UNIVERSIDAD ADOLFO IBÁÑEZ

Semana 1

TICS413: SEGURIDAD TI

ADMINISTRATIVO

PROFESORES:

JAIME GÓMEZ (COORDINADOR)

NICOLAS CENZANO

ROMINA TORRES – NIVELACIÓN REDES: DANILO BORQUEZ

ROMINA TORRES

- Doctor en Ingeniería Informática (+ Magister en Ciencias de la Ingeniería Informática + Ingeniero Civil Informático)
- Profesor Asociado - FIC UAI Informática y Ciencia de datos - Líneas: Salud, ciberseguridad
- Director de intrusion.aware – FONDEF TI – ANID – 2024-2026
- Colaborador línea 5 Inteligencia Artificial Responsable de Centro Nacional de Inteligencia Artificial (CENIA) – Investigador Titular Data Observatory
- Arquitecto de Software (*secure by default and by design*)
- Co-fundadora de Mujeres en IA https://www.mujeresia.cl
- Co-director de Consorcio latinoamericano de seguridad en la investigación
- Local chair de https://icprs.org

RESULTADOS DE APRENDIZAJE

Al final del curso, el estudiante deberá ser capaz de:

- • [RA1] Comprender conceptos básicos de Seguridad de la Información en escenarios prácticos y casos empresariales..
- • [RA2] Distinguir vulnerabilidades y riesgos en el tratamiento de información, y controles de seguridad apropiados.
- • [RA3] Identificar herramientas que permitan controlar riesgos de seguridad de la información.
- • [RA4] Proponer soluciones ante situaciones y riesgos que atenten contra la confidencialidad, integridad y disponibilidad de la información empresarial , considerando aspectos éticos y legales.

EVALUACIÓN DEL CURSO

- La evaluación del curso se basa en tres notas evaluados con promedio simple:
- **NF = (T1 + T2 + T3) / 3**
- Donde se tiene una nota por unidad temática (TX) la cual se calcula como: **TX = 0.8 × PruebaX + 0.2 × CTFX**
- **Nota:** Las pruebas se realizan de forma simultánea para todos los grupos (a confirmar).
- **Examen:** Solo se considera examen para aquellos alumnos que no aprueban el curso.

EVALUACIÓN DEL CURSO

- **Evaluaciones (fuera del horario de clases - a confirmar):**
- **Evaluación Unidad Temática 1 - incluye CTF:** Semana del 29 de septiembre, 2025
- **Evaluación Unidad Temática 2 - incluye CTF:** Semana del 3 de noviembre, 2025
- **Evaluación Unidad Temática 3 - incluye CTF:** Semana del 24 de noviembre, 2025

UNIVERSIDAD ADOLFO IBÁÑEZ

Semana 1

TICS413: SEGURIDAD TI

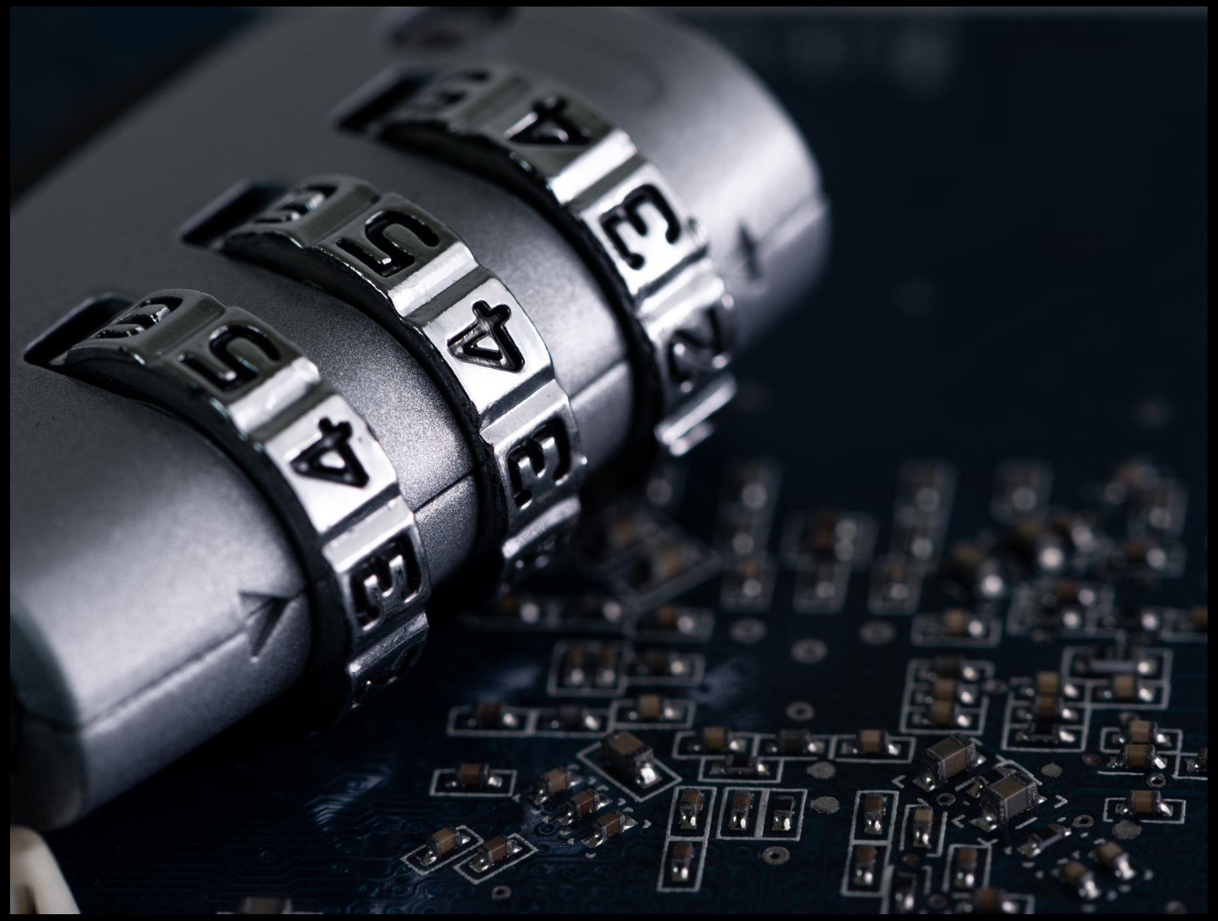
INTRODUCCIÓN

[RA1] Comprender conceptos básicos de Seguridad de la Información en escenarios prácticos y casos empresariales./ [RA2] Distinguir vulnerabilidades y riesgos

EL INFORME INTERNO/INTERINSTITUCIONAL DEL NIST (NISTIR 7298) (GLOSARIO DE TÉRMINOS CLAVE DE SEGURIDAD DE LA INFORMACIÓN, MAYO DE 2013) DEFINE EL TÉRMINO

SEGURIDAD INFORMÁTICA DE LA SIGUIENTE MANERA

- "Medidas y controles que garantizan la **confidencialidad, integridad y disponibilidad** de los activos de un sistema de información, incluyendo hardware, software, firmware e información que está siendo procesada, almacenada y comunicada."



SEGURIDAD DE LA INFORMACIÓN

- Definición:
- La Seguridad de la Información, según ISO27001, se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan, estos pueden ser:
  - Electrónicos
  - En papel
  - Audio y vídeo, etc.

CIBERSEGURIDAD

- Definición:

- Prevención de daños, protección y restauración de computadoras, sistemas de comunicaciones electrónicas, servicios de comunicaciones electrónicas, comunicaciones por cable y comunicaciones electrónicas, incluida la información contenida en ellas, para garantizar su disponibilidad, integridad, autenticación, confidencialidad y no repudio.

INTRODUCCIÓN

- Estadística

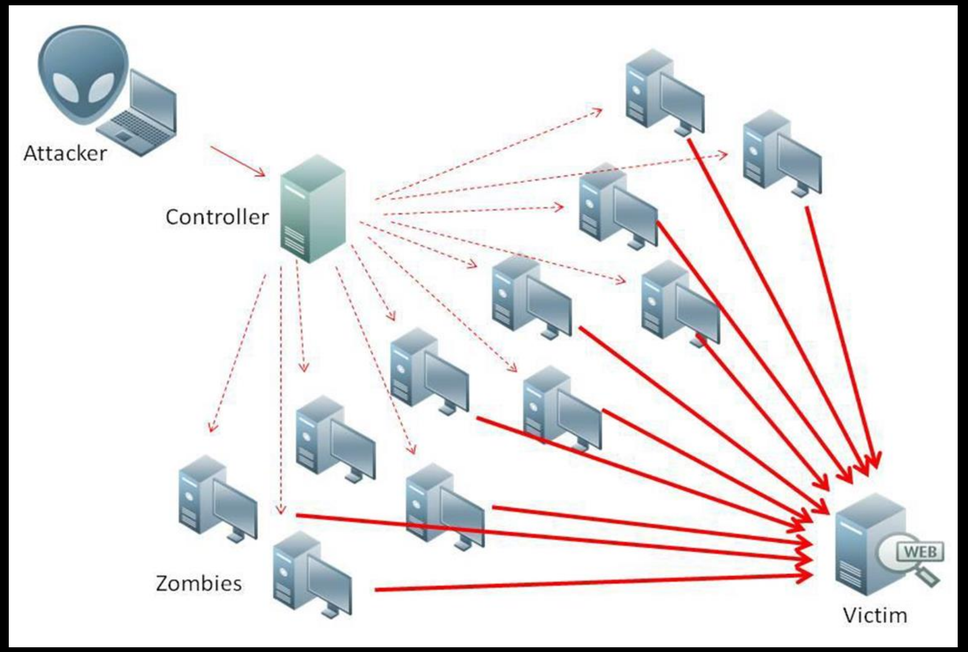
25 junio, 2025

La ciberseguridad se ha convertido en una preocupación clave para gobiernos, empresas y ciudadanos en todo el mundo. Chile no ha sido la excepción. En 2024, el país enfrentó una cifra sin precedentes en intentos de ciberataques: 27.600 millones, lo que representa un aumento casi cuadruplicado respecto a los 6.000 millones registrados en 2023, según el informe global de FortiGuard Labs de Fortinet. Este alarmante incremento posiciona a Chile como el tercer país más atacado de América Latina, sólo detrás de Brasil y México, y refleja una escalada crítica en la actividad cibernética maliciosa.

Fuente:
Fortinet 2025

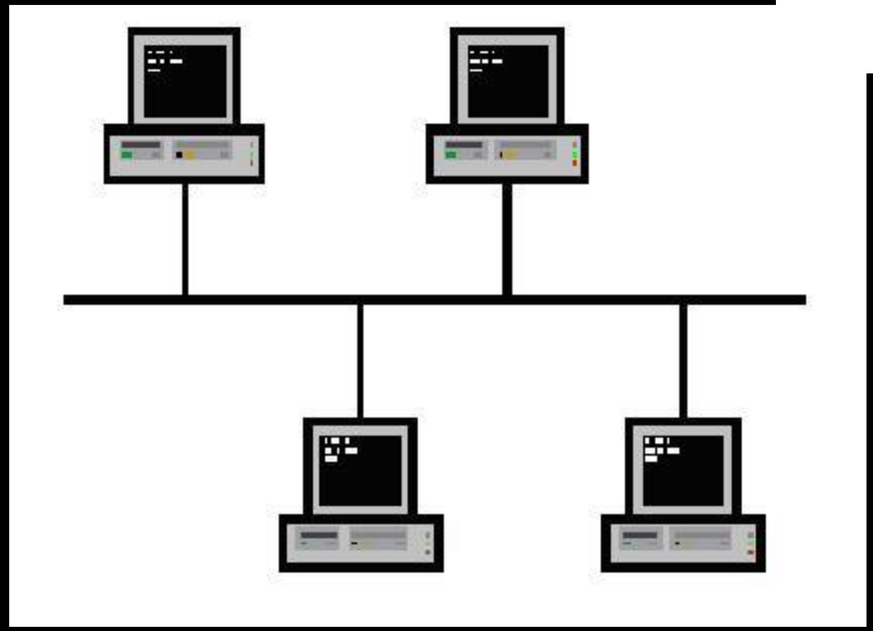
¿POR QUE OCURREN LOS ATAQUES?

- **Motivadores de ataques**
- Cada ataque tiene un motivador, los principales son:
  - Disminuir la continuidad de servicios
  - Robo y venta de datos
  - Perdidas financieras
  - Propaganda política
  - Objetivos militares
  - Causas sociales
  - Demanda de dinero (ransomware)



TIPOS DE AMENAZAS

- **Red**
- Captura de tráfico
- Falsificación de peticiones
- Hombre en el medio (MitM)
- Robo de credenciales
- Denegación de servicio
- Ataques a controles de seguridad (Firewall, IPS)

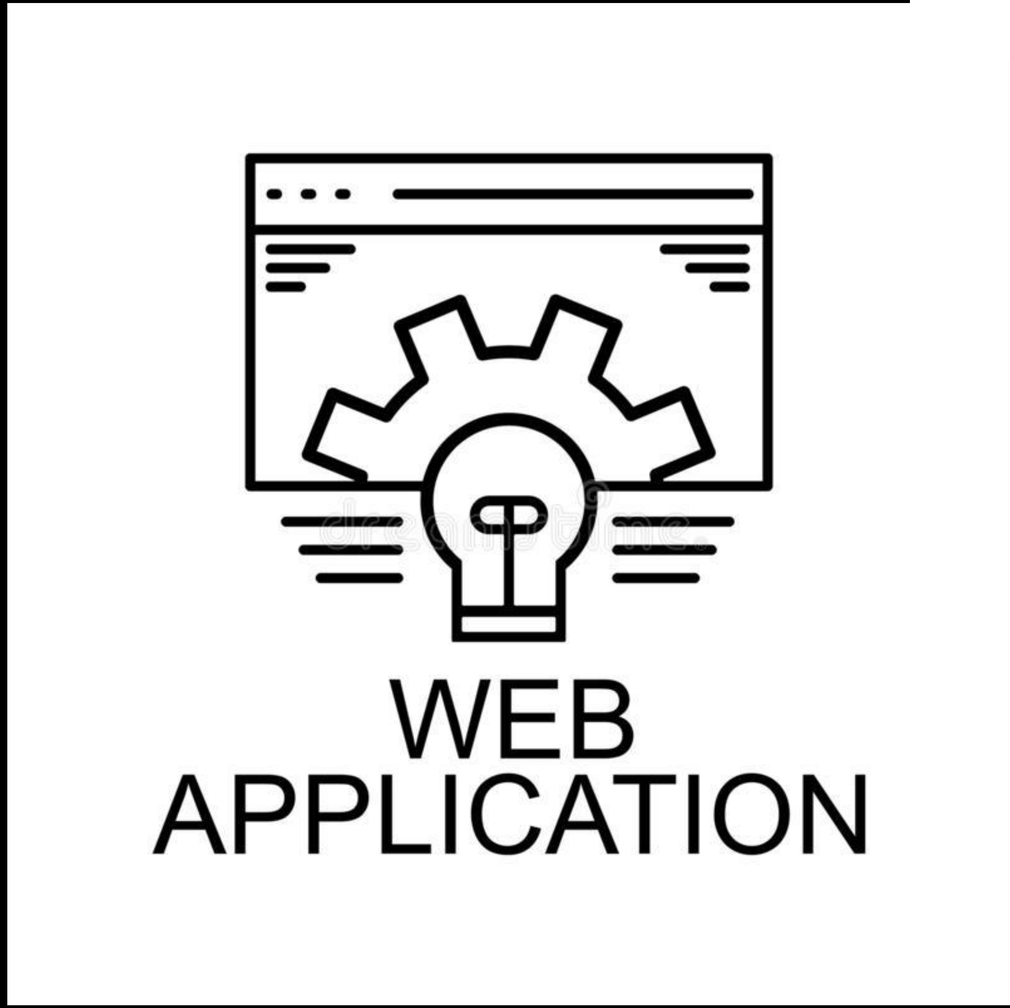


TIPOS DE AMENAZAS

- **Host (Servidores)**
- Ataques de malware
- Ejecución de código
- Escalamiento de privilegios
- Backdoor
- Acceso no autorizado
- Denegación de servicio

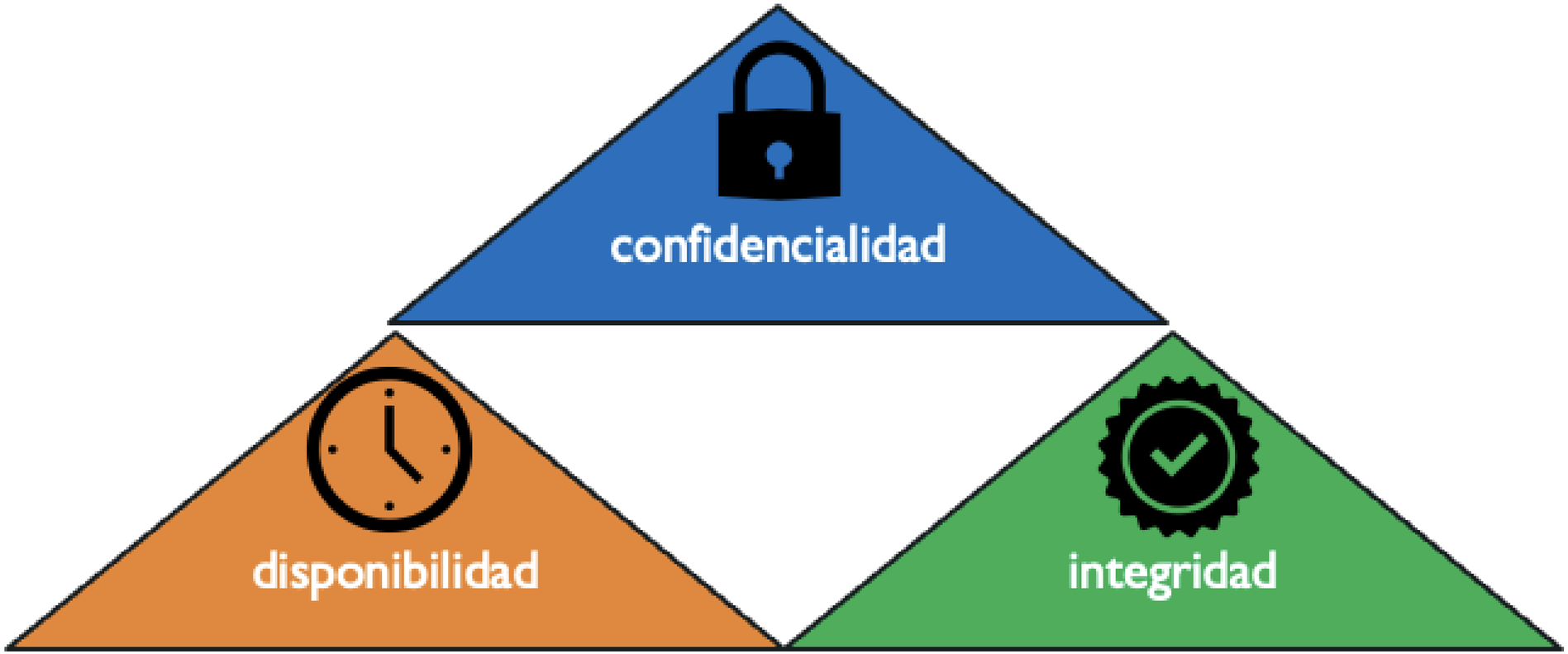
TIPOS DE AMENAZAS

- **Aplicación**
- Alteración de data
- Acceso no autorizado
- Robo de datos
- Buffer Overflow
- Inyección SQL
- Cross Site Scripting
- Phishing



CIBERSEGURIDAD

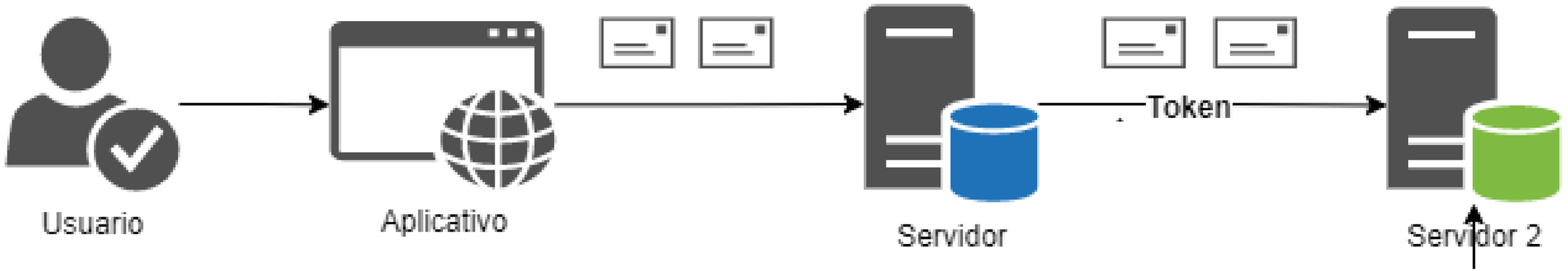
NIST FIPS 199 (*Estándares para la Categorización de Seguridad de la Información y los Sistemas de Información Federales*, febrero de 2004)



INTRODUCCIÓN

- **Triada de la Seguridad de la Información**

¿DÓNDE ESTÁ SIENDO PROCESADA, ALMACENADA Y COMUNICADA ?



CONCEPTOS CLAVES

Confidencialidad

- Preservar las restricciones autorizadas sobre el acceso y la divulgación de la información, privacidad personal, información propietaria

Integridad

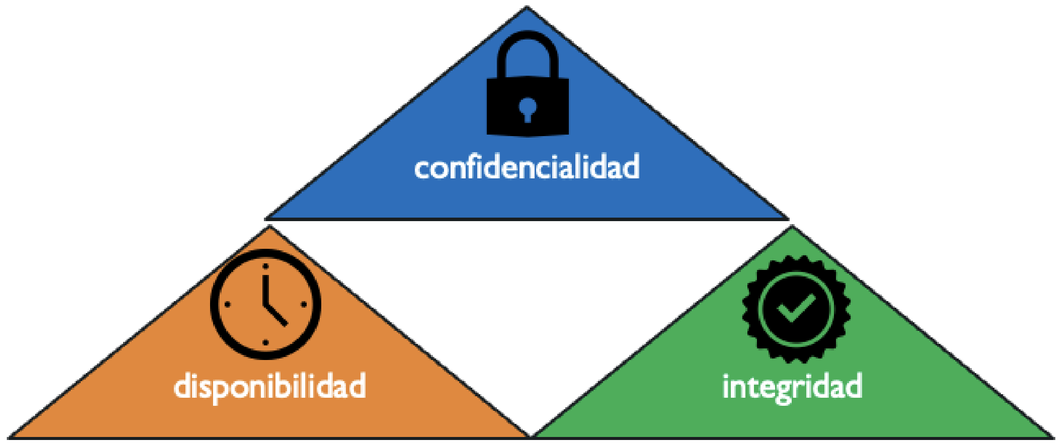
- Proteger contra la modificación o destrucción indebida de la información, garantizando la no repudio y la autenticidad de la información.

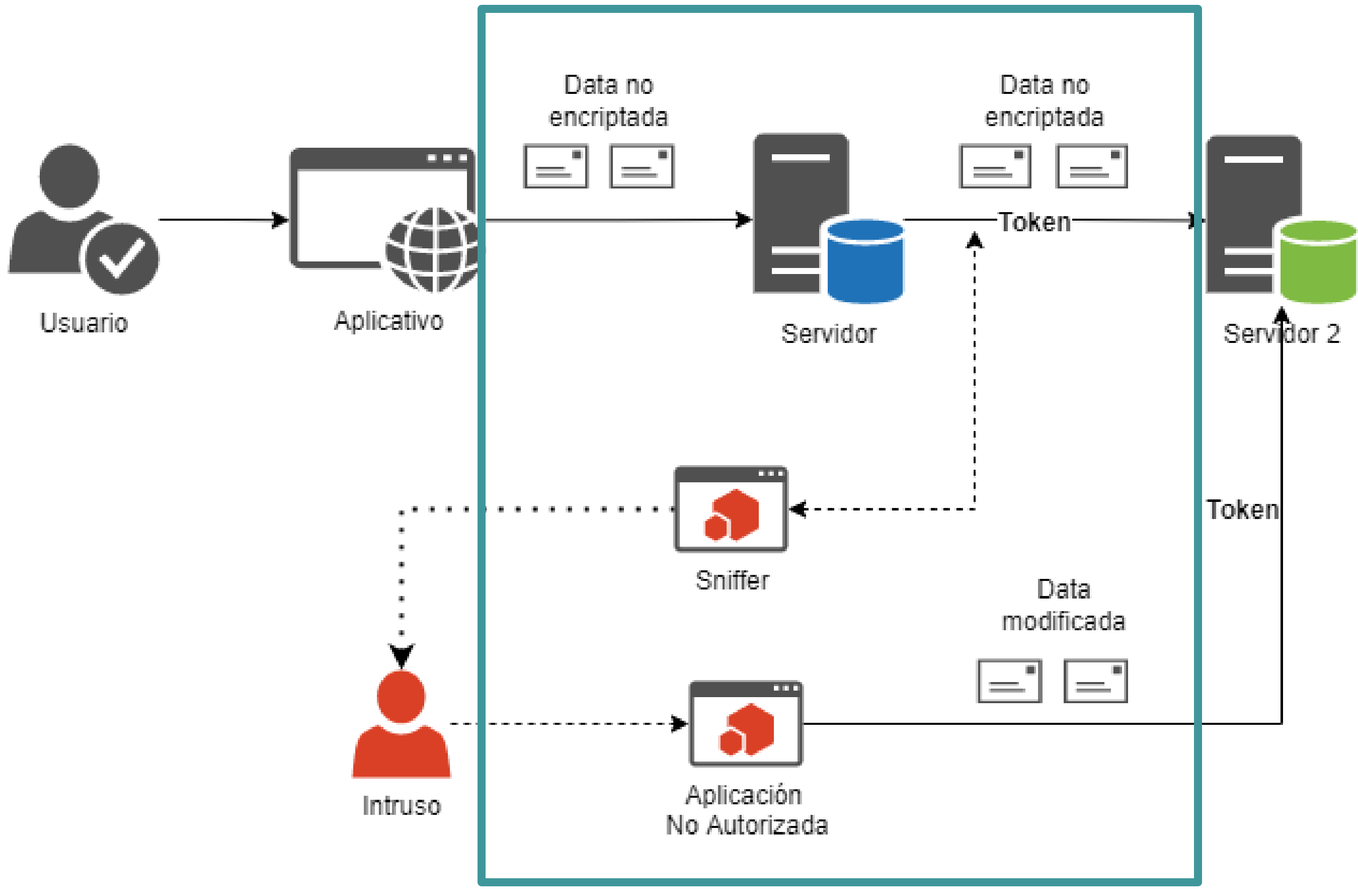
Disponibilidad

- Garantizar el acceso oportuno y confiable a la información, así como su uso adecuado.

CIBERSEGURIDAD

PRINCIPIO SE VE AFECTADO Y EN QUE CASO?
DIGA SUS SUPUESTOS





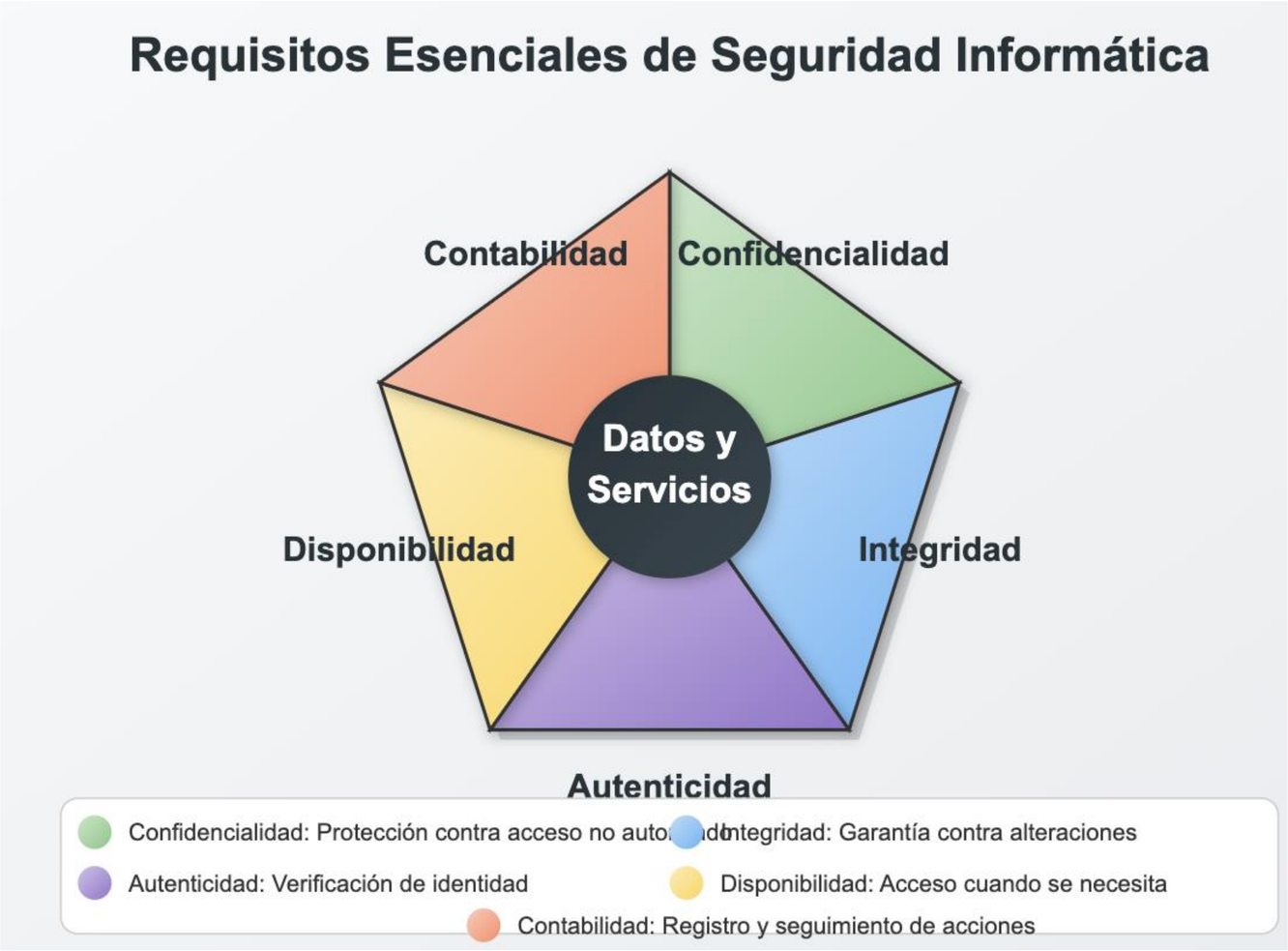
Join at menti.com | use code 8172 1694

Mentimeter

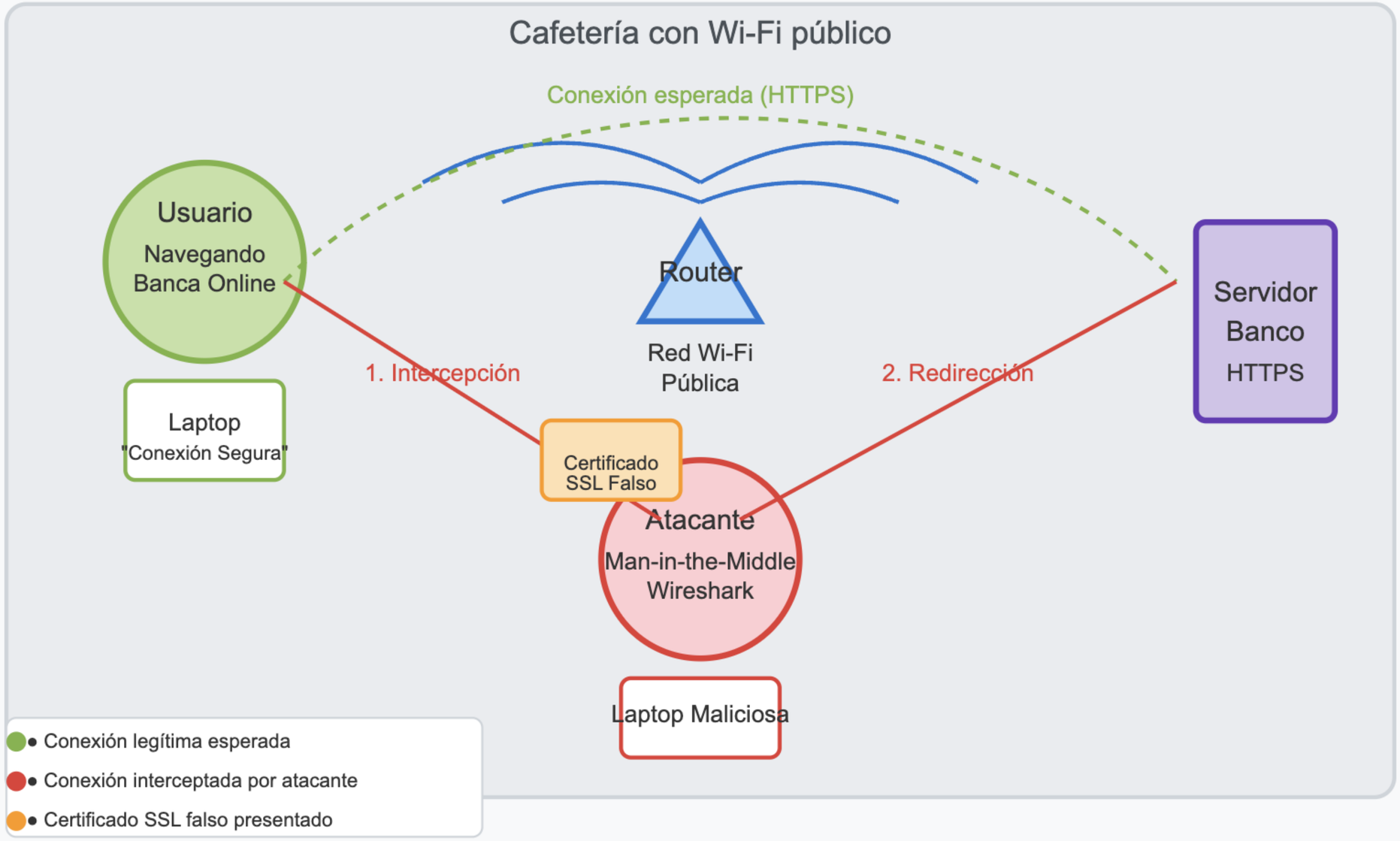
Cuestionario sobre la Triada CIA

Confidencialidad, Integridad y Disponibilidad

TRIADA EXTENDIDA



Ataque Man-in-the-Middle en Red Wi-Fi Pública



¿ESTAMOS 100% SEGUROS EN ESTE SCENARIO?

NIVELES DE IMPACTO

Bajo

- La pérdida **se espera que tenga un efecto adverso limitado** en las operaciones de la organización, sus activos o los individuos.

Moderado

- **La pérdida se espera que tenga un efecto adverso serio en las operaciones de la organización, sus activos o los individuos**

Alto

- **La pérdida se espera que tenga un efecto adverso grave o catastrófico en las operaciones de la organización, sus activos o los individuos.**

UNIVERSIDAD ADOLFO IBÁÑEZ

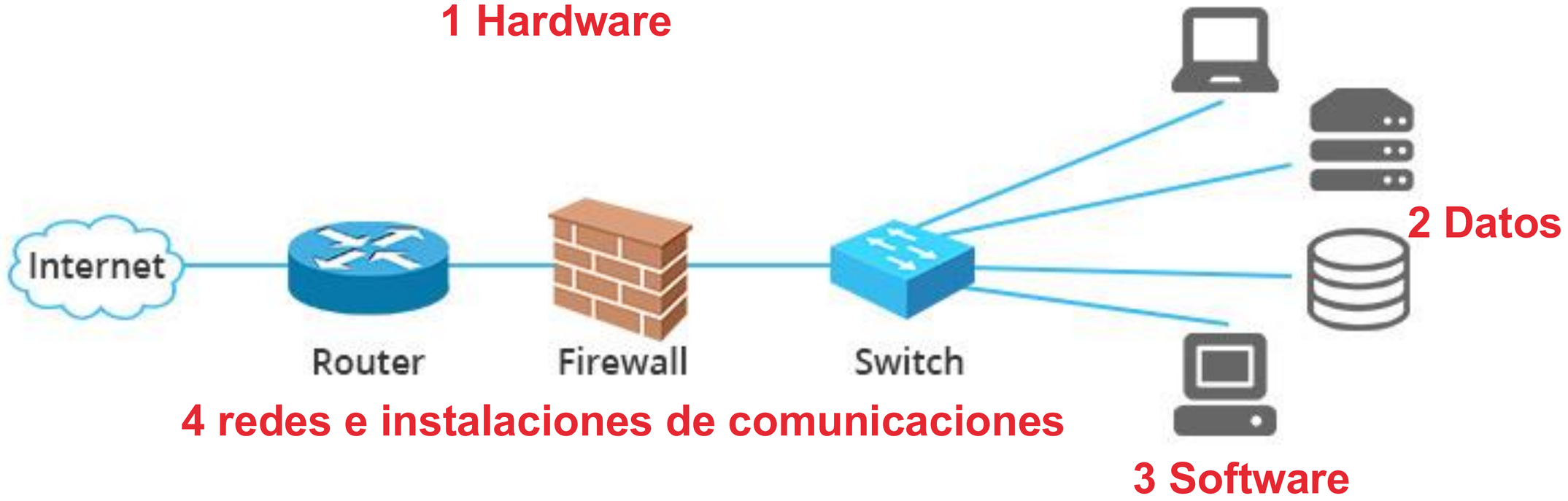
Semana 1

TICS413: SEGURIDAD TI

¿QUÉ ELEMENTOS CONSIDERAMOS?

[RA1] Comprender conceptos básicos de Seguridad de la Información en escenarios prácticos y casos empresariales./ [RA2] Distinguir vulnerabilidades y riesgos

CUALES SON LOS ACTIVOS DE UN SISTEMA COMPUTACIONAL

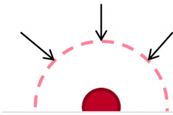


CORRESPONDENCIA DE ACTIVOS CON LA TRÍADA CIA

Tipo de Activo	Disponibilidad	Confidencialidad	Integridad
Hardware	Equipo robado o deshabilitado	Medio físico robado	Hardware modificado para incluir rastreo o control (por ejemplo, keylogger o emulador de teclado)
Software	Archivos del sistema operativo o programas corruptos, causando pérdida de servicio	Software propietario robado	Software modificado para incluir rastreo o control malicioso (por ejemplo, malware)
Datos	Base de datos o archivos eliminados o corruptos, causando pérdida de servicio	Lectura no autorizada de datos de usuario	Archivos modificados por un actor malicioso
Comunicaciones	Mensajes bloqueados o línea de comunicación dañada o deshabilitada	Mensajes interceptados y leídos o análisis de patrones de tráfico	Mensajes modificados, duplicados, fabricados o alterados durante la transmisión

SUPERFICIE DE ATAQUE (ATTACK SURFACE)

- **¿De cuántas maneras puede interactuar un atacante con el sistema?**
  - Incluye el propio software, la red y los humanos.
- Consiste en las **vulnerabilidades accesibles y explotables** en un sistema.
- **Ejemplos:**
  - **Puertos abiertos** en servidores web expuestos al exterior y el código que escucha en esos puertos.
  - **Servicios disponibles** dentro de un firewall.
  - **Código que procesa datos entrantes**, como correos electrónicos, XML, documentos de oficina y formatos personalizados de intercambio de datos específicos de la industria.
  - **Interfaces, consultas SQL y formularios web**.
  - **Un empleado con acceso a información sensible** que sea vulnerable a un ataque de **ingeniería social**.



SUPERFICIE DE ATAQUE

- **Ejemplos de superficies de ataque en sistemas operativos de escritorio:**
  - **Gran superficie de ataque:** *Windows 95*, cuando se conecta, escucha conexiones en varios números de puerto con diversos servicios grandes y complejos.
  - **Superficie de ataque más pequeña:** *Windows 10*, cuando se conecta, escucha en algunos puertos y tiene un firewall que bloquea la mayoría de las conexiones (**pero el firewall tiene excepciones por defecto que aún permiten algunos servicios complejos**).
  - **Superficie de ataque aún más pequeña:** *Ubuntu Linux 20.04*, cuando se conecta, no escucha en ningún puerto.

CATEGORÍAS DE SUPERFICIE DE ATAQUE

Superficie de Ataque en Redes (Network Attack Surface)

Vulnerabilidades en una **red empresarial, red de área amplia (WAN) o Internet**.

Se incluyen vulnerabilidades en **protocolos de red**, como aquellas utilizadas en **ataques de denegación de servicio (DoS)**, interrupción de enlaces de comunicación y diversas formas de ataques de intrusión.

Superficie de Ataque en Software (Software Attack Surface)

Vulnerabilidades en el código de **aplicaciones, utilidades o sistemas operativos**.

Se presta especial atención al **software de servidores web**, ya que es un objetivo frecuente de los atacantes.

Superficie de Ataque Humana (Human Attack Surface)

Ingeniería social, donde los atacantes manipulan a las personas para obtener acceso no autorizado.

Errores humanos, como la configuración incorrecta de sistemas o el uso de contraseñas débiles.

Insider threats (amenazas internas), cuando empleados con acceso legítimo abusan de sus privilegios

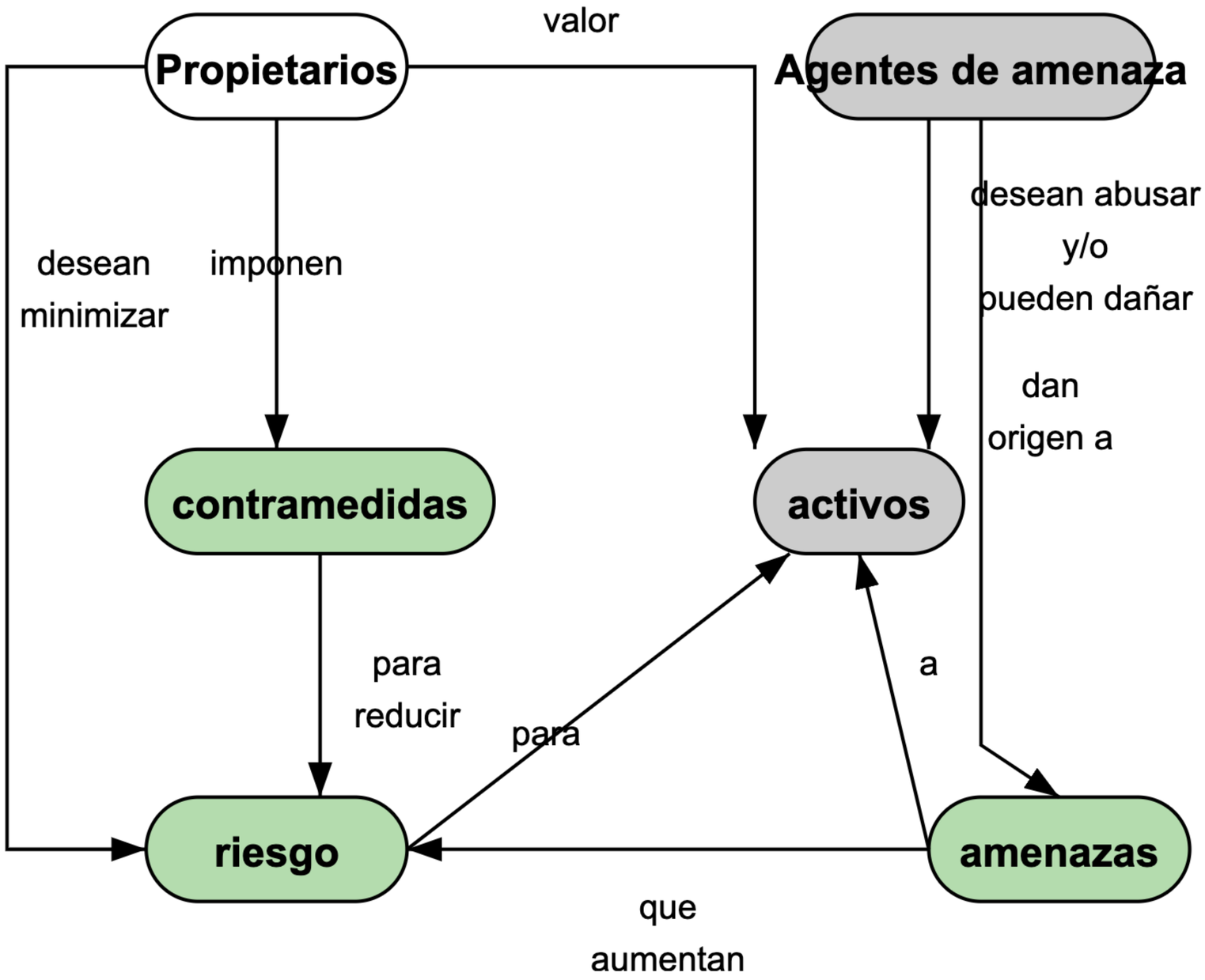
UNIVERSIDAD ADOLFO IBÁÑEZ

Semana 1

TICS413: SEGURIDAD TI

¿QUÉ CASOS ESTUDIAREMOS?

[RA1] Comprender conceptos básicos de Seguridad de la Información en escenarios prácticos y casos empresariales./ [RA2] Distinguir vulnerabilidades y riesgos


Propietarios
valor
Agentes de amenaza
desean
minimizar
imponen
desean abusar
y/o
pueden dañar
dan
origen a
contramedidas
activos
para
reducir
para
a
riesgo
amenazas
que
aumentan

MODELOS DE AMENAZAS

TODO ESTO LO IREMOS VIENDO EN EL CURSO

- Al diseñar una defensa, **debes conocer el objetivo**.
- **Define:**
  - **Activo(s)** en riesgo.
  - Tipo de **vulnerabilidad** que asumes que existe y contra la cual te proteges.
  - **Capacidades/conocimientos del atacante**.
- Solo entonces puedes determinar **cómo tu defensa previene que el ataque tenga éxito a pesar de la vulnerabilidad** (o lo **detecta, responde a él o se recupera de él**).

ESCENARIO

Una empresa de comercio electrónico, **SecureShop**, maneja miles de transacciones diarias, procesando pagos y almacenando información sensible de sus clientes. La empresa es un **propietario (Owner)** de sus **activos (Assets)**, que incluyen bases de datos, servidores web y credenciales de clientes.

- **Historia: Un Ciberataque a SecureShop**
- 📌 **Paso 1: Identificación de los Activos**
- 📌 **Paso 2: Aparición de Agentes de Amenaza (Threat Agents)**

ESCENARIO

- **Paso 3: Generación de Amenazas (Threats)**

- 📌 **Paso 4: Evaluación del Riesgo (Risk)**

  Si el ataque tiene éxito, podría resultar en:

ESCENARIO

- **Paso 5: Implementación de Contramedidas (Countermeasures)**

- **Paso 6: Reducción del Riesgo**

LECCIÓN APRENDIDA:

- Este caso demuestra cómo los **propietarios de activos** deben **anticipar amenazas y aplicar contramedidas** para minimizar riesgos en un entorno digital en constante evolución.

UNIVERSIDAD ADOLFO IBÁÑEZ

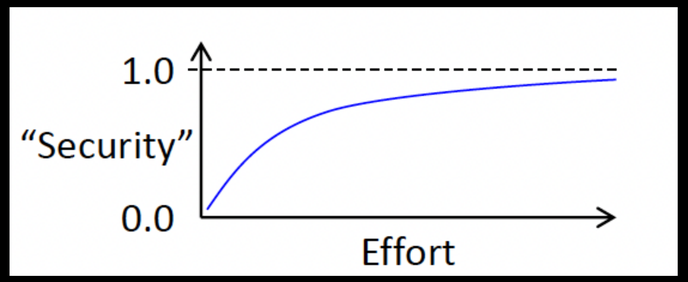
Semana 1

TICS413: SEGURIDAD TI

¿QUÉ MÁS VEREMOS?

[RA1] Comprender conceptos básicos de Seguridad de la Información en escenarios prácticos y casos empresariales./ [RA2] Distinguir vulnerabilidades y riesgos

CONTRAMEDIDAS



Medidas para enfrentar ataques de seguridad

Prevenir (*Prevent*).

Detectar (*Detect*).

Recuperar (*Recover*).

Es posible que queden vulnerabilidades residuales en el sistema

Podría introducir nuevas vulnerabilidades

El objetivo es minimizar el nivel residual de riesgo que afecta a los activos

ESTRATEGIA DE SEGURIDAD

TODO ESTO LO IREMOS VIENDO EN EL CURSO

🔵 Spec (Especificación) → 🔵 **Impl** (Implementación) → 🔵 **Eval** (Evaluación)

- **Especificación/política:** ¿Cuál es tu objetivo? Considera las compensaciones entre facilidad de uso y costo.
- **Implementación:** Identificar mecanismos de **prevención, detección, respuesta y recuperación**.
- **Evaluación:** No asumas que funcionó; **pruébalo**

SecureShop

Objetivo: Proteger la información del cliente y garantizar la continuidad del negocio, minimizando riesgos sin afectar la experiencia del usuario.

ESTRATEGIA DE SEGURIDAD

TODO ESTO LO IREMOS VIENDO EN EL CURSO

🔵 Spec (Especificación) → 🔵 **Impl** (Implementación) → 🔵 **Eval** (Evaluación)

- **Compensaciones a considerar:**
  - **Facilidad de uso vs. Seguridad:** Agregar autenticación multifactor (MFA) aumenta la seguridad, pero puede incomodar a los clientes.
  - **Costo vs. Protección:** Implementar soluciones avanzadas de detección de intrusos puede ser costoso, pero previene ataques graves.
- **Política de Seguridad:**
  ✅ Todos los accesos administrativos requieren **autenticación multifactor (MFA)**.
  ✅ **Solo se almacenan datos cifrados**, cumpliendo con normativas como **PCI DSS** para pagos.
  ✅ Se establece un **plan de continuidad del negocio** para mitigar el impacto de un ataque.

ESTRATEGIA DE SEGURIDAD

TODO ESTO LO IREMOS VIENDO EN EL CURSO

Implementación: Para cumplir con la política, SecureShop implementa mecanismos en cuatro niveles clave:

🔵 Spec (Especificación) → 🔵 **Impl** (Implementación) → 🔵 **Eval** (Evaluación)

- ✅ **Prevención:**

- Firewalls y segmentación de red para proteger los sistemas críticos.
- Encriptación de datos sensibles tanto en tránsito como en reposo.
- Capacitación en seguridad para empleados, reduciendo riesgos de phishing.

- ✅ **Detección:**

- Uso de un **Sistema de Detección de Intrusos (IDS)** para monitorear actividad sospechosa en la red.
- Alertas automáticas cuando se detectan intentos de acceso no autorizado..

- ✅ **Respuesta:**

- Un **equipo de respuesta a incidentes (CSIRT)** con procedimientos claros en caso de ataque.
- Bloqueo automático de cuentas sospechosas después de múltiples intentos fallidos.

- ✅ **Recuperación:**

- **Backups diarios cifrados** almacenados en una ubicación segura.
- Procedimiento para restaurar sistemas en menos de 4 horas tras una interrupción

ESTRATEGIA DE SEGURIDAD

TODO ESTO LO IREMOS VIENDO EN EL CURSO

🔵 Spec (Especificación) → 🔵 **Impl** (Implementación) → 🔵 **Eval** (Evaluación)

- ✅ **Pruebas de seguridad periódicas:**
- **Pentesting interno y externo:** Simulación de ataques para encontrar vulnerabilidades.
- **Auditorías de seguridad trimestrales** para verificar el cumplimiento de políticas.
- ✅ **Simulaciones de incidentes:**
- Ejercicio de ataque simulado: Se ejecuta un ataque controlado para evaluar la respuesta del equipo.
- Simulación de recuperación: Se prueba la restauración de backups para garantizar que los datos puedan recuperarse en un ataque real.
- ✅ **Revisión y mejora continua:**
- Análisis de incidentes pasados para identificar **patrones y ajustar estrategias**.
- Actualización de políticas basadas en nuevas amenazas y normativas.

EJEMPLO DE MODELADO DE AMENAZAS: HTTPS

HTTPS: Forma cifrada de HTTP para tráfico web seguro.

- **Modelo de Amenaza:**
  - **Activo(s):** Comunicaciones privadas de los usuarios, incluyendo credenciales.
- **Vulnerabilidad:** Los paquetes pueden ser interceptados en tránsito (*por ejemplo, en una red Wi-Fi abierta*).
  - **Capacidades/conocimientos del atacante:** Sabe cuándo y cómo interceptar paquetes dirigidos a un usuario específico o a todo el sitio web.
- **La Defensa:**
  - **Nuestra solución:** Negociamos una clave en comunicación abierta, conocida solo por el usuario y el servidor; todo el contenido se cifra con esta clave.
- **Cómo lo soluciona:**
  - Incluso con el tráfico completo, el atacante no puede deducir la clave y, por lo tanto, **no puede descifrar las comunicaciones**.
  - Sin embargo, **pueden saber que la comunicación ocurrió y aproximadamente cuánto tráfico se intercambió**.

CASO: ANÁLISIS DE RIESGOS DE DIVULGACIÓN DE SECRETOS PROPIETARIOS

- Imagina que trabajas como analista de seguridad en una empresa de tecnología llamada **TechSecure**, que desarrolla software innovador. La empresa tiene dos edificios: uno es la sede central y el otro alberga los servicios de red y computación. La propiedad está protegida por una cerca y un guardia en la entrada. Los empleados acceden a la red a través de una VPN segura, y los usuarios de Internet se conectan a un servidor web a través de un firewall.

- Recientemente, la dirección de la empresa ha expresado su preocupación por la posible divulgación de secretos propietarios, como algoritmos de software y datos de clientes. Se te ha asignado la tarea de evaluar los riesgos y proponer medidas de mitigación.

CASO: ACTIVIDADES

1. **Identificación de Amenazas**:
- Identifica al menos cinco amenazas específicas que podrían comprometer la seguridad de los secretos propietarios de **TechSecure**.

2. **Evaluación de Impacto**:
- Para cada amenaza identificada, identifica al menos un escenario (describe brevemente cómo un atacante podría llevarla a la realidad). Evalúa el impacto potencial en la empresa si se llevara a cabo con éxito. Considera aspectos como la pérdida financiera, daño a la reputación y consecuencias legales.
3. **Propuestas de Mitigación**:
- Propón al menos dos medidas de mitigación para cada amenaza identificada. Estas medidas pueden incluir controles físicos, técnicas de ingeniería social y soluciones técnicas.
4. **Presentación**:
- Escribe en el foro tus hallazgos con el resto de la clase. Asegúrate de incluir:
  - Un resumen de las amenazas identificadas.
  - La evaluación de impacto para cada amenaza.
  - Las medidas de mitigación propuestas.

CASO

Identificación de Amenazas

1. **Acceso No Autorizado a las Instalaciones**:
- Un atacante podría intentar ingresar a las instalaciones utilizando credenciales falsas o haciéndose pasar por un empleado.
2. **Robo de Dispositivos**:
- Un ladrón podría robar laptops o dispositivos de almacenamiento USB que contengan información sensible.
3. **Suplantación de Identidad**:
- Un atacante podría hacerse pasar por un proveedor para obtener información confidencial de los empleados.
4. **Explotación de Vulnerabilidades en el Firewall**:
- Un atacante podría intentar explotar vulnerabilidades en el firewall para acceder a la red interna.
5. **Instalación de Malware**:
- Un empleado podría ser víctima de un ataque de phishing y, al hacer clic en un enlace malicioso, instalar malware que permita el acceso a secretos propietarios.

Impacto

Impacto: Alto. Podría resultar en el robo de información crítica y daño a la reputación de la empresa.

•**Impacto**: Moderado. La pérdida de dispositivos puede comprometer información, pero se pueden implementar medidas de seguridad como cifrado.

•**Impacto**: Alto. La divulgación de información confidencial podría llevar a pérdidas financieras y legales.

•**Impacto**: Alto. Un acceso no autorizado a la red podría permitir la exfiltración de datos sensibles.

•**Impacto**: Alto. El malware podría permitir el acceso a información crítica y comprometer la seguridad de la red.

CASO

Identificación de Amenazas

- **Identificación de Amenazas**

1. **Acceso No Autorizado a las Instalaciones**:
- Un atacante podría intentar ingresar a las instalaciones utilizando credenciales falsas o haciéndose pasar por un empleado.
2. **Robo de Dispositivos**:
- Un ladrón podría robar laptops o dispositivos de almacenamiento USB que contengan información sensible.
3. **Suplantación de Identidad**:
- Un atacante podría hacerse pasar por un proveedor para obtener información confidencial de los empleados.
4. **Explotación de Vulnerabilidades en el Firewall**:
- Un atacante podría intentar explotar vulnerabilidades en el firewall para acceder a la red interna.
5. **Instalación de Malware**:
- Un empleado podría ser víctima de un ataque de phishing y, al hacer clic en un enlace malicioso, instalar malware que permita el acceso a secretos propietarios.

Contramedida

Implementar controles de acceso más estrictos y capacitación para el personal sobre la identificación de intrusos.

Utilizar cifrado en todos los dispositivos y realizar auditorías regulares de seguridad.

Capacitar a los empleados sobre técnicas de ingeniería social y establecer procedimientos de verificación para proveedores.

Realizar pruebas de penetración periódicas y mantener el software del firewall actualizado.

Implementar filtros de correo electrónico para detectar phishing y capacitar a los empleados sobre la seguridad cibernética.

ÁRBOL DE ATAQUES

- El **nodo raíz** representa el **objetivo del atacante**: **comprometer la cuenta de un usuario**.
- 🟩 **Los nodos sombreados representan eventos específicos del ataque (nodos hoja).**
  ⬜ **Los nodos blancos agrupan eventos específicos en categorías de ataques.**
- 📌 **Componentes Claves en el Análisis:**

1. **Terminal y usuario (UT/U):** Ataques dirigidos al equipo del usuario (por ejemplo, robo de tokens como smartcards o claves).
2. **Canal de comunicación (CC):** Ataques que interceptan datos en tránsito.
3. **Servidor bancario (IBS):** Ataques fuera de línea dirigidos a los servidores que alojan la aplicación bancaria.

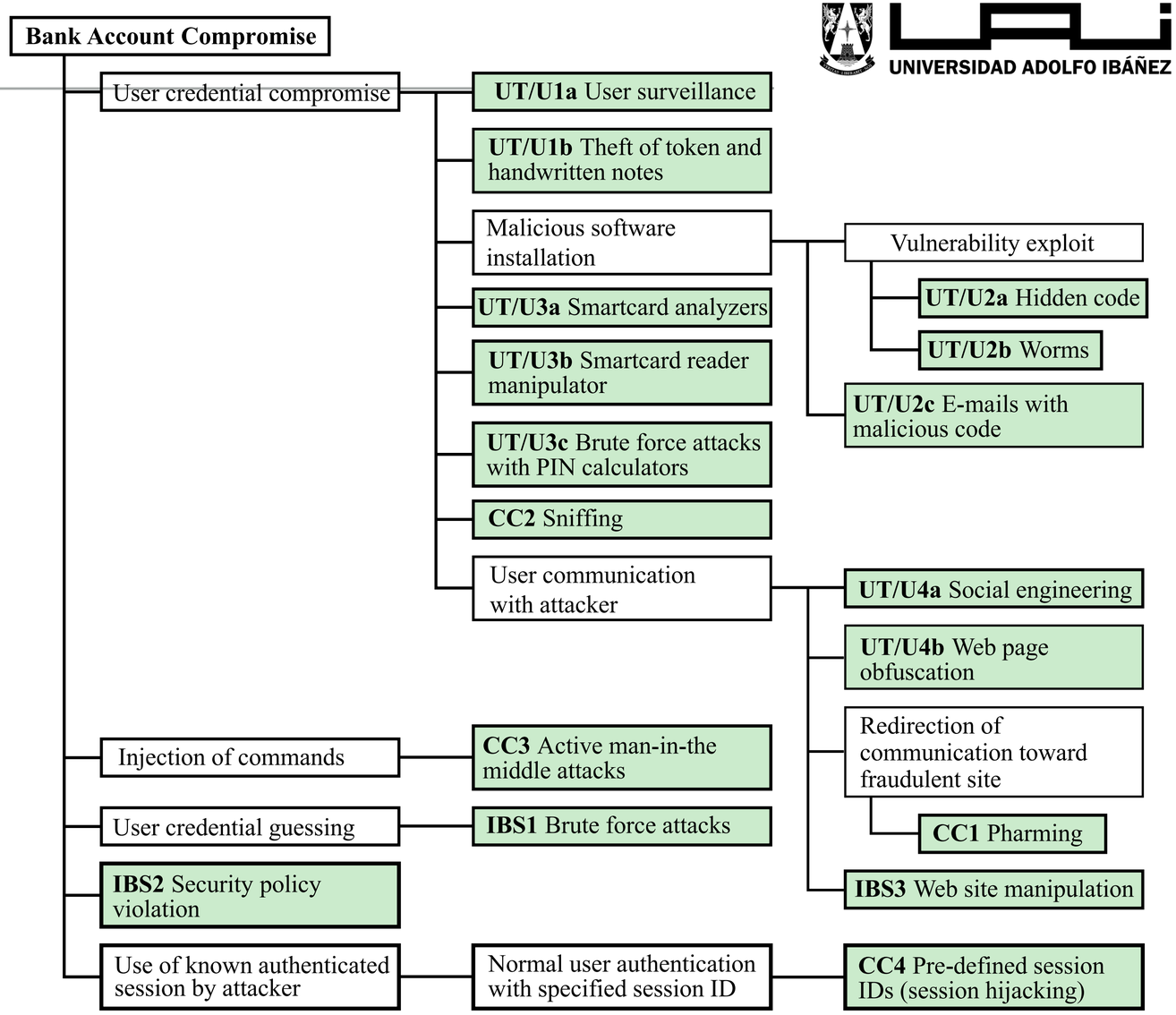
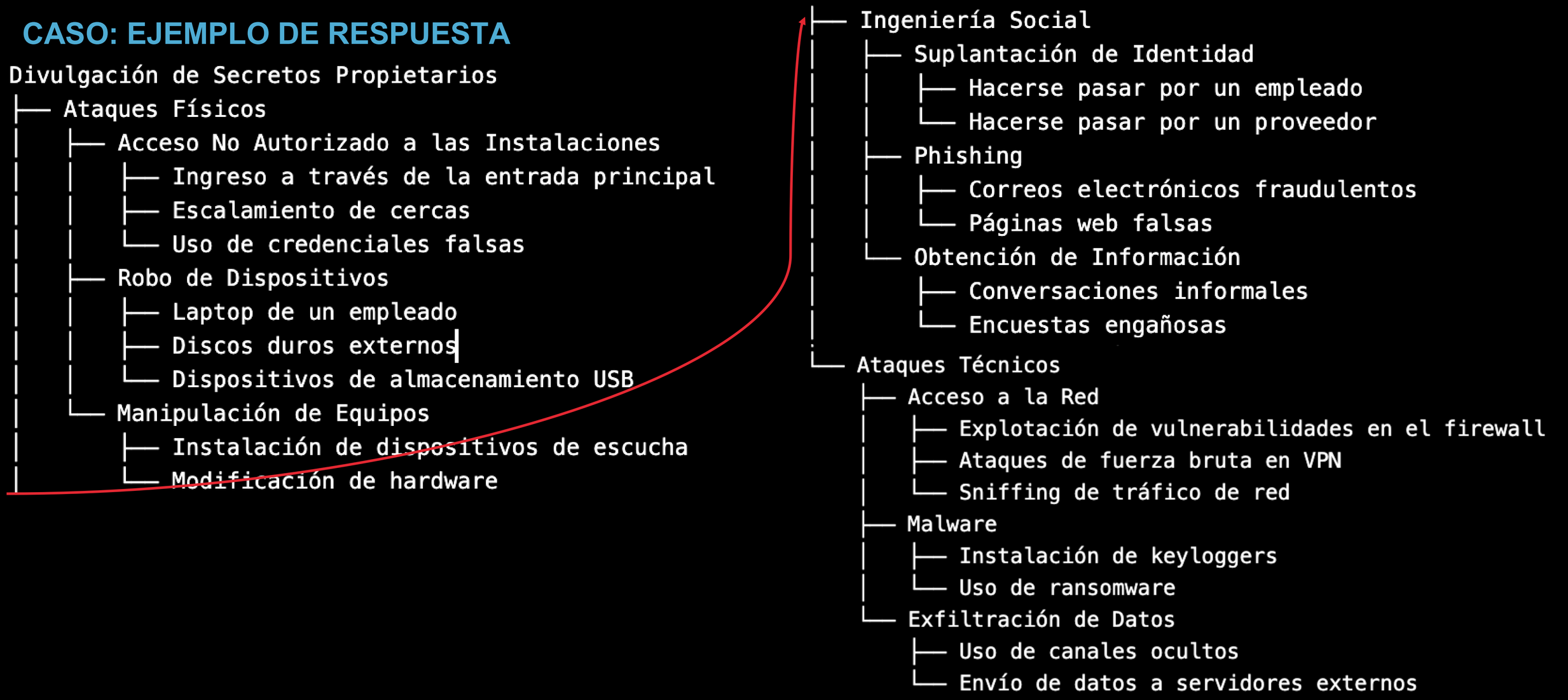


Figure 1.5 An Attack Tree for Internet Banking Authentication

CASO: ANÁLISIS DE RIESGOS DE DIVULGACIÓN DE SECRETOS PROPIETARIOS

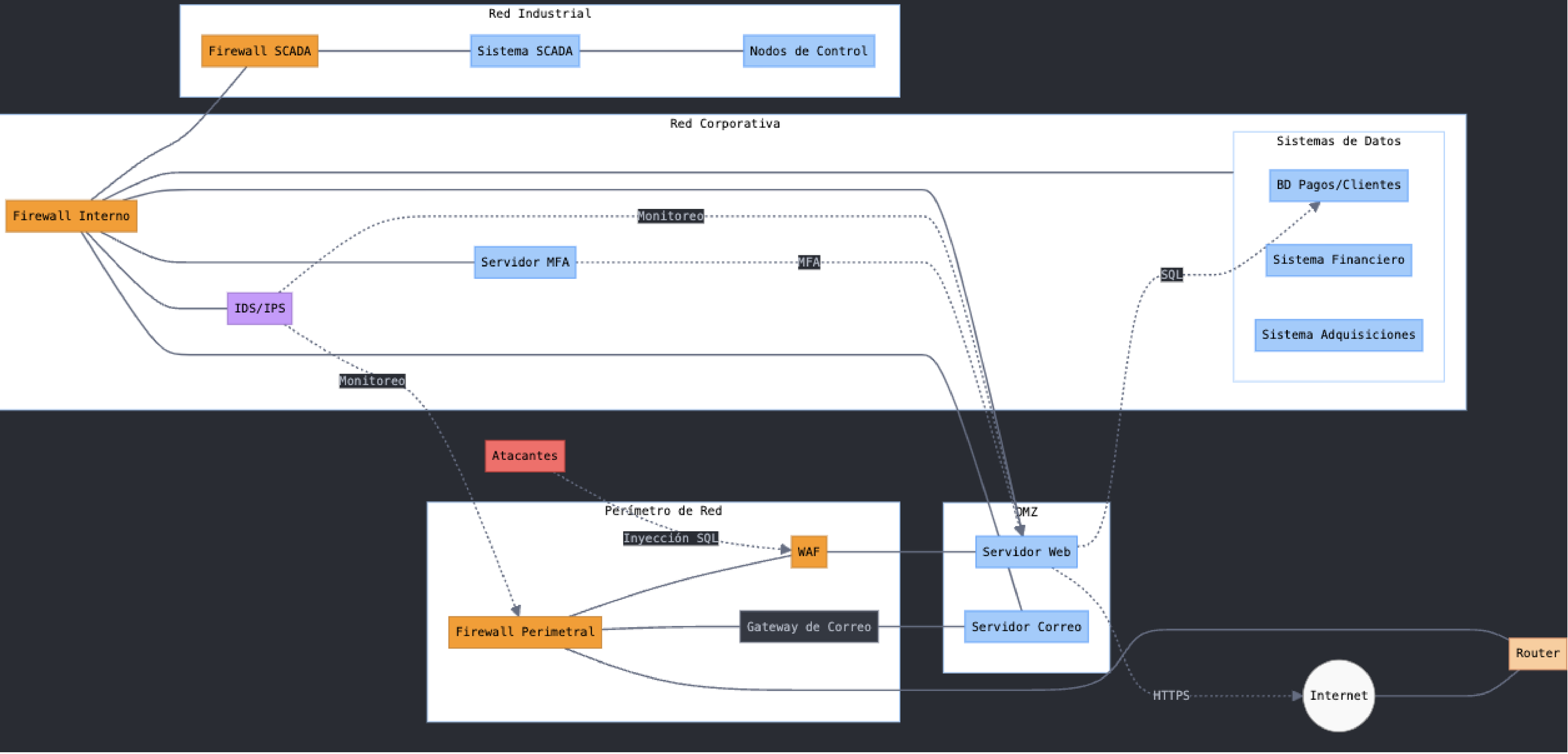
Considera una empresa cuyas operaciones se encuentran en dos edificios en la misma propiedad: un edificio es la sede central; el otro edificio contiene servicios de red y computación. La propiedad está protegida físicamente por una cerca alrededor del perímetro. La única entrada a la propiedad es a través de una puerta de entrada custodiada. Las redes locales están divididas entre la LAN de la sede central y la LAN de servicios de red. Los usuarios de Internet se conectan al servidor web a través de un firewall. Los usuarios remotos de VPN acceden a un servidor específico en la LAN de servicios de red. Desarrolla un árbol de ataque en el que el nodo raíz represente la divulgación de secretos propietarios. Incluye ataques físicos, de ingeniería social y técnicos. Desarrolla un árbol que tenga al menos 15 nodos hoja

CASO: EJEMPLO DE RESPUESTA



GESTIÓN DE RIESGOS EN SILVER STAR MINES

- **Contexto**: Silver Star Mines opera en el sector minero, con una infraestructura de TI extensa que incluye sistemas críticos como SCADA y bases de datos.
- **Importancia de la Gestión de Riesgos**: Proteger activos críticos y garantizar la continuidad del negocio.
- **Objetivo**: Identificar, evaluar y tratar los riesgos asociados con las amenazas a los activos de información.


Red Industrial
Firewall SCADA
Sistema SCADA
Nodos de Control
Red Corporativa
Sistemas de Datos
BD Pagos/Clientes
Sistema Financiero
Sistema Adquisiciones
Firewall Interno
Monitoreo
Servidor MFA
MFA
SQL
IDS/IPS
Monitoreo
Atacantes
Perímetro de Red
Inyección SQL
WAF
DMZ
Servidor Web
Firewall Perimetral
Gateway de Correo
Servidor Correo
Router
HTTPS
Internet

IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS

- Identificación de Activos:
- Sistemas SCADA
- Bases de datos de clientes
- Servidores de producción
- Amenazas Potenciales:
- Acceso no autorizado
- Inyección SQL
- Ataques de red
- Evaluación de Riesgos:

$$\text{Riesgo} = (\text{Probabilidad de ocurrencia}) \times (\text{Costo para la organización})$$

TABLAS RIESGOS

Table 1: Clasificación de la Probabilidad de Ocurrencia

Rating	Descripción	Definición Expandida
1	Rara	Puede ocurrir solo en circunstancias excepcionales y puede considerarse "desafortunado" o muy poco probable.
2	Poco Probable	Podría ocurrir en algún momento, pero no se espera dado los controles actuales.
3	Posible	Podría ocurrir en algún momento, pero también podría no ocurrir.
4	Probable	Probablemente ocurrirá en algunas circunstancias.
5	Casi Cierto	Se espera que ocurra en la mayoría de las circunstancias.

Table 2: Clasificación de Consecuencias

Rating	Consecuencia	Definición Expandida
1	Insignificante	Resultado de una brecha de seguridad menor. El impacto es breve y requiere poca o ninguna intervención.
2	Menor	Resultado de una brecha de seguridad que puede ser manejada sin intervención de la alta dirección.
3	Moderado	Brecha de seguridad que requiere intervención significativa y puede tener consecuencias graves.
4	Mayor	Brecha de seguridad que requiere intervención significativa y puede resultar en daños severos y prolongados.
5	Catastrófico	Brecha de seguridad que resulta en daños severos y prolongados, afectando gravemente a la organización.

PRIORIDAD ACORDE AL NIVEL DE RIESGO

Table 3: Registro de gos de Silver Star Mines

Activo	**Amenaza/Vu**	**Control Existent**	**Prob.**	**Consec.**	**Nivel de Riesgo**
Fiabilidad e integridad de los nodos SCADA	Compromiso no autor-izado	Firewalls capas	Rara	Mayor	Alto
Disponibilidad, integridad y confidencial-idad de los servicios de correo	Ataques de red	Firewalls gateway correo	Casi Cierto	Menor	Alto

UNIVERSIDAD ADOLFO IBÁÑEZ

Semana 1

TICS413: SEGURIDAD TI

¿ES IMPORTANTE ESTO?

[RA1] Comprender conceptos básicos de Seguridad de la Información en escenarios prácticos y casos empresariales./ [RA2] Distinguir vulnerabilidades y riesgos

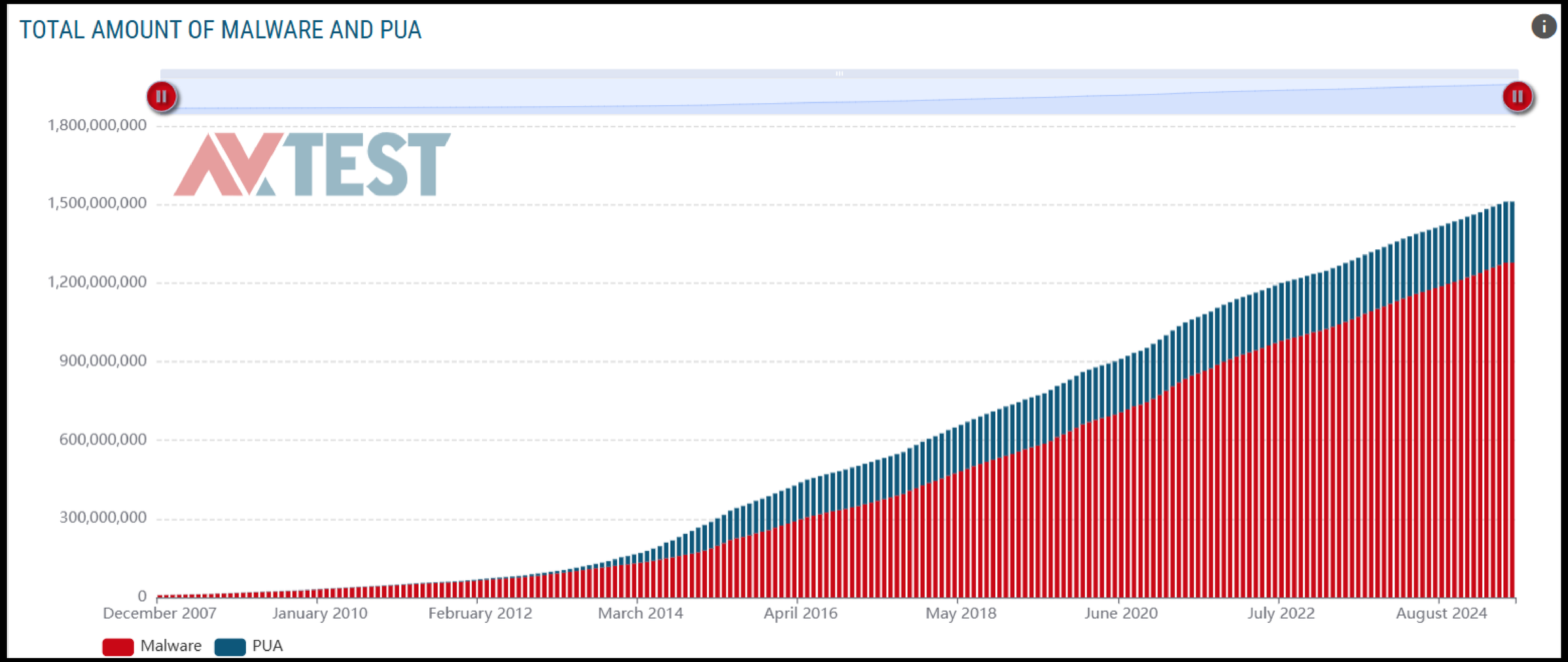
CIERRE

- La seguridad perfecta es imposible.
- **Pensamiento sistemático guiado por modelos, por ejemplo:**
  - La **tríada CIA**.
  - El **modelo de seguridad de la información** (*activo/vulnerabilidad/amenaza/ataque*).
  - El **modelo de estrategia de seguridad** (*especificar/implementar/evaluar*).
  - El **modelado de la superficie de ataque**.
  - El **modelado de amenazas** (*activo/vulnerabilidad/atacante*).

UNIVERSIDAD ADOLFO IBÁÑEZ

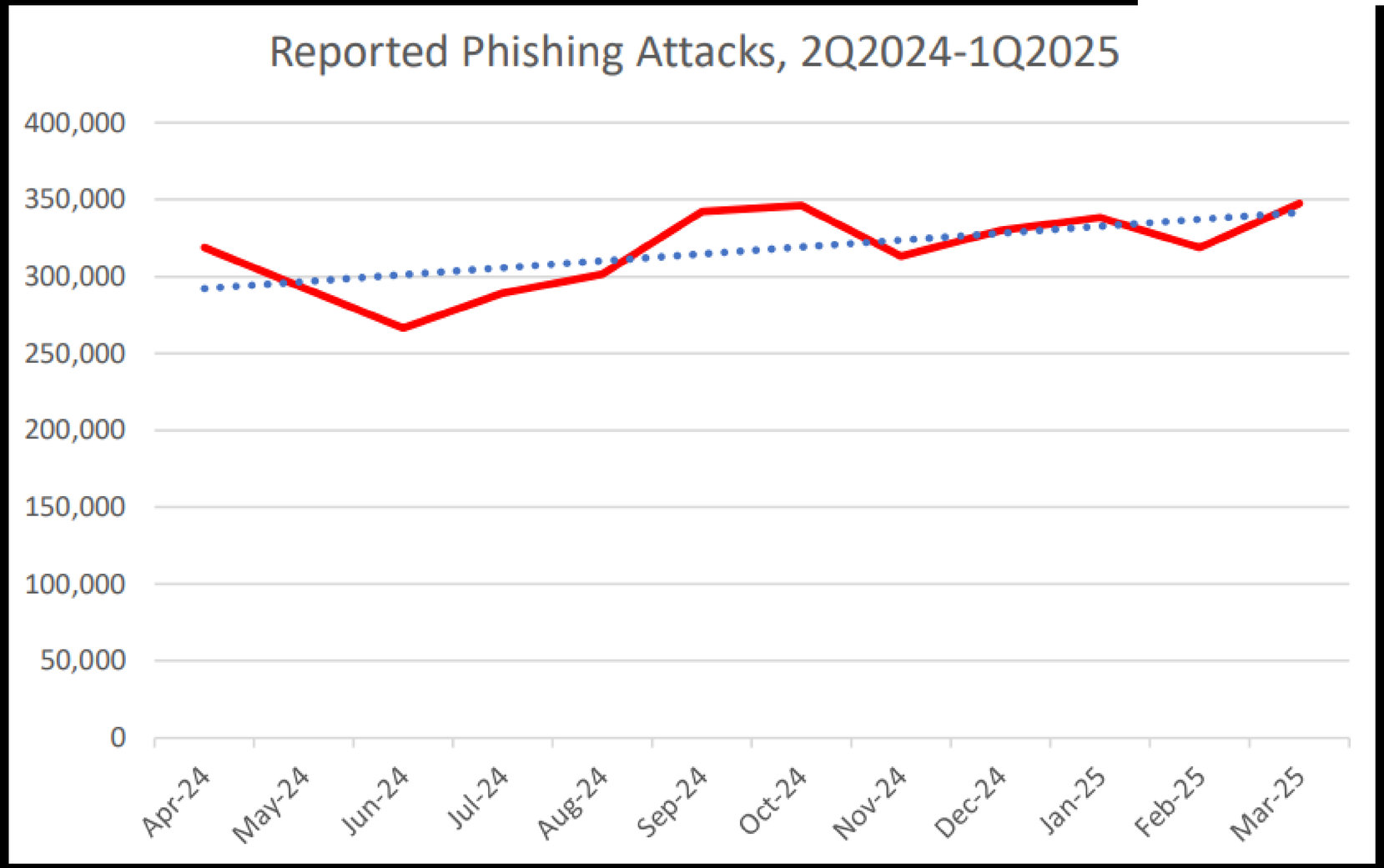
ESTADÍSTICAS

- **Malware**



ESTADÍSTICAS

- **Phishing**

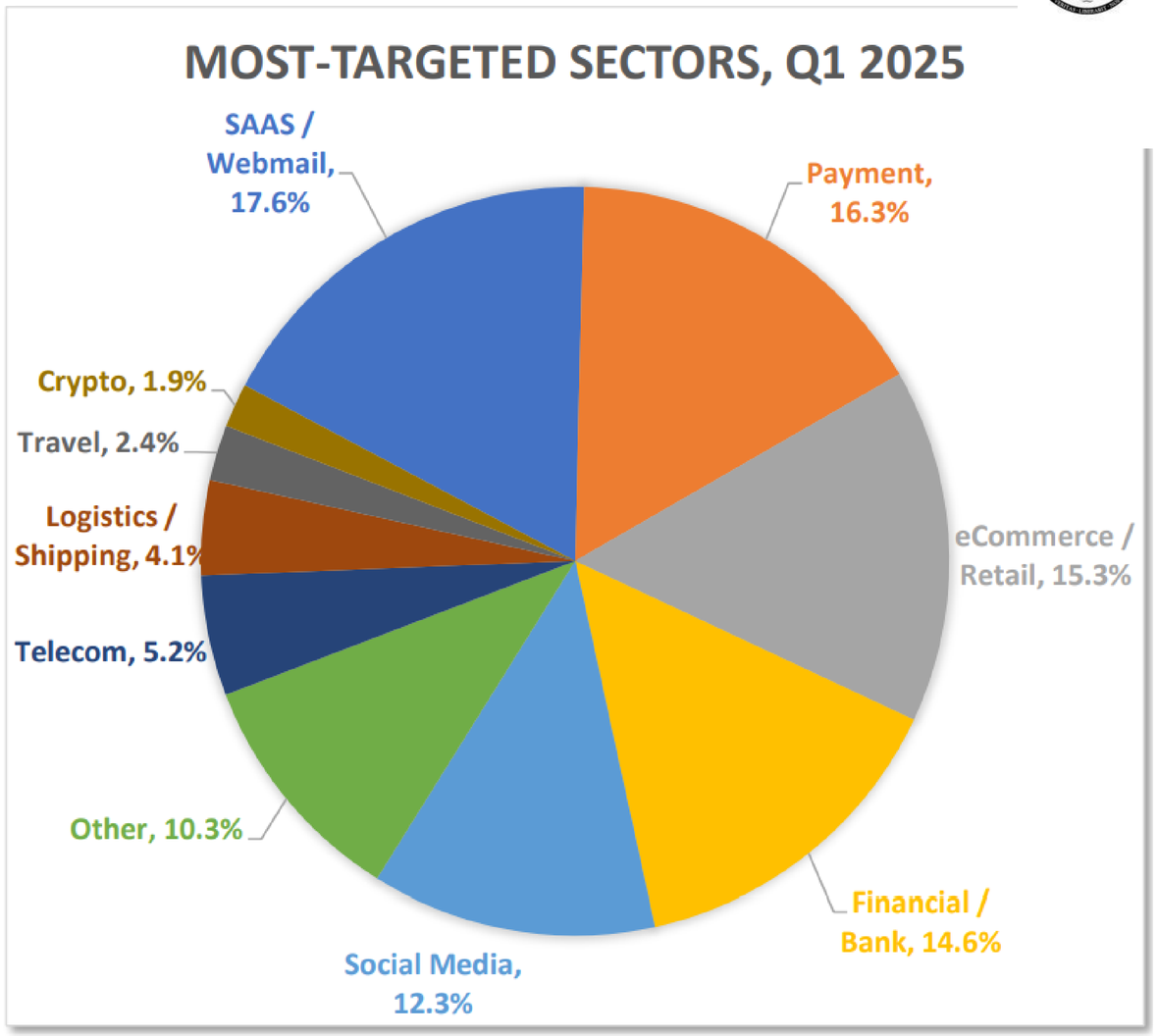


Fuente:
APWG 2025

ESTADÍSTICAS

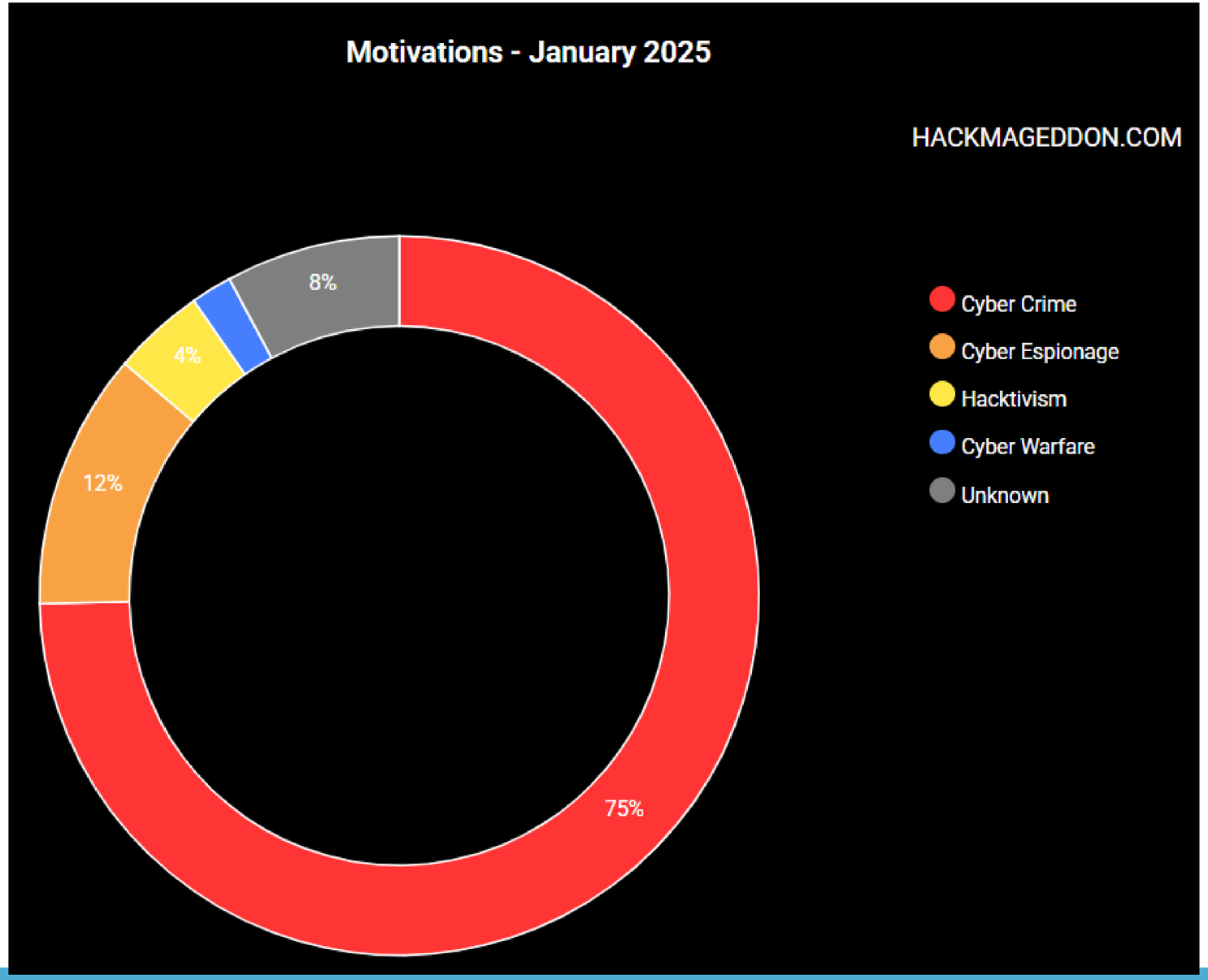
- **Phishing**

Fuente:
APWG 2025



ESTADÍSTICAS

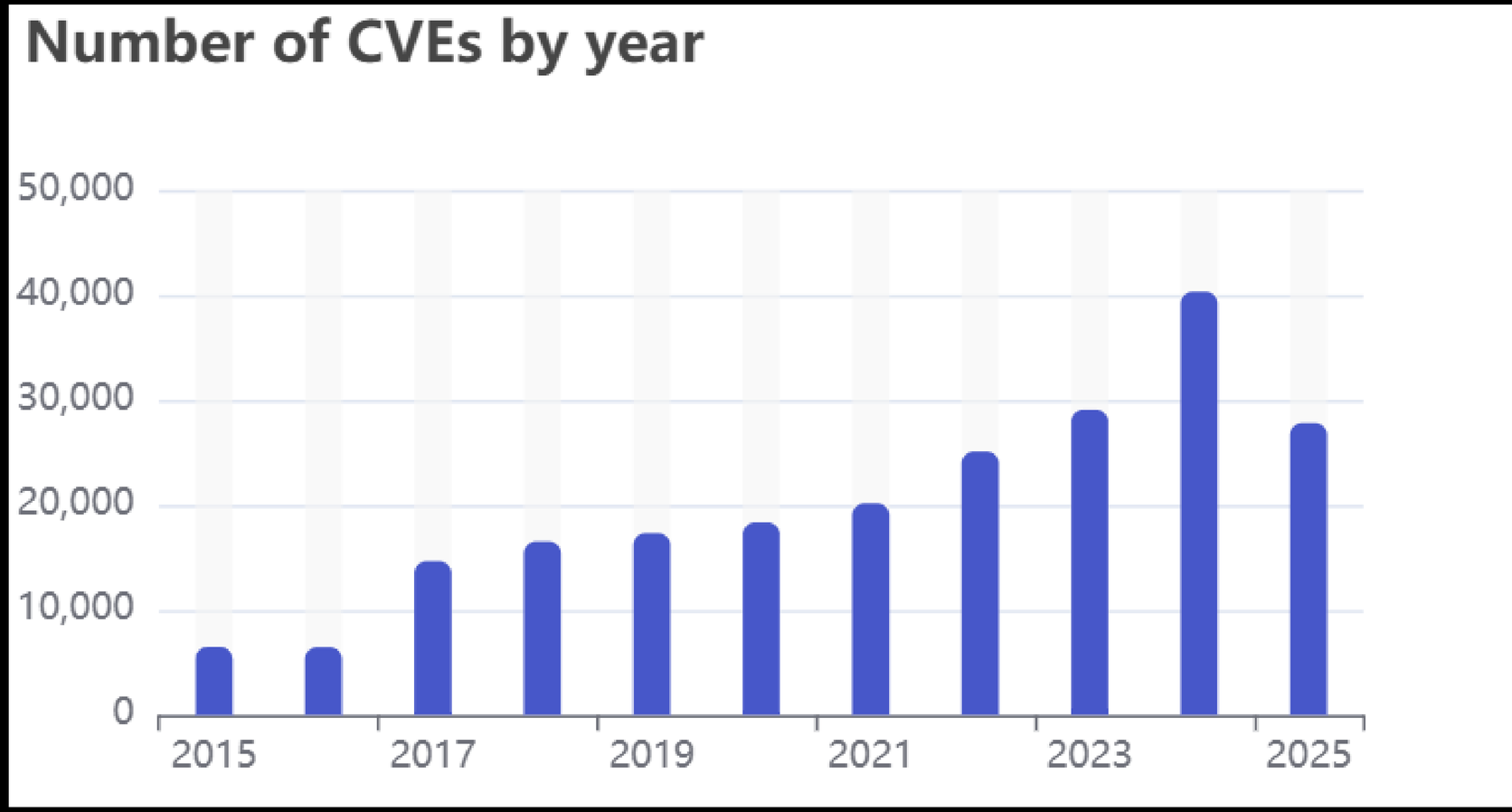
- **Ataques**



Fuente: Hackmageddon

ESTADÍSTICAS

- **Vulnerabilidades**



Fuente: CVE details 2025

CONTEXTO EMPRESARIAL

UNIVERSIDAD ADOLFO IBÁÑEZ

BIBLIOGRAFÍA

- • Stallings, W., & Brown, L. (2019). Computer security: Principles and practice (4th ed.). Pearson.
  - "Cap 1.1 Computer Security Concepts | Cap 1.2 Threats, Attacks, and Assets | Cap 1.6 Computer Security Strategy
  - Gestión de Riesgos (14.1-14.2)"