APUNTES: FUNDAMENTOS DE LA SEGURIDAD INFORMÁTICA (PARTE 1)

Seguridad Informática

A lo largo de la historia, los seres humanos han tenido que **proteger lo que consideraban valioso**, como la vida y la supervivencia. Por ejemplo, en la **prehistoria**, el activo más valioso era **la vida misma**, y las amenazas eran externas, como el hambre o los depredadores. Lo que se protegía entonces era la **supervivencia**, y los elementos a cuidar eran los **activos** físicos.

- Hoy en día, los **activos** pueden incluir no solo la vida, sino también la **información**, que es un activo intangible pero de gran valor. Un **activo** se define como cualquier cosa que **aporte valor** a una persona o una organización. Por lo tanto, debemos proteger, gestionar y cuidar estos activos.
- En el contexto de la seguridad informática, debemos entender conceptos como **amenazas**, **vulnerabilidades** y **activos**. Una **vulnerabilidad** es la debilidad que tiene un activo o el sistema que lo protege, lo que lo hace susceptible a un ataque. Por ejemplo, en la **prehistoria**, las vulnerabilidades podrían haber sido la falta de **protección física** durante la noche o la exposición a predadores.
- La **información** y su protección han sido una preocupación constante a lo largo del tiempo.
- Surgen **amenazas** que buscan comprometer la confidencialidad, integridad o disponibilidad de los datos.
- Una **vulnerabilidad** es una debilidad o falla en un activo que puede ser explotada por una amenaza (como una falla de seguridad, falta de actualización, errores de configuración, etc.). **vulnerabilidad** se refiere a una debilidad en cualquier componente que protege nuestros activos, ya sea físico, tecnológico o incluso humano. Las **amenazas** son los agentes externos que intentan explotar esas vulnerabilidades.
- Para enfrentar estos riesgos, se implementan **mecanismos de seguridad**, como cifrado, autenticación, control de accesos y monitoreo.
- Se utilizan **frameworks** (como ISO/IEC 27001, NIST, COBIT, etc.) que establecen buenas prácticas para la gestión de la seguridad de la información.
- La seguridad puede entenderse como un conjunto de **barreras o murallas** que protegen los sistemas frente a ataques.
- Existe un constante conflicto entre **atacantes** (ciberdelincuentes) y **defensores** (profesionales en ciberseguridad) que buscan resguardar la información.

- Los **ciberdelincuentes** emplean técnicas cada vez más sofisticadas para vulnerar sistemas con fines maliciosos o delictivos.

¿qué más podríamos considerar como debilidades?

Si los activos están indefensos, es mucho más complicado protegerlos. Vemos que las posibilidades de vulnerabilidad surgen en situaciones donde no se cuenta con las medidas de protección necesarias, como en lugares abiertos o expuestos, como se menciona en ejemplos donde las personas no tienen barreras físicas.

Este tipo de **vulnerabilidad** era evidente en tiempos antiguos, cuando no existían **puertas** ni **protección estructural**. Esto hacía que los humanos fueran más **vulnerables**, más débiles frente a las amenazas. La **falta de protección** o de medios defensivos era una clara vulnerabilidad, aunque también, podemos reflexionar sobre cómo en aquellos tiempos las condiciones de vida eran tan duras que, incluso el frío o las inclemencias del tiempo representaban amenazas para la **supervivencia**.

Con el tiempo, el concepto de **seguridad** se fue expandiendo. Otros tipos de **activos** comenzaron a protegerse, como los **conocimientos**. En muchas culturas antiguas, el **conocimiento** no era accesible a todos; solo un pequeño grupo de personas privilegiadas tenía acceso a él. Este conocimiento se protegía cuidadosamente, a veces en **temples** o **pirámides**, lugares diseñados específicamente para resguardar **información valiosa**, **reliquias** o **escrituras religiosas**.

A medida que la humanidad avanzaba, los **mecanismos de seguridad** también evolucionaban. Desde la protección física en lugares como templos y pirámides, hasta la codificación de **mensajes** a través de lenguajes o símbolos que solo unos pocos podían entender. Estos métodos de **codificación** se utilizaban para mantener a salvo el **conocimiento** de los demás.

En la Edad Media, la seguridad comenzó a tomar una forma más estructurada. Los **gobernantes** implementaron **métodos de protección** para resguardar **recursos** valiosos, como riquezas o secretos de Estado. La **seguridad** estaba intrínsecamente relacionada con el control de la **información**, un concepto que sigue siendo relevante hoy en día.

🧠 **Evolución de la Seguridad de la Información**

- En sus inicios, la seguridad de la información se enfocaba principalmente en **proteger el contenido de los mensajes**.
- Con el tiempo, surgieron técnicas de **cifrado** que permitían ocultar el contenido a través de la codificación de la información (**criptografía**).

En la seguridad informática, el concepto de **ataque** se asemeja al **castigo**: el atacante busca identificar las **vulnerabilidades** y **debilidades** en un sistema para **explotarlas** y acceder a la

información valiosa, de la misma manera que un asaltante busca la forma de llegar a las **joyas de la corona** en un castillo.

En las **frameworks** de seguridad, se enfatiza la importancia de proteger los **puntos clave** de un sistema, aquellos elementos que, si se ven comprometidos, pondrían en riesgo la integridad de la organización.

La protección física se traslada a la seguridad informática moderna, donde el objetivo es crear barreras tecnológicas (como **firewalls**, **cifrado** y **sistemas de detección de intrusos**) para proteger la información valiosa de las **instituciones y empresas**.

En un contexto bélico, la **información** es un recurso clave que se debe proteger para evitar que caiga en manos del enemigo. Este concepto de **protección de la información** da paso al desarrollo de la **criptografía**, una de las primeras formas de protección de datos.

🔐 Técnicas de Cifrado a lo largo del tiempo

- **Cifrado y Descifrado:**
  - **Escítala espartana**: uno de los primeros métodos de cifrado militar.
  - **Máquina Enigma**: utilizada en la Segunda Guerra Mundial por Alemania.
  - **Heródoto**: relatos históricos de mensajes ocultos en la antigüedad.

En tiempos antiguos, los mensajes se codificaban de forma sencilla, como cuando los **griegos y romanos** usaban tablas para escribir mensajes y luego los cubrían con cera para proteger su contenido. Este método rudimentario, aunque simple hoy en día, era innovador en su época y representaba una forma de **transmitir mensajes seguros** entre dos puntos, evitando que el enemigo los interceptara. El uso de **tablillas** que contenían mensajes escritos y luego cubiertos con cera. Para leer el mensaje, era necesario **raspar la cera**. Además, otra historia muy conocida cuenta cómo los **mensajeros** que transportaban mensajes secretos usaban un sistema de **cadenas de caracteres**. Cada vez que el mensaje pasaba de una persona a otra, se **cambiaba el código** para asegurarse de que si el mensajero era capturado, el contenido de la información no fuera descubierto. Esta es una **técnica temprana** de protección de datos.

En el ámbito militar, se usaban estrategias similares para proteger **información crítica**. Estas ideas y principios se siguen aplicando en la protección de **sistemas de información** en la actualidad.

Un principio importante de la estrategia que proviene de la filosofía militar es "Conócete a ti mismo y conoce a tu enemigo". Este concepto tiene aplicaciones directas en el campo de la seguridad informática.

🧬 Avances Modernos

- **Observación del terreno**: análisis del entorno y evolución de las amenazas.
- **Cifrado moderno**: desarrollo de teorías matemáticas aplicadas a algoritmos seguros (RSA, AES, ECC).
- **Computación cuántica**: representa un nuevo paradigma en seguridad, ya que podría romper muchos de los sistemas criptográficos actuales.

🕵️ Esteganografía

- Técnica que permite **ocultar información** dentro de otro contenido (como imágenes, videos o audio), de forma que pase desapercibida.

En un contexto de **sistemas de información**, significa que los defensores deben entender **cómo funciona su infraestructura** y cuáles son sus **vulnerabilidades**. Conocer las debilidades del sistema es clave para **fortalecerlo** y para diseñar **estrategias de defensa efectivas**.

Además, es esencial **conocer al enemigo**. En el mundo de la seguridad informática, el "enemigo" son los **ataques cibernéticos** y los **ciberdelincuentes**. Si un atacante comprende cómo funciona el sistema, sus protocolos, aplicaciones y redes, podrá ejecutar un **ataque preciso y eficaz**. Es por esto que los atacantes más **habilidosos** se dedican a estudiar profundamente los sistemas, lo que les da ventaja sobre los defensores, que a veces no tienen tanto conocimiento técnico del entorno en el que están operando.

Por esta razón, los **defensores** deben conocer muy bien lo que están protegiendo. Si no entienden completamente los **activos** que están resguardando (por ejemplo, los sistemas, aplicaciones o redes), es como construir un **muro** sin entender por dónde podrían entrar los atacantes. En la seguridad informática, si los defensores no conocen a fondo su **infraestructura**, las vulnerabilidades pueden ser explotadas, dejando al sistema abierto a posibles brechas de seguridad.

En tiempos pasados, las amenazas eran principalmente físicas, como en las guerras armadas. Un buen ejemplo de esto fueron las **guerras de Kuwait e Irak en los años 90**. Durante ese tiempo, la tecnología bélica, como armas, aviones y vehículos, desempeñaba un papel crucial en las victorias.

Sin embargo, con el tiempo, la **guerra cibernética** ha reemplazado parcialmente las batallas físicas, y ahora los **soldados** luchan con **computadoras**. Un ejemplo claro de esto es la **guerra en Ucrania**, donde la seguridad informática entre países involucró **ataques patrocinados por gobiernos**. Estos ataques no eran realizados por soldados, sino por **expertos en tecnología** o **hackers** contratados específicamente para llevar a cabo estos ataques cibernéticos.

El principio de **"conocer al enemigo y a ti mismo"** es aplicable en la **seguridad informática** de manera similar a la guerra. Si comprendes cómo funciona tu **sistema** y cómo operan los **atacantes**, puedes anticipar sus movimientos y **fortalecer tus defensas**.

📚 **Disciplinas relacionadas:**

- **Criptografía**: ciencia que estudia los métodos de codificación de información para mantenerla segura.
- **Criptoanálisis**: ciencia que busca descubrir o romper los métodos de cifrado sin conocer la clave.
- **Criptología**: disciplina que integra tanto la criptografía como el criptoanálisis.

la **criptoanálisis** y la **criptografía** evolucionaron como métodos de **protección de la información**.

Cada vez que se desarrolla una **nueva tecnología de protección**, también surgen **nuevas formas de ataque**. Los **ciberdelincuentes** encuentran maneras de romper las barreras de seguridad y acceder a la información que se intenta proteger. Esto crea un ciclo constante de **desarrollo de tecnologías de protección** y de **técnicas de ataque**.

> *Por ejemplo, la **computación cuántica** se está posicionando como una amenaza para los sistemas de **cifrado moderno**. En un futuro, los algoritmos actuales, que hoy consideramos seguros, podrían ser descifrados en **segundos** por computadoras cuánticas. Aunque la **fluctuación cuántica** se utiliza también para mejorar la seguridad de los cifrados, los atacantes igualmente podrían utilizarla para **romper esos cifrados**. Esto nos muestra que siempre habrá una **competencia** entre los **buenos** y los **malos** en el mundo de la seguridad.*

El desafío global: proteger los **datos**, especialmente cuando la mayor parte de nuestra vida está **digitalizada**. Hoy en día, nuestras **transacciones bancarias**, **estudios**, **compras** e incluso nuestras **comunicaciones** ocurren en línea, lo que significa que cada vez hay más puntos de **vulnerabilidad**.

> *Un ejemplo claro de esto ocurrió en 2015, cuando el equipo **Hacking Team**, una empresa italiana que vendía software de espionaje, fue hackeado. Los atacantes robaron **400 GB de información** de la empresa, incluyendo **código fuente**, **contratos** y **emails comprometedores**. A pesar de que la empresa vendía software de seguridad, el hecho de que sus sistemas fueran vulnerados muestra que **ni los expertos en seguridad** están a salvo. Nadie está completamente protegido,*

*y, aunque tomemos todas las medidas necesarias para mitigar **riesgos** y **amenazas**, siempre puede haber una **brecha de seguridad**.*

*Otro ejemplo importante fue el **ataque de ransomware** que afectó a empresas como **Telefónica** y **AT&T** en 2017. Estas empresas cuentan con **equipos altamente capacitados**, **certificaciones** y **políticas de seguridad**, pero aun así fueron vulneradas. Este incidente demuestra que **las certificaciones y las políticas de seguridad no son suficientes** por sí solas para detener un ataque. Los atacantes no se detienen por un **cartelito de ISO 25001**. En la **batalla de la seguridad**, lo que realmente importa es **cómo se implementan las medidas de seguridad**, no solo tener los papeles en regla.*

La verdadera seguridad no se logra con **certificaciones** o **protocolos estándar**, sino con la capacidad de adaptarse a las **nuevas amenazas** y de entender en **profundidad** el sistema que se está protegiendo.

En cuanto al **enfoque normativo** y la gestión de la seguridad de los activos, este incluye una serie de **buenas prácticas**, **frameworks**, **políticas**, y **cumplimiento de normas** que nos ayudan a administrar la seguridad de la información de manera efectiva. Es un proceso que abarca desde **normativas** y **gestión de riesgos** hasta **capacitación** y **entendimiento organizacional**.

Seguridad de la Información

- Es importante resaltar que **seguridad informática** y **seguridad de la información** no son lo mismo
- Representa la **esencia central de la disciplina**, ya que su objetivo es **proteger la información** en todas sus formas (física, digital, verbal) frente a accesos no autorizados, alteraciones o pérdidas.
- Se basa en tres principios fundamentales: **confidencialidad, integridad y disponibilidad**.
- La **seguridad de la información** consiste en preservar la confidencialidad, integridad y disponibilidad de los datos (ISO 27000, 2008).
- La **seguridad de la información** es una función de negocio. (ISACA, 2008), que busca proteger los sistemas y la información frente a accesos no autorizados, manipulación, modificación o destrucción indebida.
- Su gestión suele estar a cargo del **CISO** (Chief Information Security Officer) y se basa en el uso de factores de negocio y riesgos cibernéticos para guiar las acciones de seguridad.
- Este enfoque incluye no solo tecnología, sino también procesos, políticas y personal, formando parte integral de la gestión de riesgos organizacional. (Lainhart et al., ISACA Journal, 2016)

💻 Seguridad Informática

- También conocida como **Computer Security** o **IT Security**.
- Es una **rama de la seguridad de la información** que se enfoca exclusivamente en proteger los **sistemas informáticos y redes** frente a amenazas cibernéticas.
- Comprende tanto **técnicas preventivas** (como antivirus, firewalls, autenticación) como **acciones correctivas** (respuestas ante incidentes, recuperación de sistemas).
- La **seguridad informática** (IT Security / Computer Security) es la dimensión **táctica y operativa** de la seguridad de la información.
  Se enfoca en la **implementación técnica** de medidas como **antivirus, firewalls, detección de intrusos, análisis de anomalías y gestión de incidentes**.
- Estas acciones se articulan con las **prácticas de gobierno de TI** para proteger los sistemas y responder ante fallas parciales o totales, donde la **información es el activo en riesgo**.
- Según la RAE, "seguridad" es la cualidad de estar libre de peligro, pero esta definición no aplica completamente a los **sistemas informáticos**, ya que **no existen sistemas totalmente libres de riesgo**.
- La **seguridad informática no es un producto, sino un proceso** continuo que involucra métodos, herramientas y personas.
- Una definición más adecuada sería:
  "Conjunto de métodos y herramientas para proteger la información y los sistemas informáticos frente a amenazas, donde las personas juegan un rol clave."
  La **concientización del factor humano** es fundamental para el éxito de la seguridad.

🔐 Seguridad de la Información vs Seguridad Informática

- **Seguridad de la Información**: es un campo más amplio que abarca no solo medios digitales, sino también físicos, administrativos, etc. Se enfoca en proteger la confidencialidad, integridad y disponibilidad de la información en cualquier formato.
- **Seguridad Informática**: es una subdisciplina que se centra exclusivamente en proteger sistemas informáticos y redes contra accesos no autorizados, ataques y otras amenazas tecnológicas.

🧠 ISACA y COBIT

- ISACA: organización global que promueve la seguridad y gobernanza en tecnologías de información.
- COBIT: marco de trabajo desarrollado por ISACA para el gobierno y gestión de TI empresarial.

Los niveles mencionados (táctico, estratégico, operativo, técnico) son capas de decisión y aplicación de políticas y controles en seguridad informática.

seguridad física

Mientras que la seguridad informática se refiere a la parte técnica (protección de sistemas, redes y dispositivos), la seguridad de la información se enfoca en la protección global de la **información** dentro de una organización, independientemente de su formato (digital o físico).

Un referente importante en este campo es **ISACA**, una organización que originalmente surgió como un grupo de auditores y contadores, pero que ahora se enfoca en la **gestión de riesgos de tecnología de la información** y el **gobierno de la seguridad informática**. ISACA ha sido clave en el desarrollo de estándares y frameworks que ayudan a las organizaciones a gestionar la seguridad de sus sistemas.

- No es lo mismo tener un **director de seguridad informática** (enfoque técnico) que un **gerente de seguridad de la información** (enfoque estratégico). Ambos deben trabajar de forma **interdependiente**, alineando lo **técnico y lo estratégico**.
- Juntos deben construir un enfoque **socio-estratégico**, integrando la seguridad como parte natural del negocio, especialmente en un entorno **móvil, interconectado y basado en el flujo constante de información**.

En cuanto a la **parte estratégica** de la seguridad, esta se relaciona con la **gestión global** de la seguridad de la información dentro de la organización. La seguridad debe ser vista como un **proceso transversal**, no solo como un producto que se adquiere. Es un conjunto de **acciones** que afectan a todos los activos y actividades dentro de la organización. La forma en que cada empresa gestiona la seguridad depende de sus necesidades específicas, que pueden variar dependiendo de sus objetivos y tipo de información.

Sin embargo, en muchas organizaciones, existe una **falta de integración** entre los equipos estratégicos y operativos. En muchas ocasiones, los responsables de **gestión estratégica** (como los gerentes de seguridad) se encuentran desconectados de los **analistas operativos** (como los pentesters, que son los encargados de realizar pruebas de penetración y detectar vulnerabilidades). Esta falta de

comunicación y colaboración puede llevar a que no se implementen las medidas de seguridad más adecuadas para los riesgos reales a los que se enfrenta la organización.

→ 🧠 **Nivel Estratégico**

El nivel **estratégico** se encarga de definir la **visión, misión y objetivos generales** de la seguridad dentro de una organización. Aquí se toman decisiones a largo plazo, considerando la seguridad como parte fundamental del **modelo de negocio** y del entorno competitivo. Los líderes en este nivel, como gerentes generales o CISOs, establecen el rumbo que deben seguir las políticas de seguridad, alineándolas con los **objetivos corporativos**. Es un enfoque más **conceptual y directivo**.

🎯 **Nivel Táctico**

En el nivel **táctico**, se traduce la estrategia en **planes concretos y medibles**. Este nivel es responsable de diseñar las acciones necesarias para alcanzar los objetivos estratégicos. Por ejemplo, definir qué controles de acceso se implementarán, cómo se capacitará al personal o qué medidas se tomarán ante incidentes. Involucra a mandos intermedios, como jefes de área o coordinadores de seguridad, quienes supervisan y optimizan la ejecución de los planes, con una visión **de mediano plazo**.

⚙️ **Nivel Operativo**

El nivel **operativo** se enfoca en la **ejecución diaria** de las tareas relacionadas con la seguridad. Aquí se implementan políticas, se monitorean sistemas, se responden incidentes y se aplican las **buenas prácticas organizacionales**. También se asegura el cumplimiento del **código de conducta y las normas internas**. Este nivel incluye a técnicos, analistas y personal de soporte, quienes se encargan del funcionamiento efectivo y seguro de los sistemas. Se trata de un enfoque **práctico y de corto plazo**, centrado en mantener la seguridad activa y funcional.

En el campo de la **seguridad**, muchas veces las organizaciones se enfocan en **normas, certificaciones y estándares** para cumplir con los requisitos, pero descuidan la parte **operativa** de la seguridad, que es donde realmente se toma acción para proteger los sistemas. Aunque tener las **certificaciones** es importante, la **gestión de la seguridad** debe ser **integral** y no solo una cuestión de **cumplimiento** normativo.

La seguridad no solo debe verse como una obligación para cumplir con requisitos legales, sino como un proceso continuo para proteger los activos. En muchos casos, las empresas cumplen con los estándares y procedimientos solo para **cumplir** y no por un verdadero compromiso con la mejora de la seguridad. Esto es un problema, ya que a menudo se usan **herramientas automatizadas** para detectar vulnerabilidades, pero lo importante es realmente **resolver** los problemas que se detectan.

*Un ejemplo de esto es cuando los bancos, por ejemplo, deben presentar informes anuales sobre pruebas de seguridad. Si bien pueden hacer todo lo necesario para cumplir con los requisitos, muchas veces no se está haciendo de manera **efectiva**. El enfoque se limita a tener el **reporte** listo, pero no se toma acción para realmente **mejorar** la seguridad.*

Por lo tanto, debemos integrar tanto la parte **técnica** como la **estratégica** de la seguridad, con una **gestión efectiva**. Muchas veces se ve una desconexión entre los **líderes estratégicos** y los **operativos**. Los primeros, por lo general, se enfocan más en las **normas** y la **gestión**, mientras que los segundos se encargan del trabajo de campo, como las pruebas de penetración o la **detección de vulnerabilidades**. Esta **falta de comunicación** entre estos dos niveles puede generar un **desajuste** en la seguridad global de la organización.

A menudo, las personas optan por especializarse en **seguridad de la información** o en **seguridad informática**, pero debemos tener claro que ambas disciplinas son necesarias y complementarias. La seguridad informática se enfoca en proteger los **sistemas** y **redes**, mientras que la seguridad de la información abarca un enfoque más amplio, incluyendo **políticas**, **normativas** y **gestión de riesgos**.

En cuanto a las filosofías de seguridad, existen enfoques como la **seguridad perimetral** (con cortafuegos, antivirus y filtros) y la **seguridad en capas** (como la protección de aplicaciones, redes, etc.). Sin embargo, todos los sistemas **deben estar interconectados**, porque en el mundo digital actual, la mayoría de la **información** ya está digitalizada y almacenada en redes. Las **empresas** y las **instituciones** deben implementar mecanismos adecuados para **proteger** y **gestionar** esa información de manera efectiva.

El trabajo de los **encargados de la seguridad** es complejo, ya que deben detectar **amenazas**, analizar si un incidente es un **ataque real** o un **falso positivo**, y gestionarlo adecuadamente. Las **brechas de seguridad** siempre están presentes, y es difícil **tapar todos los huecos**. Incluso después de aplicar un **parche de seguridad**, podrían surgir **nuevas vulnerabilidades**.

La **seguridad ofensiva** y **defensiva** se complementan, pero los defensores siempre estarán en una posición más reactiva, mientras que los atacantes pueden aprovechar **brechas no detectadas**. Existen diferentes tipos de **perfiles profesionales** en ambos campos: desde **hackers éticos** (sombrero blanco) hasta **ciberdelincuentes** (sombrero negro), pero independientemente del rol, lo que importa es **conocer las herramientas** y **comprender cómo funcionan** para poder gestionarlas de manera adecuada.

Seguridad Defensiva

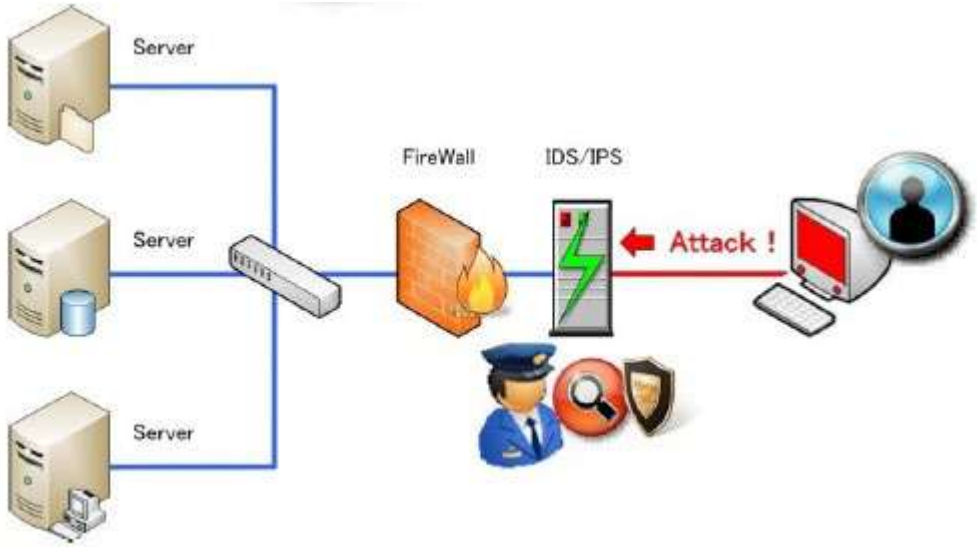
→ La **seguridad defensiva** se refiere al conjunto de medidas y estrategias destinadas a **proteger los sistemas de información** frente a amenazas externas e internas.
→ Su objetivo principal es **cubrir todas las posibles vulnerabilidades**, implementando controles

preventivos, detectivos y correctivos como firewalls, antivirus, sistemas de detección de intrusos, y políticas de acceso.

→ Se ocupa de la **configuración efectiva** de los equipos, dispositivos y sistemas de seguridad como: antivirus, IDS/IPS, antispam, webfilter, firewall, etc.

→ Una parte fundamental de este enfoque es la **detección de amenazas y gestión de incidentes de seguridad**, lo que permite reaccionar con rapidez y minimizar el impacto de los ataques.

- Se refiere a todas las medidas que buscan prevenir ataques: firewalls, antivirus, sistemas de detección de intrusos, políticas de acceso, etc.
- Incluye aspectos legales, normativos y técnicos.
- Es la base más utilizada en la práctica profesional.



*Cuando se trata de **exploits** o **herramientas de explotación**, hay que ser muy cauteloso. Algunos usuarios descargan herramientas sin revisar el código y simplemente las ejecutan, lo que puede llevar a consecuencias no deseadas. Un ejemplo es el **WannaCry**, un ransomware que explotaba una vulnerabilidad en versiones antiguas de **Windows**. Si bien el código estaba disponible públicamente, muchos simplemente lo ejecutaron sin saber realmente lo que hacía, lo que llevó a consecuencias graves. ¿Por qué pasó esto? Porque no se **revisó el código** antes de usarlo, ni se entendió con qué se estaba conectando o qué acciones realizaba.*

Es esencial tener **desconfianza saludable** cuando trabajas con herramientas de seguridad. Como profesionales, debemos ser **más precavidos** y entender qué hace la herramienta antes de usarla. No solo se trata de usar una herramienta, sino de saber cómo funciona, qué hace exactamente y cuáles son sus riesgos. Si una herramienta no funciona como esperábamos, no debemos **continuar ejecutándola** sin investigar por qué. A veces, lo que parece ser una solución

rápida puede terminar siendo una brecha de seguridad por la que los atacantes pueden **explotar** el sistema.

> *Por ejemplo, si descargas un **código** y tienes que modificarlo para que funcione correctamente, debes entender completamente lo que estás cambiando. No basta con ajustar algo sin saber las implicaciones. Yo he tenido que hacer ajustes en códigos para que funcionen correctamente, pero también he visto cómo una **herramienta** aparentemente sencilla puede traer **riesgos ocultos**, como abrir puertos adicionales o cargar software malicioso. Esto es lo que sucede con muchas herramientas que no están verificadas o son **maliciosas** por diseño, incluso si su propósito inicial parecía legítimo.*

Es importante también tener en cuenta los riesgos de utilizar **software gratuito o de código abierto**, como **SPSS** o **R**. Aunque son potentes, algunas veces pueden tener vulnerabilidades que pueden ser explotadas si no se usan correctamente. En última instancia, la elección de usar una herramienta o software debe ser una **decisión consciente** basada en la evaluación de los **riesgos y beneficios**.

⚔️ Seguridad Ofensiva

- La **seguridad ofensiva** se basa en el uso de técnicas proactivas para **identificar y explotar vulnerabilidades** en sistemas, con el fin de evaluar su nivel de seguridad. A diferencia del enfoque defensivo, no se limita a proteger, sino que busca **atacar de manera controlada** para descubrir puntos débiles antes de que lo hagan los ciberdelincuentes.
- Este tipo de seguridad requiere un **conocimiento profundo de sistemas, redes y técnicas de ataque**, por lo que suele ser ejecutada por especialistas conocidos como **hackers éticos** o **hackers blancos**, quienes operan bajo permisos y con fines legales.
- Enfoque que aborda el lado del análisis de vulnerabilidades y las pruebas de penetración, bajo metodologías de *Ethical Hacking* o*Pentesting*
- Curiosamente, muchos ataques reales comienzan por los **servicios aparentemente menos importantes o más descuidados**, ya que suelen ser los más vulnerables. Por eso, en seguridad ofensiva, **nada se subestima**.

En el mundo de la **seguridad ofensiva** (como el **pentesting**), algunas veces las tareas están muy limitadas. Por ejemplo, cuando nos piden realizar una **prueba de penetración**, a menudo solo se nos permite probar ciertos activos, sin poder realizar una **explotación total** o **post-explotación**. Esto puede ser frustrante, ya que muchas veces descubrimos vulnerabilidades críticas, pero no podemos explotarlas completamente debido a las **restricciones contractuales** del cliente.

Además, a menudo los clientes nos limitan a una **fase inicial** del proceso, lo que impide hacer un análisis completo y evitar **riesgos adicionales**. Por ejemplo, encontré una vulnerabilidad que permitía

el acceso sin autenticación a un servicio, lo que habría permitido **extraer claves de bases de datos**. Sin embargo, el cliente me pidió que no realizara pruebas más profundas, limitándome a verificar la vulnerabilidad y no a explotarla completamente. En estos casos, como **profesionales de la seguridad**, debemos **respetar las condiciones** del contrato, pero siempre destacando la importancia de una revisión más profunda para evitar problemas futuros.

Cuando hablamos de **autenticación** y **acceso sin autenticación**, es fundamental entender cómo los atacantes pueden explotar vulnerabilidades en sistemas sin la necesidad de autenticar. Si, por ejemplo, no hay control sobre los **puertos** abiertos y accesibles, un atacante podría **explotar esa vulnerabilidad** y entrar directamente en el sistema, sin ninguna restricción, lo que permite un acceso completo. Aunque no siempre sabremos si un atacante **descubre esa vulnerabilidad**, lo que es cierto es que si lo encuentra, **lo explotará** al máximo, obteniendo acceso a **información crítica** como cuentas válidas, servicios o datos sensibles.

Es común que muchos **servicios no se fortifiquen correctamente**. Por ejemplo, algunos servicios dejan **contraseñas predeterminadas** o **mal configuradas**, lo que los hace **vulnerables**. Sin embargo, aunque algunos administradores aseguren que sus sistemas tienen **contraseñas fuertes** y **actualizaciones constantes**, muchos dejan **agujeros de seguridad** al no proteger adecuadamente otros aspectos del sistema. Esto es lo que se llama una **defensa inadecuada**: un sistema que, aunque parece seguro a simple vista, tiene brechas que los atacantes pueden explotar fácilmente.

Lo que se recomienda en este tipo de situaciones es **pensar como un atacante**. No solo asumir que ciertas áreas están seguras o que no existe un acceso a ciertos servicios. Un atacante, incluso con pocos recursos, puede **buscar cualquier punto de entrada** y explotar **cualquier vulnerabilidad** que encuentre. **Es importante no subestimar** lo que un atacante podría hacer si tiene tiempo y motivación para explorar un sistema.

En cuanto a las herramientas que usamos, debemos estar **informados y ser cautelosos**. Si encontramos un servicio abierto en un puerto desconocido, **probemos** y **analicemos** su funcionamiento. **Conocer el sistema detalladamente** es crucial para prevenir que los atacantes encuentren una brecha. Si no conoces el terreno, te será difícil defenderlo. Además, hay que recordar que el **conocimiento técnico** es clave, y si no sabes algo, **investiga**. La seguridad no es algo que se pueda hacer a ciegas, hay que ser **proactivos**.

En el campo de la **seguridad ofensiva** (como el **pentesting**), la idea es emular las tácticas de los atacantes para probar las defensas de una organización. No se trata de **competir** o de ver quién tiene la mejor técnica, sino de **complementar** las defensas con la ofensiva para mejorar la postura de seguridad. Las **pruebas de penetración** son una forma de **verificar** si las defensas son efectivas, y aunque los resultados pueden ser positivos (sin vulnerabilidades encontradas), siempre es importante recordar que esos resultados son solo **una instantánea en el tiempo**. Es decir, **en el momento de las pruebas** se puede estar **a salvo**, pero eso puede cambiar con el tiempo debido a actualizaciones o configuraciones nuevas.

🔵 Blue Team vs 🔴 Red Team

En ciberseguridad, los equipos **Blue** (defensivos) y **Red** (ofensivos) representan dos enfoques complementarios dentro de la protección de los sistemas informáticos:

- El **Red Team** simula ataques reales para detectar vulnerabilidades, utilizando técnicas como pentesting, ingeniería social o explotación de fallos.
- El **Blue Team**, por su parte, se encarga de defender, detectar intrusiones, reforzar sistemas y responder a incidentes.

Ambos equipos trabajan sobre los **elementos fundamentales de la seguridad de la información**, conocidos como la **tríada CID**:

Por lo tanto, se recomienda que las empresas implementen tanto **equipos de seguridad defensiva (Blue Team)** como **equipos de seguridad ofensiva (Red Team)**. Esto permite realizar ejercicios continuos para mejorar la seguridad. En algunos lugares, estos equipos trabajan juntos para detectar y corregir vulnerabilidades, manteniendo un enfoque equilibrado que ayude a la **mejora continua**.

En cuanto a las **herramientas** y **técnicas utilizadas**, debemos **evaluarlas cuidadosamente** antes de implementarlas. Un **exploit** puede ser útil, pero también puede abrir la puerta a **riesgos adicionales** si no se utiliza correctamente. En resumen, el trabajo de defensa y ataque debe ser complementario, no como una competencia, sino como un esfuerzo conjunto para mejorar la **seguridad** de la organización.

*Las habilidades de un **profesional de seguridad informática** no solo se limitan al desarrollo de programas, pero tener un conocimiento básico de programación **ayuda significativamente**, especialmente cuando se trata de un enfoque más técnico, como en la seguridad **ofensiva** o **defensiva**.*

*En cuanto a las empresas, muchas están adoptando enfoques de seguridad **ofensiva y defensiva** de manera interna. Contratar a un equipo especializado, como un **Red Team** para realizar pruebas de penetración (pentesting) y un **Blue Team** para defender y fortalecer la infraestructura, se ha vuelto una práctica común. Este enfoque permite simular ataques cibernéticos reales para evaluar la efectividad de las defensas de una organización y **fortalecer su seguridad** antes de que un atacante real pueda explotar una vulnerabilidad.*

Sin embargo, muchas veces, las empresas no realizan **pruebas de seguridad adecuadas** antes de lanzar sus aplicaciones al mercado. Durante la pandemia, por ejemplo, muchos servicios fueron lanzados sin las pruebas adecuadas de **calidad** o **seguridad**. La necesidad de **agilizar procesos** debido a las circunstancias llevó a que se lanzaran productos sin haber sido probados en su totalidad. Un caso específico de esta situación fue la **mesa de partes virtual** utilizada durante la pandemia en varios países, la cual fue lanzada sin realizar una revisión de seguridad exhaustiva, lo que resultó en **fallos de seguridad** importantes. Esto resalta la importancia de realizar pruebas de **seguridad** antes de cualquier lanzamiento de producto, aunque no sea posible garantizar al 100% que no haya vulnerabilidades.

El proceso de pruebas de seguridad es **fundamental** para **mitigar riesgos**. No significa que se pueda alcanzar una **seguridad absoluta**, pero las pruebas permiten que las vulnerabilidades sean **detectadas y corregidas** antes de que sean explotadas. Aun así, hay que tener en cuenta que los atacantes no tienen las mismas **limitaciones de tiempo** que los equipos de seguridad. Mientras que los **defensores** tienen un tiempo limitado (como 10, 15 o 30 días) para realizar pruebas de penetración, los **atacantes** pueden pasar meses o incluso años dentro de las redes, **esperando pacientemente** el momento adecuado para atacar. Por lo tanto, los atacantes tienen una **ventaja de tiempo** importante, ya que pueden estar observando y recopilando información sin ser detectados.

El **tiempo de exposición** que los atacantes tienen es un factor crítico.

Además, los **criminales cibernéticos** ahora venden **equipos infectados** a organizaciones, lo que sigue siendo un problema. En términos de **formas de distribución de malware**, ha habido una **evolución**: en el pasado, el malware se distribuyó principalmente mediante **archivos adjuntos** o **virus en correos electrónicos**. Aunque esa forma sigue existiendo, **los canales de distribución** ahora son mucho más variados y accesibles.

*El ataque más común en este contexto es el **keylogging**, que registra lo que se escribe y lo envía al atacante. Esto es preocupante, ya que incluso los sistemas de doble autenticación, como los códigos de verificación enviados por SMS, no son totalmente inmunes a los ataques. Aunque esto mejora la seguridad, aún existen formas de evadirlo.*

El teléfono móvil ha pasado de ser solo un dispositivo de comunicación a convertirse en un objetivo atractivo para los atacantes. Al igual que los keyloggers capturan lo que se teclea en un teclado, también pueden capturar los códigos de autenticación de dos factores (2FA) que se envían al teléfono. De hecho, el robo de teléfonos hoy es mucho más peligroso, ya que pueden obtener acceso a la cuenta bancaria, a las aplicaciones y hasta a datos privados almacenados en el dispositivo.

> *Una de las maneras en las que pueden eludir el doble factor es* ***evadiendo el flujo de la aplicación****. Por ejemplo, si un* ***código OTP*** ***(One Time Password)*** *llega al correo, los atacantes podrían* ***saltarse*** *el paso de autenticación al manipular el flujo de la aplicación, lo que les permite reutilizar el código sin necesidad de entrar en el paso de verificación.*

Es importante **probar y revisar constantemente** las aplicaciones y sistemas para detectar **fallos de seguridad**, como **inyecciones SQL**, **cross-site scripting (XSS)** o **errores en la lógica de negocio** que puedan ser explotados por los atacantes. Estos fallos de seguridad pueden ser **críticos** si no se abordan adecuadamente.

Existen múltiples formas en que los fraudes pueden llegar a nuestras manos. En el caso de las **transacciones bancarias en línea**, muchos bancos ahora **exigen** el uso de sus aplicaciones móviles como una medida de **seguridad adicional**. Aunque algunas personas, como un amigo mío que trabaja en el sector, eran **reacios a realizar transacciones bancarias** en línea, se vio forzado a adaptarse a la **nueva realidad**: usar la **app** del banco. Este tipo de tecnología, aunque ayuda a proteger, también introduce ciertos riesgos, ya que **todos los dispositivos están cada vez más conectados a Internet**, lo que aumenta la superficie de ataque para los ciberdelincuentes.

La conectividad también ha incrementado la **cantidad de servicios**, **aplicaciones** e **infraestructuras** que manejamos a diario, lo que hace que la seguridad sea aún más crítica. Un ejemplo de esto es el **Stuxnet**, un **malware sofisticado** que se utilizó para atacar sistemas industriales, específicamente en una **central nuclear**. Este ataque se dirigió a los **controladores industriales** que gestionan **infraestructuras críticas** como **redes eléctricas**, **agua potable**, y **servicios de comunicaciones**. Estos sistemas, que son esenciales para el funcionamiento de nuestras ciudades, están **interconectados** a través de lo que conocemos como **Internet de las Cosas (IoT)**.

Un aspecto interesante de este ataque es que, aunque el sistema estaba **aislado de Internet**, los atacantes **encontraron formas de infiltrarse** mediante **técnicas no relacionadas directamente con la red**. Este tipo de incidentes subraya la **vulnerabilidad** de los sistemas industriales y cómo la seguridad **no solo depende de Internet**, sino de las **técnicas sofisticadas** que pueden explotarse fuera de las redes tradicionales.

🔐 Principios de la Seguridad de la Información (CID)

TRES PILARES

🔒 Confidencialidad

Los componentes del sistema o la información serán accesibles sólo por aquellos usuarios autorizados.

📜 Integridad

Los componentes del sistema o la información sólo pueden ser creados y modificados por los usuarios autorizados.

🕓 Disponibilidad

Los usuarios deben tener disponibles todos los componentes del sistema o la información cuando así lo deseen.

Ahora, en términos generales, la seguridad se basa en tres pilares fundamentales: **confidencialidad**, **integridad** y **disponibilidad**. Estos son los principios básicos sobre los que descansan todos los sistemas de seguridad. A continuación, explico brevemente cada uno:

- **Confidencialidad**: Este principio asegura que la **información sensible** solo sea accesible a usuarios autorizados. Un ejemplo básico es tu **correo electrónico**; es **confidencial** porque solo tú (o personas autorizadas) debes tener acceso a él.

*Por otro lado, **la confidencialidad** se asegura de que solo las **personas autorizadas** puedan acceder a la información, lo que implica que nadie más, salvo los interesados legítimos, debe poder ver o usar esa información.*

El **requerimiento de confidencialidad** varía según el contexto y la importancia de la información. En cuanto a la **integridad**, esta siempre debe garantizar que los **datos no sean alterados** sin la debida autorización. Por ejemplo, en un sistema de gestión académica, **las calificaciones** solo deben ser alteradas por **personas autorizadas** (como un profesor o administrador).

- **Integridad**: La integridad asegura que los **datos** no se modifiquen o alteren sin la debida autorización. Por ejemplo, si una **universidad emite un certificado digital** de que un estudiante completó un curso, cualquier alteración no autorizada del documento (como cambiar el nombre o la calificación) **pierde la integridad** del documento. La **integridad** de un sistema o dato se refiere a que **no debe ser alterado** sin la autorización de quienes tienen privilegios para modificarlo. Si una modificación es realizada por una persona no autorizada, la **integridad** se pierde y, con ello, también se pierde la **confianza** en el sistema o dato.

  *En el caso de la **integridad**, si un alumno modificara su calificación sin autorización, como por ejemplo alterando un certificado digital o cambiando los datos en un sistema académico, **eso sería una violación de la integridad**. Solo las personas **autorizadas** (por ejemplo, un profesor o administrador) deberían tener la capacidad de modificar esos datos de forma justificada.*

  ***La integridad** garantiza que solo los **usuarios autorizados** pueden alterar o modificar los datos, y que cualquier intento no autorizado de modificación hace que se pierda esa confianza. Por ejemplo, un docente tiene el privilegio de **modificar las notas** de los estudiantes, pero un estudiante no puede hacerlo. Si un estudiante cambia su nota sin autorización, se pierde la **integridad** del sistema.*

- **Disponibilidad**: Este principio asegura que los **sistemas y datos** estén disponibles cuando sean necesarios. Si un sistema de **banco** o **servicio online** no está disponible en el momento de realizar una transacción, **la disponibilidad** se ve comprometida.

  *En cuanto a **disponibilidad**, se refiere a que los **sistemas, componentes e información** deben estar disponibles cuando los usuarios autorizados lo necesiten. Si un sistema debe estar disponible las **24 horas del día** y solo está funcionando de **7 a 3**, entonces no cumple con su **requisito de disponibilidad**.*

  *Sin embargo, si el sistema tiene un **horario de disponibilidad** establecido, como en el caso de algunos **servicios bancarios**, que solo están disponibles durante **horario laboral**, **es aceptable** que no estén disponibles fuera de ese horario. Por ejemplo, un sistema que funciona de **7:00 AM a 3:00 PM** pero que se cae fuera de ese horario no afectaría la disponibilidad **si ese es el requisito** previamente establecido. Es importante entender que **disponibilidad** no significa que un sistema debe estar operativo **todo el***

***tiempo**, sino que debe cumplir con las condiciones establecidas por la organización o el servicio.*

*La **disponibilidad** se refiere a que la **información** y los **sistemas** deben estar **disponibles para los usuarios autorizados** cuando lo necesiten. Sin embargo, la **disponibilidad** no significa que los sistemas deban estar operativos **24/7**. Si un sistema solo necesita estar disponible durante **horario laboral**, y está **caído fuera de ese horario**, no necesariamente se consideraría un problema de disponibilidad. **Lo importante es que esté disponible** cuando los usuarios lo necesiten, según las especificaciones de la organización.*

La clave aquí es que **la disponibilidad debe ajustarse a los requisitos específicos de cada sistema o servicio**, y si no está disponible cuando se requiere según esos parámetros, entonces se considera que **ha fallado** en cuanto a disponibilidad.

Confidencialidad, integridad y disponibilidad son los tres pilares fundamentales de la seguridad informática. Sin embargo, cada uno de estos principios puede variar dependiendo de los **requerimientos específicos de cada organización**. Por ejemplo, en una **universidad**, la **información personal** de los docentes y estudiantes puede no ser tan sensible como la **información de un agente de inteligencia** o de una **agencia gubernamental**. Exponer los datos personales de un **agente de inteligencia** podría tener **consecuencias mucho más graves** que exponer los datos de un docente o estudiante en una universidad.

Además de estos principios fundamentales, hay otros conceptos importantes en la seguridad informática. El primero es que **los atacantes buscan siempre las debilidades del sistema**. No se enfrentan a las **defensas más robustas**; en cambio, buscan las **vulnerabilidades más fáciles de explotar**. Este concepto es similar a lo que ocurre en el ámbito militar, donde los **atacantes** no se enfrentan directamente a la **fortaleza** más fuerte, sino que buscan **puntos débiles** en las defensas.

*Un ejemplo de esto se vio recientemente en un ataque cibernético relacionado con **el Museo del Interior**. En este caso, un **usuario** de trabajo fue la **puerta de entrada** para los atacantes. Los ciberdelincuentes probablemente **explotaron una debilidad humana**, ya sea por **negligencia** o **prácticas inseguras**. A veces, un **usuario** puede ser **engañado** por un **phishing** (un enlace malicioso), o en otros casos, podría ser simplemente por **descuidos** como dejar **sesiones abiertas** o compartir **credenciales**.*

*En el caso de la **Reniec** (Registro Nacional de Identificación y Estado Civil), se **filtraron datos sensibles de ciudadanos** debido a una **mala práctica** de gestión de acceso. A pesar de que el sistema estaba administrado por una entidad gubernamental, el **mala gestión de credenciales** o el uso incorrecto de **APIs** permitió que los atacantes obtuvieran acceso a una gran cantidad de **información personal**. En este tipo de situaciones, el problema no es solo la tecnología, sino también **la gestión de las cuentas** y **el acceso**.*

*En 2021, participé (docente) en una **evaluación de seguridad** de una **aplicación web** del **Ministerio del Interior** para cursos de capacitación. Un error común que vi en muchas páginas*

*del estado es el **ingreso de datos sensibles** sin una **autenticación adecuada**. Por ejemplo, en muchos sistemas se solicita el **DNI** para **validar la identidad**, lo cual es riesgoso si no se cuenta con una **autenticación robusta** y medidas adecuadas de **protección de datos**.*

*En cuanto al consumo de **APIs**, uno de los problemas clave es que a veces **no hay restricciones** en el uso, lo que permite un **consumo indiscriminado** de la información. Por ejemplo, en un caso reciente, se podía hacer un bucle o un script que **extraía datos** de forma masiva, como **DNI** de un rango específico (por ejemplo, del 40101010 al 40909090). Este tipo de vulnerabilidad puede ser muy peligrosa, ya que no había un **control de uso** para limitar la cantidad de datos que se podían obtener.*

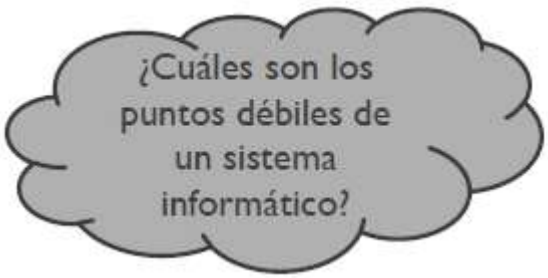
El otro problema en este caso es la **banda ancha** y la **cantidad de información** que se podía recibir, ya que la **API** no solo estaba enviando los datos requeridos, sino también información adicional, como fotos, estados civiles, fechas de nacimiento, direcciones, entre otros, que no eran necesarios para la función principal de la web. **El consumo indiscriminado de esta API** hizo posible que se accediera a toda la **data** personal y sensible de los ciudadanos.

Este tipo de situaciones plantea una gran pregunta: **¿Cómo se están administrando las APIs en las instituciones públicas?** Es fundamental que las **políticas de seguridad** sean implementadas adecuadamente, pero también que **el personal interno** no abuse de su acceso, ya que un solo error o mal uso podría exponer una enorme cantidad de información. Los datos personales son más **valiosos** de lo que se podría pensar, y el problema no solo radica en la **tecnología** o la **configuración del sistema**, sino también en el **factor humano**, como un **empleado que, por error o negligencia**, da acceso a información sensible.

PRINCIPIOS DE LA SEGURIDAD INFORMÁTICA

P1: El intruso al sistema utilizará el artilugio que haga más fácil su acceso y posterior ataque.

Existirá una diversidad de frentes desde los que puede producirse un ataque, tanto internos como externos. Esto dificultará el análisis de riesgo ya que el delincuente aplicará la filosofía del ataque hacia el punto más débil: el equipo o las personas.



El **principio de seguridad** más importante para los atacantes es que siempre **buscarán los puntos débiles**. No se enfrentan a las **defensas más robustas**, sino que intentarán **explotar las vulnerabilidades más fáciles de penetrar**. Este principio también se aplica al ámbito militar, donde los atacantes buscan **romper las líneas más débiles** en lugar de enfrentarse a la **defensa más**

fuerte. En el contexto de la seguridad informática, **las personas** son una de las **vulnerabilidades más comunes**, ya sea por **mala configuración**, **errores de desarrollo** o **exposición de recursos**. Los atacantes, por lo tanto, se van a dirigir siempre hacia lo más fácil de atacar.

P2: los datos confidenciales deben protegerse sólo hasta que ese secreto pierda su valor como tal.

Se habla, por tanto, de la caducidad del sistema de protección: tiempo en el que debe mantenerse la confidencialidad o secreto del dato.

Esto significa que, a medida que pasa el tiempo, ciertos datos pueden perder su valor y, por lo tanto, ya no deben ser tan estrictamente protegidos. Sin embargo, la protección de los datos debe ser **proporcional** a su **valor** en un momento dado.

> *Por ejemplo, en **nuestros dispositivos personales**, como **celulares** o **laptops**, tenemos **información valiosa** que debemos proteger adecuadamente. Esto incluye **cuentas bancarias**, **contraseñas**, **información laboral**, y **datos personales**. Hace solo unos años, los celulares eran utilizados únicamente para llamar o enviar mensajes. Hoy en día, nuestros teléfonos **almacenan toda nuestra vida**: redes sociales, correos electrónicos, compras en línea, datos bancarios, entre otros.*

¿Cómo estamos protegiendo esos dispositivos? ¿Estamos tomando las medidas necesarias para evitar un robo o pérdida de esta información tan sensible?

Protección de datos personales y confidenciales

> *La **protección de la información personal** depende del valor que le asignamos. Por ejemplo, si tienes un celular con información valiosa como **cuentas bancarias** o **informes laborales**, tomarás **medidas de seguridad más estrictas** para protegerlo. Sin embargo, si tu celular solo tiene juegos y mensajes, probablemente no tomes las mismas precauciones, ya que no consideras que esa información tenga **valor significativo**. Esto también se aplica a la **información digital**; si los datos almacenados son valiosos, es necesario **protegerlos adecuadamente**.*

El valor de la información con el tiempo

Un principio clave es que los **datos confidenciales** deben protegerse solo hasta que **pierdan su valor**. Por ejemplo, una tesis universitaria o un informe laboral son activos valiosos mientras aún están en proceso, pero una vez que **finalizas tu título** o entregas el informe, el valor de esos datos disminuye. No significa que ya no sean valiosos, pero la **necesidad de protección** ya no es la misma.

> *Este concepto también se aplica a las **fórmulas** o **secretos industriales**, como la famosa **fórmula de Coca-Cola**. En algún momento, esta fórmula podría perder su **valor estratégico** si se descubre o si ya no es relevante en el mercado, lo que llevaría a la empresa a **reducir los recursos invertidos en protegerla**.*

La información también puede **perder valor** con el tiempo. Un **libro** de texto de la universidad puede ser **extremadamente valioso al principio**, pero a medida que pasa el tiempo y los **contenidos se actualizan**, **pierde valor**. Del mismo modo, las **patentes** de ciertos productos pueden perder valor cuando son **superadas por tecnologías más avanzadas**.

La protección de la información a lo largo del tiempo

Las **empresas y organizaciones** deben entender que la **información** tiene un valor **proporcional al momento** en que se necesita. **Los atacantes** siempre intentarán **robar datos valiosos** que puedan usar para **extorsionar**, **vender**, o **aprovecharse**. Si la información ya no tiene valor, los atacantes no se interesarán en ella.

> Por ejemplo, **una tesis** de un estudiante puede ser valiosa mientras está en proceso, pero una vez que se ha entregado y titulada, **su valor disminuye** para la persona. Lo mismo ocurre con los datos que las **empresas recopilan**. Si la información ya no es útil o relevante, los **atacantes** probablemente no intentarán robarla.

P3: las medidas de control se implementan para que tengan un comportamiento efectivo, eficiente, sean fáciles de usar y apropiadas al medio.

Efectivo: que funcionen en el momento oportuno.

Eficiente: que optimicen los recursos del sistema.

Apropiadas: que pasen desapercibidas para el usuario.

Medidas de control adecuadas

El tercer principio en la seguridad de la información establece que las **medidas de control implementadas deben ser efectivas, eficientes, fáciles de usar y apropiadas para el medio**. Esto significa que las **medidas de protección** deben ser **prácticas y eficaces**. Por ejemplo, en un dispositivo como un **celular**, si lo proteges guardándolo y apagándolo siempre, estarías utilizando una **medida efectiva**, pero **poco práctica**.

*Una **buena medida de seguridad** es **asegurarse de no compartir tu contraseña** o **información sensible** de manera descuidada. En lugar de eso, debes ser **consciente** de tu entorno y tomar precauciones como **usar contraseñas fuertes** y **configurar autenticación de dos factores**.*

En cuanto a las **medidas tecnológicas**, como los **antivirus**, **firewalls** y **antimalware**, estas deben ser **efectivas y actualizadas**. Un **antivirus desactualizado** o un **software con vulnerabilidades** pueden convertirse en la **puerta de entrada** para los atacantes. Un ejemplo claro de esto fue el caso de **FireEye**, una empresa de seguridad cuyo propio software fue utilizado como **caballo de Troya** para infiltrarse en los sistemas de sus clientes.

¿Cómo sabemos si los fabricantes están recopilando datos personales?

Una pregunta que surge con frecuencia es cómo sabemos si un **fabricante de dispositivos** o **software** está recopilando nuestros datos sin que lo sepamos. Por ejemplo, cuando **actualizamos un sistema operativo** o un **software**, ¿cómo sabemos si los **datos personales** que manejamos están siendo enviados a los servidores de la empresa que lo fabrica? En muchos casos, **las empresas** podrían estar recopilando información sobre **cómo utilizamos sus productos**, **qué configuraciones usamos**, o incluso **qué datos cruzamos a través de sus sistemas** para **vender productos adicionales** o simplemente para **comercializar esa información**.

Esto es una **especulación**, pero en la práctica, muchas empresas **tienen la capacidad** de recopilar datos a través de sus **productos conectados**. Por ejemplo, dispositivos como **routers**, **sensores** y otros productos de seguridad están conectados a **servidores centrales** donde los fabricantes pueden analizar datos en tiempo real sobre **ataques** o **comportamientos** de los usuarios. Pero, **¿cómo sabemos que solo están recopilando datos técnicos de la red** y no están recopilando también **información personal** o de la empresa? La **respuesta es difícil** porque muchos de estos productos están diseñados para enviar información de vuelta a sus servidores, y puede que no tengamos **acceso completo** a lo que realmente se está enviando.

*Un ejemplo de esto es **Whatsapp**, que afirma que la **información está cifrada** entre los extremos (usuario a usuario). Sin embargo, el **mensaje pasa por servidores centrales**, lo que genera la pregunta: **¿puede Whatsapp acceder a la información cifrada**? Técnicamente, no deberían poder hacerlo debido al cifrado de extremo a extremo, pero hay un **problema adicional**: algunos gobiernos exigen que los proveedores de servicios de internet, como Whatsapp, tengan la **capacidad de acceder a la información cifrada** por razones de **seguridad nacional**.*

Esto crea un **conflicto** entre la **privacidad** del usuario y los **intereses de seguridad** del gobierno. En este caso, los **gobiernos** pueden solicitar acceso a los datos cifrados para **protegerse de amenazas** (por ejemplo, **terrorismo** o **ataques cibernéticos**). El dilema es que, al garantizar **seguridad** para prevenir **delitos**, se podría estar comprometiendo la **privacidad** de los usuarios, ya que los gobiernos o entidades de seguridad tendrían acceso a toda la información cifrada.

¿Cómo podemos asegurarnos de que nuestra información está protegida?

Es importante **preguntarnos** cómo podemos **garantizar** que nuestras **informaciones personales** no están siendo **recopiladas o mal utilizadas** sin nuestro consentimiento. Aunque las **empresas** implementen medidas de **seguridad**, siempre existe el **riesgo de que** nuestros **datos sean comprometidos** por mal uso, fallas de seguridad, o incluso políticas internas de **monitoreo de usuarios**. La **única manera de asegurarnos** es ser **conscientes de las políticas de privacidad** de las empresas que utilizamos y **aplicar medidas adicionales de seguridad**, como **cifrado personal** o **uso de VPNs**, para proteger nuestras **comunicaciones**.

Privacidad vs. Seguridad: La Confusión y las Implicaciones

La **privacidad** y la **seguridad** son conceptos estrechamente relacionados pero con enfoques diferentes. Mientras que la **seguridad** busca proteger los sistemas de información de posibles ataques y accesos no autorizados, la **privacidad** se enfoca en asegurar que la información personal no sea expuesta o compartida sin el consentimiento del propietario. Un ejemplo de esta tensión entre seguridad y privacidad es el **cifrado de datos**. Si bien muchos servicios afirman que la **información está cifrada**, no siempre podemos estar seguros de que **nuestra información realmente esté protegida** de manera efectiva.

Por ejemplo, **Whatsapp** afirma que sus mensajes están **cifrados de extremo a extremo**. Sin embargo, **hay situaciones en las que incluso los gobiernos pueden exigir acceso a los datos cifrados**, lo que plantea un dilema de privacidad. Si bien los **estados** pueden argumentar que necesitan acceso a los datos por **seguridad nacional**, esto genera una **tensión con la privacidad** de los usuarios. Este conflicto plantea la pregunta: **¿Cómo sabemos si nuestras comunicaciones realmente están protegidas?**

Además, las empresas también tienen la capacidad de **recopilar datos** a través de sus **productos conectados**. Por ejemplo, los dispositivos como **routers** y **sensores** están diseñados para enviar datos a **servidores centrales**. El **problema es que no siempre sabemos qué datos están siendo recopilados** ni si se están **enviando más datos** de los que nos dicen. Este tipo de **recopilación de datos** a veces no está claramente explicado en las políticas de privacidad, lo que deja a los usuarios en la oscuridad sobre cómo se manejan sus **informaciones personales**.

No repudio

Está asociado a la **aceptación de un protocolo de comunicación entre emisor y receptor** (cliente y servidor) normalmente a través del intercambio de sendos certificados digitales de autenticación. (*Jorge Ramió Aguirre -2006*)

Requiere que ni el emisor ni el receptor del mensaje puedan negar la transmisión. (*BORGHELLO, CRISTIAN -2005*)

No Repudio y Autenticidad: Conceptos Clave en Seguridad

Un concepto clave en seguridad informática es el **no repudio**, que se refiere a la capacidad de **garantizar que una persona no pueda negar que ha enviado o recibido información**. Este principio es fundamental para evitar fraudes y malentendidos, especialmente en transacciones electrónicas. Por ejemplo, en el ámbito de **firmas digitales** o **certificados de autenticación**, el **no repudio** asegura que una persona no pueda negar que ha enviado una información o firmado un documento. Esto se logra mediante **certificados digitales** que permiten verificar la autenticidad de la información.

> *Un **ejemplo práctico** de este principio es el **DNI electrónico** o las **firmas electrónicas institucionales**. Aunque las **firmas escaneadas** o **firmas simples en papel** pueden ser fácilmente manipuladas, las **firmas digitales** son más seguras porque están **respaldadas por un sistema de verificación**. **Las firmas electrónicas con un certificado digital** tienen valor legal solo en el entorno digital, y no cuando son **impresas en papel**, ya que el valor está en la verificación de la firma en el sistema digital.*

Autenticidad

Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Contra la autenticidad de la información podemos tener manipulación del origen o el contenido de los datos. Contra la autenticidad de los usuarios de los servicios de acceso, podemos tener suplantación de identidad (MAGERIT v3).

Trazabilidad

Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia. La trazabilidad se materializa en la integridad de los registros de actividad (por ejemplo,logs). (MAGERIT v3)

Trazabilidad: El Registro de Todo lo Que Sucede

La **trazabilidad** se refiere a la capacidad de **seguir el rastro de todas las acciones que ocurren en un sistema**, almacenando **registros o logs** que documentan eventos, acciones y cambios. Estos registros son esenciales para **analizar incidentes**, **detectar ataques** y **aprender de experiencias pasadas**. Por ejemplo, los **logs de seguridad** de un sistema informático permiten a los administradores **ver qué sucedió**, **cuándo ocurrió** y **cómo sucedió**, lo que es crucial para **resolver incidentes de seguridad**.

> *En este contexto, los **logs** también ayudan a las empresas a **perseguir a los atacantes**, identificar vulnerabilidades y aprender de los errores. Sin estos registros, sería mucho más difícil reconstruir un ataque o una intrusión.*

¿Cómo podemos acceder a los registros de seguridad?

Un ejemplo práctico de trazabilidad es el ***registro de eventos en Windows****. Los usuarios pueden acceder a estos logs para ver* ***qué acciones han ocurrido en su sistema*** *y detectar* ***posibles problemas de seguridad****. Estos registros son fundamentales para entender cómo* ***los sistemas operativos*** *manejan la* ***seguridad*** *y cómo reaccionan ante* ***posibles amenazas****.*

Monitoreo de Registros en Windows: *En los sistemas operativos,* ***Windows*** *ofrece una herramienta llamada* ***Visor de Eventos****, que permite acceder a registros sobre lo que está sucediendo en el sistema. A través de esta herramienta, los administradores pueden obtener información sobre* ***errores****,* ***advertencias****,* ***accesos*** *y otros eventos importantes. Sin embargo,* ***el Visor de Eventos*** *a veces contiene una* ***gran cantidad de información*** *que, sin un buen análisis, puede ser difícil de interpretar.*

Problema de Logs en Cortafuegos: *Los* ***logs de cortafuegos*** *en* ***Windows*** *no están activos por defecto. Si un administrador desea saber qué conexiones se han realizado o qué tipo de tráfico ha pasado, debe activar estos logs manualmente. El sistema permite registrar conexiones correctas, paquetes descartados y otros detalles importantes. Es necesario configurar los logs en los* ***perfiles de seguridad*** *de Windows para poder empezar a recopilar esta información.*

El Trabajo Manual y la Solución Automática: *El proceso de revisar los logs manualmente puede llevar mucho tiempo, especialmente si se trata de* ***volúmenes grandes de datos****. Por ejemplo, buscar las* ***IP's de conexión*** *y determinar si están en listas negras o identificar qué sitios web fueron visitados, puede ser engorroso sin herramientas de automatización.* ***Soluciones de monitoreo y análisis*** *como los* ***dashboards*** *pueden ayudar a visualizar esta información de manera más clara y útil, transformando los registros en algo comprensible y fácil de analizar.*

Ataques a los Usuarios y La Importancia de los Logs: *La* ***información de los logs*** *es crucial cuando se busca rastrear ataques, como los que provienen de enlaces maliciosos en correos electrónicos. Saber* ***desde qué dirección IP se originó el ataque*** *o qué* ***conexiones extrañas*** *se realizaron, es fundamental para prevenir futuros incidentes. Los sistemas de registro integrados en Windows permiten obtener detalles sobre* ***autenticaciones****,* ***accesos a carpetas*** *y* ***recursos de red****.*

La Importancia de un Análisis Eficiente: *Los registros de eventos pueden ser* ***abrumadores*** *debido a la cantidad de datos generados, por lo que es esencial tener un sistema organizado y herramientas adecuadas para analizarlos. Las soluciones profesionales como* ***anti-malware****,* ***herramientas de supervisión*** *y sistemas de* ***gestión de registros*** *permiten analizar estos logs de manera más eficiente y proteger así a los usuarios de posibles amenazas.*

AMENAZAS, VULNERABILIDADES Y ATAQUES

Vulnerabilidad, Amenaza y Ataque:

Las **vulnerabilidades**, **amenazas** y **ataques** son conceptos que, aunque a menudo se confunden, son muy distintos y desempeñan roles específicos en la seguridad informática.

1. **Vulnerabilidad**: Una **vulnerabilidad** es una **debilidad interna** en un sistema o activo tecnológico. Puede ser un componente de hardware, software o incluso un error de configuración que deja una brecha que puede ser aprovechada por un atacante. Las vulnerabilidades son inherentes a los sistemas, son parte de su diseño o implementación y son la principal puerta de entrada para un **ataque**. Por ejemplo, puede ser una contraseña mal gestionada o el hecho de que un servidor no tenga actualizaciones de seguridad. Los administradores a menudo descuidan estas vulnerabilidades, dejando contraseñas en texto claro o configuraciones débiles que pueden ser aprovechadas.

2. **Amenaza**: Una **amenaza** es cualquier entidad o agente que **explotará** las vulnerabilidades con el objetivo de hacer daño a un sistema o robar información. La **amenaza** puede provenir de diferentes orígenes, como ciberdelincuentes, hackers, insiders o incluso desastres naturales. En el ámbito informático, las amenazas son externas al sistema pero internas en relación al tipo de activo, como un atacante que intenta penetrar la red de una empresa para robar datos o interrumpir su servicio.

3. **Ataque**: El **ataque** es la acción concreta tomada por una amenaza para **explotar** una vulnerabilidad. Un atacante puede realizar un **phishing**, un **ataque DDoS** o usar alguna otra técnica de intrusión para aprovechar la debilidad de un sistema y acceder a información sensible. Los ataques a menudo apuntan a la **vulnerabilidad** del sistema, aprovechando errores humanos o configuraciones incorrectas.

Principales vulnerabilidades:

A menudo, las **personas** son la mayor vulnerabilidad en un sistema. Los usuarios finales, los administradores y el personal de TI suelen ser el objetivo de los atacantes porque tienen acceso a información sensible o pueden tener configuraciones inseguras, como contraseñas mal almacenadas o sistemas mal protegidos. Un **atacante** no necesariamente buscará un sistema completo para atacar, sino que apuntará a los puntos más **débiles**: la gente que administra esos sistemas o las contraseñas compartidas o mal gestionadas.

Amenazas comunes: En cuanto a las **amenazas físicas**, un ejemplo sería el robo de un equipo de trabajo o la manipulación física de servidores. Los atacantes en este caso se aprovechan de las **vulnerabilidades** físicas de las instalaciones o de la falta de control de acceso.

La importancia de los controles de seguridad: Como se menciona en los ejemplos, los atacantes a menudo se aprovechan de las debilidades más simples, como contraseñas repetidas o mal almacenadas. Los **gestores de contraseñas** y las **prácticas de seguridad** son esenciales para mitigar

estas vulnerabilidades. Además, las **políticas de seguridad** como la gestión adecuada de las sesiones y el uso de autenticación multifactor son cruciales para prevenir el acceso no autorizado.

Resumen:

- Las **vulnerabilidades** son debilidades internas.
- Las **amenazas** son actores externos o internos que explotan esas debilidades.
- Los **ataques** son la ejecución de la amenaza para explotar la vulnerabilidad.

*La clave para mantener un sistema seguro es minimizar las **vulnerabilidades** a través de controles y prácticas de seguridad adecuadas, y estar siempre atentos a las **amenazas** que puedan aprovecharlas.*

AMENAZAS A UN SISTEMA INFORMÁTICO

Las amenzas en el contexto de un sistema informático están relacionadas con los riesgos que corren el software, hardware y datos. Las amenazas son de naturaleza **EXTERNA**.

Vulnerabilidad, Amenaza y Ataque:

Una vulnerabilidad es una debilidad interna en un sistema, un componente o activo tecnológico. Es algo que está presente en el propio sistema, como una falla de configuración o una debilidad en el diseño. Las vulnerabilidades pueden ser aprovechadas por un atacante para explotar esas debilidades y hacer daño. Es posible que esta vulnerabilidad no sea explotada intencionalmente, pero usuarios que desconocen cómo manejar adecuadamente contraseñas o cómo usar una aplicación pueden compartir información sin darse cuenta, creando una oportunidad para los atacantes.

Por ejemplo, si alguien comparte su contraseña con un jefe o colega pensando que está siendo útil, sin saber que esto expone información sensible, se está creando una **vulnerabilidad**. Al hacerlo, la amenaza se concreta: el atacante puede explotar esta vulnerabilidad para obtener acceso no autorizado a datos o sistemas. Esto finalmente se convierte en un **ataque** o incidente de seguridad cuando el atacante utiliza esa vulnerabilidad para hacer daño.

Analogía con la Salud:

Un ejemplo clásico para explicar la vulnerabilidad es el resfriado. Las personas son más vulnerables a resfriarse cuando el clima es frío o lluvioso, pero no todas las personas son igual de vulnerables. Aquellos con un sistema inmunológico más fuerte son menos propensos a enfermarse. Sin embargo, si alguien vulnerable se expone al virus, la amenaza se convierte en un ataque y la persona enferma, lo que es similar a un sistema informático que es vulnerable y es atacado.

Interrupción

Una parte del sistema resulta destruida o no disponible en un momento dado. **Amenazas de Interrupción**: Las amenazas de interrupción afectan la **disponibilidad** de un sistema.

Ejemplos:

- *Destrucción de una componente del hardware*

- *Corte de una línea de comunicación.*

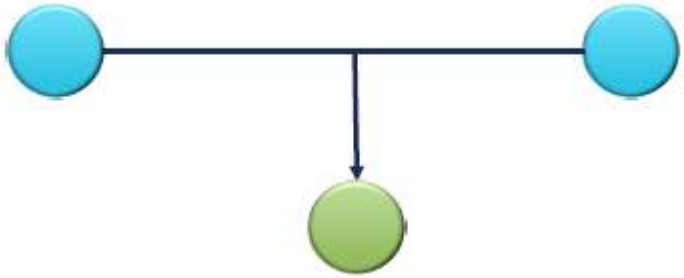
- *Fallas en los sistemas operativos.*

- *Borrado de datos.*

Un ejemplo de esto es cuando un sistema, como un portal académico, se vuelve inaccesible debido a un corte de energía, daño a los discos duros o un ataque DDoS. Esto impide que los usuarios accedan a la información, lo que impacta directamente la disponibilidad de los servicios.

Interrupción: Afecta la **disponibilidad**. Si se corta el acceso a un servicio, el sistema no puede ser utilizado. Por ejemplo, si un servidor se cae o si un sistema no responde por un ataque de denegación de servicio, la disponibilidad se ve comprometida.

Interceptación



Una entidad (persona, programa) no autorizada accede a información, utilizando privilegios no asignados. Dificil detección. **Amenazas de Interceptación**: Este tipo de amenaza es más difícil de detectar. En el contexto de la tecnología, **interceptar** significa espiar la comunicación entre dos partes.

Ejemplos:

- *Sniffing (escucha de datos)*

- *Escuchas de canales telefónicos.*

Por ejemplo, cuando realizas una llamada telefónica o navegas por internet, podrías estar enviando información privada sin saber que alguien está interceptando esos datos. A pesar de que todo parece normal, la información puede ser capturada y utilizada sin tu conocimiento, lo que puede comprometer la seguridad de tus datos. Este tipo de ataque no es fácil de detectar porque no hay alteraciones visibles en la comunicación; todo parece estar funcionando correctamente.

No se está eliminando el ataque, simplemente se está copiando la información. Desde el punto de vista de la red, no pasó nada. Pero en realidad, sí está ocurriendo una **escucha**. Como se mencionó antes, la información se está descifrando, y si existe alguna forma de romper el cifrado y obtener los datos en texto claro, esa es una vulnerabilidad que debe ser considerada. El desafío aquí es que **no todo algoritmo de cifrado** es robusto. Algunos algoritmos criptográficos tienen sus propias debilidades. Pero si se captura información mientras está siendo transmitida y no se nota ninguna alteración, se puede decir que está ocurriendo una **escucha activa**.

El proceso de modificación es más evidente y tangible. Si se altera la información de forma detectable, como en el caso de un cambio en una base de datos, eso es una **modificación**, y **afecta la integridad** del sistema. Esto es un claro ejemplo de vulnerabilidad que afecta directamente a la **integridad**. Si alguien modifica información sin autorización, se compromete la integridad del sistema.

En la **generación** de información, en lugar de modificar datos existentes, se agregan nuevos registros o datos. En un contexto de base de datos, esto podría ser la inserción de registros falsos. Esto también afecta la **integridad** de los datos.

Intercepción: Afecta la **confidencialidad**. Esta amenaza ocurre cuando alguien intercepta la comunicación sin autorización. Por ejemplo, si se están enviando contraseñas a través de un canal inseguro, los atacantes pueden capturar esos datos. Si alguien accede a tu cuenta y obtiene tus credenciales, eso afecta directamente la confidencialidad. Además, si luego se modifican los datos o se borran, se afecta tanto la **confidencialidad** como la **integridad**.

Modificación

Una entidad (persona, programa) no autorizada accede a información, utilizando privilegios no asignados; pero **además, altera o modifica la información o los componentes del sistema.**

Ejemplos:

- Modificación de bases de datos (planillas, cuentas bancarias, etc.)

- Modificación de componentes de hardware. (configuración de puertos de red, tareas programadas, etc.)

Modificación: Es cuando los datos son alterados de manera no autorizada. Esto puede ocurrir a través de un ataque de **modificación** en el que los datos se cambian, afectando directamente la **integridad**.

Generación o Fabricación

Generación de nuevos objetos o datos dentro del sistema o información.

Ejemplos:

- Adición de registros en una base de datos

- Adición de transacciones en una red.

Además de las amenazas mencionadas, también se consideran aquellas que son del entorno, de caracter ambiental.

Cuando se trata de amenazas, hay cuatro tipos generales que afectan la seguridad de un sistema:

Generación: Es la inserción de datos falsos en el sistema. Esto también afecta la **integridad** de los datos.

Los ataques de **interrupción** afectan la disponibilidad de un sistema, los de **intercepción** afectan la confidencialidad, y los de **modificación** y **generación** afectan la integridad de los datos.

*Por último, las amenazas también pueden estar relacionadas con factores **ambientales**, como cortes de energía, humedad, polvo o fuego. Por ejemplo, un corte de energía en el campus puede dañar dispositivos y componentes informáticos. Además, el **uso de software pirata** o **crackeado** también es una amenaza, ya que estos programas pueden contener vulnerabilidades que comprometan la seguridad. Es importante utilizar software legal, como las versiones para estudiantes de algunas herramientas, para evitar riesgos de seguridad.*

Al final, cada componente de hardware y software en un sistema puede estar sujeto a diferentes tipos de amenazas que deben ser gestionadas adecuadamente.

Ejemplos:

Hardware

Humedad, agua, energía eléctrica (picos de voltaje), polvo, fuego.

Software

Borrado accidental o intencionado, copias ilegales, fallas en los discos duros, estática.

Datos

Tiene las mismas amenazas que el software. Pero hay dos aspectos importantes:

- No tienen valor intrínseco (su interpretación, si)

- Datos de carácter personal y privado que las leyes los protegen.

VULNERABILIDADES

Una vulnerabilidad se considera de naturaleza **INTERNA**. Es una debilidad del sistema

Hardware

Politicas de protección débiles. Ambientes inadecuados para los equipos. Componentes de baja calidad o poco confiables.

Software

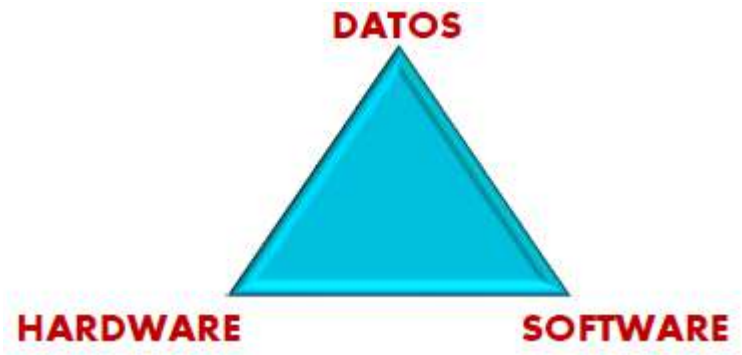
Sistema de licenciacimiento y activación deficiente o no robusto.

Programación deficiente.

Datos

Credenciales de usuarios (constraseñas débiles)

Datos importantes o críticos sin cifrar.



LOS PRIMEROS ATAQUES

¿Cuál es la diferencia entre un virus y un gusano?

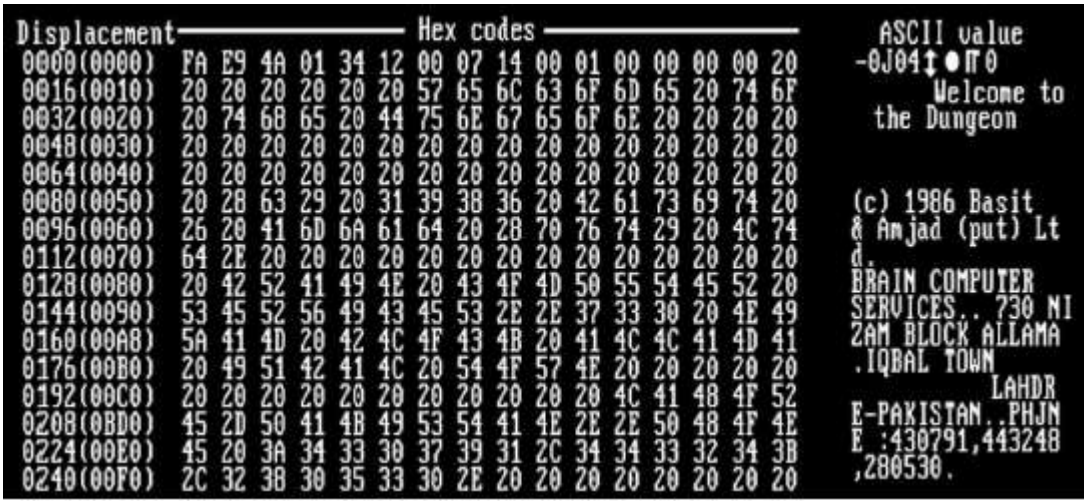
Un virus y un gusano son tipos de **malware**, es decir, software malicioso que hace daño a tu sistema, pero su comportamiento es diferente.

Virus: Un virus necesita un "huésped" para propagarse. Es decir, requiere de un archivo o programa dentro del cual se inserta, y luego se activa cuando el archivo es ejecutado. Estos virus suelen necesitar de la intervención del usuario, por ejemplo, al hacer clic en un archivo adjunto o abrir un documento infectado. Los virus se almacenan en lugares específicos, como discos duros o disquetes, y se activan cuando esos archivos o dispositivos son utilizados.

Gusano: A diferencia del virus, un gusano no necesita un archivo huésped para ejecutarse. Puede propagarse por sí mismo a través de redes, aprovechando vulnerabilidades de los sistemas, y no requiere intervención del usuario. Un gusano puede infectar una red entera sin que el usuario lo note.

Ambos tipos de malware pueden hacer mucho daño, pero su forma de replicarse y propagarse varía.

Primer Virus de PC



Primer virus para plataformas IBM PC (MS-DOS). Creado por dos hermanos de Pakistán (BasitFarooqAlvi y AmjadFarooqAlvi). El virus que crearon infecta el sector de arranque de los *floppydisk*.

Los primeros virus conocidos fueron creados en los años 80. Por ejemplo, el virus "Brain" era uno de los primeros virus para PC y se propagaba a través de disquetes. A medida que avanzó la tecnología, los virus comenzaron a propagar por medio de correo electrónico. Los primeros virus de correo electrónico eran conocidos como **macrovirus** y afectaban documentos de Word, Excel y otros programas de oficina. Los usuarios debían abrir un archivo infectado para que el virus se activara.

Primer Virus por correo electrónico

Melissa Email Virus - March, 1999. Below is the actual email as distributed.

From: ******
Subject: Important Message From ******
To: (50 names from alias list)

Here is that document you asked for ... don't show anyone else ;-)

Attachment: LIST.DOC

El resultado de este virus es el desbordamiento de la memoria en los servidores de correo de Internet. **David Smith** (autor) fue sentenciado a 20 meses en prisión federal y una multa de US$ 5,000.

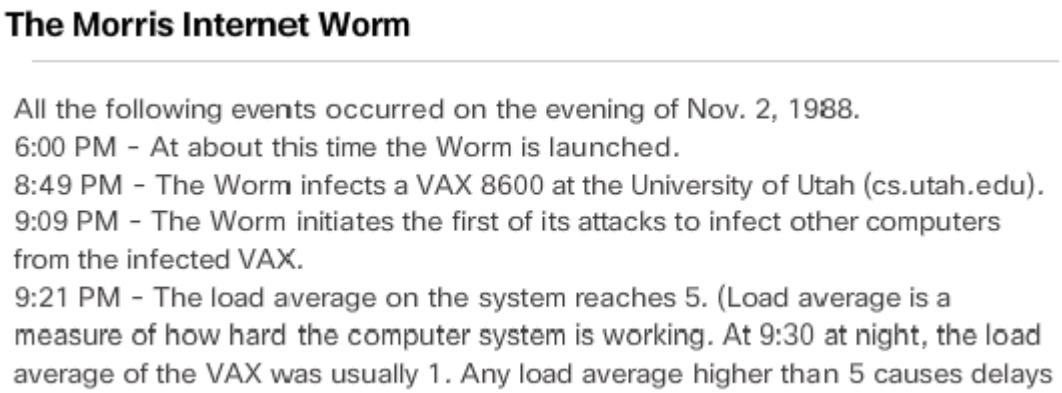
Spam y su evolución

El **spam**, o correo no deseado, también tiene una larga historia. Se empezó a propagar en los años 70 y se refiere a los mensajes masivos enviados con fines publicitarios. Originalmente, el spam se enviaba por correo electrónico, pero con el tiempo ha evolucionado. Hoy en día, el spam no solo se limita al correo electrónico, sino que también se extiende a mensajes de texto, llamadas telefónicas y redes sociales. El objetivo del spam es llenar las bandejas de entrada o los recursos de una red, consumiendo espacio y recursos, lo cual puede afectar el rendimiento del sistema.

El riesgo actual

A medida que avanzan los años, las amenazas digitales como los virus, gusanos y el spam han evolucionado, pero el riesgo de ser víctima sigue presente. La forma en que se atacan los sistemas se hace cada vez más sofisticada. Lo importante es mantenerse informado y protegido para evitar ser víctima de estos ataques.

Primer Gusano


The Morris Internet Worm

All the following events occurred on the evening of Nov. 2, 1988.
6:00 PM - At about this time the Worm is launched.
8:49 PM - The Worm infects a VAX 8600 at the University of Utah (cs.utah.edu).
9:09 PM - The Worm initiates the first of its attacks to infect other computers from the infected VAX.
9:21 PM - The load average on the system reaches 5. (Load average is a measure of how hard the computer system is working. At 9:30 at night, the load average of the VAX was usually 1. Any load average higher than 5 causes delays

Robert Morris creó el primer gusano de Internet con 99 líneas de código. Cuando el Gusano Morris fue puesto liberado, el 10% de los sistemas de Internet se paralizó. Robert Morris fue acusado y recibió tres años de libertad condicional, 400 horas de servicio comunitario y una multa de US$ 10,000

Virus (*viruses*)

Un virus es un software malicioso que se une a otro programa para ejecutar una función específica no deseados en un equipo.

La mayoría de los virus requieren la activación del usuario final y pueden estar inactivos durante un largo período y luego activarse en un momento determinado o en una fecha.

Gusano (*worm*)

Los gusanos son un tipo de código especialmente peligroso. Se replican a sí mismos de forma independiente para la explotación de vulnerabilidades en las redes. Los gusanos generalmente vuelven más lentas las redes.

Mientras que un virus requiere de un programa anfitrión para ejecutarse, los gusanos pueden ejecutarse asi mismos. Ellos no requieren la participación del usuario y pueden extenderse muy rápido sobre la red.

¿Qué es un gusano?

El gusano Morris es un ejemplo clásico. Este gusano fue una de las primeras grandes amenazas que se liberó en 1988 y afectó al 10% de los sistemas en Internet en ese momento. Lo que hacía este gusano era que se **auto-reproducía**. Los gusanos más sofisticados, conocidos como **gusanos mutantes**, eran capaces de modificar su código, lo que los hacía más difíciles de detectar.

A diferencia de un virus, el **gusano no necesita un archivo** o un "huésped" para propagarse. Es autónomo, lo que lo hace más letal. No requiere que el usuario haga nada para que se active. El gusano simplemente se **auto-replica** y se propaga por la red. Esto lo convierte en una herramienta peligrosa, ya que puede infectar múltiples dispositivos rápidamente sin intervención humana.

En términos de **botnets** (redes de dispositivos infectados), el gusano es el encargado de propagar estos dispositivos zombis que luego pueden ser utilizados para ataques de **denegación de servicio**. Es como un ejército de zombies controlados por los atacantes para realizar ataques masivos. Para infectar estos dispositivos, el gusano busca vulnerabilidades específicas en la red, como el puerto 445 en sistemas Windows o ciertas cámaras de seguridad con firmware vulnerable.

El objetivo del gusano no es solo infectar, sino hacer daño a través de la propagación masiva.

Ransomware

En los últimos años, el **ransomware** se ha vuelto cada vez más común. Aunque el principio de ransomware no es algo nuevo (se ha conocido durante más de dos décadas), el aumento de la popularidad se debe a la evolución de **criptografía** y **criptomonedas** como Bitcoin. El uso de criptomonedas hace que el cobro del rescate sea **anónimo**, lo que lo convierte en una opción preferida para los atacantes. Además, los algoritmos de cifrado se han vuelto más robustos, lo que hace más difícil para las víctimas recuperar sus datos sin pagar.

Caballo de Troya (*Trojan Horses*)

Un caballo de Troya en el mundo de la informática es el *malware*que lleva a cabo operaciones maliciosas bajo el disfraz de una función deseada. Un virus o un gusano podría llevar a un caballo de Troya. Un caballo de Troya tiene oculto, el código malicioso que aprovecha los privilegios del usuario que lo ejecuta.

Los Juegos pueden tener un caballo de Troya unidos a ellos. Cuando se ejecuta el juego, el juego funciona, pero en el fondo (segundo plano), el caballo de Troya se ha instalado en el sistema del usuario y sigue ejecutándose después de que el juego ha sido cerrado.

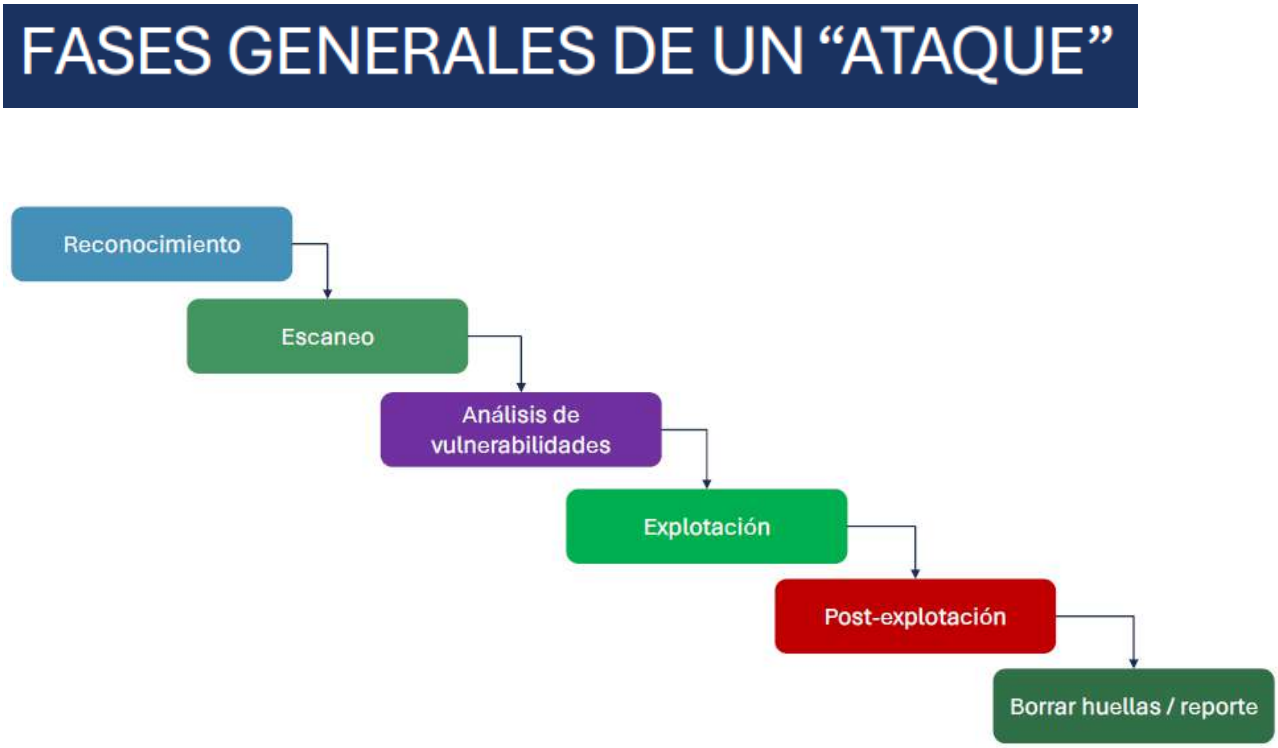
Puede causar daños inmediatos, proporcionar acceso remoto al sistema (una puerta trasera), o realizar acciones con las instrucciones de forma remota, tales como "envíar el archivo de contraseñas, una vez por semana“, etc.

El **caballo de Troya** es otro tipo de ataque que ha existido durante años. Aunque las técnicas y los objetivos han cambiado, la idea básica sigue siendo la misma: un programa aparentemente inofensivo que, una vez ejecutado, permite que otro tipo de malware se infiltre en el sistema de la víctima.

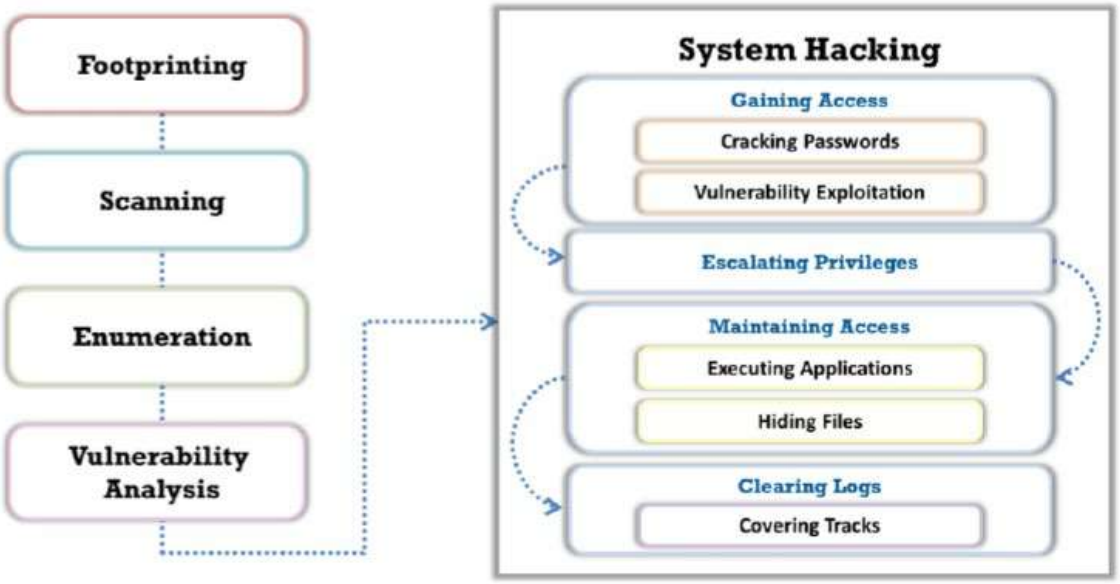
Chistes y precauciones sobre software no confiable

Un ejemplo clásico de este tipo de ataque es cuando utilizamos software de fuentes no confiables o pirateado. A menudo, los usuarios descargan programas aparentemente útiles, como herramientas para descomprimir archivos, pero estos programas pueden estar acompañados de malware o virus que se instalan junto con el software principal. Aunque el software parece gratuito y útil, en realidad está llevando un **"regalito"** no deseado que puede poner en peligro la seguridad de los dispositivos.

Este fenómeno es similar a **el regalo que los griegos hicieron a los troyanos**, donde lo que parecía un obsequio terminó siendo una trampa mortal.



FASES GENERALES DE UN "ATAQUE" – EC-COUNCIL



Fases de un ataque

En general, los ataques informáticos siguen una serie de fases. Los atacantes primero **recopilan información** sobre su objetivo, lo que a menudo implica técnicas de **ingeniería social**. Esta es una de las tácticas más comunes para obtener acceso a sistemas, ya sea a través de la manipulación de empleados, la suplantación de identidad o el uso de fraudes como el phishing.

Cuando los atacantes ejecutan un **ataque controlado** o **ethical hacking**, realizan un proceso metódico que les permite encontrar vulnerabilidades en los sistemas de su objetivo. Esto se realiza para **evaluar la seguridad**, pero también puede ser usado de forma maliciosa para **explotar esas vulnerabilidades**.

¿Qué harían los atacantes al comenzar un ataque?

Lo primero que harían es **buscar vulnerabilidades**. Luego, realizarían un **análisis** y un **planeamiento**. Pero, ¿cómo hacen este análisis? ¿Cómo llevan a cabo el planeamiento? Todo comienza con la recopilación de **información**.

Para poder planificar un ataque o conocer las vulnerabilidades, es esencial tener **información sobre el objetivo**. La recopilación de esta información es la base de todo lo que sigue. El siguiente paso es analizar los activos del objetivo, identificar las vulnerabilidades y luego definir las acciones a seguir. **La primera fase** de cualquier ataque es el **reconocimiento**, que es básicamente buscar información sobre el objetivo.

¿Dónde buscar esta información?

¿Es suficiente con buscar en Internet? **¿Dónde en Internet?** Sí, una parte importante de la información se puede obtener de fuentes públicas en línea, pero no todo está disponible en la red. Hay **información que no está en Internet** y que requerirá un **reconocimiento físico**.

¿Qué implica un reconocimiento físico?

Eso significa ir a las instalaciones del objetivo, observar el entorno, hacer mediciones, verificar si hay cámaras de seguridad, ver quiénes están entrando y saliendo, etc. Es como el trabajo que a veces se muestra en las películas: un trabajo de observación directa.

Aunque Internet es un lugar clave para obtener información, no es suficiente. Además, algunas veces el **reconocimiento físico** es crucial. El **reconocimiento** no debe confundirse con la **ingeniería social**, que es el uso de la información recopilada para manipular a las personas. El primer paso es **reconocer**: es obtener datos sobre el entorno, la infraestructura, la seguridad, y los accesos. Luego, con esa información, se puede proceder a la ingeniería social.

¿Qué información está disponible de nosotros en Internet?

Es posible que algunos de ustedes ya hayan buscado información sobre ustedes mismos en Internet. ¿Han encontrado algo? ¿Sabían que, a menudo, información personal, como sus nombres, direcciones de correo electrónico, etc., están disponibles públicamente? A veces, incluso en bases de datos o páginas que no conocemos, nuestra información puede estar expuesta.

¿Se han buscado a ustedes mismos en Internet? ¿Qué es lo que encuentran cuando lo hacen?

Algunos de ustedes podrían haber descubierto páginas que contienen detalles personales sin saberlo. Es importante ser consciente de qué información sobre ti está circulando en la web, ya que eso puede ser utilizado para un ataque de ingeniería social o incluso para el robo de identidad.

¿Qué hay realmente detrás de las amenazas cibernéticas y cómo podemos protegernos?

Lo que quiero que entiendan es que, así como ustedes han encontrado información personal en Internet, los atacantes también pueden hacerlo. Esto no solo se aplica a individuos, sino también a empresas. Si una empresa no es consciente de la información que está exponiendo, o si los usuarios o empleados no están atentos a lo que están compartiendo, esa información puede quedar expuesta. Si una empresa sigue usando contraseñas comprometidas o información sin protección, eso puede ser aprovechado por atacantes.

¿Cómo se preparan los atacantes?

Ellos buscan vulnerabilidades, recopilan información y esperan pacientemente a que alguien cometa un error. Esta es una de las lecciones importantes: las amenazas siempre están ahí, y los atacantes tienen el tiempo y la paciencia para aprovechar esas vulnerabilidades. De hecho, tanto los buenos como los malos hacen este trabajo, pero los malos lo hacen todo el tiempo.

¿Cómo puede una empresa protegerse?

Es fundamental que las empresas sean conscientes de qué información tienen expuesta y tomen medidas preventivas y correctivas para defenderse. **A veces no podemos eliminar por completo los riesgos**, pero podemos estar preparados para enfrentarlos y mitigarlos de la mejor manera posible.

La importancia de la recopilación de información

El primer paso en cualquier ataque es el reconocimiento, la recopilación de información. Si no conocemos bien la información que está disponible públicamente o la que podría ser vulnerable, no podemos planificar adecuadamente una defensa. La recopilación de datos es fundamental, y tanto los atacantes como los defensores deben estar al tanto de esta fase crítica del proceso.

¿Qué información está disponible de ti en Internet?

Muchos de nosotros no sabemos qué información sobre nosotros está expuesta en la web. Un buen ejercicio es buscar tu nombre en Internet y ver qué aparece. Es posible que encuentres páginas que contienen información personal que no sabías que estaba disponible públicamente. Esto es solo un ejemplo de lo que los atacantes pueden hacer.

El proceso de planificación de un ataque

Una vez que se ha realizado el reconocimiento, el siguiente paso es el escaneo de los activos expuestos a Internet, como servidores, dominios y aplicaciones. Al conocer qué servicios están usando, qué plataformas están expuestas, los atacantes pueden encontrar vulnerabilidades conocidas. Por ejemplo, si descubren que un servidor está utilizando una versión vulnerable de Apache, podrían aprovechar esa vulnerabilidad para explotar el sistema.

Fases del ataque y explotación de vulnerabilidades

El siguiente paso después de encontrar las vulnerabilidades es **explotarlas**. Si un atacante puede aprovechar una vulnerabilidad, tomará el control de la máquina o el dispositivo afectado. A partir de ahí, puede intentar expandir su acceso a otros sistemas o servicios. Este proceso se llama **post explotación**, y consiste en obtener información valiosa, como credenciales de acceso o datos confidenciales, lo que puede llevar a un mayor daño.

El daño posterior y la limpieza de huellas

Cuando un atacante ha explotado una vulnerabilidad, lo que sigue es el intento de eliminar cualquier rastro de su presencia. Los atacantes suelen limpiar los registros, borrar archivos y ejecutar scripts para cubrir sus huellas. Sin embargo, a veces, aunque intenten borrar todo, algunos rastros pueden quedar, como archivos o códigos maliciosos que pueden ser detectados posteriormente.

Proceso de Reporte y Recomendaciones en Ciberseguridad

En este proceso, el reporte es crucial. El cliente necesita entender **cómo se explota una vulnerabilidad**, cómo afecta a su sistema y cómo puede solucionarlo. El valor agregado de las actividades específicas de hacking es, principalmente, la recomendación y solución al cliente. Un buen pentester no solo demuestra cómo explotar la vulnerabilidad, sino que también ofrece una solución que el cliente pueda implementar para protegerse.

Es esencial que el **reporte incluya recomendaciones**. En muchos casos, las empresas prefieren que se descubra una vulnerabilidad durante un ejercicio controlado, como un pentesting, en lugar de

ser explotada por un atacante real. Por eso, es importante reportar todos los hallazgos y las soluciones propuestas.

Fases del Reconocimiento y Explotación

1. **Reconocimiento y Enumeración**
   El proceso de reconocer un puerto, como el **443** (HTTPS), es parte del reconocimiento inicial. La numeración de puertos y la identificación de vulnerabilidades específicas es clave para el análisis de un sistema. Por ejemplo, enumerar las versiones de los servidores, comprobar las cabeceras de los servicios y las configuraciones puede revelar debilidades.

2. **Explotación y Post Explotación**
   Una vez que se identifica una vulnerabilidad, el siguiente paso es explotarla. Esto se refiere a obtener acceso al sistema, escalar privilegios y **mantener el acceso**. Mantener el acceso significa buscar alternativas que permitan continuar la conexión, incluso si se detecta una y se corta. Esto es crucial para los atacantes, ya que necesitan tener múltiples formas de ingresar y no depender de una sola vía.

3. **Limpieza de Huellas**
   El proceso de limpiar huellas implica borrar cualquier rastro que deje el atacante, como scripts o archivos creados durante la explotación, para evitar ser detectado.

Fuentes y Certificaciones

Es importante basarse en fuentes confiables para obtener información sobre vulnerabilidades y ataques. Algunas fuentes recomendadas son:

- **Talos** (de Cisco)
- **White Hat** (comunidad de seguridad ética)
- **Self** (seguridad informática)
- **ZGM** (noticias y posts sobre ciberseguridad)

Para quienes están investigando certificaciones, es útil consultar fuentes como **SANS**, **ISEE**, y **IBCS**, que proporcionan guías y recursos sobre metodologías de seguridad y análisis de vulnerabilidades.

Clasificación de Vulnerabilidades y Ataques

Es necesario saber clasificar la gravedad de una vulnerabilidad o ataque. Algunos ataques son **críticos**, otros son **medianamente críticos**, y algunos solo son **informativos**. La clasificación depende de factores como el impacto potencial, la facilidad de explotación y la presencia de

mitigaciones. La metodología para determinar estas categorías se basa en marcos de trabajo como **CVSS (Common Vulnerability Scoring System)** y otros estándares de la industria.

Principios de la Seguridad Informática (SI)

Para evaluar un ataque o incidente, se utilizan principios y métricas basadas en sistemas como **CUCCUSS**. Estos sistemas asignan un valor a cada vulnerabilidad encontrada, evaluando aspectos como la complejidad de la red, la interacción con el usuario, los cambios en el alcance, y los impactos en la confidencialidad y disponibilidad.

Por ejemplo, al evaluar un ataque, se pueden usar escalas para determinar si la vulnerabilidad es alta, media o baja, dependiendo de factores como:

- **Complejidad de la red**: baja o alta
- **Interacción con el usuario**: si es necesaria o no
- **Impacto en la confidencialidad y disponibilidad**: alto, medio o bajo

Estas métricas se basan en documentación detallada y ayudan a calificar las vulnerabilidades encontradas. Si una vulnerabilidad tiene una puntuación alta (por ejemplo, de 8 a 9), se considera crítica y es una prioridad a resolver.

Además, **SANS** es una empresa norteamericana que provee recursos y certificaciones en seguridad informática. Ofrecen materiales y servicios tanto privados para empresas como recursos públicos para la comunidad. Sus certificaciones son algunas de las más caras en el mercado, con cursos que pueden costar entre 5000 y 7000 dólares por un curso de 24 horas.