



SEGURIDAD INFORMÁTICA

JOSÉ PABLO
HERNÁNDEZ

SEGURIDAD INFORMÁTICA

2.3.0.MF0487_3. Capítulo 3
Parte 1 de 2

Análisis de riesgos de los sistemas de información

JOSÉ PABLO HERNÁNDEZ

1. INTRODUCCIÓN

Las organizaciones tienen multitud de recursos vulnerables ante ataques de seguridad.

Las herramientas de gestión de riesgos sirven para estas funcionalidades: ayudan a identificar los recursos importantes en la organización, los riesgos a los que están sometidos y el daño que pueden sufrir en caso de producirse una amenaza de cualquier tipo.

2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS

Un riesgo es un evento o conjunto de eventos que puede poner en peligro un proyecto de la organización o que puede impedir su éxito.

Riesgo informático:

Incertidumbre: el evento que caracteriza al riesgo puede ocurrir o no ocurrir, no hay certeza sobre su ocurrencia.

Pérdida: en caso de materializarse el riesgo, habría varias consecuencias negativas para la organización. Si no hay efectos negativos, no hay riesgo en sí.

2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS



2.1. CONCEPTOS BÁSICOS DE LA GESTIÓN DE RIESGOS

La gestión de riesgos se define como el conjunto de procesos desarrollados por una organización con el fin de disminuir la probabilidad y ocurrencia de amenazas y de aumentar la probabilidad y ocurrencia de oportunidades con efectos negativos.

Seguridad de la información se define como el conjunto de medidas y capacidades de los sistemas de información para resistir a las amenazas manteniendo la disponibilidad, autenticidad, integridad y confidencialidad de los datos.

2.1. CONCEPTOS BÁSICOS DE LA GESTIÓN DE RIESGOS

Características básicas de la información

Disponibilidad

Integridad

Confidencialidad

Autenticidad

Trazabilidad

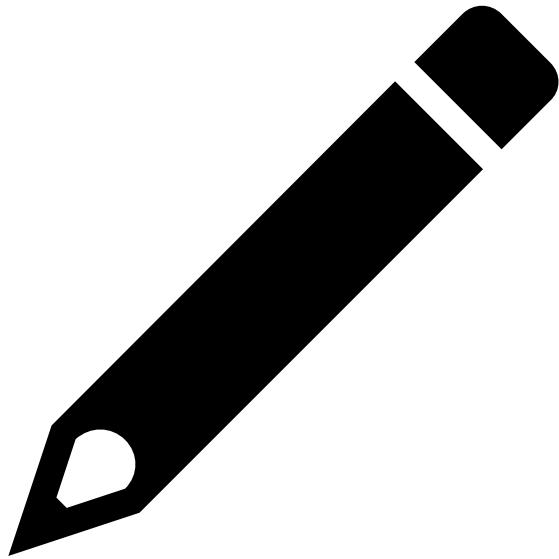
2.1. CONCEPTOS BÁSICOS DE LA GESTIÓN DE RIESGOS

Riesgo: estimación de las probabilidades de que una amenaza se materialice sobre los activos de la organización, causando efectos negativos o pérdidas.

Análisis de riesgos: proceso y metodología utilizados para estimar la magnitud de los riesgos a los que se expone una organización.

Tratamiento del riesgo: procesos realizados para modificar los riesgos de una organización.

Ejemplo



UTILIZANDO UN EQUIPO DE SU EMPRESA, LE HA SALTADO EL ANTIVIRUS Y LE HA INDICADO QUE SE HA PRODUCIDO UNA INCIDENCIA Y QUE SE HA ELIMINADO UN CONJUNTO DE DATOS.

¿QUÉ HA SIDO LO QUE SE HA PRODUCIDO: RIESGO, PREOCUPACIÓN O PROBLEMA? ¿HAY INCERTIDUMBRE DE SU OCURRENCIA? ¿Y EFECTOS NEGATIVOS?

Ejemplo. Solución.



CUANDO UN ANTIVIRUS INDICA QUE SE HA PRODUCIDO UNA INCIDENCIA, YA NO HAY INCERTIDUMBRE SOBRE SU OCURRENCIA, YA QUE EL ANTIVIRUS DICE CLARAMENTE QUE HA OCURRIDO. AL INDICAR TAMBIÉN QUE HA HABIDO BORRADO DE ARCHIVOS, TAMBIÉN HAY CONSTANCIA DE EFECTOS PERJUDICIALES PARA EL EQUIPO.

POR LO TANTO, SI YA NO HAY INCERTIDUMBRE Y HAY EFECTOS NEGATIVOS, LO QUE SE HA PRODUCIDO HA SIDO UN PROBLEMA.

2.2. ESTÁNDAR ISO 31 000 DE GESTIÓN Y TRATAMIENTO DE RIESGOS

En cuanto a gestión, análisis y tratamiento de riesgos existe un estándar ISO (ISO 31000:2009) que incluye una serie de recomendaciones y actividades para que las organizaciones gestionen sus riesgos de un modo más adecuado y eficaz.

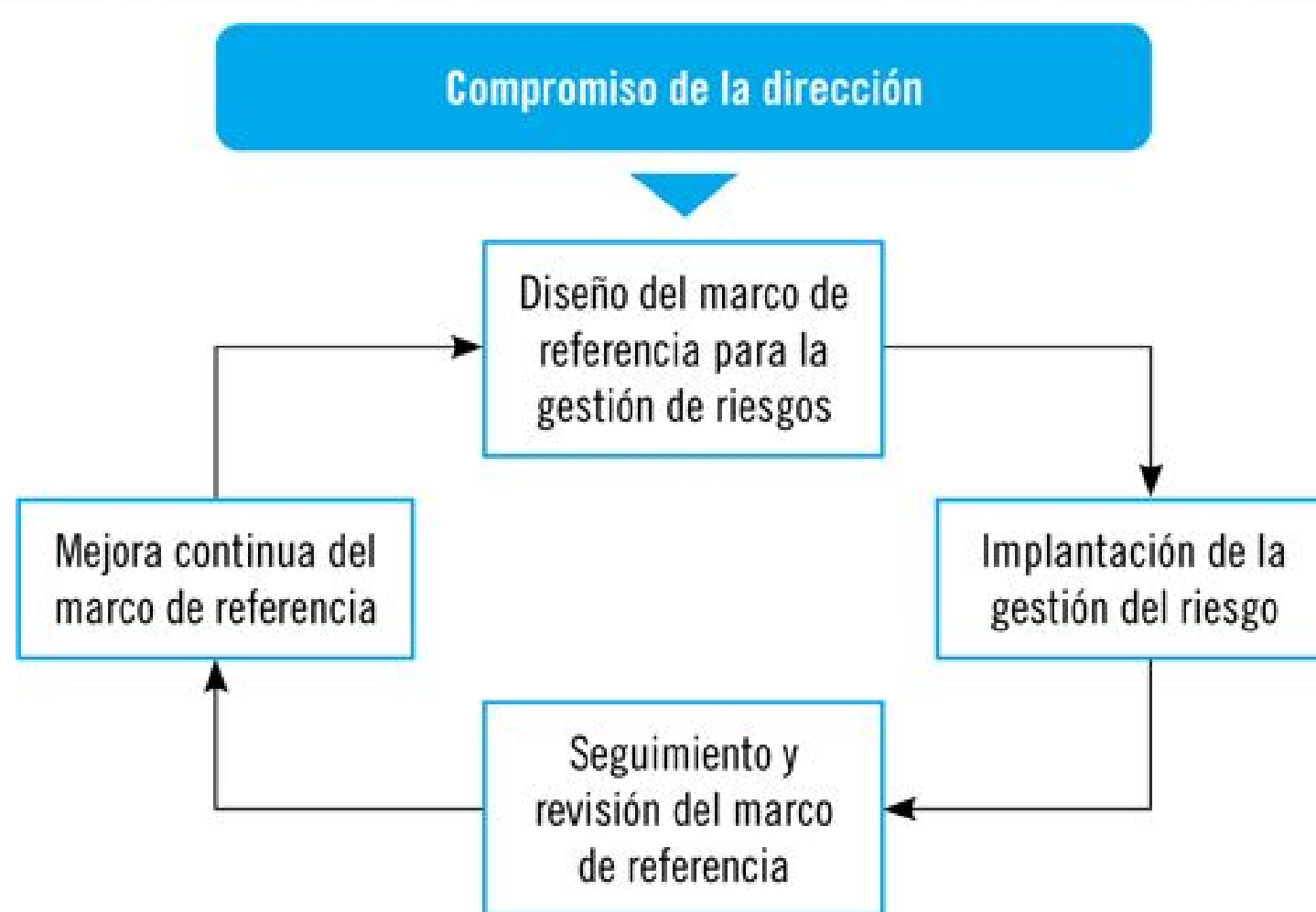
No obstante, aunque sea un estándar, no ofrece certificación, por lo que solo debe ser tomada como una guía en la que encontrar los principios, el marco y el proceso para lograr una gestión de riesgos transparente, sistemática y creíble. A raíz de la ISO31000:2009, las organizaciones deben ser capaces de desarrollar sus propias estrategias de gestión de riesgos.

2.2. ESTÁNDAR ISO 31 000 DE GESTIÓN Y TRATAMIENTO DE RIESGOS

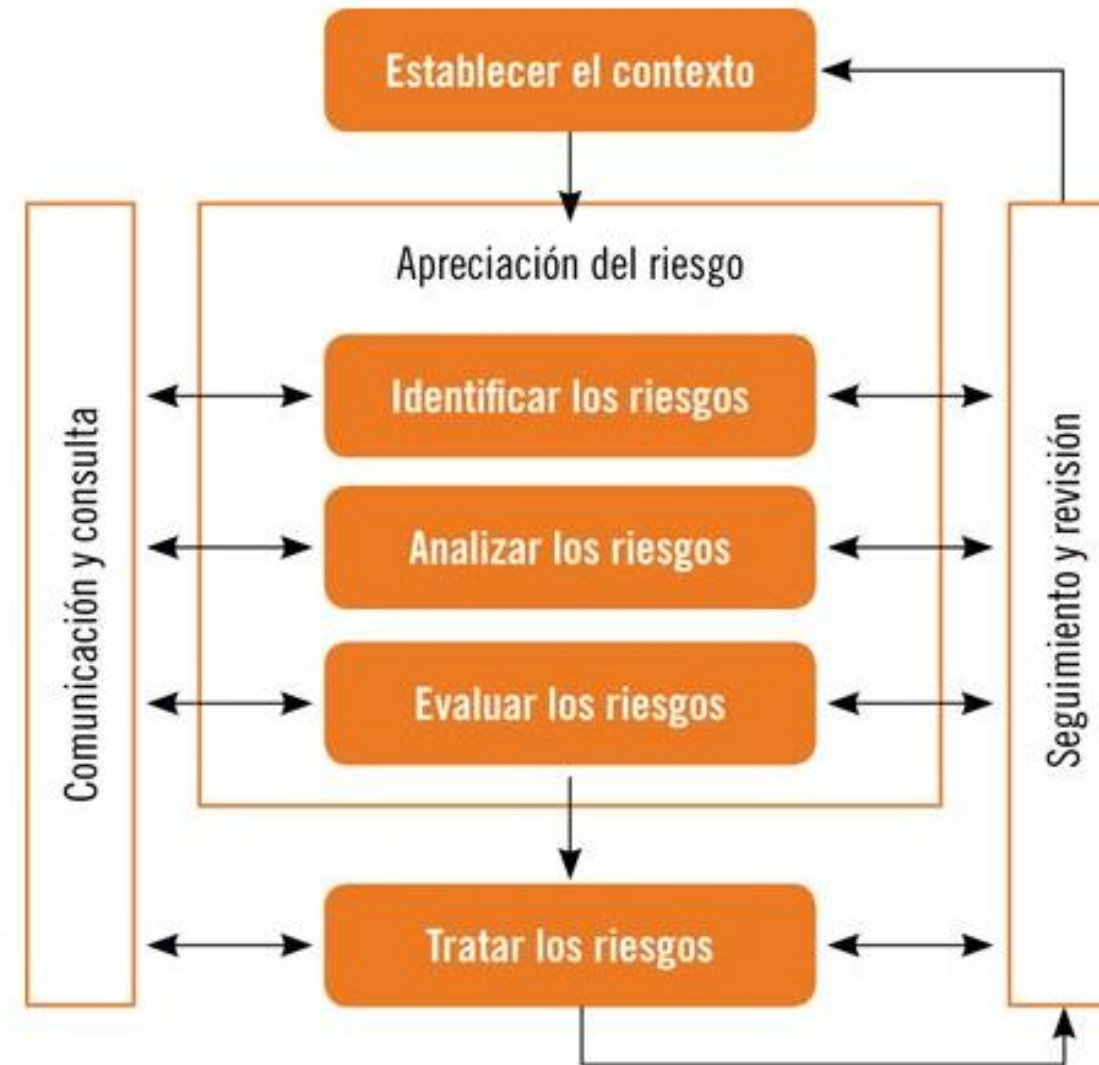
Principios de la norma ISO 31000: La gestión de riesgos:

- 1. Crea valor.**
- 2. Está integrada en los procesos de la organización.**
- 3. Forma parte de la toma de decisiones.**
- 4. Trata explícitamente la incertidumbre.**
- 5. Es sistemática.**
- 6. Está basada en la mejor información disponible.**
- 7. Está hecha a medida.**
- 8. Tiene en cuenta factores humanos y culturales.**
- 9. Es transparente e inclusiva.**
- 10. Es dinámica, iterativa y sensible al cambio.**
- 11. Facilita la mejora continua de la organización.**

2.3. MARCO DE TRABAJO PARA LA GESTIÓN DEL RIESGO



2.4. PROCESO DE GESTIÓN DEL RIESGO



3. PRINCIPALES TIPOS DE VULNERABILIDADES

Para una correcta y completa gestión del riesgo de un sistema de información, hay que prestar atención a los distintos tipos de agentes e incidencias que pueden afectar al flujo de datos. Los más importantes a considerar son las vulnerabilidades o fallos de programa y los programas maliciosos (software malicioso).

3.1. PRINCIPALES TIPOS DE VULNERABILIDADES/FALLOS DE PROGRAMA

Una vulnerabilidad es un fallo de seguridad en un programa o en un sistema de información.

Las vulnerabilidades son, en numerosas ocasiones, el origen de muchos fallos de seguridad y, por ello, deben tomarse en consideración cuando se planifica la gestión de riesgos del sistema de información.

3.1. PRINCIPALES TIPOS DE VULNERABILIDADES/FALLOS DE PROGRAMA

Vulnerabilidades de configuración

Son vulnerabilidades generadas por una mala gestión del software por parte del usuario final. No se originan por un fallo del diseño en sí, sino que se originan en el momento en el que el usuario configura el sistema erróneamente.

3.1. PRINCIPALES TIPOS DE VULNERABILIDADES/FALLOS DE PROGRAMA

Validación de entrada

Se trata de una vulnerabilidad que se genera cuando la aplicación no comprueba adecuadamente la entrada de datos que provienen desde el exterior.

3.1. PRINCIPALES TIPOS DE VULNERABILIDADES/FALLOS DE PROGRAMA

Salto de directorio

Es una vulnerabilidad que se aprovecha de la falta de seguridad de los servicios de red para moverse por los directorios de la aplicación hasta llegar a su directorio raíz.

En caso de sistemas operativos, esta vulnerabilidad puede ocasionar que usuarios no autorizados accedan a su directorio raíz y puedan conectarse a ellos para ejecutar acciones de modo remoto.

3.1. PRINCIPALES TIPOS DE VULNERABILIDADES/FALLOS DE PROGRAMA

Inyección de comandos en el sistema operativo

La inyección de comandos en el sistema operativo consiste en la capacidad que tiene el usuario para ejecutar comandos en el sistema operativo que puedan poner en peligro su integridad.

3.1. PRINCIPALES TIPOS DE VULNERABILIDADES/FALLOS DE PROGRAMA

Inyección SQL

Se trata de una vulnerabilidad que se localiza en el nivel de base de datos del programa o aplicación. Se produce cuando el filtrado de las variables utilizadas con código SQL no se realiza correctamente.

Al realizarse un filtrado incorrecto, los atacantes pueden inyectar nuevo código SQL para modificar el comportamiento de la aplicación e, incluso, introducir código malicioso en el sistema.

3.1. PRINCIPALES TIPOS DE VULNERABILIDADES/FALLOS DE PROGRAMA

Error de búfer

Un búfer es un espacio de la memoria de un disco o de un instrumento digital reservada para el almacenamiento de información digital de forma temporal hasta que esta se procese.

Se producen errores de búfer cuando se intentan almacenar datos de forma incontrolada en su espacio (provocando daños en zonas de la aplicación) o cuando la velocidad de entrada de datos en el búfer es inferior a la velocidad de lectura de los mismos (provocando fallos y la detención momentánea de la ejecución de la aplicación).

3.1. PRINCIPALES TIPOS DE VULNERABILIDADES/FALLOS DE PROGRAMA

Fallo de autenticación

Vulnerabilidad que se origina cuando el programa no puede autenticar correctamente al usuario que intenta acceder en él.

3.1. PRINCIPALES TIPOS DE VULNERABILIDADES/FALLOS DE PROGRAMA

Error en la gestión de recursos

Este tipo de vulnerabilidad ocurre cuando el fallo de programa permite al usuario no autorizado provocar una gestión deficiente de los recursos del sistema, provocando un consumo excesivo en estos.

Cuando esto sucede, la aplicación suele dejar de responder e interrumpe el servicio.

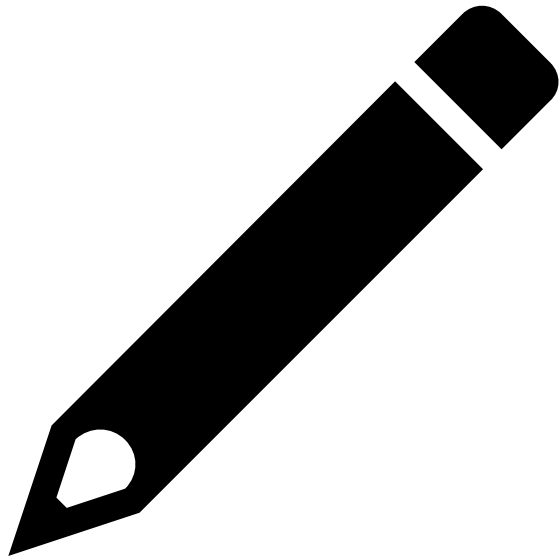
3.1. PRINCIPALES TIPOS DE VULNERABILIDADES/FALLOS DE PROGRAMA

Error de diseño

Son vulnerabilidades ocasionadas cuando el programador realiza el diseño de la aplicación con fallos y errores, tanto en el diseño inicial como en su desarrollo posterior.

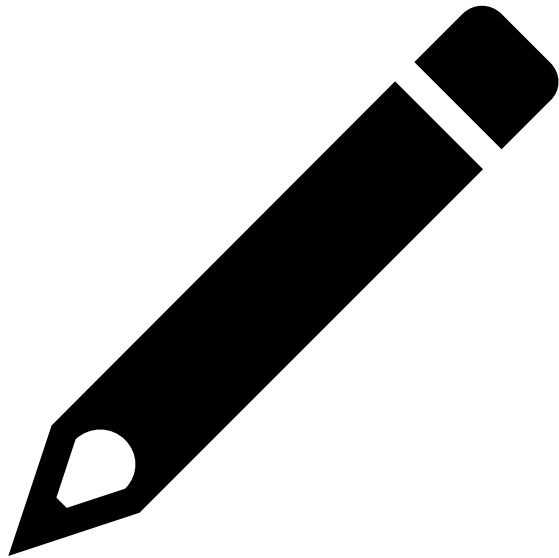
Estos errores pueden llevar a un mayor riesgo de entrada de atacantes que intenten aprovecharse de los fallos de diseño para introducir código malicioso en la aplicación.

Ejemplo.



USTED SE ENCUENTRA INTENTANDO ACCEDER CON SU USUARIO Y CONTRASEÑA AL PROGRAMA DE GESTIÓN DE SU EMPRESA Y ESTE LE DEVUELVE UN MENSAJE DE ERROR INDICÁNDOLE QUE HAY UN FALLO DE AUTENTICACIÓN Y QUE NO PUEDE ACCEDER. ¿ES POSIBLE QUE EL PROGRAMA TENGA ALGUNA VULNERABILIDAD? ¿DE QUÉ TIPO?

Ejemplo. Solución.



SI SE INTENTA ACCEDER A UNA APLICACIÓN QUE REQUIERE AUTENTICACIÓN Y NO PUEDE, ES POSIBLE QUE LA APLICACIÓN TENGA UNA VULNERABILIDAD DEL TIPO FALLO DE AUTENTICACIÓN. ESTE TIPO DE VULNERABILIDADES SE ORIGINA PRECISAMENTE CUANDO EL PROGRAMA NO AUTENTICA BIEN AL USUARIO Y LE IMPIDE EL ACCESO Y SU UTILIZACIÓN.


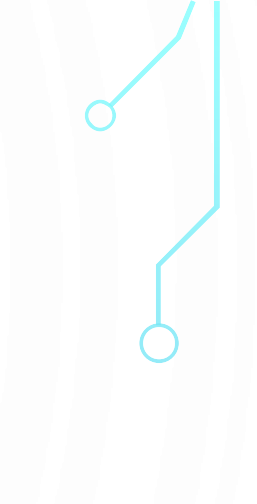
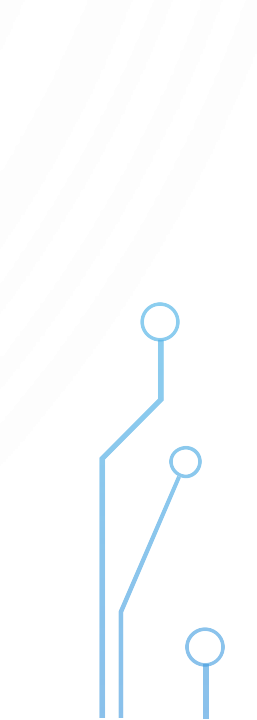
3.2. PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE

Un programa malicioso o malware es un tipo de programa diseñado para que usuarios no autorizados accedan a un sistema de información sin autorización de su propietario y producir efectos indeseados en este: virus, troyanos, gusanos, spyware, etc., que se describirán más adelante.

- **Modificar datos**
- **Eliminar datos**
- **Secuestrar datos**
- **Control de la máquina**



3.3. CRITERIOS DE PROGRAMACIÓN SEGURA

- **Protección de los desbordamientos de pila.**
 - **Utilizar el flujo de datos.**
 - **Realización de pruebas.**
 - **Actualizaciones de programas continuas.**
 - **Utilización de técnicas.**
- 
- 
- 

4. CÓDIGO MALICIOSO

- **Destrucción o modificación de información.**
- **Robo de información y de claves de acceso.**
- **Propagación a otros equipos de una misma red o a través de Internet.**
- **Introducir publicidad de forma masiva.**
- **Comprometer la integridad de aplicaciones y sistemas operativos.**

La evolución de las tecnologías de la información provoca que los códigos maliciosos sean cada vez más complejos y variados.

4.1. TIPOS DE CÓDIGOS MALICIOSOS

Según su forma, origen, los daños que provocan o la finalidad para la que son diseñados:

- Virus.
- Cookies.
- Troyanos.
- Keyloggers.
- Spyware.
- Gusanos o worms.

4.1. TIPOS DE CÓDIGOS MALICIOSOS

Virus

Los virus son un tipo de software malicioso que se diseñan para dañar el equipo al que acceden, pasando desapercibidos por el usuario.

4.1. TIPOS DE CÓDIGOS MALICIOSOS

Cookies

Las cookies no son una amenaza de seguridad en sí, pero pueden afectar a la privacidad y confidencialidad de los usuarios.

Se trata de un tipo de software informático que detecta y almacena los datos de navegación de un usuario para conocer sus preferencias.

4.1. TIPOS DE CÓDIGOS MALICIOSOS

Trojanos

Los troyanos son aplicaciones que contienen funcionalidades ocultas con finalidades maliciosas para el usuario.

4.1. TIPOS DE CÓDIGOS MALICIOSOS

Keyloggers

Los keyloggers son otro tipo de software malicioso que se diseña con la finalidad de recopilar y almacenar remotamente el comportamiento de los usuarios.

Actúan almacenando toda la información tecleada por el usuario del sistema y enviándola al atacante

4.1. TIPOS DE CÓDIGOS MALICIOSOS

Spyware

Aplicación diseñada para obtener información del usuario con fines lucrativos.

Su procedimiento de actuación es el siguiente:

- Acceso al sistema del usuario.
- Obtención y recopilación de la información del usuario almacenada en el sistema.
- Monitorización del sistema del usuario.
- Registro y venta de la información del comportamiento del usuario.
- Actuación de los terceros ante la información comprada al atacante.

4.1. TIPOS DE CÓDIGOS MALICIOSOS

Gusanos o worms

Los gusanos o worms son programas maliciosos autocontenidos cuya finalidad principal es su propagación a otros sistemas para mermar su rendimiento.

5. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS

Cuando se pretende implantar un proceso de gestión de riesgos en la organización para aumentar el nivel de seguridad de la información, deben conocerse previamente una serie de conceptos y las relaciones existentes entre ellos.

5.1. ELEMENTOS DEL ANÁLISIS DE RIESGOS

El proceso de gestión de riesgos conlleva el análisis de una serie de elementos importantes del sistema de información: los elementos más vulnerables ante posibles amenazas y aquellos cuyo deterioro pueda suponer un daño mayor en el sistema.

5.1. ELEMENTOS DEL ANÁLISIS DE RIESGOS

Activo

Un activo es un recurso del sistema de información, necesario para garantizar el correcto funcionamiento de los procesos de la organización.

5.1. ELEMENTOS DEL ANÁLISIS DE RIESGOS

Amenaza

Una amenaza es cualquier evento que puede afectar al activo de un sistema de información, provocando un incidente de seguridad y produciendo efectos adversos (materiales o inmateriales) o pérdidas de información.

5.1. ELEMENTOS DEL ANÁLISIS DE RIESGOS

Vulnerabilidad

Una vulnerabilidad consiste en alguna característica o capacidad de un activo del sistema de información que lo hace susceptible a amenazas.

5.1. ELEMENTOS DEL ANÁLISIS DE RIESGOS

Riesgo

Como se ha mencionado anteriormente, un riesgo es la posibilidad de que una amenaza se materialice causando efectos negativos o positivos.

5.1. ELEMENTOS DEL ANÁLISIS DE RIESGOS

Control atenuante

Se consideran atenuantes aquellos activos y medidas que consiguen reducir las posibilidades de amenazas y, por tanto, el nivel de riesgo del sistema de información de la organización.

5.1. ELEMENTOS DEL ANÁLISIS DE RIESGOS

Impacto

El impacto es la magnitud del daño que provoca un ataque exitoso en el que se han perjudicado la confidencialidad, la disponibilidad, la integridad y la autenticidad de la información del sistema.

5.2. MODELOS DE RELACIONES DE CONCEPTOS DE GESTIÓN DE RIESGOS



6. METODOLOGÍAS DE ANÁLISIS DE RIESGOS

Tipos de controles de seguridad

Control	Descripción
---------	-------------

Disuasorio	Su finalidad principal es reducir la probabilidad de recibir un ataque.
-------------------	---

Preventivo	Su finalidad es proteger al sistema de información de sus vulnerabilidades, intentando impedir el acceso de los atacantes o reduciendo el impacto de los daños causados.
-------------------	--

Correctivo	Tienen como finalidad principal reducir el impacto de una amenaza.
-------------------	--

Detectivo	Se encargan de detectar e impedir posibles ataques.
------------------	---

6.1. METODOLOGÍA CUANTITATIVA DE ANÁLISIS DE RIESGOS

El enfoque cuantitativo del análisis de riesgos tiene en cuenta dos elementos: la probabilidad de ocurrencia de un evento y el impacto que puede provocar en caso de que suceda.

Para determinar y analizar los riesgos, la metodología cuantitativa se basa en un modelo matemático que sirva de apoyo a la toma de decisiones.

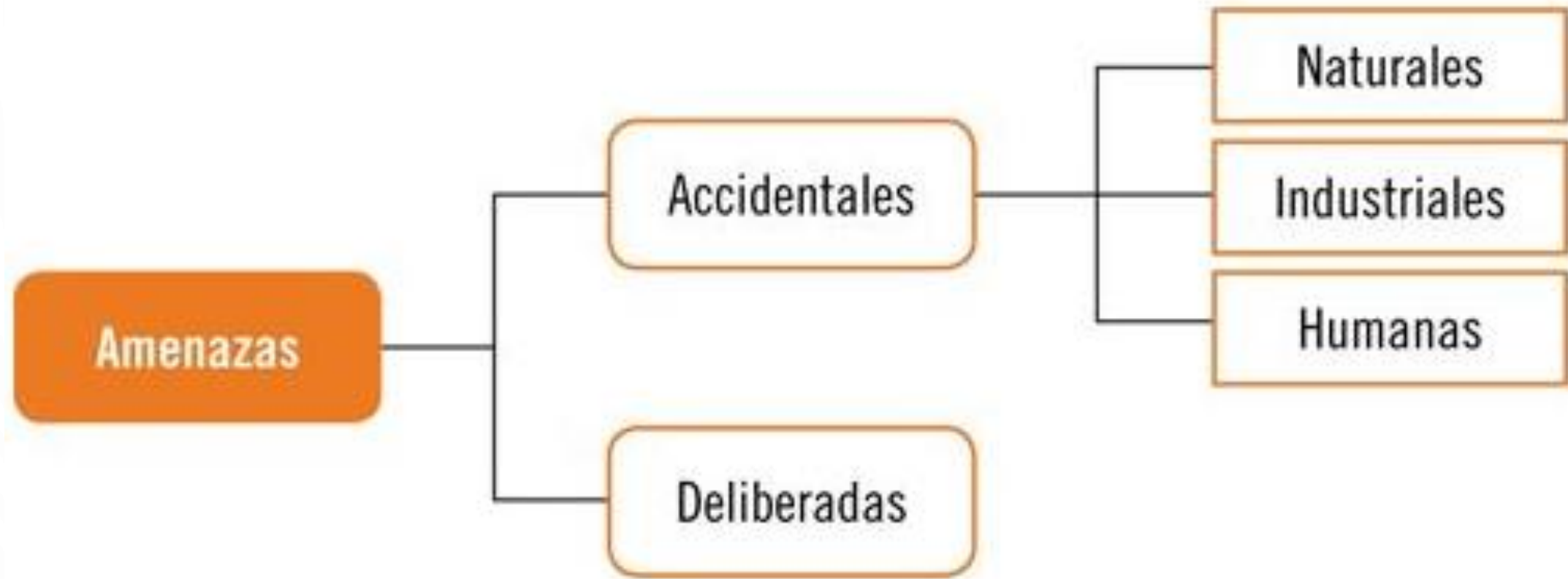
6.2. METODOLOGÍA CUALITATIVA DE ANÁLISIS DE RIESGOS

La metodología cualitativa se basa en el raciocinio humano para calcular las pérdidas potenciales estimadas sin necesidad de utilizar métodos probabilísticos.

Es la metodología utilizada con más frecuencia para el análisis de riesgos.

Esta metodología suele utilizarse cuando el nivel de riesgo no es elevado o cuando los datos numéricos no son adecuados para una correcta estimación del riesgo.

8. IDENTIFICACIÓN DE LAS AMENAZAS



8.1. EJEMPLOS DE AMENAZAS FRECUENTES

Suplantación.

Alteración.

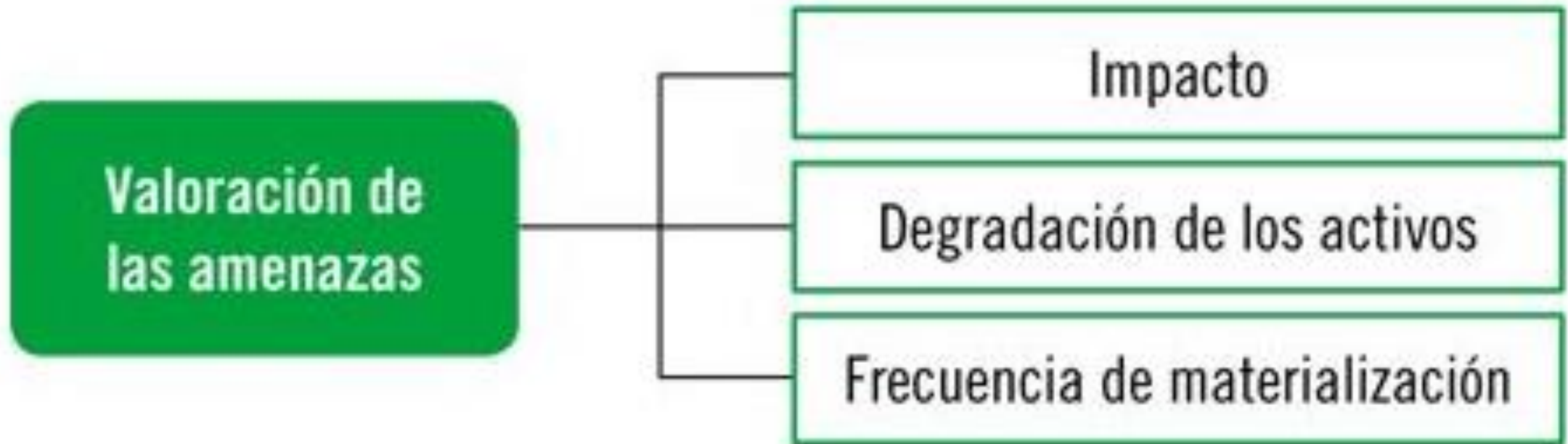
Repudio.

Divulgación de información.

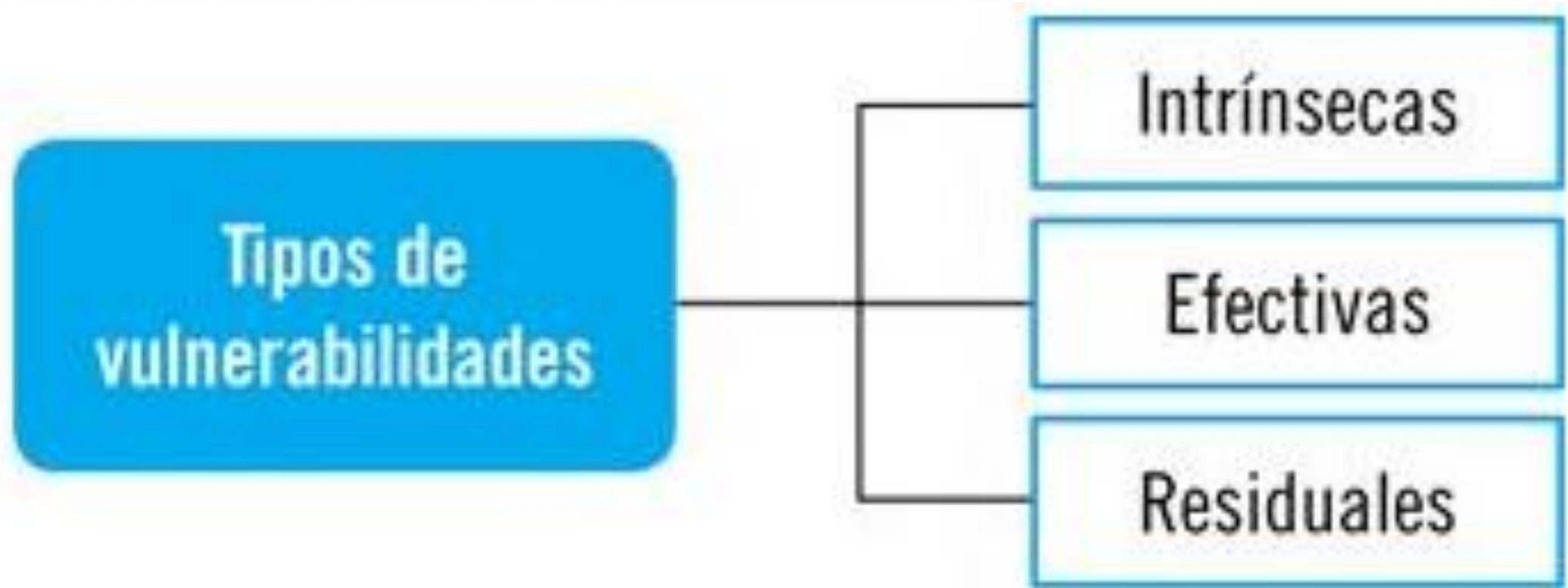
Denegación del servicio.

Elevación de privilegios.

8.2. VALORACIÓN DE LAS AMENAZAS



9. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES



9.1. ANÁLISIS LOCAL PARA LA DETECCIÓN DE VULNERABILIDADES

El análisis local de vulnerabilidades en un sistema de información se realiza mediante la ejecución de pruebas de software.

Pruebas estáticas: pruebas que no requieren la ejecución del código de la aplicación para poder realizarse.

Pruebas dinámicas: al contrario que las estáticas, las dinámicas necesitan que se esté ejecutando la aplicación en el momento de la realización de la prueba.

9.2. ANÁLISIS REMOTO DE CAJA BLANCA

El análisis remoto de caja blanca se realiza con la ejecución de pruebas que examinan la estructura interna de la aplicación y de los componentes del sistema.

Antes de la ejecución de las pruebas de caja blanca, los auditores informáticos deberán recopilar toda la información que sea posible para la evaluación de la seguridad y de las vulnerabilidades del sistema de información: código fuente de las aplicaciones, archivos de configuración, etc.

9.3. ANÁLISIS DE CAJA NEGRA

Los análisis de caja negra consisten en una serie de pruebas que evalúan exclusivamente las entradas y salidas del sistema de información.

Su finalidad principal es conseguir simular los ataques de un intruso: imitan lo que el intruso haría y obtienen información bastante real sobre los riesgos a los que se expone el sistema evaluado. La base de estas pruebas es que si un auditor de seguridad informática es capaz de detectar alguna vulnerabilidad con estas pruebas de caja negra, un intruso también podría detectarlas con facilidad.