



SEGURIDAD01



“El único sistema seguro es aquel que está apagado y desconectado, enterrado en un refugio de cemento, rodeado por gas venenoso y custodiado por guardianes bien pagados y muy bien armados. Aún así, yo no apostaría mi vida por él”.



Eugene Spaffrord

Importancia de la Seguridad Informática

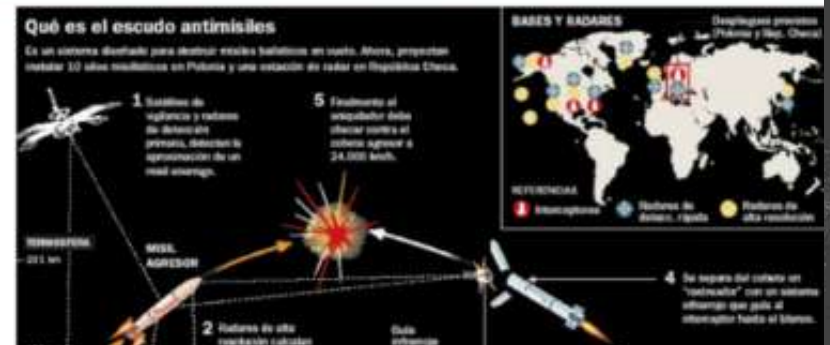
La afirmación de que ahora todo está controlado por ordenadores es cierta:

- Cuentas bancarias
- Comercio internacional
- Plantas de energía eléctrica
- Ejército
- Satélites
- Sistema judicial
- Sistema sanitario
- ...

Ataques a la bolsa

EUROPA		
Nombre		Puntos
IBEX 35	▲	11.148,90
BEL 20	▼	3.220,18
DAX	▲	9.747,02

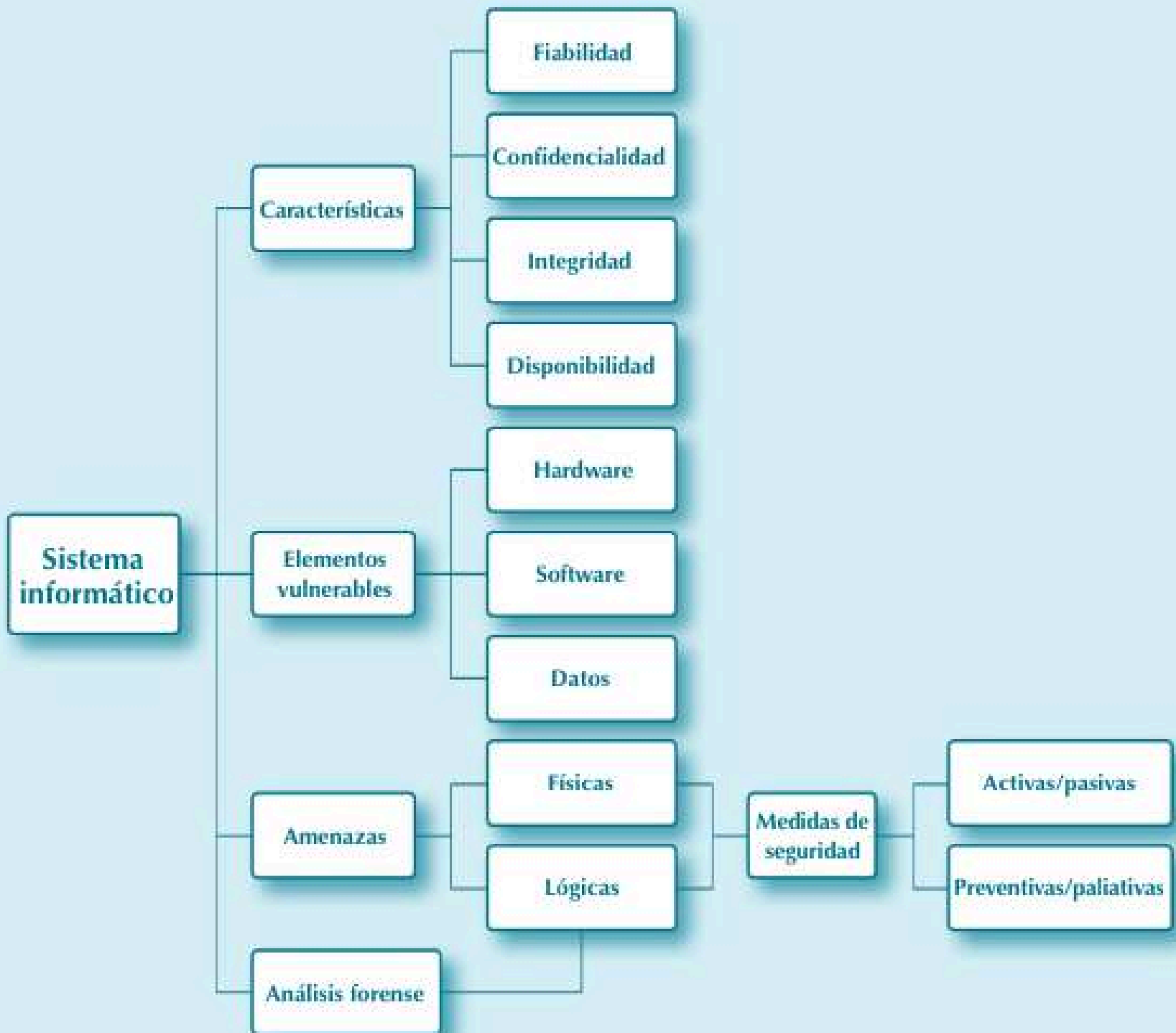
Ataques a sistemas de misiles

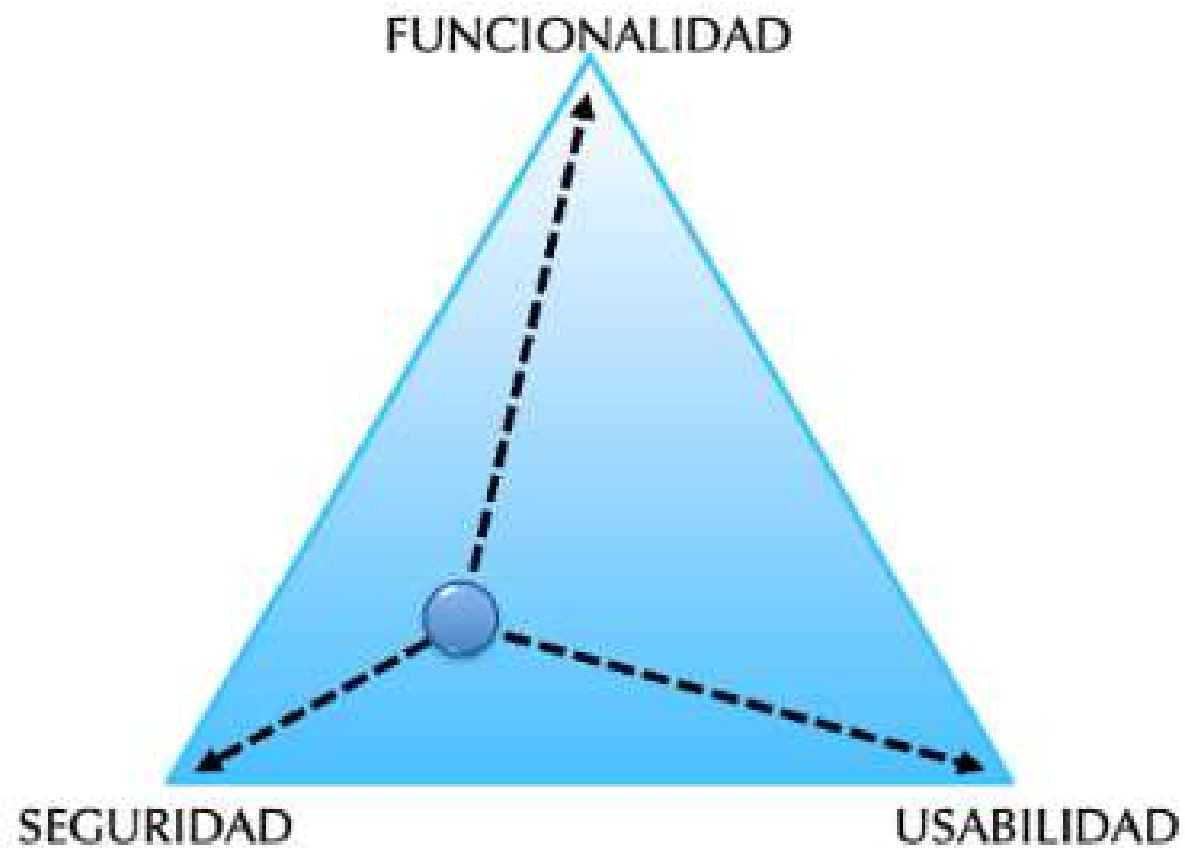


Conclusiones!!!



- La **Protección** de los sistemas y redes de computadoras es, por tanto, **crítica**.
- La estrategia actual es adoptar **medidas preventivas** para adelantarse al atacante.
- Tenemos que asegurar la **infraestructura**, la **información** y las **comunicaciones**.





La paradoja de la seguridad

DEFINICIÓN DE CIBERSEGURIDAD, SEGURIDAD INFORMÁTICA Y SEGURIDAD DE LA INFORMACIÓN

CIBERSEGURIDAD

Es la **práctica de defender**, con tecnologías o prácticas ofensivas, las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos **de ataques maliciosos**.

SEGURIDAD INFORMÁTICA

Es la disciplina que se encarga de **proteger la integridad y la privacidad** de la información almacenada en el sistema informático de ciberdelinquentes.

SEGURIDAD DE LA INFORMACIÓN

Es el conjunto de **medidas preventivas y reactivas** que afectan al tratamiento de los datos almacenados y que permiten almacenar y proteger la información.



¿Qué es la Ciberseguridad?

La ciberseguridad es la **práctica de proteger la infraestructura tecnológica (sistemas, redes, aplicaciones, datos...)** de posibles **amenazas digitales**

Las organizaciones tienen la responsabilidad de proteger la infraestructura para mantener la confianza del cliente y cumplir diferentes normativas

Para lograrlo se implementan diferentes procesos, controles y herramientas de seguridad



Blue Team vs Red Team vs Purple Team

Blue Team: Están orientados a Ciberseguridad defensiva. **Establecen y mantienen las medidas de seguridad necesarias para proteger la infraestructura tecnológica** de una organización

Red Team: Están orientados a Ciberseguridad ofensiva. **Su objetivo es probar la eficacia de las medidas de seguridad implementadas por el Blue Team.** Para ello, simulan las acciones llevadas a cabo por atacantes reales sobre la infraestructura tecnológica de una organización. El objetivo no es causar daño, sino identificar debilidades que necesiten ser abordadas

Purple Team: Combina los roles de Red Team y Blue Team. Su objetivo es **asegurar que el Blue Team aprenda de las técnicas y tácticas utilizadas por el Red Team** y mejore las medidas de seguridad correspondientes. En lugar de trabajar de manera confrontativa, el Purple Team tiene como objetivo promover la colaboración y el aprendizaje conjunto

Triada CIA (Confidencialidad, Integridad, Disponibilidad)

La triada CIA (Confidencialidad, Integridad, Disponibilidad) ha sido la base de la Ciberseguridad durante mucho tiempo

Estos principios básicos **se utilizan como un marco para guiar las políticas, prácticas y controles de Ciberseguridad que se establecen en un entorno tecnológico**



Triada CIA | Confidencialidad

El concepto de confidencialidad se refiere a la **capacidad de garantizar que la información no se encuentra disponible o es revelada a individuos que no tienen autorización para consultarla**

Deben aplicarse una serie de controles, que aseguren que se cumplen afirmaciones como las siguientes:

- La información almacenada en un sistema de información no puede ser consultada por error o de manera intencionada sin la autorización de quien la ha almacenado
- La información que se transmite desde un punto A a un punto B, no puede ser consultada por error o de manera intencionada sin la autorización de quien la ha transmitido



Triada CIA | Integridad

El concepto de integridad se refiere a la **capacidad de garantizar la exactitud y completitud de la información a lo largo de todo su ciclo de vida**

Deben aplicarse una serie de controles, que aseguren que se cumplen afirmaciones como las siguientes:

- La información almacenada en un sistema de información no puede ser modificada por error o de manera intencionada sin el conocimiento de quien la ha almacenado
- La información que se transmite desde un punto A a un punto B, no puede ser modificada por error o de manera intencionada sin el conocimiento de quien la ha transmitido



Triada CIA | Disponibilidad

El concepto de disponibilidad se refiere a la **capacidad de garantizar que la información se encuentra disponible siempre que se requiere** acceder a ella

Deben aplicarse una serie de controles, que aseguren que se cumplen afirmaciones como las siguientes:

- La información almacenada en un sistema de información debe poder ser accesible siempre que sea necesario




Triada CIA | ¿Es suficiente?

Autenticación: es el **proceso de verificar la identidad de un usuario**. Cuando un usuario intenta acceder a un recurso o servicio, se le solicita que proporcione credenciales, como un nombre de usuario y contraseña. Estos datos se comparan con la información almacenada en el sistema. Si coinciden, el proceso de autenticación ha sido exitoso y el usuario es reconocido por el sistema como legítimo.

Autorización: es el proceso que **sigue a la autenticación**. Una vez que el sistema ha autenticado la identidad de un usuario, el siguiente paso es **determinar qué recursos puede acceder y qué acciones puede realizar**. Esto se logra a través de políticas de autorización que definen los derechos de acceso de un usuario.

No repudio: se refiere a la capacidad de garantizar que, **cuando se realiza un intercambio de información, el receptor de la información no puede negar haberla recibido**, y el emisor de la información no puede negar haberla enviado.



AUTENTICACIÓN \neq AUTORIZACIÓN



- Usuarios y grupos de usuarios
- Listas de control de accesos (ACL, *Access Control List*)

Verificación en dos pasos

Además de precisar del usuario algo que conoce (la contraseña), también se requiere algo que posee (el teléfono móvil).



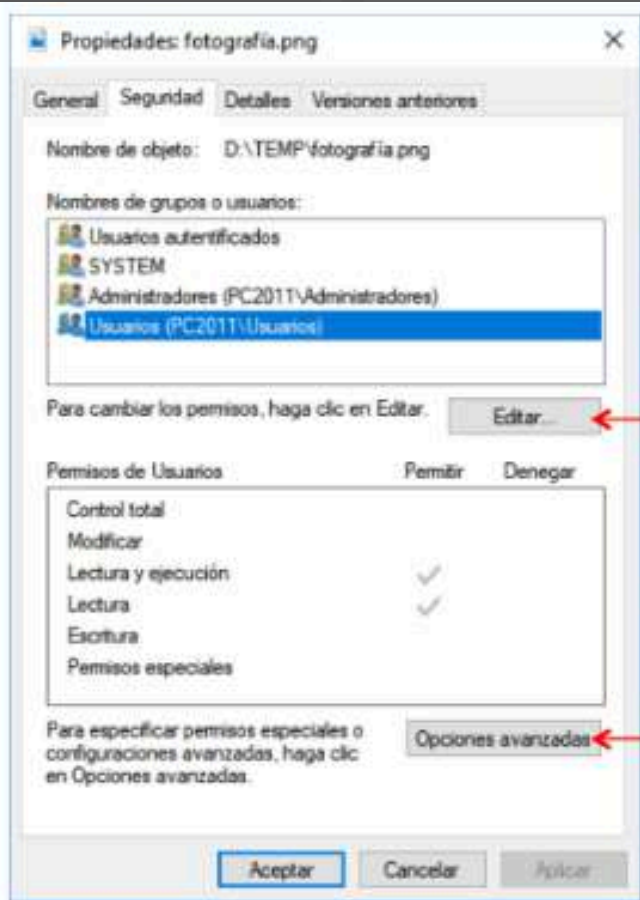
Verificación en dos pasos (2FA)

Permisos avanzados

- Lectura
 - Entrar en carpeta / ejecutar fichero
 - Listar carpeta / leer fichero
 - Leer atributos
 - Leer permisos
- Escritura
 - Crear ficheros en carpeta / escribir datos
 - Crear carpetas / anexar datos
 - Escribir atributos
 - Eliminar subcarpetas y ficheros
 - Eliminar carpeta / fichero
- Administración
 - Tomar posesión
 - Cambiar permisos
- Control total: todo lo anterior.



Protocolo U2F/FIDO2.



- Fichero sobre el que estamos definiendo permisos
- Grupos (y usuarios) con algún tipo de permiso para acceder al fichero
- Botón que nos permite alterar los permisos, ya que el cuadro de diálogo actual solo permite consultarlos
- Permisos asignados al grupo/usuario arriba seleccionado
- Además de cambiar permisos, como el botón *Editar*, puede cambiar el propietario del fichero y llegar a mayor nivel de detalle en los permisos

ACL en Windows



Permisos en Linux

Tipos de amenazas

➤ Físicas:

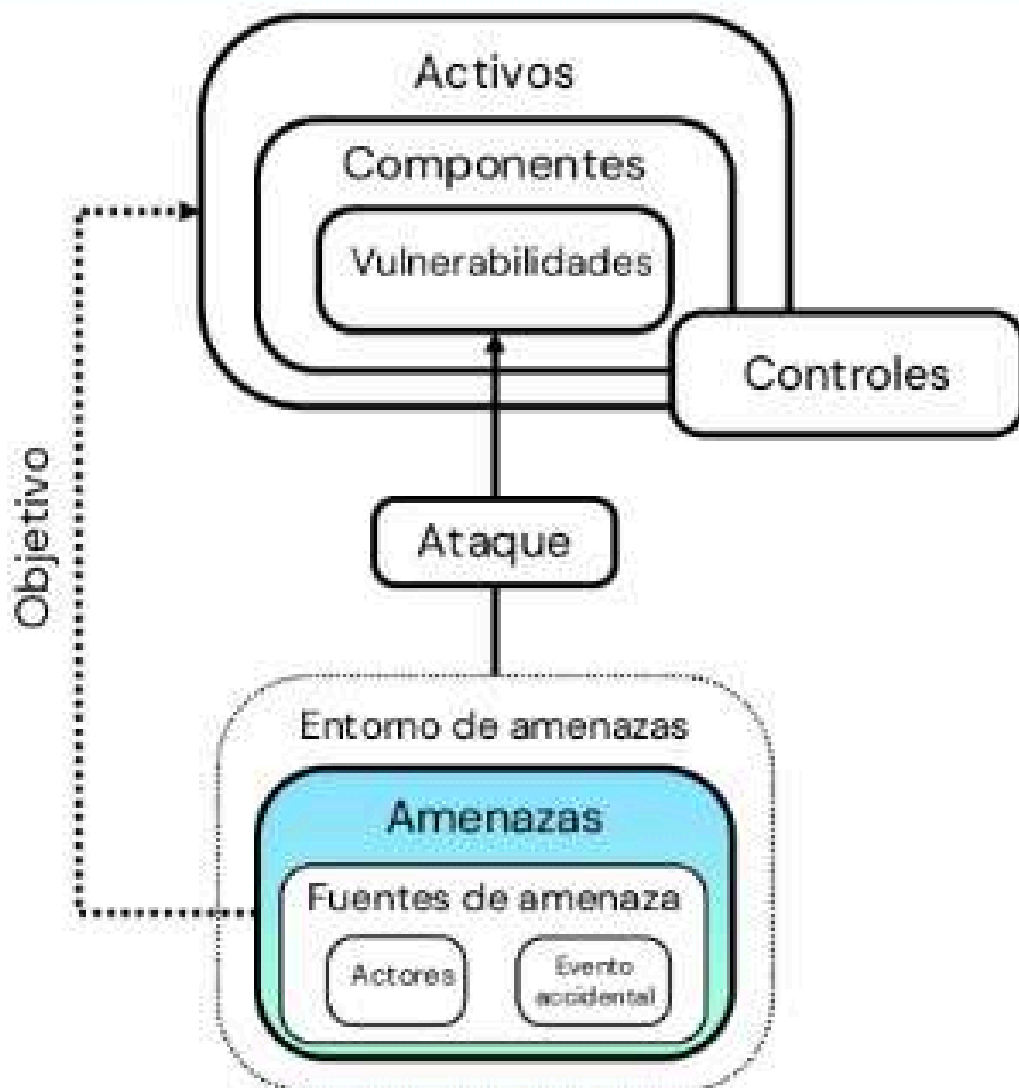
- Desgracias sobrevenidas: incendios, inundaciones, terremotos.
- Exceso de temperatura.
- Picos de tensión y cortes en el suministro eléctrico.
- Averías o fin de vida útil del hardware.
- Robos.
- Acceso no autorizado a ficheros o dispositivos.

➤ Lógicas:

- Acceso ilegítimo al sistema informático.
- Software malicioso.
- Privacidad de los datos y las comunicaciones.

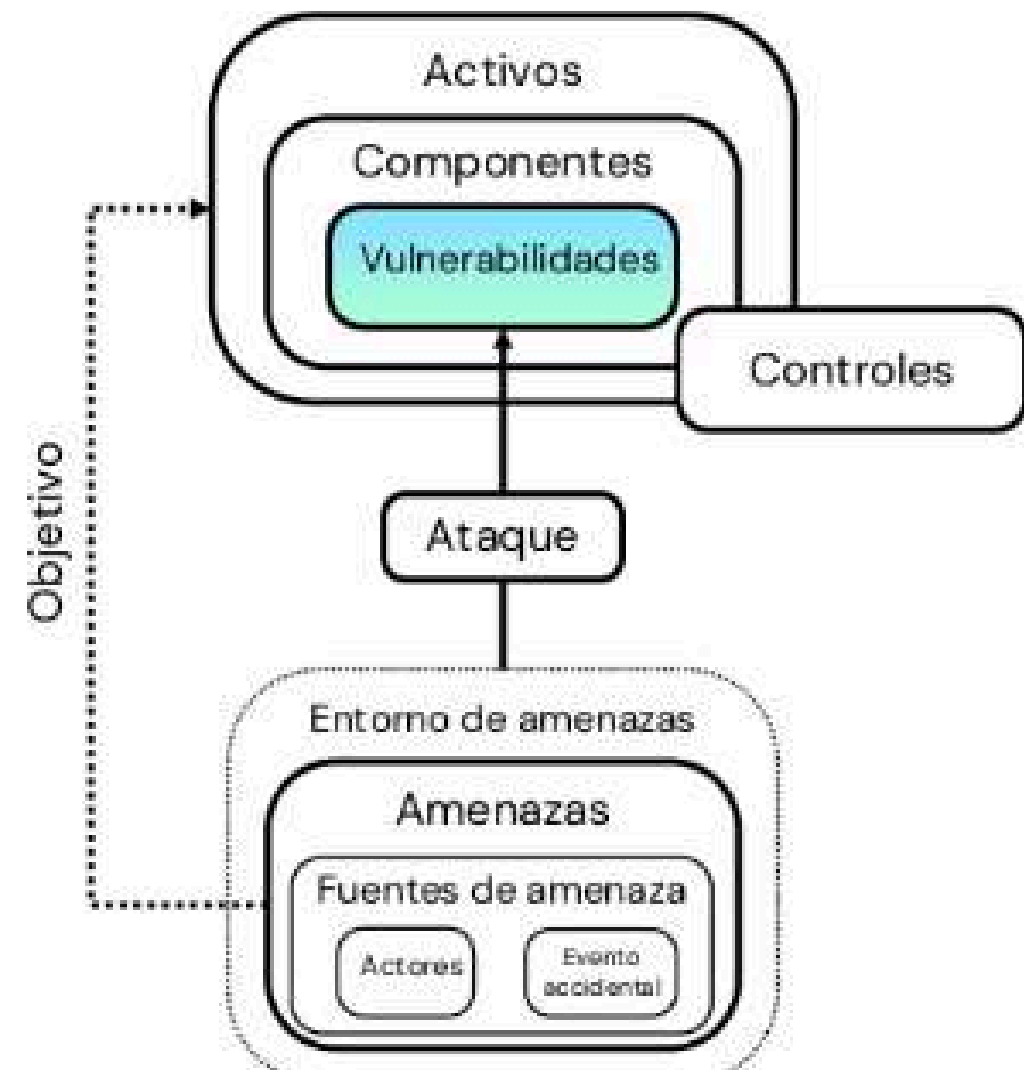
FACTOR
HUMANO

Amenaza, ataque y vulnerabilidad



Cualquier circunstancia o evento con el potencial de afectar negativamente a las operaciones de una organización, activos de la organización o individuos, a través del acceso no autorizado a un sistema de información, la destrucción, divulgación o modificación de información y/o la denegación de servicio

Amenaza, ataque y vulnerabilidad



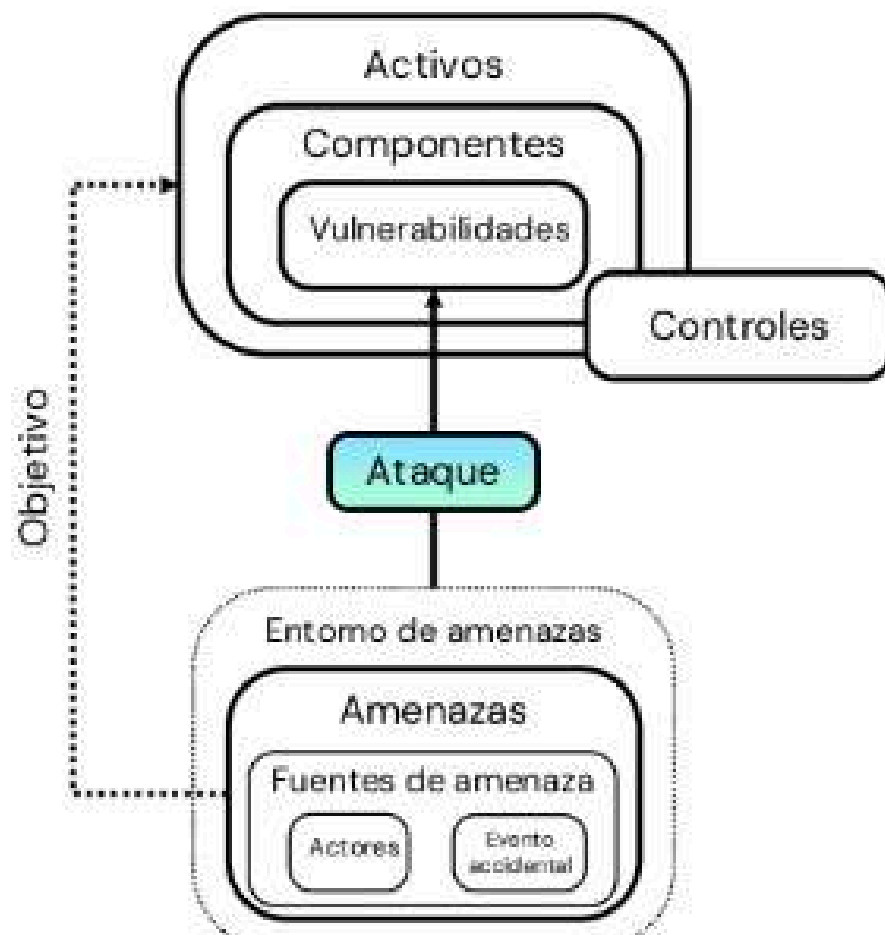
Una **falla o debilidad** en los procedimientos de seguridad de un sistema de información, diseño, implementación o controles internos **que podría explotarse accidental o intencionadamente** y provocar como resultado una violación de los controles o de la política de seguridad del sistema



Ciclo de supervisión de vulnerabilidades

La tarea de supervisión de vulnerabilidades es constante. La figura del administrador del sistema es, pues, fundamental en todos los sistemas informáticos.

Amenaza, ataque y vulnerabilidad



Mecanismo a través del cual una amenaza explota una vulnerabilidad para causar un impacto de seguridad que afecte a la confidencialidad, integridad o disponibilidad de un sistema de información



Ataque por diccionario

Un ataque por diccionario es un mecanismo utilizado por intrusos para intentar averiguar una contraseña probando una lista de palabras contenidas en un diccionario.

Ataque por fuerza bruta

Un ataque por fuerza bruta se realiza probando todas las combinaciones posibles de letras, números y caracteres especiales hasta encontrar aquella que permite el acceso.