto y mitigación.

Al ser un grupo de tres integrantes, optamos por realizar una **investigación concentrada**, que permitiera no solo narrar hechos, sino **entender técnicamente cómo operaron estos ciberataques**, quiénes fueron los actores involucrados, y qué vulnerabilidades fueron aprovechadas. Esta decisión buscó aportar calidad analítica antes que cantidad superficial.

Sabemos que otros equipos presentaron tablas con decenas de registros. En nuestro caso, **sí se consultaron múltiples fuentes** que reportaban más de 50 o 60 ataques, pero se priorizó seleccionar seis **confirmados, documentados y con impacto relevante**, lo cual permite realizar un estudio más detallado y didáctico.

Vectores de acceso inicial detectados

Aunque los seis ataques finalmente se concretaron mediante ransomware o exfiltración de datos, **los métodos de acceso inicial fueron variados**, entre ellos:

- **Explotación de vulnerabilidades de día cero**, como en el caso de *Kaseya*.
- **Acceso remoto mediante VPN comprometida**, como ocurrió en *Colonial Pipeline*.

- **Uso de credenciales filtradas o débiles**, presumiblemente en el caso de *CNA Financial*.
- **Suplantación de identidad (phishing avanzado)**, en el caso vinculado al dominio del *FBI*.

Cada caso permitió observar **cómo una brecha pequeña en seguridad puede convertirse en un incidente de gran magnitud** si no se detecta y mitiga a tiempo.

Orígenes atribuidos de los grupos atacantes

En los seis casos analizados, los actores detrás de los ataques fueron **grupos APT (Amenazas Persistentes Avanzadas)**, patrocinados o relacionados con gobiernos o redes delictivas internacionales. A continuación, los orígenes más frecuentes:

- **Rusia**: grupos como *REvil*, *DarkSide* y *Evil Corp* estuvieron implicados en al menos tres de los seis casos.
- **Irán**: vinculado a ataques patrocinados por el Estado según informes de agencias de EE. UU., Reino Unido y Australia.
- **Interno (colateral)**: en el caso del uso indebido de servidores del FBI, se sospecha de un uso interno malicioso con fines de manipulación pública.

Conclusión general

Los ataques del año 2021 analizados muestran que las organizaciones continúan siendo vulnerables a:

- **Errores humanos** (como el uso de VPN sin MFA).
- **Falta de parches de seguridad actualizados**.
- **Vulnerabilidades de día cero** que fueron explotadas antes de ser corregidas.

Nuestro informe, aunque limitado en cantidad de casos, busca **profundizar y explicar con claridad cómo ocurre un ciberataque desde su inicio hasta sus consecuencias**, fomentando el análisis y la prevención en entornos reales.

---

4. ¿Qué es una vulnerabilidad de día cero?

- **Respuesta:** Es una vulnerabilidad que aún no ha sido descubierta ni parchada por el fabricante, por lo que los atacantes pueden explotarla sin que exista una solución disponible.

---

5. ¿Qué servicio se ejecuta en el puerto UDP 500, mencionado en el caso de Dinamarca?

- **Respuesta:** Ese puerto se utiliza comúnmente para servicios de VPN (IPSec), por lo que los atacantes explotaron vulnerabilidades en servicios VPN expuestos para obtener acceso.

---

6. ¿Cuál fue el tipo de acceso inicial más común en los casos analizados?

- **Respuesta:** Variaron, pero los principales vectores iniciales fueron:
  - Explotación de día cero (Kaseya).
  - VPN vulnerada (Colonial Pipeline).
  - Credenciales filtradas o débiles (CNA Financial).
  - Suplantación de identidad (FBI spoofing).

---

7. ¿Cuál fue el tipo de ataque más frecuente?

- **Respuesta:** El **ransomware** fue el tipo de ataque más común en los casos estudiados, seguido por explotación de vulnerabilidades y fuga de datos.

---

8. ¿Se mencionó el país de origen de los grupos atacantes?

- **Respuesta:** Sí. Los grupos identificados estaban vinculados principalmente a:
  - **Rusia** (REvil, DarkSide, EvilCorp).
  - **Irán** (APT patrocinado por el Estado).
  - En algunos casos, origen colateral o desconocido (caso FBI).

---

9. ¿Qué mecanismos de persistencia usaron los atacantes?

- **Respuesta:** En general, persistían mediante:
  - Instalación de backdoors (puertas traseras).
  - Uso de credenciales robadas.
  - Mantenimiento de acceso vía VPN o malware personalizado.

---

10. ¿Por qué no se detalló el acceso inicial en algunos casos como CNA?

- **Respuesta:** La empresa afectada evitó publicar detalles específicos debido a razones legales y de confidencialidad (por ejemplo, por las sanciones al pagar rescates a grupos considerados como terroristas).