Resumen Teórica 1 : Introducción

Tomás F. Melli

August 2025

Índice

1 Conceptos generales

- **Información** : la información se refiere a toda comunicación o **representación de conocimiento como datos** en cualquiera de sus formas (textuales, numéricas, gráficas, cartográficas, narrativas o audiovisules) y **en cualquier medio**, que puede ser magnético, en papel, audiovisual, entre otros.
  A forma de ejemplo, consideramos información a documentos, informes, archivos, comunicaciones, sistemas, datos personales, claves, entre otros datos relevantes.

- **Seguridad de la información**: es la **preservación** de los siguientes **tres pilares**

  1. **Confidencialidad** : se garantiza que la información sea accesible sólo a aquellas personas que están autorizadas a tener acceso a la misma.
     A modo de ejemplo, cifrar una declaración de impuestos no permite que nadie la lea. Si el dueño quiere leerla, deberá descifrarla con su clave que sólo él tiene. Sin embargo, si por algún motivo alguien que no es el dueño tiene esa clave para descifrar la declaración de impuestos, *su confidencialidad ha sido comprometida.*
  2. **Integridad**: se resguarda la exactitud y totalidad de la información y los métodos de procesamiento. La integridad incluye la integridad de los datos (el contenido) y el origen de los mismos.
     Veamos un ejemplo, un diario puede dar información que obtiene de la casa rosada pero atribuirla a una fuente incorrecta. En este ejemplo, la *integridad de origen es corrupta.*
     Mirando la definición, nos dice algo sobre *los métodos de procesamiento*, miremos el siguiente ejemplo, tenemos un sistema bancario que calcula intereses, por tanto tiene, datos (los saldos de las cuentas) y métodos de procesamiento (algoritmo para calcular interés). La idea es que para preservar la integridad de los datos, nadie sin permisos debería modificarlos y tampoco el algoritmo que realiza el cálculo.
  3. **Disponibilidad**: se garantiza que sólo los usuarios autorizados tengan acceso a la información y a los recursos asociados a la misma, toda vez que lo requieran (en todo momento).
     Ejemplo : es el último día de inscripciones en la facu y se produce un corte de luz que se extiende durante todo el día. Las UPS (Uninterruptible Power Supply) funcionan durante 2 horas y luego apagan los servidores. Como consecuencia, los alumnos rezagados no se pueden inscribir.

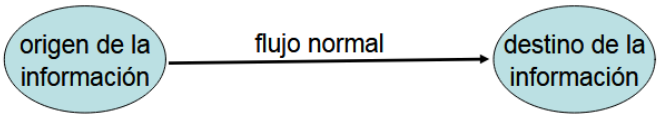
- **Vulnerabilidad** : una vulnerabilidad es una debilidad en un activo. Esto quiere decir, que una vulnerabilidad es un punto débil a partir del cuál se puede atacar a un sistema. El activo es justamente ese componente del sistema, como puede ser el hardware, software, personas, procesos, redes, entre otros.

- **Amenaza** : es una **potencial violación** de la seguridad. No es necesario que ocurra, pero sí que esté ahí como a la espera. Estas amenazas **"explotan"** vulnerabilidades. Por tanto, siempre hay que estar preparado para las acciones que podrían causar dichas violaciones.

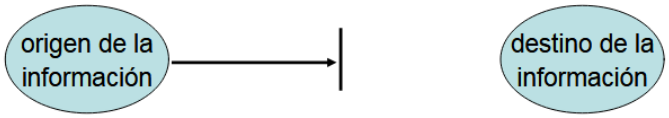
- **Ataques** : son las acciones que ejecutan los **atacantes o intrusos** para explotar las vulnerabilidades de un sistema.

2 Tipos de Amenazas

A partir del flujo normal de la información podemos representar distintas situaciones

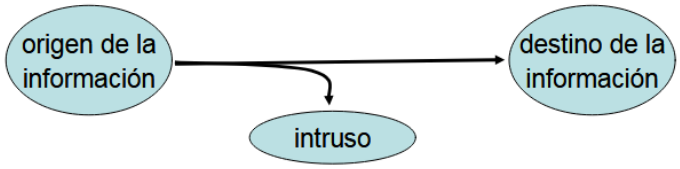


2.1 Interrupción del flujo de información



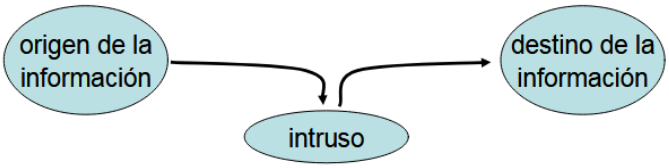
Que puede darse por la destrucción del recurso, algún bloqueo o saturación del mismo. Esto es los que comunmente nos referimos como una **amenaza a la disponibilidad** de la información.

2.2 Intercepción de la información



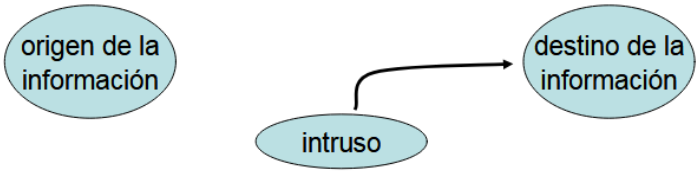
Sucede cuando se realiza un acceso no autorizado al recurso, cuando se realiza un monitoreo de la información (alguien que observa información sin permiso), o puede darse en casos de ingeniería social (no es una falla técnica sino que el intruso se aprovecha de la confianza de las personas (se hace pasar por otro por ejemplo)). En estos escenarios es que consideramos una **amenaza a la confidencialidad** de la información.

2.3 Alteración de la información



Ocurre cuando el intruso modifica el recurso. Es un caso de **amenaza a la integridad** de la información.

2.4 Fabricación de la información



Se dan en los casos en que el intruso incorpora información en un sistema con la intención de hacerlos parecer legítimos. Un ejemplo típico es el **phishing** que se da cuando el atacante crea un mensaje (mail o SMS) que simula ser de una fuente confiable para engañar al usuario. Estos son casos claros de una **amenaza a la autenticidad** de la información.

2.5 Amenazas pasivas (espionaje)

Existen otros tipos de amenazas como las **pasivas** en las que el atacante **observa, recopila o analiza** información pero **no modifica ni interfiere directamente con los sistemas o datos**. Generalemente son muy difíciles de detectar, y dependen del medio físico de transmición (redes cableadas, wifi,...). El objetivo principal es **amenazar la confidencialidad** de la información. Los ejemplos clásicos son **sniffing** (el intruso "escucha" el tráfico de una red para capturar información) y el **Side Channel Attack** (consiste en un atacante que no mira los datos directamente sino sus características secundarias como los tiempos de respuesta (servidor), consumo energético, ...).

2.6 Amenazas activas

En este tipo de amenazas, el intruso **interviene en los sistemas o en la información**, provocando alteraciones, interrupciones o insertando información. Como consecuencia, son más fáciles de detectar ya que los efectos son visibles. Tenemos varios ejemplos :

- **Keylogger** (captura de información) : suele ser un programa o dispositivo que **registra cada tecla que se presiona**. La idea del atacante es robar credenciales de cierto usuario cuando inicia sesión.
- **Spoofing** (suplantación de identidad) : ocurre cuando el atacante se hace pasar por otra persona o sistema. Normalmente el atacante lo hace con un correo que aparenta ser de un banco o a través de la falsificación de la IP/MAC.
- **Replay Attack** (retransmisión de mensajes) : consiste en capturar mensajes legítimos y reenviarlos más tarde para engañar al sistema. La típica es volver a enviar una orden de transferencia bancaria ya procesada.

- **Tampering** (falsificación de datos) : alterar la información transmitida o almacenada. El atacante lo que hace es cambiar un paquete en tránsito o modifica algún archivo en una base de datos.
- **Port Scanning** (escaneo de puertos) : es una técnica para descubrir los servicios abiertos en el sistema.
- **Exploit** (aprovechamiento de software vulnerable) : usar un código o técnica para aprovechar un bug o debilidad en un programa.
- **Man in the Middle** (intercepción activa) : el atacante se posiciona en el "medio" de la comunicaci+ ´ón, interceptando, alterando o inyectando datos.
- **DoS / DDoS (Denial of Service o su versión Distributed)** : la idea del atancante es saturar un sistema con solicitudes falsas para que no pueda atender a usuarios legítimos. La típica son millones de bots bombardean un sitio web con tráfico.

2.7 Origen de las amenazas

Las amenazas las podemos clasificar según la **intención** y el **lugar de origen**.

2.7.1 Según la intención

- **Intencionales** : son aquellas en las que el atacante deliberadamente busca causar daño o aprovecharse del sistema. Como un empleado que borra archivos de forma maliciosa, un hacker que roba info de tarjetas de crédito,...
- **Accidentales** : son aquellas en las que no hay intención de dañar, pero se generan consecuencias como un corte eléctrico, un usuario que borra un archivo por error, un administrador que configura mal un firewall y deja expuesta la red,...

2.7.2 Según el origen

- **Interno** : surge dentro de la organización, de personas con acceso legítimos (como un empleado que copia datos confidenciales o una mala configuración hecha por el personal de IT).
- **Externo** : desde fuera de la organización como un virus que llega por correo por ejemplo.

3 Políticas y Mecanismos

Existen formas de reducir riesgos, proteger la confidencialidad integridad, autenticidad y disponibilidad de la información y evitar pérdidas económicas de una organización. Estas son :

3.1 Política de seguridad

Es una declaración de lo que está permitido y lo que no. Es decir, un conjunto de reglas y objetivos que una organización define para proteger su información y sistemas. Define quién tiene acceso, cómo se manejan los datos. El objetivo es que sea clara, conocida y aplicada por todos en la organización. Es el **qué se quiere lograr**

3.2 Mecanismo de seguridad

Es una herramienta, técnica o procedimiento concreto para hacer cumplir una política de seguridad. Es el **cómo se logra lo definido en la política de seguridad**. No necesariamente son técnicos. Se pueden aplicar mediante software, hardware u otros procesos.

4 Obejetivos de la Seguridad

4.1 Prevención

Significa que el ataque fallará. Ejemplo : si uno intenta entrar a un sistema a través de nternet, pero el mismo no esta conectado a dicha red, el ataque fue prevenido.

4.2 Detección

Puede ser usado cuando un ataque no puede ser prevenido, o para medir la efectividad de los mecanismos de prevención. Los mecanismos de detección dan por hecho que un ataque va a ocurrir, y su objetivo es reportar los ataques que se produzcan.

4.3 Recuperación

Luego de producido un ataque, se procede a detenerlo. Se debe determinar y reparar daños. Volver a operar correctamente. Ejemplo: Si un atacante borrá un archivo, se puede recuperar el mismo de los back-ups.

5 Cuestiones Operacionales

Cualquier política y mecanismo útil deben balancear los beneficios de la protección con el costo del diseño, implementación y utilización del mecanismo.
Este balance puede ser determinado analizando los riesgos y la probabilidad de ocurrencia.
Ej: Una base de datos provee la información de salario de los empleados de una empresa, y es utilizada para imprimir los cheques. Si dicha información es alterada, la compañia puede sufri graves perdidas financieras. Por eso, es claro que se deben utilizar mecanismos que permitan garantizar la integridad de la información. Sin embargo, si tenemos un segundo sistema que copia diariamente dicha base de datos a cada filial, para que tenga valores de referencia a la hora de contratar nuevo personal (la decisión es de la casa central), la necesidad de mantener la integridad en cada filial no es tan alta.

6 Leyes

Las leyes restringen la disponibilidad y el uso de la tecnología y afectan los controles y procedimientos.

- Restricciones a la exportación de software criptográfico en EEUU, año 2000.
- Ley 25.506 de Firma Digital.
- Ley 25.326 Protección de Datos Personales
- Ley 26.338 Délito Informático
- Ley 27.411 Convenio de ciberdelito (Budapest)
- Ley 27.699 Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal

Toda política y sus mecanismos asociados deben tener en cuenta consideraciones legales.

7 Evaluación de riesgos

Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria de la organización.

8 Cuestiones Humanas

Es complejo implementar controles de seguridad informática, y en una organización grande los controles pueden volverse vagos o incómodos.
Si se los configura en forma inadecuada o se los usa incorrectamente, hasta los mejores controles de seguridad se vuelven inútiles y hasta en algunos casos peligrosos.
Personal no entrenado puede ser una amenaza para la seguridad de un sistema. Ej: Un operador que no sabe que debe verificar el contenido de los backups antes de almacenarlos.
El entrenamiento necesario no solamente es técnico. Muchos ataques exitosos provienen del uso de la Ingeniería Social. Si los operadores cambian las claves de acceso a través de pedidos telefónicos, todo lo que un atacante necesita es saber el nombre de uno de los usuarios del sistema y hacer un llamado.