MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL
SERVICIO PÚBLICO DE EMPLEO ESTATAL SEPE SERVEI PÚBLIC D'OCUPACIÓ ESTATAL
MINISTERIO DE EDUCACIÓN, FORMACIÓN PROFESIONAL Y DEPORTES
Generalitat de Catalunya
SOC Servei d'Ocupació de Catalunya
IRON HACK SPAIN

Auditoria en seguridad informática

IFCT0109 – Seguridad informática

MF0487_3 (90 horas)

Análisis de riesgos de los sistemas de información

- Introducción
- Introducción al análisis de riesgos
- Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura
- particularidades de los distintos tipos de código malicioso (malware)
- Principales elementos del análisis de riesgos y sus modelos de relaciones
- Metodologías cualitativas y cuantitativas de análisis de riesgos
- Identificación de los activos involucrados en el análisis de riesgos y su valoración
- Identificación de las amenazas que pueden afectar a los activos identificados previamente
- Análisis e identificación de las vulnerabilidades existentes en los sistemas de información que permitirían la materialización de amenazas, incluyendo análisis local, análisis remoto de caja blanca y de caja negra
- Optimización del proceso de auditoría y contraste de vulnerabilidades e informe de auditoría
- Identificación de las medidas de salvaguarda existentes en el momento de la realización del análisis de riesgos y su efecto sobre las vulnerabilidades y amenazas
- Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse

Análisis de riesgos de los sistemas de información

- Determinación de la probabilidad e impacto de materialización de los escenarios
- Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza
- Determinación por parte de la organización de los criterios de evaluación del riesgo, en función de los cuales se determina si unriesgo es aceptable o no
- Relación de las distintas alternativas de gestión de riesgos
- Guía para la elaboración del plan de gestión de riesgos
- Exposición de la metodología NIST SP 8OO-3O
- Exposición de la metodología Magerit
- Resumen

Introducción

Los sistemas de información de las organizaciones albergan una gran cantidad de recursos susceptibles a ataques de seguridad. Por ello, es fundamental que las organizaciones implementen estrategias y herramientas para identificar y evaluar estos recursos, así como para obtener información sobre las amenazas y los daños potenciales que pueden afectarles.

Las herramientas de gestión de riesgos cumplen con estas funciones: ayudan a identificar los recursos críticos de la organización, los riesgos a los que están expuestos y el impacto potencial que podrían sufrir en caso de materializarse una amenaza.

En este capítulo se presenta una descripción de las herramientas fundamentales para la gestión de riesgos, se ofrecen guías de apoyo para la identificación de todos los factores involucrados en este proceso y se analizan diversas técnicas que permiten a las organizaciones combatir los riesgos y mejorar la seguridad de sus sistemas de información.

Introducción al análisis de riesgos

Introducción

Un **riesgo** se define como un evento o conjunto de eventos que podrían poner en peligro un proyecto de la organización o dificultar su éxito.

La definición de riesgo ha sido objeto de debate, pero existe un consenso sobre las características comunes que debe tener todo riesgo informático:

- Incertidumbre: No hay certeza absoluta sobre la ocurrencia del evento que caracteriza al riesgo.
- Pérdida: Si el riesgo se materializa, la organización sufrirá consecuencias negativas. La ausencia de efectos negativos implica que no hay riesgo.

Es común confundir los conceptos de problema, preocupación y riesgo. Es importante comprender sus diferencias:

- Preocupación: Situación sobre la que hay dudas y que debe ser evaluada como un posible riesgo. Tras el análisis, puede determinarse que no hay efectos negativos y, por lo tanto, no se considera un riesgo.
- Problema: Un riesgo que ya se ha materializado. En este caso, no hay incertidumbre, ya que hay certeza sobre su ocurrencia. Por lo tanto, tampoco se considera un riesgo.

Introducción al análisis de riesgos

Concepto	Definición	Características
Preocupación	Situación sobre la que hay dudas	No hay certeza sobre su impacto en la organización
Riesgo	Evento que puede poner en peligro un proyecto	Incertidumbre sobre su ocurrencia
Problema	Riesgo que ya se ha materializado	Certeza sobre su ocurrencia

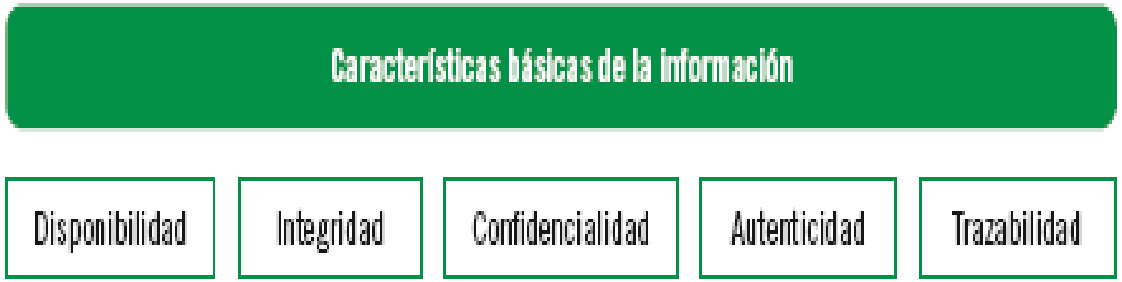
Introducción al análisis de riesgos

Conceptos básicos de la gestión de riesgos

La **gestión de riesgos** se define como el conjunto de procesos que una organización implementa para minimizar la probabilidad de que se materialicen las amenazas y maximizar la probabilidad de aprovechar las oportunidades.
Se trata de una metodología o conjunto de metodologías que permiten gestionar las incertidumbres asociadas a las amenazas.

En el contexto de la gestión de riesgos, la seguridad de la información juega un papel fundamental. La **seguridad** se define como el conjunto de medidas y capacidades que protegen los sistemas de información de las amenazas, manteniendo la disponibilidad, autenticidad, integridad y confidencialidad de los datos.

Una correcta gestión de riesgos se basa en la implementación de medidas de seguridad que protejan los datos e información en cuanto a:



Introducción al análisis de riesgos

Conceptos básicos de la gestión de riesgos

Una correcta gestión de riesgos se basa en la implementación de medidas de seguridad que protejan los datos e información en cuanto a:

- Disponibilidad: La información debe estar disponible para los usuarios cuando la necesiten. La falta de disponibilidad provoca interrupciones del servicio y reduce la calidad del mismo.
- Integridad: La información debe ser correcta y completa. La seguridad debe evitar que se manipule, corrompa o elimine información sin autorización.
- Confidencialidad: La información debe estar disponible solo para los usuarios autorizados. La seguridad debe proteger la información de accesos no autorizados.
- Autenticidad: Se debe garantizar la procedencia de los datos. La seguridad de la organización debe asegurar que los datos provengan de fuentes confiables y no hayan sido manipulados.
- Trazabilidad: Se debe poder conocer en todo momento quién y cuándo ha realizado cada acción con la información. Esta característica es muy útil para analizar incidentes y detectar atacantes.

Introducción al análisis de riesgos

Conceptos básicos de la gestión de riesgos

Además de los conceptos relacionados con las características de la información, para comprender la gestión de riesgos es importante tener claros los siguientes conceptos:

- Riesgo: Estimación de la probabilidad 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.

Introducción al análisis de riesgos

Estándar ISO 31000 de gestión y tratamiento de riesgos

En el ámbito de la gestión, análisis y tratamiento de riesgos, existe un estándar internacional **ISO (ISO 31000)** que ofrece una serie de recomendaciones y actividades para que las organizaciones gestionen sus riesgos de forma más adecuada y eficaz.

Es importante destacar que, si bien se trata de un estándar, no ofrece certificación.

Por lo tanto, debe ser utilizada como una guía que proporciona los principios, el marco y el proceso para lograr una gestión de riesgos transparente, sistemática y creíble.

A partir de la ISO 31000, las organizaciones deben ser capaces de desarrollar sus propias estrategias de gestión de riesgos.

La norma ISO 31000 no es específica a ningún sector en particular y puede ser utilizada por cualquier tipo de entidad, pública o privada, y por cualquier tipo de usuario.

Introducción al análisis de riesgos

Estándar ISO 31000 de gestión y tratamiento de riesgos

Principios de la ISO 31000

Para una correcta y efectiva gestión de riesgos, la norma ISO 31000 propone once principios fundamentales a las organizaciones:

- Creación de valor: La gestión de los riesgos debe crear valor y mantenerlo.
- Integración en los procesos de la organización: La gestión de riesgos debe ser una actividad integrada dentro de los procesos de la organización y no debe ser tratada como un proceso aislado.
- Toma de decisiones: La gestión de riesgos debe estar presente en la toma de decisiones de la organización.
- Trato de la incertidumbre: La gestión de riesgos debe tratar explícitamente la incertidumbre, analizando las amenazas y aspectos inciertos para conocer el origen de su incertidumbre y su posible tratamiento.
- Enfoque sistemático: La gestión de riesgos debe ser sistemática, estructurada y utilizada en el momento oportuno.
- Basarse en la mejor información disponible: La gestión de riesgos se debe llevar a cabo tomando en consideración la opinión de profesionales especializados y la experiencia acumulada.
- Adaptación a las circunstancias: La gestión de riesgos debe adaptarse a las circunstancias locales y específicas. Para una correcta gestión de riesgo, las organizaciones deben tener en cuenta el sector de su actividad y el entorno en el que trabajan.

Introducción al análisis de riesgos

Marco de trabajo para la gestión del riesgo

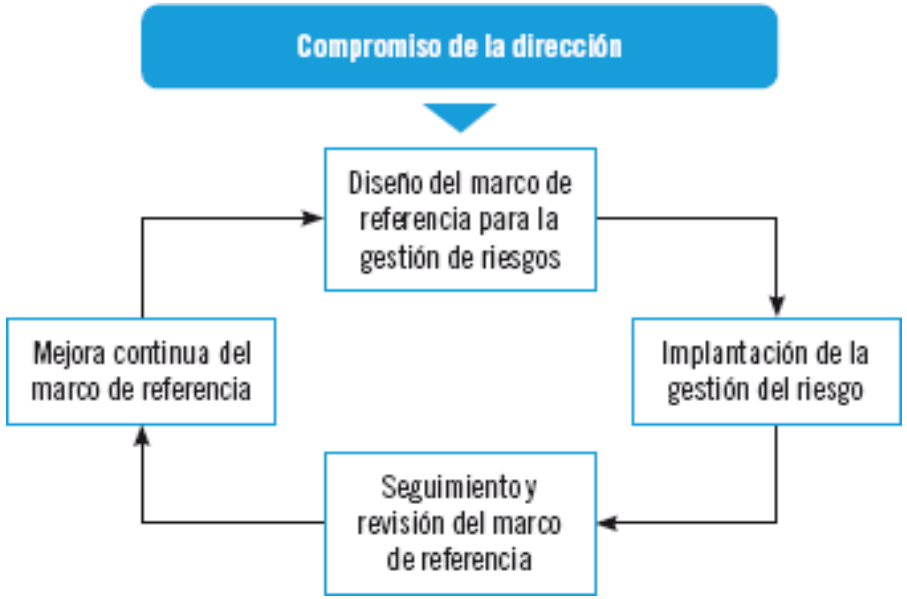
La norma ISO 31000 también establece un marco de referencia o framework para la gestión de riesgos, compuesto por las siguientes actividades:

- Diseño del marco de referencia: Las organizaciones deben diseñar un marco de referencia para la gestión de riesgos que tenga en cuenta sus propias particularidades y su entorno.
- Implantación de la gestión del riesgo: Una vez diseñado el marco de referencia, deberán implantar la gestión del riesgo para poder disminuir la probabilidad de amenazas y pérdidas.
- Evaluación y revisión: La gestión de riesgos debe ser evaluada y revisada periódicamente para valorar si sigue siendo eficiente y es necesario realizar algún cambio.
- Mejora continua: Con estas revisiones periódicas, las organizaciones deben ser capaces de aprender de los fallos detectados y entrar en un proceso de mejora continua que garantice una mejor gestión de riesgos.
- Apoyo y compromiso de la dirección: Todas estas actividades y fases deben contar con el apoyo y compromiso de la dirección de la organización para que puedan ser implantadas de modo global en todas sus tareas y procedimientos.

Introducción al análisis de riesgos

Marco de trabajo para la gestión del riesgo

Marco de referencia o framework para la gestión de riesgos (actividades)



Introducción al análisis de riesgos

Proceso de gestión del riesgo

Introducción:

La norma ISO 31000, después de establecer los principios y el marco de trabajo para la gestión del riesgo, define un proceso con un conjunto de fases y pasos recomendados para que las organizaciones lo adapten e implementen correctamente.

Este proceso busca mejorar la efectividad y precisión en la identificación, análisis y tratamiento de las amenazas potenciales.

Fases del proceso de gestión del riesgo:

Introducción al análisis de riesgos

Proceso de gestión del riesgo

Fases del proceso de gestión del riesgo:

- Establecimiento del entorno y contexto:
  - Análisis: Se examinan las características de la organización, su entorno y sus sistemas de información.
  - Objetivo: Desarrollar una estrategia de gestión de riesgos personalizada.
- Fase de apreciación del riesgo:
  - Identificación: Se detectan y se definen las características básicas de los riesgos.
  - Análisis: Se realiza un estudio profundo de cada riesgo para comprender sus características y comportamientos.
  - Evaluación: Se determina la importancia y magnitud de los riesgos, considerando sus potenciales daños y efectos negativos.
- Fase de tratamiento del riesgo:
  - Toma de decisiones: Se seleccionan las medidas y estrategias para minimizar la probabilidad de ocurrencia y el impacto potencial de los riesgos.
  - Implementación: Se ponen en marcha las medidas y estrategias definidas.

Introducción al análisis de riesgos

Proceso de gestión del riesgo

Fases del proceso de gestión del riesgo: (continuación)

- Monitorización y revisión:
  - Seguimiento: Se monitorea el proceso de gestión de riesgos para asegurar su integración en la organización.
  - Revisiones: Se realizan evaluaciones periódicas para detectar y corregir posibles fallos.
  - Revisiones durante la implantación: Se verifican el desarrollo y la correcta implementación del proceso.
- Comunicación y consulta:
  - Interacción: La organización se comunica con los diferentes actores del sistema de información durante todas las fases del proceso.
  - Objetivos:
    - Establecer el contexto adecuado.
    - Asegurar la información y participación de las partes interesadas.
    - Validar la correcta identificación de los riesgos.
    - Brindar apoyo al sistema de gestión de riesgos.
    - Desarrollar una política de comunicación interna y externa clara y transparente.

Introducción al análisis de riesgos

Proceso de gestión del riesgo

Beneficios del proceso de gestión del riesgo:

- Mejora la capacidad de la organización para anticipar y afrontar las amenazas.
- Reduce la probabilidad de pérdidas y daños.
- Optimiza la toma de decisiones estratégicas.
- Aumenta la eficiencia y la eficacia de la organización.
- Genera un ambiente de trabajo más seguro y confiable.

Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura

Introducción

Para una correcta y completa gestión del riesgo de un sistema de información, es fundamental prestar atención a los distintos tipos de agentes e incidencias que pueden afectar al flujo de datos.

Entre los más importantes a considerar se encuentran las vulnerabilidades o fallos de programa y los programas maliciosos (software malicioso).

Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura

Principales tipos de vulnerabilidades/fallos de programa

Una vulnerabilidad es un fallo de seguridad en un programa o en un sistema de información. No todos los fallos de programas son fallos de seguridad, algunos simplemente provocan que funcione incorrectamente o que tenga comportamientos inesperados, sin que ello suponga un riesgo para la información que manejan.

Sin embargo, las vulnerabilidades son, en numerosas ocasiones, el origen de muchos fallos de seguridad y, por ello, deben tomarse en consideración al planificar la gestión de riesgos del sistema de información.

La variedad de vulnerabilidades y fallos de programa es muy amplia y se distingue su tipología atendiendo a sus características especiales.

Entre las vulnerabilidades más importantes, cabe destacar las que se describen a continuación:

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 generan en el momento en el que el usuario configura el sistema erróneamente.
- También pueden surgir vulnerabilidades cuando la configuración por defecto del programa contiene fallos y es insegura.

Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura

Principales tipos de vulnerabilidades/fallos de programa

Entre las vulnerabilidades más importantes, cabe destacar las que se describen a continuación: y (II)

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.

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.

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.
- La vulnerabilidad referente a la inyección de comandos en el sistema operativo puede encontrarse en varios sistemas operativos como Unix/Linux o Microsoft Windows.

Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura

Principales tipos de vulnerabilidades/fallos de programa

Entre las vulnerabilidades más importantes, cabe destacar las que se describen a continuación: y (III)

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.

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).

Fallo de autenticación

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

Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura

Principales tipos de vulnerabilidades/fallos de programa

Entre las vulnerabilidades más importantes, cabe destacar las que se describen a continuación: y (IV)

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.

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.

Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura

Programas maliciosos y su actualización permanente

Un programa malicioso, también conocido como **malware**, es un tipo de software diseñado para que usuarios no autorizados accedan a un sistema de información sin la autorización de su propietario y produzcan efectos indeseados en él.

Dentro de estos programas se engloba una gran variedad de software:

- Virus: Programas que se replican a sí mismos e infectan otros archivos.
- Troyanos: Programas que se camuflan como software legítimo para engañar al usuario y obtener acceso al sistema.
- Gusanos: Programas que se replican a sí mismos y se propagan a través de redes.
- Spyware: Programas que espían la actividad del usuario y recopilan información personal.
- Ransomware: Programas que bloquean el acceso a los archivos del usuario y exigen un rescate para desbloquearlos.

Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura

Programas maliciosos y su actualización permanente

Los programas maliciosos suelen diseñarse para:

- Modificar, obtener o eliminar datos e información almacenada en sistemas de almacenamiento.
- Obtener información generada por el propio usuario o sistema al utilizar un dispositivo determinado.
- Obtener el control de un sistema de información para ser controlado por un atacante o para infectar otros sistemas.

El software malicioso está en continua actualización para conseguir mayor daño e impacto, con el fin de acceder a más sistemas de información. Por ello, es necesario:

- Mantener los sistemas operativos y aplicaciones actualizados, incluyendo antivirus.
- Utilizar sistemas de seguridad más complejos como IDS, IPS, WAFs o SIEMs en las organizaciones.
- Concienciar al personal en materia de ciberseguridad, ya que la mayoría de la transmisión de malware se realiza mediante engaños (ingeniería social), siendo el correo electrónico el medio más usado.

Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura

Criterios de programación segura

La programación segura se define como una rama de la programación que se encarga de la seguridad del código fuente de una aplicación con el fin de solucionar fallos y errores de programa.

Los criterios de programación segura incluyen:

- Protección contra desbordamientos de pila: Se utilizan funciones seguras para evitar problemas provocados por el exceso de flujo de datos en la pila de una función.
- Control del flujo de datos: Se utiliza el flujo de datos para un control continuo del trabajo realizado.
- Pruebas y testeos: Se realizan pruebas y testeos de programas en ejecución para analizar sus fallos y errores.
- Creación de parches: Se crean parches y actualizaciones de programas para arreglar los fallos detectados en las aplicaciones.
- Criptografía y cifrado: Se utilizan técnicas criptográficas y de cifrado para evitar que el software sea modificado por usuarios no autorizados.

Programación segura y gestión de riesgos

La programación segura juega un papel fundamental en la gestión de riesgos de un sistema de información. Al reducir la cantidad de vulnerabilidades y fallos en el código fuente, se minimiza la posibilidad de que los atacantes exploten estas debilidades para acceder a los datos o sistemas sensibles.

Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura

Criterios de programación segura

Beneficios de la programación segura:

- Reduce la probabilidad de ataques: Al eliminar las vulnerabilidades, se reduce la superficie de ataque a la que están expuestos los sistemas.
- Minimiza el impacto de los ataques: Si un ataque tiene éxito, el daño causado será menor si se han implementado prácticas de programación segura.
- Mejora la confianza en los sistemas: Los sistemas desarrollados con seguridad en mente son más confiables y generan mayor confianza en los usuarios.
- Reduce los costes: La prevención de ataques es mucho más económica que la gestión de las consecuencias de un ataque.

La programación segura sirve para:

- Reducir la cantidad de vulnerabilidades y fallos en el código fuente.
- Minimizar la posibilidad de que los atacantes exploten estas debilidades para acceder a los datos o sistemas sensibles.
- Mejorar la seguridad y confiabilidad de los sistemas.

Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura

Criterios de programación segura

La programación segura puede afectar a la gestión de riesgos de un sistema de información de las siguientes maneras:

- Reduciendo la probabilidad de ataques: Al eliminar las vulnerabilidades, se reduce la superficie de ataque a la que están expuestos los sistemas.
- Minimizando el impacto de los ataques: Si un ataque tiene éxito, el daño causado será menor si se han implementado prácticas de programación segura.
- Facilitando la detección de intrusiones: Los sistemas desarrollados con seguridad en mente son más fáciles de monitorizar y detectar intrusiones.
- Ayudando a cumplir con las normas y regulaciones: La implementación de prácticas de programación segura puede ayudar a las organizaciones a cumplir con las normas y regulaciones de seguridad de datos.

La programación segura es una herramienta fundamental para la gestión de riesgos de un sistema de información. Al implementar prácticas de programación segura, las organizaciones pueden proteger sus datos y sistemas de forma más eficaz.

Particularidades de los distintos tipos de código malicioso (malware)

Introducción

Como se ha mencionado en apartados anteriores, malware son un conjunto de programas informáticos diseñados para acceder a un sistema de información de forma no autorizada y provocar daños en este.

Sus principales objetivos son:

- 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 el malware sea cada vez más complejo y variado.

Particularidades de los distintos tipos de código malicioso (malware)

Tipos de Malware

La variada tipología de malware viene dada por su forma, origen, los daños que provocan o la finalidad para la que son diseñados, siendo los más importantes:

- Virus
- Ransomware
- Troyanos
- Keyloggers
- Spyware
- Gusanos o worms

Particularidades de los distintos tipos de código malicioso (malware)

Tipos de Malware

Virus

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

Su funcionamiento también varía según el tipo de virus:

- Suelen alojarse en un archivo "huésped" y provocar daños desde su ubicación.
- Su nivel de daño puede variar: desde la aparición de mensajes molestos hasta el borrado de archivos o del sistema operativo.
- Se contagian principalmente por Internet, pero también por dispositivos de almacenamiento o redes locales.

Ejemplos de virus:

- Virus informático "ILOVEYOU": provocó daños por valor de 5.500 millones de dólares en el año 2000.
- Virus CryptoLocker: cifraba los archivos del usuario y exigía un rescate para descifrarlos.

Particularidades de los distintos tipos de código malicioso (malware)

Tipos de Malware

Ransomware

- El ransomware es un tipo de malware que cifra los archivos del usuario y exige un rescate para descifrarlos.
- Es una amenaza creciente, ya que los ataques son cada vez más sofisticados y los rescates son cada vez más altos.

Ejemplos de ransomware:

- WannaCry: infectó a más de 200.000 equipos en 150 países en 2017.
- REvil: ha sido utilizado para atacar a empresas como Kaseya y JBS.

Troyanos

- Son aplicaciones que contienen funcionalidades ocultas con finalidades maliciosas para el usuario.
- No se propagan por sí mismos, sino que se instalan en el equipo del usuario a través de engaños.

Ejemplos de troyanos:

- Zeus: utilizado para robar información bancaria.
- Emotet: utilizado para descargar otros tipos de malware.

Particularidades de los distintos tipos de código malicioso (malware)

Tipos de Malware

Keyloggers

- Los keyloggers son programas que registran las pulsaciones del teclado del usuario.
- Esta información puede ser utilizada para robar contraseñas, números de tarjeta de crédito y otros datos

Ejemplos de keyloggers:

- GoldenEye: utilizado para robar información de gobiernos y empresas.
- Predator Pain: utilizado para robar información de usuarios de videojuegos.

Spyware

- El spyware es un tipo de malware que recopila información sobre el usuario sin su consentimiento.
- Esta información puede ser utilizada para fines publicitarios o para el robo de identidad.

Ejemplos de spyware:

- Pegasus: utilizado por gobiernos para espiar a disidentes políticos y periodistas.
- FinFisher: utilizado por las fuerzas del orden para espiar a sospechosos de delitos.

Particularidades de los distintos tipos de código malicioso (malware)

Tipos de Malware

Gusanos o worms

- Los gusanos son programas maliciosos que se propagan por sí mismos a través de redes informáticas.
- No suelen causar daños graves, pero pueden consumir recursos del sistema y ralentizar el rendimiento.

Ejemplos de gusanos:

- Morris: el primer gusano de Internet, que infectó a más de 6.000 equipos en 1988.
- I Love You: un gusano que se propagó por correo electrónico en el año 2000.

Herramientas para combatir el malware

- No existe una única herramienta que sirva para combatir todos los tipos de malware.
- Las herramientas más importantes son:
  - Antivirus: detectan y eliminan virus, troyanos, gusanos y otros tipos de malware.
  - Antispyware: detectan y eliminan spyware.

Principales elementos del análisis de riesgos y sus modelos de relaciones

Elementos del análisis de riesgos

El proceso de gestión de riesgos conlleva el análisis de una serie de elementos importantes del sistema de información:

- Activos: Recursos del sistema de información necesarios para el correcto funcionamiento de la organización.
- Amenazas: Eventos que pueden afectar a un activo, provocando un incidente de seguridad y produciendo efectos adversos.
- Vulnerabilidades: Características o capacidades de un activo que lo hacen susceptible a amenazas.
- Riesgo: Posibilidad de que una amenaza se materialice causando efectos negativos o positivos.
- Control atenuante o Salvaguardas: Activos y medidas que reducen las posibilidades de amenazas y el nivel de riesgo.
- Impacto: Magnitud del daño que provoca un ataque exitoso.
- Probabilidad: Estimación de las posibilidades de que se materialice un riesgo.

Principales elementos del análisis de riesgos y sus modelos de relaciones

Elementos del análisis de riesgos

Activos:

- Un activo es cualquier recurso del sistema de información que es necesario para el correcto funcionamiento de la organización.
- Los activos pueden ser tangibles (hardware, software) o intangibles (información, datos).
- Es importante identificar todos los activos de la organización y clasificarlos según su importancia.

Amenazas:

- Una amenaza es cualquier evento que puede ocurrir y que puede causar daño a un activo.
- Las amenazas pueden ser de origen interno (errores humanos, fallos técnicos) o externo (ataques cibernéticos, desastres naturales).
- Es importante identificar todas las amenazas potenciales y evaluar su probabilidad de ocurrencia.

Vulnerabilidades:

- Una vulnerabilidad es una debilidad en un activo que lo hace susceptible a una amenaza.
- Las vulnerabilidades pueden ser técnicas (fallos de seguridad en el software) o humanas (falta de formación del personal).
- Es importante identificar todas las vulnerabilidades del sistema de información y tomar medidas para mitigarlas.

Principales elementos del análisis de riesgos y sus modelos de relaciones

Elementos del análisis de riesgos

Riesgo:

- El riesgo es la probabilidad de que una amenaza se materialice y cause daño a un activo.
- El riesgo se calcula como la probabilidad de ocurrencia de la amenaza multiplicada por el impacto potencial de la amenaza.
- Es importante evaluar el riesgo de cada amenaza y tomar medidas para reducirlo a un nivel aceptable.

Controles atenuantes:

- Un control atenuante es una medida que se toma para reducir la probabilidad de ocurrencia de una amenaza o el impacto potencial de una amenaza.
- Los controles atenuantes pueden ser técnicos (firewalls, antivirus) o humanos (políticas de seguridad, formación del personal).
- Es importante implementar una serie de controles atenuantes para proteger los activos de la organización.

Impacto:

- El impacto es el daño que se produce cuando una amenaza se materializa.
- El impacto puede ser financiero, operativo, reputacional o legal.
- Es importante evaluar el impacto potencial de cada amenaza para poder tomar las medidas adecuadas para proteger los activos de la organización.

Principales elementos del análisis de riesgos y sus modelos de relaciones

Elementos del análisis de riesgos

Probabilidad:

- La probabilidad es la posibilidad de que una amenaza se materialice.
- La probabilidad se puede estimar en función de la frecuencia de ocurrencia de la amenaza en el pasado y de las medidas de seguridad que se han implementado.
- Es importante evaluar la probabilidad de cada amenaza para poder tomar las medidas adecuadas para reducir el riesgo.

Análisis cualitativo y cuantitativo:

- El análisis de riesgos puede ser cualitativo o cuantitativo.
- El análisis cualitativo se basa en la identificación y evaluación de los riesgos de forma subjetiva.
- El análisis cuantitativo se basa en la asignación de valores numéricos a los riesgos para poder compararlos y priorizarlos.
- El análisis de riesgos es un proceso continuo que debe revisarse y actualizarse periódicamente. Esto es importante para asegurar que la organización está protegida contra las amenazas emergentes.

Principales elementos del análisis de riesgos y sus modelos de relaciones

Elementos del análisis de riesgos

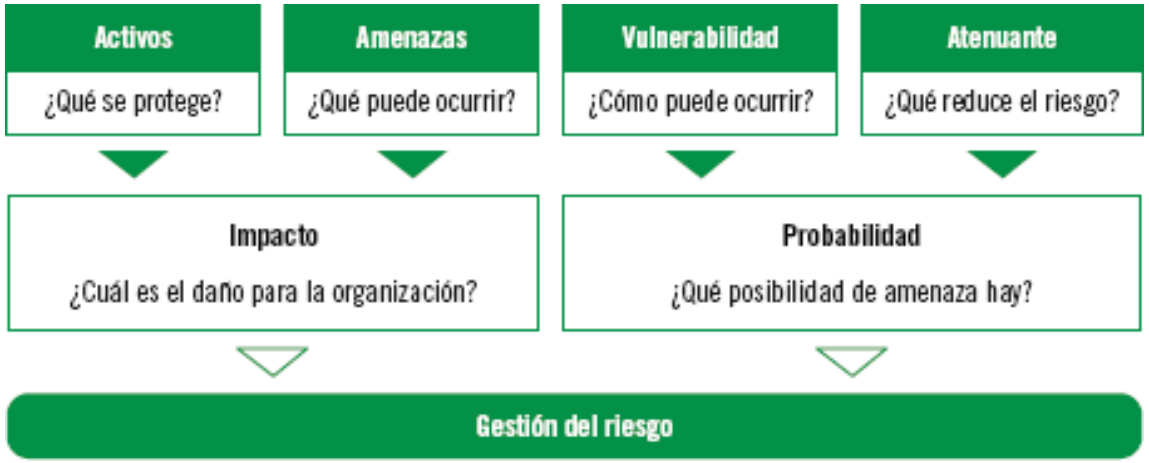
Además de los elementos mencionados anteriormente, el análisis de riesgos también puede considerar otros factores, como:

- El contexto legal y regulatorio: Las organizaciones deben cumplir con las leyes y regulaciones que se aplican a su sector.
- La cultura de la organización: La cultura de la organización puede influir en la forma en que se gestionan los riesgos.
- Los recursos disponibles: La organización debe tener los recursos necesarios para implementar las medidas de control necesarias.

Principales elementos del análisis de riesgos y sus modelos de relaciones

Modelos de relaciones de conceptos de gestión de riesgos

Las relaciones entre los conceptos definidos anteriormente se reflejan de la siguiente manera:



Una correcta gestión del riesgo se basa en determinar el impacto y la probabilidad de un riesgo potencial:

- Impacto: Se calcula con un análisis profundo de los activos y las amenazas.
- Probabilidad: Se calcula con un análisis de las vulnerabilidades y los atenuantes.

A mayor impacto y probabilidad, mayor riesgo. A menor impacto y probabilidad, menor riesgo.

Principales elementos del análisis de riesgos y sus modelos de relaciones

Modelos de relaciones de conceptos de gestión de riesgos

Ejemplo:

- Activo: Servidor web
- Amenaza: Ataque cibernético
- Vulnerabilidad: Software desactualizado
- Riesgo: Robo de datos
- Impacto: Pérdida financiera, daño reputacional
- Probabilidad: Media

Para reducir el riesgo, se pueden implementar medidas de control atenuantes, como:

- Implementar un firewall
- Actualizar el software
- Capacitar al personal en seguridad informática

Metodologías cualitativas y cuantitativas de análisis de riesgos

Introducción

Los controles de seguridad son medidas que se implementan para mitigar las vulnerabilidades y reducir el riesgo en un sistema de información. Existen cuatro tipos principales de controles:

- Disuasorios: Su objetivo principal es reducir la probabilidad de un ataque.
- Preventivos: Protegen al sistema de información de sus vulnerabilidades, intentando impedir el acceso de los atacantes o reduciendo el impacto de los daños causados.
- Correctivos: Su objetivo principal es reducir el impacto de una amenaza.
- Detectivos: Se encargan de detectar e impedir posibles ataques.

La gestión de riesgos debe determinar qué controles son los más adecuados, eficientes y rentables para cada caso. Para ello, existen dos metodologías principales para realizar el análisis de riesgos:

- Metodología cuantitativa. Se basa en la asignación de valores numéricos a los riesgos para poder compararlos y priorizarlos. Permite obtener una evaluación precisa del riesgo, pero requiere de datos históricos y modelos matemáticos complejos. Es útil para organizaciones con grandes volúmenes de datos y recursos para invertir en análisis sofisticados.
- Metodología cualitativa. Se basa en la evaluación subjetiva del riesgo por parte de expertos. Es más rápida y menos costosa que la metodología cuantitativa, pero puede ser menos precisa. Es útil para organizaciones con recursos limitados o que necesitan una evaluación rápida del riesgo.

Metodologías cualitativas y cuantitativas de análisis de riesgos

Metodología cuantitativa.

La metodología cuantitativa de análisis de riesgos se basa en la asignación de valores numéricos a los riesgos para poder compararlos y priorizarlos. Este enfoque tiene en cuenta dos elementos principales:

- Probabilidad de ocurrencia: Es la posibilidad de que un evento de riesgo se materialice.
- Impacto: Es el daño potencial que un evento de riesgo puede causar si se materializa.

Para determinar y analizar los riesgos, la metodología cuantitativa se basa en un modelo matemático que combina la probabilidad y el impacto. Este modelo permite obtener una evaluación precisa del riesgo, lo que facilita la toma de decisiones sobre la implementación de medidas de control.

Ventajas de la metodología cuantitativa:

- Facilita la comparación de riesgos: Permite comparar riesgos con características muy diferentes, lo que facilita la toma de decisiones sobre la asignación de recursos.
- Apoya la toma de decisiones: Proporciona información numérica que puede ser utilizada para justificar la aplicación de medidas de gestión de riesgos.
- Sirve como herramienta de medición: Permite medir la eficacia de las medidas de control implementadas.

Metodologías cualitativas y cuantitativas de análisis de riesgos

Metodología cuantitativa.

Desventajas de la metodología cuantitativa:

- Requiere de datos históricos: Para obtener resultados precisos, se necesitan datos históricos sobre la probabilidad de ocurrencia e impacto de los eventos de riesgo.
- Puede ser costosa: El desarrollo e implementación de modelos matemáticos puede ser costoso y requerir de la participación de profesionales especializados.
- Dificultad de actualización: Los modelos matemáticos pueden ser difíciles de actualizar y mantener al día con los cambios en el entorno de riesgo.
- Limitaciones en la cuantificación: No todos los riesgos pueden ser cuantificados, lo que limita la utilidad de la metodología cuantitativa en algunos casos.

Metodologías cualitativas y cuantitativas de análisis de riesgos

Metodología cualitativa.

La metodología cualitativa de análisis de riesgos se basa en el juicio y la experiencia de expertos para evaluar los riesgos. A diferencia de la metodología cuantitativa, no utiliza valores numéricos para calcular la probabilidad o el impacto de los eventos de riesgo.

En esta metodología, se utilizan técnicas como:

- Análisis FODA (Fortalezas, Oportunidades, Debilidades, Amenazas): Permite identificar las fortalezas y debilidades de la organización, así como las oportunidades y amenazas del entorno.
- Brainstorming: Permite a un grupo de expertos generar ideas y opiniones sobre los riesgos que enfrenta la organización.
- Delphi: Es una técnica que permite obtener la opinión de un grupo de expertos de forma anónima y estructurada.

La metodología cualitativa es útil para:

- Identificar riesgos: Es especialmente útil para identificar riesgos nuevos o desconocidos, así como riesgos que son difíciles de cuantificar.
- Evaluar riesgos: Permite obtener una comprensión profunda de los riesgos y sus posibles impactos.
- Priorizar riesgos: Permite ordenar los riesgos según su importancia y urgencia.

Metodologías cualitativas y cuantitativas de análisis de riesgos

Metodología cualitativa.

Ventajas de la metodología cualitativa:

- Flexibilidad: Permite adaptar el análisis a las necesidades específicas de la organización.
- Rapidez: Es una metodología relativamente rápida y sencilla de aplicar.
- Costo: Es menos costosa que la metodología cuantitativa.
- Participación: Permite la participación de un grupo de expertos con diferentes perspectivas.

Desventajas de la metodología cualitativa:

- Subjetividad: Los resultados del análisis dependen de la experiencia y el juicio de los expertos.
- Inconsistencia: Los resultados pueden ser inconsistentes si no se utilizan técnicas adecuadas.
- Dificultad de comparación: Es difícil comparar los resultados de diferentes análisis cualitativos.

Identificación de los activos involucrados en el análisis de riesgos y su valoración

Introducción

El análisis de riesgos es un proceso fundamental para la seguridad de la información. Este proceso implica la identificación, evaluación y tratamiento de los riesgos que pueden afectar a un sistema de información.

Las primeras etapas del análisis de riesgos son la identificación y valoración de los activos.

Identificación de activos

Un activo es cualquier recurso del sistema de información o relacionado con este que es necesario para el correcto funcionamiento de la organización y para que se alcancen los objetivos definidos por esta.

Los activos pueden ser:

- Información: Datos, documentos, registros, etc.
- Servicios: Prestados con la utilización de la información.
- Equipos y soportes de información: Ordenadores, dispositivos de almacenamiento, etc.
- Equipos informáticos: Que permiten la gestión de la información.
- Aplicaciones: Que permiten gestionar la información y los servicios que se proporcionan a través de esta.
- Redes de comunicaciones: Que permiten el intercambio de información.
- Instalaciones: En las que se ubican los equipos informáticos, dispositivos, sistemas de almacenamiento y redes de comunicaciones.
- Recursos humanos: Que utilizan todos los elementos anteriores.
- Cada organización debe conocer sus peculiaridades y analizar los activos que son más relevantes para su sistema de información.

Identificación de los activos involucrados en el análisis de riesgos y su valoración

Valoración de activos

La valoración de los activos es una parte fundamental del análisis y gestión del riesgo. Permite determinar la importancia de cada activo para la organización y, por lo tanto, el nivel de riesgo que se debe asumir para protegerlo.

El valor de un activo se define como el coste que implicaría recuperarse de un fallo del mismo.

Este coste puede ser:

- Financiero: Coste de mano de obra, ingresos perdidos, coste de reposición, etc.
- Reputacional: Pérdida de confianza y calidad de los clientes y proveedores.
- Legal: Infracciones y sanciones por incumplimiento de leyes o contratos.
- Operativo: Daños a otros activos, daños al medio ambiente, daños a personas.

Los factores que influyen en la valoración de un activo son:

- Criticidad: Impacto que el fallo del activo tendría en la organización.
- Valor monetario: Coste de adquisición y reposición del activo.
- Sensibilidad: Vulnerabilidad del activo a las amenazas.
- Requisitos legales y reglamentarios: Obligaciones legales relacionadas con el activo.

Identificación de los activos involucrados en el análisis de riesgos y su valoración

Valoración de activos

Existen dos tipos principales de valoraciones de activos:

Valoración cuantitativa:

Se basa en la asignación de valores numéricos a los activos. Permite obtener una evaluación precisa del valor de los activos. Requiere de datos históricos y modelos matemáticos complejos. Es útil para organizaciones con grandes volúmenes de datos y recursos para invertir en análisis sofisticados.

Valoración cualitativa:

- Se basa en la asignación de valores no numéricos a los activos (por ejemplo, bajo, medio, alto). Es más rápida y menos costosa que la valoración cuantitativa. Puede ser menos precisa que la valoración cuantitativa.
- Es útil para organizaciones con recursos limitados o que necesitan una evaluación rápida del valor de los activos.

Existen otros métodos para valorar activos, como:

- Análisis del impacto en el negocio (BIA): Evalúa el impacto que la pérdida o el daño de un activo tendría en la organización.
- Análisis del valor del activo (AVA): Determina el valor monetario del activo.
- Análisis de riesgos legales y reglamentarios: Evalúa los requisitos legales y reglamentarios relacionados con el activo.

Identificación de los activos involucrados en el análisis de riesgos y su valoración

Valoración de activos

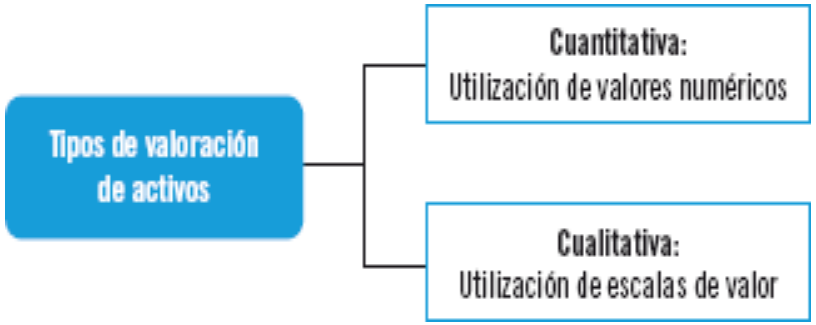
Independientemente del tipo de valoración que se utilice, es importante tener en cuenta dos aspectos básicos:

- Homogeneidad:

  Es necesario poder comparar los valores de los activos, aunque sean de diferentes tipos. Esto se puede lograr utilizando unidades de medida comunes o normalizando los valores.

- Relatividad:

  Es importante tener en cuenta el valor de un activo en relación con los demás activos. Un activo puede tener un valor alto en términos absolutos, pero bajo en comparación con otros activos. Al tener en cuenta estos dos aspectos, se puede obtener una valoración más precisa y útil de los activos.



Identificación de los activos involucrados en el análisis de riesgos y su valoración

Dimensiones en la valoración de activos

La valoración de un activo no puede basarse en una única dimensión, sino que debe considerar todas las dimensiones relevantes. Las principales dimensiones de valoración de los activos son:

Disponibilidad:

¿Cuál sería la importancia del activo si no estuviera disponible?

Se refiere al tiempo durante el cual el activo está disponible para su uso. Un activo con alta disponibilidad es aquel que está disponible la mayor parte del tiempo.

Integridad:

¿Qué importancia tendría que el activo sufriera modificaciones descontroladas?

Se refiere a la precisión y completitud del activo. Un activo con alta integridad es aquel que es preciso y completo.

Confidencialidad:

¿Cuál sería la importancia del conocimiento del activo por usuarios no autorizados?

Se refiere a la protección del activo contra el acceso no autorizado. Un activo con alta confidencialidad es aquel que solo es accesible para usuarios autorizados.

Identificación de los activos involucrados en el análisis de riesgos y su valoración

Dimensiones en la valoración de activos

La valoración de un activo no puede basarse en una única dimensión, sino que debe considerar todas las dimensiones relevantes. Las principales dimensiones de valoración de los activos son:

Autenticidad:

¿Cuál sería la importancia del acceso al activo por parte de personas no autorizadas?

Se refiere a la seguridad de que el activo es lo que dice ser. Un activo con alta autenticidad es aquel que es genuino y no ha sido falsificado.

Trazabilidad:

¿Cuál sería la importancia de la falta de constancia de la utilización del activo?

Se refiere a la capacidad de rastrear el uso del activo. Un activo con alta trazabilidad es aquel que se puede rastrear desde su origen hasta su destino.

Habitualmente en la valoración de activos utilizamos básicamente los tres pilares fundamentales de la ciberseguridad (Disponibilidad, Integridad y confidencialidad) para agilizar los procesos.

Identificación de las amenazas que pueden afectar a los activos identificados previamente

Introducción

Una amenaza es un evento o acción que puede ocurrir y que tiene el potencial de causar daño a un activo.

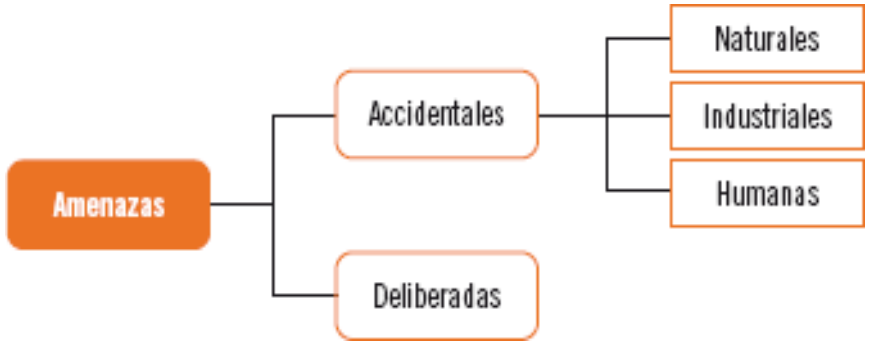
Las amenazas pueden ser:

- Accidentales: Ocurren sin la intención de causar daño.

  Ejemplos: desastres naturales, fallos eléctricos, errores humanos.

- Deliberadas: Se llevan a cabo con la intención de causar daño.

  Ejemplos: ataques cibernéticos, robo de información, fraude.



Identificación de las amenazas que pueden afectar a los activos identificados previamente

Identificación de amenazas

La identificación de las amenazas es un paso crucial en el análisis de riesgos. Permite a la organización comprender los peligros que enfrenta y tomar medidas para proteger sus activos.

Para identificar las amenazas, se pueden utilizar diferentes técnicas:

- Análisis de activos: Permite identificar los activos de la organización y sus características, como su valor, criticidad y vulnerabilidades.
- Análisis del entorno: Permite identificar las amenazas que existen en el entorno de la organización, como las amenazas naturales, las amenazas tecnológicas y las amenazas sociales.
- Brainstorming: Permite a un grupo de expertos generar ideas sobre las posibles amenazas que enfrenta la organización.
- Análisis de vulnerabilidades: Permite identificar las debilidades del sistema de información que pueden ser explotadas por las amenazas.

Es importante tener en cuenta que las amenazas pueden cambiar con el tiempo. Por lo tanto, es necesario realizar un análisis de riesgos de forma regular para identificar las nuevas amenazas y actualizar las medidas de control.

Una vez que se han identificado las amenazas, se debe proceder a su evaluación. La evaluación de las amenazas consiste en determinar la probabilidad de que ocurran y el impacto que podrían causar si se materializan.

Identificación de las amenazas que pueden afectar a los activos identificados previamente

Identificación de amenazas

Ejemplos de las amenazas más frecuentes:

- Suplantación: Envío de correos electrónicos con la identidad de otro usuario.
- Alteración: Modificación no autorizada de los datos de un archivo.
- Repudio: Empleado que elimina datos importantes del sistema y que, posteriormente, niega este hecho.
- Divulgación de información: Envío por error de correos electrónicos con datos confidenciales de los clientes de la organización.
- Denegación del servicio: Ataque de denegación del servicio mediante el envío excesivo de datos al sistema de información, provocando su saturación y evitando el acceso de otros usuarios.
- Elevación de privilegios: Obtención y utilización de los privilegios y permisos del administrador sin autorización.

Identificación de las amenazas que pueden afectar a los activos identificados previamente

Valoración de las amenazas

Las amenazas se valoran en función del impacto que generan sobre un activo y de la vulnerabilidad de ese activo.

El impacto de una amenaza se define como la medición del daño potencial que puede causar a uno o varios activos. Se calcula considerando los siguientes elementos:

- Daños a los activos de la organización: Pérdida financiera, daño a la reputación, interrupción del negocio, etc.
- Capacidad de reproducción y expansión de la amenaza: Probabilidad de que la amenaza se propague a otros activos del sistema.
- Capacidad de explotación de la amenaza: Facilidad con la que un atacante puede aprovechar la vulnerabilidad del activo.
- Usuarios que se pueden ver afectados: Número de usuarios que podrían verse afectados por la materialización de la amenaza.
- Capacidad de detección y descubrimiento de la amenaza: Facilidad con la que se puede identificar la amenaza una vez que se ha producido.

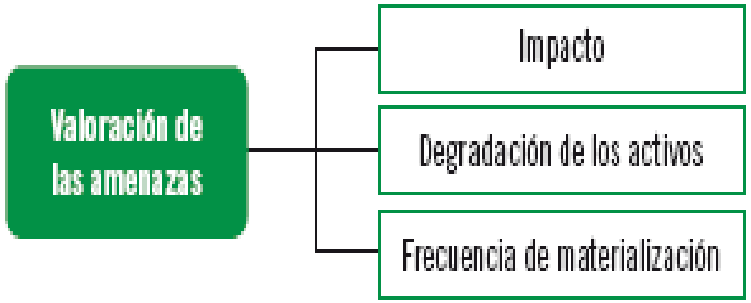
¿Qué es la vulnerabilidad de un activo? La vulnerabilidad de un activo se refiere a la facilidad con la que puede ser explotado por una amenaza. Se considera:

- Degradación del activo: Perjuicio que sufriría el activo si la amenaza se materializa.
- Frecuencia de la amenaza: Probabilidad de que la amenaza ocurra en un período de tiempo determinado.

Identificación de las amenazas que pueden afectar a los activos identificados previamente

Valoración de las amenazas

Las amenazas por tanto se valoran en función del impacto que generan, la degradación de los activos afectados y la frecuencia con la que se materializan.



Análisis e identificación de las vulnerabilidades existentes en los sistemas de información

Introducción

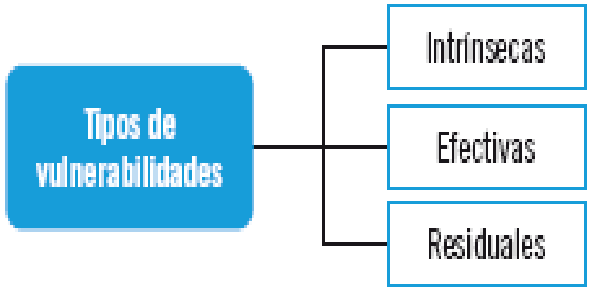
Una vulnerabilidad es una debilidad en un sistema de información que puede ser explotada por una amenaza para causar daño. El análisis e identificación de vulnerabilidades es un paso crucial para proteger los activos de la organización.

Tipos de vulnerabilidades

- Vulnerabilidad intrínseca: Propia del activo y de la amenaza.
- Vulnerabilidad efectiva: Generada por una salvaguarda existente en el sistema.
- Vulnerabilidad residual: Generada por la aplicación de salvaguardas tras el análisis de riesgos.

Medición de la vulnerabilidad

- Periodo de tiempo: Transcurrido entre la amenaza potencial y su materialización.
- Frecuencia: Probabilidad de que la amenaza se materialice.



Análisis e identificación de las vulnerabilidades existentes en los sistemas de información

Introducción

Ejemplos de vulnerabilidades

- Seguridad física: Accesos no autorizados, desastres naturales, incendios.
- Conexiones de red: Fallos en el cortafuegos, intrusiones no autorizadas.
- Infraestructura de red: Fallos en routers, hubs, switches.
- Correo electrónico.
- Aplicaciones de gran valor y sistemas operativos.

Escalas de valor de vulnerabilidades

Valor	Frecuencia	Probabilidad
Muy frecuente	Varias veces al día	Entre el 75 y el 100%
Bastante frecuente	Una vez al día	Entre el 50 y el 75%
Frecuente	Una vez en semana	Entre el 25 y el 50%
Poco frecuente	Una vez al mes	25% o menos

Análisis e identificación de las vulnerabilidades existentes en los sistemas de información

Introducción

Herramientas y técnicas de análisis de vulnerabilidades

- Análisis local: Se realiza en el propio sistema de información.
- Análisis remoto de caja blanca: Se realiza desde un equipo externo con acceso al código fuente del sistema.
- Análisis de caja negra: Se realiza desde un equipo externo sin acceso al código fuente del sistema.

Análisis e identificación de las vulnerabilidades existentes en los sistemas de información

Análisis local para la detección de vulnerabilidades

El análisis local de vulnerabilidades se basa en la ejecución de pruebas de software dentro del sistema de información. Estas pruebas buscan obtener información objetiva sobre la calidad de las aplicaciones y sistemas operativos presentes.

Tipos de pruebas:

- Pruebas estáticas: No requieren la ejecución del código de la aplicación. Se analizan elementos como el código fuente, la estructura del programa o la configuración del sistema.
- Pruebas dinámicas: Se ejecutan mientras la aplicación está en funcionamiento. Permiten observar el comportamiento real del sistema y detectar errores o vulnerabilidades que no se manifiestan en el análisis estático.

Herramientas y métodos:

Las pruebas, tanto estáticas como dinámicas, utilizan diversas herramientas y métodos para detectar y medir las vulnerabilidades. Algunas de las más comunes son:

- Análisis de código fuente: Revisión del código para identificar errores de programación, debilidades de seguridad o prácticas no recomendables.
- Herramientas de escaneo de vulnerabilidades: Automatizan la búsqueda de vulnerabilidades conocidas en el sistema.
- Pruebas de penetración: Simulaciones de ataques reales para evaluar la capacidad del sistema para resistirlos.

Análisis e identificación de las vulnerabilidades existentes en los sistemas de información

Análisis de caja blanca

Enfoque:

- Se basa en el examen minucioso del código fuente, la estructura interna y los componentes del sistema.
- Requiere acceso completo al código, archivos de configuración, documentación y demás información relevante.

Objetivos:

- Detectar errores de programación, debilidades de seguridad y prácticas no recomendables.
- Evaluar la lógica interna del sistema y su susceptibilidad a ataques.
- Identificar vulnerabilidades potenciales que no se manifiestan en pruebas superficiales.

Técnicas:

- Análisis estático: Revisión manual del código fuente para identificar errores y debilidades.
- Herramientas de análisis estático: Automatizan la búsqueda de patrones de código que representan vulnerabilidades conocidas.
- Pruebas de penetración de caja blanca: Simulaciones de ataques que aprovechan el conocimiento del código fuente para encontrar vulnerabilidades.

Análisis e identificación de las vulnerabilidades existentes en los sistemas de información

Análisis de caja blanca

Ejemplos de herramientas de análisis de caja blanca:

- Fortify: Herramienta de análisis estático que identifica una amplia gama de vulnerabilidades en código fuente.
- AppScan: Herramienta de análisis estático y dinámico que escanea aplicaciones web en busca de vulnerabilidades.
- IDA Pro: Desensamblador de código que permite analizar el código máquina de forma detallada.

Ventajas:

- Mayor precisión en la detección de vulnerabilidades, tanto inmediatas como potenciales.
- Recomendaciones más precisas y eficaces para la mejora de la seguridad.
- Permite comprender mejor el funcionamiento interno del sistema.

Desventajas:

- Requiere más tiempo, recursos y conocimientos técnicos especializados.
- No siempre es posible obtener acceso completo al código fuente.
- No simula intrusiones reales, lo que limita la evaluación de la efectividad de las medidas de seguridad

Análisis e identificación de las vulnerabilidades existentes en los sistemas de información

Análisis de caja negra

Enfoque:

- Se basa en la evaluación de las entradas, salidas y comportamiento del sistema sin acceso a su estructura interna.
- Se asemeja a la perspectiva de un atacante que no tiene conocimiento del código fuente.

Objetivos:

- Identificar vulnerabilidades que pueden ser explotadas por un atacante sin conocimiento interno del sistema.
- Obtener información real sobre los riesgos a los que se expone el sistema.
- Simular ataques y evaluar la capacidad del sistema para resistirlos.

Técnicas:

- Pruebas de caja negra: Simulación de diferentes tipos de ataques, como inyección de código, ataques de denegación de servicio y ataques de phishing.
- Análisis de tráfico de red: Monitoreo y análisis del tráfico de red para identificar patrones sospechosos que puedan indicar un ataque.
- Herramientas de fuzzing: Automatizan la generación de entradas maliciosas para probar la robustez del sistema..

Análisis e identificación de las vulnerabilidades existentes en los sistemas de información

Análisis de caja negra

Ejemplos de herramientas de análisis de caja blanca:

- Nessus: Escáner de vulnerabilidades que identifica una amplia gama de vulnerabilidades en sistemas y aplicaciones.
- Nmap: Herramienta para el mapeo de redes y la identificación de hosts y servicios vulnerables.
- Metasploit: Framework de pruebas de penetración que incluye una gran cantidad de exploits para diferentes tipos de vulnerabilidades.

Ventajas:

- Menores recursos necesarios para la realización de las pruebas.
- Permite obtener una perspectiva real de las amenazas a las que se enfrenta el sistema.
- No requiere acceso al código fuente.

Desventajas:

- Las vulnerabilidades más profundas pueden pasar desapercibidas.
- Dificultad para obtener información pública relevante.
- Las recomendaciones son menos precisas y de carácter más general.

Optimización del proceso de auditoría y contraste de vulnerabilidades e informe de auditoría

Informe de auditoría

El informe de auditoría es un componente fundamental para la mejora continua de la seguridad de un sistema de información. Este documento debe reflejar la información recopilada durante la evaluación, las conclusiones obtenidas y las recomendaciones para optimizar el proceso de auditoría en el futuro.

Influencia de la conservación de datos históricos

La conservación de datos históricos de amenazas y vulnerabilidades detectadas es fundamental para optimizar el proceso de auditoría en futuras evaluaciones. Permite:

- Identificar tendencias y patrones: Observar la evolución de las amenazas y vulnerabilidades a lo largo del tiempo ayuda a predecir futuros riesgos y a enfocar las medidas de seguridad de forma más efectiva.
- Evaluar la eficacia de las medidas correctoras: Comparar los datos históricos con los resultados de nuevas auditorías permite determinar si las medidas tomadas para corregir las vulnerabilidades han sido efectivas.
- Mejorar la planificación de las auditorías: El conocimiento de las amenazas y vulnerabilidades más comunes en el sector o en la organización facilita la priorización de las áreas a evaluar en futuras auditorías.
- Justificar las inversiones en seguridad: Los datos históricos pueden ser utilizados para demostrar la necesidad de invertir en medidas de seguridad específicas para mitigar riesgos concretos.

Optimización del proceso de auditoría y contraste de vulnerabilidades e informe de auditoría

Informe de auditoría

Contenido del informe de auditoría

- Objetivos de la auditoría: Descripción clara de los propósitos de la evaluación.
- Metodologías utilizadas: Detalle de las técnicas y herramientas empleadas en la auditoría.
- Resultados obtenidos: Descripción precisa de las vulnerabilidades y amenazas detectadas.
- Conclusiones y recomendaciones: Resumen de los hallazgos de la auditoría y propuestas de medidas para mejorar la seguridad del sistema.
- Histórico de vulnerabilidades: Registro de las vulnerabilidades detectadas en auditorías anteriores, su evolución y las medidas tomadas para corregirlas.
- Modificaciones del sistema de información: Detalle de las modificaciones realizadas en el sistema en base a las recomendaciones de auditorías previas.

Características del informe de auditoría

- Claridad y concisión: El lenguaje utilizado debe ser comprensible para los diferentes lectores del informe.
- Oportunidad: El informe debe ser presentado en un plazo razonable tras la finalización de la auditoría.
- Objetividad e imparcialidad: Las conclusiones y recomendaciones deben basarse en los resultados de la auditoría y no en opiniones subjetivas.
- Independencia: El informe debe ser elaborado por auditores independientes que no tengan ningún conflicto de intereses con la organización auditada.

Optimización del proceso de auditoría y contraste de vulnerabilidades e informe de auditoría

Informe de auditoría

Fundamentación de las recomendaciones

Es crucial que las recomendaciones del informe de auditoría estén debidamente fundamentadas en los resultados obtenidos. Esto significa que las propuestas deben:

- Estar basadas en las vulnerabilidades y amenazas detectadas.
- Ser realistas y viables desde el punto de vista técnico y económico.
- Considerar las necesidades y objetivos de la organización.
- Estar acompañadas de un plan de acción para su implementación.

Identificación de las medidas de salvaguarda existentes en el momento de la realización del análisis de riesgos y su efecto sobre las vulnerabilidades y amenazas

Introducción

Las medidas de salvaguarda o seguridad son esenciales para reducir o eliminar los riesgos asociados a un sistema de información. La identificación y evaluación de estas medidas, junto con su impacto en las vulnerabilidades y amenazas, es un paso crucial para la gestión eficaz de la seguridad.

Efectos de las medidas de salvaguarda

Las medidas de salvaguarda pueden actuar de dos maneras:

- Reducción de la probabilidad de materialización de las amenazas: Son las salvaguardas preventivas, ideales para evitar por completo la materialización de cualquier amenaza.
- Reducción del impacto de las amenazas sobre la organización: Limitan o reducen la degradación del activo ante una amenaza, impidiendo que el daño se expanda. Algunas incluso pueden restaurar el sistema cuando ha sido dañado.

Identificación de las medidas de salvaguarda existentes en el momento de la realización del análisis de riesgos y su efecto sobre las vulnerabilidades y amenazas

Introducción

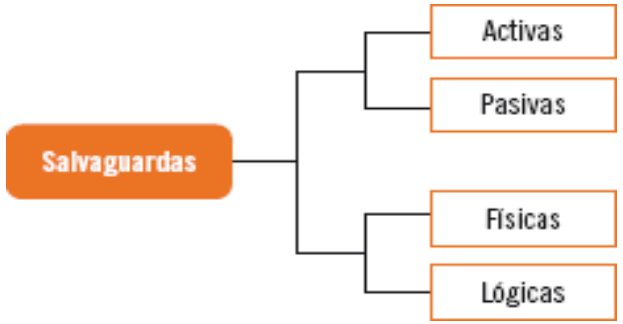
Clasificación de las medidas de salvaguarda (Diferentes criterios)

Momento de actuación:

- Salvaguardas activas: Reducen o eliminan el riesgo de una amenaza.
- Salvaguardas pasivas: Reducen el impacto sobre la organización después de un incidente de seguridad.

Composición y tipo de protección:

- Salvaguardas físicas: Protegen el acceso físico a los activos y las condiciones ambientales.
- Salvaguardas lógicas: Protegen los activos mediante herramientas, técnicas y programas informáticos.



Identificación de las medidas de salvaguarda existentes en el momento de la realización del análisis de riesgos y su efecto sobre las vulnerabilidades y amenazas

Introducción

Eficacia de las salvaguardas

Una salvaguarda ideal sería 100% eficaz, pero esto requiere:

- Implantación, configuración y mantenimiento perfectos.
- Uso constante y correcto.
- Protocolo de uso claro y formación del personal para reaccionar ante incidencias.
- Controles para detectar fallos.

En la práctica, estas condiciones son difíciles de cumplir, por lo que las organizaciones deben buscar un equilibrio entre la eficacia de las salvaguardas y la viabilidad de su implementación.

Vulnerabilidades de las salvaguardas

Incluso las mejores salvaguardas pueden tener vulnerabilidades. Para reducirlas, las organizaciones deben:

- Realizar pruebas y evaluaciones periódicas.
- Implementar un seguimiento continuo.
- Detectar y corregir las vulnerabilidades que puedan aparecer.

Identificación de las medidas de salvaguarda existentes en el momento de la realización del análisis de riesgos y su efecto sobre las vulnerabilidades y amenazas

Salvaguardas y activos

Las salvaguardas son medidas de seguridad que se implementan para proteger los activos de un sistema de información. Si bien estas medidas son cruciales para reducir el riesgo, es importante considerar cómo pueden afectar a los activos y al análisis de riesgos general.

En algunos casos, las salvaguardas pueden formar parte del equipamiento de un sistema de información. Esto puede aumentar el valor del activo al que protege, convirtiéndolo en parte integral del mismo.

Es importante recordar que las salvaguardas no son infalibles. Al integrarse al sistema, también se vuelven susceptibles a los mismos riesgos que los demás activos. Esto significa que pueden tener vulnerabilidades y estar expuestas a las mismas amenazas.

Es crucial realizar un nuevo análisis de riesgos después de implementar una salvaguarda que forma parte del activo. Esto permite:

- Evaluar el impacto de la salvaguarda en el riesgo general del sistema.
- Asegurar que el nuevo riesgo es inferior al que existía antes de la implementación.
- Verificar que la salvaguarda cumple su objetivo de reducir el riesgo.
- Importancia de la gestión del riesgo

Es importante recordar que, incluso con la implementación de salvaguardas, la seguridad absoluta es imposible de alcanzar. Las organizaciones deben ser capaces de asumir un nivel de riesgo tolerable que les permita trabajar con cierta seguridad y mantener sus estándares de calidad.

Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse

Introducción

La estimación del estado del riesgo es una fase crucial en la gestión de riesgos del sistema de información. Se basa en la información recopilada sobre activos, amenazas, vulnerabilidades y salvaguardas para determinar el impacto potencial y residual del riesgo.

El objetivo principal de esta fase se divide en dos puntos:

- Estimar el impacto potencial: Evaluar el daño máximo que podría sufrir el sistema de información si se materializara una amenaza sin ninguna salvaguarda.
- Estimar el impacto residual: Calcular el daño que podría sufrir el sistema de información después de considerar las salvaguardas existentes.

Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse

Estimación del riesgo potencial

El impacto potencial es un componente crucial en la evaluación del riesgo del sistema de información. Se refiere a los efectos perjudiciales que podrían sufrir los activos del sistema si una amenaza se materializara sin ninguna salvaguarda.

Para **calcular el impacto potencial** del escenario activo-amenaza, se deben considerar dos aspectos fundamentales:

- Activos identificados y su valoración: Se analiza el valor de cada activo en términos financieros, operativos y estratégicos.
- Amenazas identificadas y su valoración: Se evalúan las posibles amenazas que pueden afectar al activo, incluyendo su probabilidad de ocurrencia y su impacto potencial.

Importancia de las Salvaguardas

Es importante destacar que las salvaguardas no se consideran en el cálculo del impacto potencial. Estas se tendrán en cuenta posteriormente para calcular el impacto residual.

Escenarios de Impacto

Teniendo en cuenta el par activo-amenaza, se pueden establecer diferentes escenarios de impacto. Estos escenarios se basan en la degradación del activo provocada por la amenaza y la valoración del mismo.

Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse

Estimación del riesgo potencial

Categorización del Valor de los Activos

El valor de los activos se categoriza en cinco niveles: (Muy alto, Alto, Medio, Bajo, Muy bajo)

Categorización de la Degradación Provocada por la Amenaza (tres niveles):

- Degradación inferior al 1% de su valor.
- Degradación entre el 1% y el 10% de su valor.
- Degradación de más del 10% de su valor.

Tabla de Escenarios de Impacto

Combinando las categorías de valor del activo y degradación provocada por la amenaza, se crea una tabla de escenarios de impacto. Esta tabla permite visualizar la prioridad de actuación para cada escenario.

IMPACTO		Degradación del activo		
		Inferior al 1 %	1-10 %	Superior al 10 %
Valor del activo	Muy alto	MEDIO	ALTO	MUY ALTO
	Alto	BAJO	MEDIO	ALTO
	Medio	MUY BAJO	BAJO	MEDIO
	Bajo	MUY BAJO	MUY BAJO	BAJO
	Muy bajo	MUY BAJO	MUY BAJO	MUY BAJO

Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse

Estimación del riesgo potencial

Priorización de Actuación

La prioridad de actuación se establece de mayor a menor, empezando por los activos de impacto muy alto y terminando por los de impacto bajo y muy bajo.

Atención a Todos los Activos

Es importante recordar que todos los activos requieren atención, independientemente de su impacto. No se deben dejar desatendidos o desprotegidos ante las amenazas de seguridad.

Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse

Estimación del riesgo residual

El impacto residual es un concepto crucial en la gestión del riesgo del sistema de información. Se refiere al daño que podría sufrir el sistema después de que las salvaguardas hayan actuado contra una amenaza.

Diferencia entre Impacto Potencial y Residual

El impacto residual se diferencia del impacto potencial en que este último no considera las salvaguardas, mientras que el residual sí. En un escenario ideal, el impacto residual debería ser siempre menor que el impacto potencial.

Elementos del Impacto Residual

Para calcular el impacto residual, se deben considerar tres elementos principales:

- Identificación y valoración de los activos: Se analiza el valor de cada activo en términos financieros, operativos y estratégicos.
- Identificación y valoración de las amenazas: Se evalúan las posibles amenazas que pueden afectar al activo, incluyendo su probabilidad de ocurrencia y su impacto potencial.
- Identificación y valoración de las salvaguardas: Se analiza la eficacia de las medidas de seguridad implementadas para reducir el impacto de las amenazas.

Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse

Estimación del riesgo residual

Eficacia de las Salvaguardas

Si las salvaguardas son eficaces y funcionan correctamente, el impacto residual de una amenaza sobre los activos del sistema de información debería ser menor que su impacto potencial.

Evaluación de las Salvaguardas

Si el impacto residual es mayor o igual al impacto potencial, es necesario realizar una evaluación de las salvaguardas para identificar sus vulnerabilidades y mejorar su eficacia.

Elemento	Impacto Potencial	Impacto Residual
Considera las salvaguardas	No	Sí
Cálculo	Activos + Amenazas	Activos + Amenazas + Salvaguardas
Resultado ideal	-	Menor que el impacto potencial

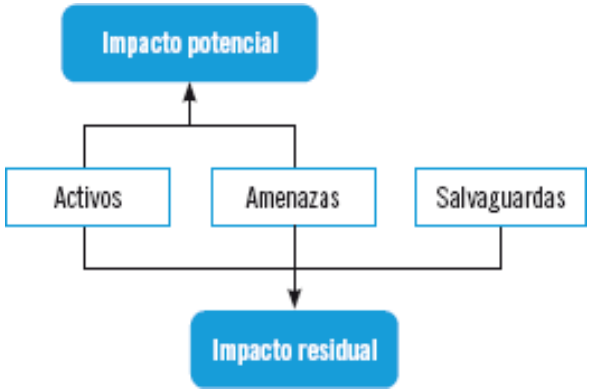
Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse

Estimación del riesgo residual

Importancia del Impacto Residual

El impacto residual es un indicador clave para la toma de decisiones en la gestión del riesgo del sistema de información y permite:

- Priorizar las medidas de seguridad: Se pueden enfocar los recursos en las áreas que presentan mayor riesgo residual.
- Evaluar la eficacia de las salvaguardas: Se puede determinar si las medidas de seguridad están funcionando correctamente.
- Justificar las inversiones en seguridad: Se puede demostrar la necesidad de invertir en medidas de seguridad para reducir el impacto residual.



Determinación de la probabilidad e impacto de materialización de los escenarios

Introducción

La determinación de la probabilidad e impacto de materialización de los escenarios de riesgo es un paso crucial en la gestión del riesgo del sistema de información. Permite evaluar el nivel de riesgo asociado a cada par activo-amenaza y tomar decisiones informadas para su tratamiento.

Probabilidad de materialización de los escenarios de riesgo

La probabilidad de materialización de un escenario se define como la posibilidad real de que se produzca una incidencia de seguridad y la frecuencia con la que puede ocurrir.

Se categoriza en cinco niveles:

Categoría	Probabilidad (%)	Calificación
Raro	0-20	1
Improbable	20-40	2
Probable	40-60	3
Altamente probable	60-80	4
Casi certeza	80-100	5

Determinación de la probabilidad e impacto de materialización de los escenarios

Introducción

Impacto de materialización de los escenarios de riesgo

El impacto se refiere a los efectos negativos que puede producir la materialización de una amenaza.

Se categoriza en cinco niveles:

Categoría	Descripción	Calificación
Muy bajo	Impacto insignificante	1
Bajo	Efectos mínimos para la organización	2
Medio	Efectos considerables sobre los activos	3
Alto	Efectos muy considerables para la organización	4
Muy alto	Efectos irreparables o difícilmente reparables	5

Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza

Introducción

El establecimiento del nivel de riesgo para cada par activo-amenaza es un paso crucial en la gestión del riesgo del sistema de información. Permite a la organización comprender el peligro que enfrenta cada activo y tomar decisiones informadas para su protección.

Nivel de Riesgo de los Escenarios de los Pares Activo/Amenaza

Los diferentes escenarios que pueden surgir de las combinaciones de las categorías de impacto sobre los activos y la probabilidad de materialización de las amenazas se clasifican en cinco niveles de riesgo:

- Nivel de riesgo despreciable: Riesgo mínimo o inexistente.
- Nivel de riesgo bajo: Riesgo tolerable que requiere atención, pero no medidas urgentes.
- Nivel de riesgo moderado: Riesgo que requiere medidas de control y seguimiento.
- Nivel de riesgo importante: Riesgo que requiere medidas de control y mitigación inmediatas.
- Nivel de riesgo crítico: Riesgo inaceptable que requiere acciones inmediatas y contundentes.

Cálculo del Nivel de Riesgo

El nivel de riesgo para cada par activo-amenaza se calcula multiplicando la calificación del impacto por la calificación de la probabilidad:

Nivel de riesgo = Impacto x Probabilidad

Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza

Cálculo del Nivel de Riesgo

El nivel de riesgo para cada par activo-amenaza se calcula multiplicando la calificación del impacto por la calificación de la probabilidad:

Nivel de riesgo = Impacto x Probabilidad

Ejemplo:

Si una amenaza tiene un impacto calificado como 1 (muy bajo) y una probabilidad de materialización de 3 (probable), el nivel de riesgo sería 3 (1 x 3 = 3).

Priorización de las Amenazas

La calificación del riesgo se utiliza para priorizar la atención a las diferentes amenazas. No obstante, es importante considerar que la categorización del riesgo tiende a valorar más la frecuencia de la amenaza que el impacto potencial que puede generar.

Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza

Escala de Calificación del Riesgo

La escala de calificación del riesgo va desde un valor mínimo de 1 (impacto 1, probabilidad 1) hasta un valor máximo de 25 (impacto 5, probabilidad 5).

Nivel de Riesgo	Siglas	Color	Significado
Despreciable	D	Verde claro	Riesgo mínimo o inexistente.
Bajo	B	Verde oscuro	Riesgo tolerable que requiere atención.
Moderado	M	Amarillo	Riesgo que requiere medidas de control y seguimiento.
Importante	I	Naranja	Riesgo que requiere medidas de control y mitigación inmediatas.
Crítico	C	Rojo	Riesgo inaceptable que requiere acciones inmediatas y contundentes.

Nivel de riesgo		Probabilidad				
		Raro	Improbable	Probable	Altamente probable	Casi certeza
Impacto	Muy bajo	D	D	D	B	B
	Bajo	D	B	B	M	M
	Medio	B	M	M	I	I
	Muy alto	M	I	I	C	C
	Alto	I	C	C	C	C

Actuación según el Nivel de Riesgo

La organización debe adaptar su actuación a cada nivel de riesgo, priorizando aquellos pares activo-amenaza con mayor riesgo y aplazando la atención a aquellos con menor riesgo.

Determinación por parte de la organización de los criterios de evaluación del riesgo, en función de los cuales se determina si un riesgo es aceptable o no

Introducción

La determinación de los criterios de evaluación del riesgo es un paso crucial en la gestión del riesgo del sistema de información. Permite a la organización definir si un riesgo es aceptable o no, y tomar decisiones informadas sobre cómo abordarlo.

Criterios de Evaluación del Riesgo

Los criterios de evaluación del riesgo se basan en la matriz de impacto/probabilidad, que se describe en el apartado anterior.

Zonas de Riesgo:

Riesgo Crítico: Probabilidad "improbable", "probable", "altamente probable" o "casi certeza" e impacto "alto" o "muy alto".

Riesgo Despreciable: Probabilidad "raro", "improbable" o "probable" e impacto "muy bajo" o "bajo".

Riesgo Bajo, Moderado o Importante: Zonas intermedias.

Nivel de riesgo		Probabilidad				
		Raro	Improbable	Probable	Altamente probable	Casi certeza
Impacto	Muy bajo	D	D	D	B	B
	Bajo	D	B	B	M	M
	Medio	B	M	M	I	I
	Muy alto	M	I	I	C	C
	Alto	I	C	C	C	C

Determinación por parte de la organización de los criterios de evaluación del riesgo, en función de los cuales se determina si un riesgo es aceptable o no

Introducción

Ejemplo:

- Implantación de una medida reductora con un coste muy elevado y una leve reducción del riesgo no compensa.
- Medida correctiva de bajo coste que elimina considerablemente riesgos importantes se debe implantar.

La evaluación de cada riesgo por separado proporciona información valiosa a la organización:

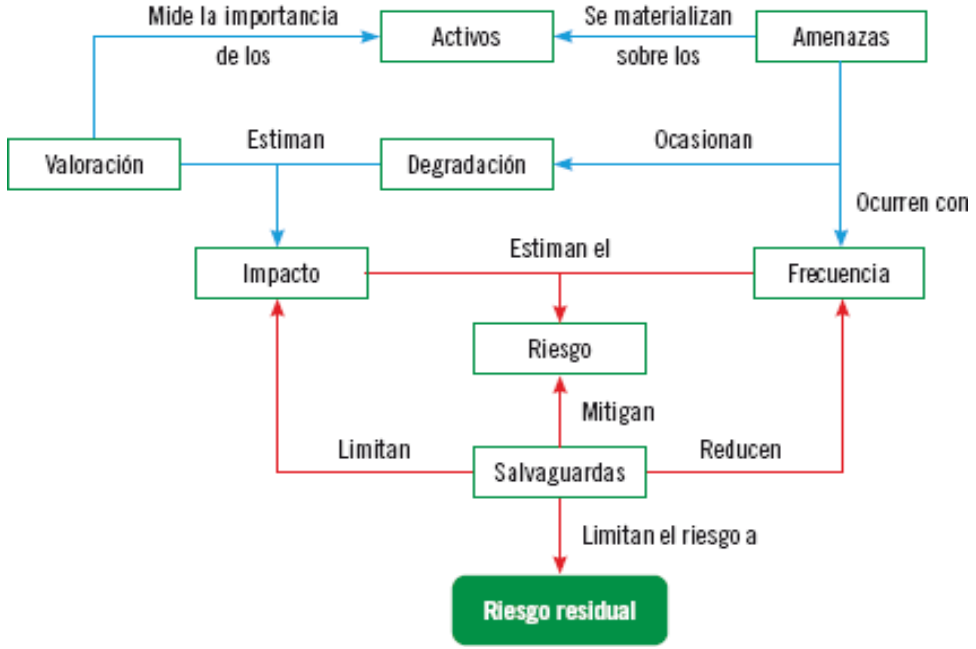
- Probabilidad de materialización de amenazas.
- Impacto de las amenazas:
  - Personas.
  - Activos.
  - Recursos.
- Selección de activos con más impacto y medidas de protección.
- Establecimiento de criterios de evaluación del riesgo.
- Toma de decisiones de seguridad adecuadas.

Determinación por parte de la organización de los criterios de evaluación del riesgo, en función de los cuales se determina si un riesgo es aceptable o no

Visión general de la gestión de riesgos

Puntos Clave:

- Las amenazas afectan a los activos, degradándolos con una frecuencia estimada.
- El valor de los activos determina su importancia dentro de la organización.
- El impacto de una amenaza se calcula a partir del valor de los activos y su degradación.
- El nivel de riesgo se determina por la frecuencia de la amenaza y su impacto sobre un activo.
- Las salvaguardas mitigan el riesgo al limitar el impacto o reducir la frecuencia de la amenaza, lo que lleva al riesgo residual.



Relación de las distintas alternativas de gestión de riesgos

Introducción

La gestión de riesgos del sistema de información de una organización implica la selección de estrategias adecuadas para cada activo y amenaza. Este análisis profundiza en las diferentes alternativas de gestión de riesgos y su relación con los tipos de controles.

Tipos de Controles:

- Controles disuasorios: Reducen la probabilidad de ocurrencia de un incidente.
- Controles preventivos: Reducen la vulnerabilidad de los activos y sus salvaguardas.
- Controles detectores: Detectan un incidente en curso o ya ocurrido.
- Controles correctivos: Limitan los efectos perjudiciales de un incidente y restauran la situación anterior.

No se recomienda seleccionar un único tipo de control. Se aconseja una estrategia integral que combine diferentes tipos de controles según el tipo de activo/amenaza y la estrategia deseada.

Ejemplo. Un activo con numerosas vulnerabilidades requiere:

- Control preventivo: Implementar medidas para reducir las vulnerabilidades.
- Control detector: Detectar a tiempo la incidencia si el control preventivo falla.
- Control correctivo: Restaurar el sistema lo antes posible.

Relación de las distintas alternativas de gestión de riesgos

Beneficios de la Estrategia Integral:

- Reducción del riesgo general de la organización: Disminución de la probabilidad de materialización de amenazas y de la degradación de los activos.
- Protección integral de los activos: Abordaje de diferentes aspectos del riesgo.
- Mayor eficacia y eficiencia en la gestión de riesgos: Optimización de recursos.

Guía para la elaboración del plan de gestión de riesgos

La elaboración de un plan de gestión de riesgos eficaz es fundamental para proteger los activos de la organización y garantizar la continuidad del negocio. Esta guía proporciona una serie de recomendaciones para el desarrollo de un plan de gestión de riesgos que se ajuste a los objetivos de la organización y obtenga resultados óptimos.

Recomendaciones Básicas:

Comprensión de la Administración de Riesgos:

- Definir claramente los conceptos de riesgo, amenaza, vulnerabilidad, activo, salvaguarda, etc.
- Comprender los factores que influyen en la definición y estimación del riesgo: amenaza, probabilidad e impacto.

Definición de las Acciones del Plan:

- Identificar los activos a evaluar.
- Definir las posibles amenazas.
- Seleccionar la metodología de análisis de riesgos.
- Establecer los umbrales de riesgo aceptables.

Apoyo de la Dirección y Profesionales Externos:

- Obtener el apoyo de la dirección para la implementación del plan.
- Considerar la contratación de profesionales externos para la gestión de riesgos complejos.

Guía para la elaboración del plan de gestión de riesgos

Recomendaciones Básicas: (II)

Identificación de las Consecuencias de cada Riesgo para priorizar su tratamiento

- Evaluar las consecuencias de cada riesgo para priorizar su tratamiento.

Eliminación de Amenazas Irrelevantes:

- Descartar las amenazas con bajo impacto y probabilidad de ocurrencia.

Inventariado de Activos Susceptibles de Riesgo:

- Crear un inventario actualizado de todos los activos de valor.

Asignación de Probabilidades:

- Estimar la probabilidad de materialización de cada amenaza para cada activo.

Asignación del Impacto:

Evaluar el grado de degradación que sufriría cada activo en caso de materializarse la amenaza.

Determinación del Riesgo para cada Activo:

Calcular el riesgo para cada activo combinando la probabilidad e impacto.

Clasificación de los Riesgos:

Ordenar los riesgos por prioridad de actuación, de mayor a menor riesgo.

Guía para la elaboración del plan de gestión de riesgos

Recomendaciones Básicas: (III)

Cálculo del Riesgo Total:

- Calcular el riesgo total del sistema de información como promedio aritmético de los riesgos de cada activo.

Diseño de Estrategias de Reducción de Riesgos:

- Seleccionar e implementar controles para reducir el riesgo global de la organización.

Desarrollo de Planes de Contingencia:

- Diseñar planes de contingencia para los riesgos más importantes.
- Análisis de la Efectividad de las Estrategias Implantadas:
- Evaluar la eficacia de las medidas de control y salvaguardas.
- Redefinir las estrategias si no se logra la reducción esperada del riesgo.

Guía para la elaboración del plan de gestión de riesgos

Consideraciones Adicionales:

Adaptación del Plan a la Organización:

- El plan de gestión de riesgos debe ser específico para cada organización.
- Los activos, amenazas y riesgos relevantes pueden variar según el sector, tamaño y objetivos de la organización.

Metodologías de Análisis de Riesgos:

- Existen diversas metodologías para el análisis de riesgos, como ISO 27001, NIST Cybersecurity Framework, etc.
- La elección de la metodología dependerá de las características de la organización y los objetivos del plan.

Comunicación y Capacitación:

- Es importante comunicar el plan de gestión de riesgos a todos los empleados.
- Capacitar al personal en la identificación, evaluación y tratamiento de riesgos.

Revisión y Actualización del Plan:

- El plan de gestión de riesgos debe revisarse y actualizarse de forma regular para asegurar su eficacia.

Exposición de la metodología NIST SP 800-30

La metodología NIST SP 800-30, desarrollada por el Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos, es una guía integral para la gestión de riesgos de la información. Se utiliza para identificar, evaluar y mitigar los riesgos que amenazan los sistemas de información de las organizaciones.

Características Clave:

- Enfoque en la seguridad de la información: Se centra en la protección de la confidencialidad, integridad y disponibilidad de la información.
- Flexibilidad: Se adapta a las necesidades y características de cualquier organización.
- Análisis en profundidad: Permite una evaluación detallada de los riesgos.
- Énfasis en la toma de decisiones: Brinda información para tomar decisiones informadas sobre la gestión de riesgos.

Fases de la Metodología:

- Caracterización del sistema: Define el alcance y los límites de la evaluación de riesgos.
- Identificación de amenazas: Determina las posibles amenazas que pueden afectar al sistema de información.
- Estimación de la probabilidad de ocurrencia: Evalúa la probabilidad de que cada amenaza se materialice.
- Análisis del impacto: Calcula el impacto potencial de cada amenaza en la organización.
- Cálculo del riesgo: Combina la probabilidad e impacto para determinar el nivel de riesgo de cada amenaza.
- Selección de controles: Implementa medidas de seguridad para mitigar los riesgos.
- Monitoreo y evaluación: Revisa y actualiza el plan de gestión de riesgos de forma regular.

Exposición de la metodología NIST SP 800-30

Ventajas:

- Metodología completa y reconocida: Ofrece un marco de trabajo integral para la gestión de riesgos.
- Mejora la seguridad del sistema de información: Reduce la probabilidad de que ocurran incidentes de seguridad.
- Optimiza la gestión de recursos: Permite enfocar los recursos en los riesgos más críticos.
- Toma de decisiones estratégicas: Facilita la toma de decisiones informadas sobre la seguridad de la información.

Desventajas:

- Proceso complejo: Requiere tiempo y esfuerzo para su implementación.
- Recursos necesarios: Puede requerir la contratación de personal especializado.
- Falta de automatización: El proceso puede ser manual y laborioso.

Exposición de la metodología Magerit V3

La metodología MAGERIT v3, desarrollada por el Centro Criptológico Nacional (CCN) de España, es una guía completa para la gestión de riesgos de los sistemas de información. Se utiliza para identificar, evaluar y mitigar los riesgos que amenazan los activos de información de las organizaciones.

Características Clave:

- Enfoque en la gestión de riesgos: Se centra en la identificación, análisis y tratamiento de los riesgos.
- Marco de trabajo integral: Ofrece un conjunto de herramientas y técnicas para la gestión de riesgos.
- Adaptabilidad: Puede adaptarse a las necesidades y características de cualquier organización.
- Énfasis en la mejora continua: Promueve la revisión y actualización del plan de gestión de riesgos.

Fases de la Metodología:

- Preparación: Define el contexto de la evaluación de riesgos y los roles de los participantes.
- Identificación de activos: Determina los activos de información que deben ser protegidos.
- Análisis de amenazas: Identifica las posibles amenazas que pueden afectar a los activos.
- Análisis de vulnerabilidades: Evalúa las vulnerabilidades que pueden ser explotadas por las amenazas.
- Estimación del impacto: Calcula el impacto potencial de cada amenaza en la organización.
- Cálculo del riesgo: Combina la probabilidad e impacto para determinar el nivel de riesgo de cada amenaza.
- Selección de controles: Implementa medidas de seguridad para mitigar los riesgos.
- Plan de respuesta a incidentes: Define un plan para responder a los incidentes de seguridad.
- Seguimiento y mejora: Revisa y actualiza el plan de gestión de riesgos de forma regular.

Exposición de la metodología Magerit V3

Ventajas:

- Metodología completa y reconocida: Ofrece un marco de trabajo integral para la gestión de riesgos.
- Mejora la seguridad del sistema de información: Reduce la probabilidad de que ocurran incidentes de seguridad.
- Optimiza la gestión de recursos: Permite enfocar los recursos en los riesgos más críticos.
- Toma de decisiones estratégicas: Facilita la toma de decisiones informadas sobre la seguridad de la información.
- Adaptable a diferentes sectores: Puede ser utilizada por organizaciones de cualquier sector.

Desventajas:

- Proceso complejo: Requiere tiempo y esfuerzo para su implementación.
- Recursos necesarios: Puede requerir la contratación de personal especializado.
- Falta de automatización: El proceso puede ser manual y laborioso.

Recursos adicionales:

- Guía de la Metodología MARGERIT v3:
  https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html
- Catálogo de elementos de la Metodología MARGERIT v3:
  https://pilar.ccn-cert.cni.es/index.php/docman/documentos/2-magerit-v3-libro-ii-catalogo-de-elementos/file

Comparación NIST SP 800-30 y Magerit V3

Similitudes:

- Ambas son metodologías reconocidas y completas para la gestión de riesgos de la información.
- Ambas cubren todas las fases principales del proceso de gestión de riesgos, desde la identificación de activos hasta la implementación de controles y el seguimiento.
- Ambas se centran en la protección de la confidencialidad, integridad y disponibilidad de la información.
- Ambas promueven la toma de decisiones informadas sobre la seguridad de la información.
- Ambas son adaptables a las necesidades específicas de cada organización.

Diferencias:

Origen:

- NIST SP 800-30: Desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos.
- Magerit v3: Desarrollado por el Centro Criptológico Nacional (CCN) de España.

Énfasis:

- NIST SP 800-30: Se centra más en la evaluación cuantitativa del riesgo y en el cálculo de la probabilidad de ocurrencia de las amenazas.
- Magerit v3: Se centra más en el análisis cualitativo del riesgo y en la identificación de las vulnerabilidades.

Comparación NIST SP 800-30 y Magerit V3

Diferencias:

Complejidad:

- NIST SP 800-30: Puede ser más complejo de implementar, especialmente para organizaciones pequeñas o sin experiencia en gestión de riesgos.
- Magerit v3: Puede ser más fácil de implementar, ya que proporciona herramientas y plantillas específicas.

Alcance:

- NIST SP 800-30: Tiene un alcance más amplio y puede ser utilizada por organizaciones de cualquier sector.
- Magerit v3: Está más enfocada al sector público español, pero puede ser adaptada a otros sectores.

Recursos:

- NIST SP 800-30: Puede requerir la contratación de personal especializado.
- Magerit v3: Cuenta con más recursos y apoyo del gobierno español.

En resumen:

- NIST SP 800-30 es una buena opción para organizaciones que buscan un marco de trabajo flexible y completo, y que tienen la capacidad de implementarlo.
- Magerit v3 es una buena opción para organizaciones que buscan una metodología más fácil de implementar y que están familiarizadas con el contexto español.

RESUMEN

Un riesgo es cualquier evento o conjunto de eventos que puede poner en peligro un proyecto o impedir que una organización alcance sus objetivos. La gestión de riesgos es un conjunto de procesos que busca reducir la probabilidad de que estas amenazas y ataques afecten a los activos más importantes de la organización.

Fases de la Gestión de Riesgos:

- Identificación y Valoración de Activos: Se determinan los activos de la organización y el impacto que sufrirían en caso de materializarse una amenaza.
- Análisis de Vulnerabilidades: Se identifican y analizan las vulnerabilidades de los activos para estimar la probabilidad de que las amenazas se materialicen.
- Cálculo del Riesgo: Se calcula el riesgo potencial de cada activo y el riesgo global de la organización.
- Análisis de Salvaguardas: Se evalúa la eficacia de las medidas de seguridad para determinar el riesgo residual.

Beneficios de la Gestión de Riesgos:

- Permite definir estrategias para reducir la probabilidad de ocurrencia de amenazas y el daño que estas pueden causar.
- Ayuda a las organizaciones a cumplir con sus objetivos.
- Promueve la toma de decisiones informadas sobre la seguridad de la información.

RESUMEN

Metodologías de Gestión de Riesgos:

- Magerit: Metodología de carácter nacional desarrollada por el Centro Criptológico Nacional (CCN) de España.
- NIST SP 800-30: Metodología de carácter internacional desarrollada por el Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos.