# 3. ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN

# CONCEPTOS DE ANÁLISIS DE RIESGOS

El análisis de riesgos en nuestros activos es importante a la hora de poder valorar el impacto que podría tener la ocurrencia de un incidente de seguridad, este impacto mayormente suele ser económico, pero también se puede traducir en una pérdida de credibilidad y de imagen de marca, que obviamente también tendrá una repercusión económica, así mismo, si ocurre un incidente, y no estamos cumpliendo las leyes, normas, procedimientos, etc. podemos ser sancionados.

Veamos los principales términos usados en la gestión de riesgos, que son activo, amenaza, vulnerabilidad, impacto y probabilidad.

**Activo**

Llamamos activo o fuente de riesgo a los recursos de la empresa para realizar sus actividades, ordenadores, servidores, etc., cuya falta de disponibilidad o deterioro pueda suponer un coste a la empresa. Por ejemplo, si eres una empresa que vende billetes de avión y tu servidor web falla durante un tiempo, durante el cual los usuarios no pueden acceder a la web tendrás una gran pérdida económica, así que en este caso el servidor, sus aplicaciones, bases de datos y todo lo relacionado que pueda ocasionar este incidente son tus activos.

La información también es un activo de la empresa, de hecho, es el mayor activo de la empresa y el que más se debe proteger.

**Amenaza**

Amenaza o suceso es la ocurrencia negativa sobre los activos que provoca su indisponibilidad, funcionamiento incorrecto o la pérdida de su valor.

**Vulnerabilidad**

Es la debilidad de los activos que permite que se materialice una amenaza.

**Impacto**

El impacto es la consecuencia negativa de la materialización de una amenaza sobre el activo por la que se aprovecha una vulnerabilidad, que se estima en porcentaje de degradación afectando al valor del activo, En caso de que este porcentaje sea del 100% implica la pérdida total del activo en cuestión.

**Probabilidad de ocurrencia**

Es la probabilidad de que ocurra ese incidente, podemos estimarla en base a datos objetivos como, por ejemplo, algo que ya ha ocurrido en la empresa o mediante datos subjetivos, por ejemplo, datos de otras empresas o expertos.

Todos estos conceptos se relacionan entre sí de la siguiente manera:

**AMENAZA explota VULNERABILIDAD afecta ACTIVO provoca IMPACTO**

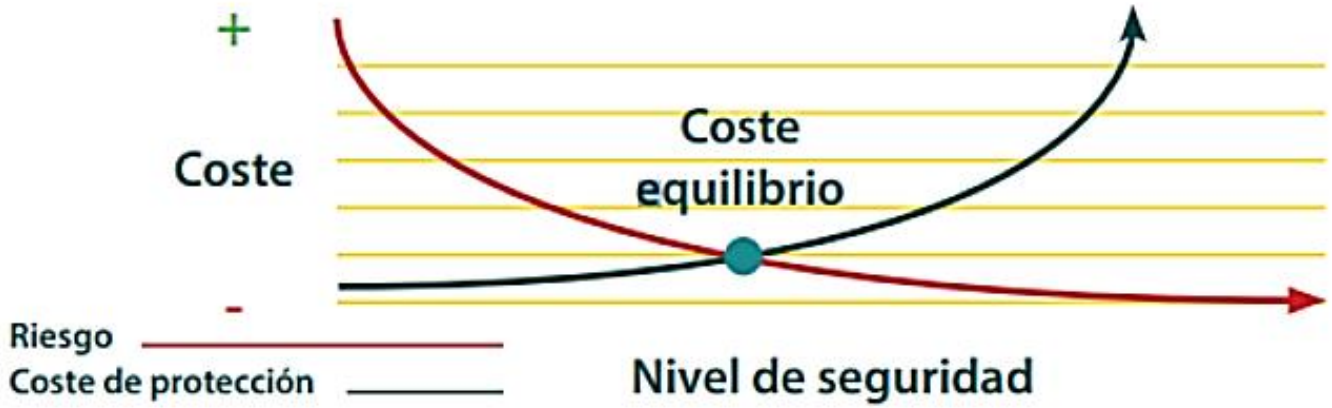
**Riesgo**

El riesgo se estima cuantitativamente y es el resultado del producto del impacto y probabilidad de ocurrencia de un suceso.

## IMPACTO x PROBABILIDAD= RIESGO

**Coste de protección**

Coste que supone a las empresas mantener la seguridad de los activos, y por tanto, mantener el nivel de riesgo en el umbral permitido.




**Análisis de riesgo**

El análisis de riesgo permite a la empresa conocer el nivel de riesgo al que está expuesta, para lo cual hay que realizar un inventario de los activos para posteriormente determinar

las amenazas a las que están expuestos y sus vulnerabilidades y la probabilidad de ocurrencia con su consecuente impacto.

**Tratamiento del riesgo**

Es la aplicación de medios correctivos para aquellos activos que superan el nivel de riesgo aceptado, en base a cuestiones económicas, a veces se decide aplicar las medidas correctivas para eliminar o minimizar el riesgo, o asumir el riesgo si la probabilidad de ocurrencia es muy baja en comparación con el coste, también se puede transferir a terceros, por ejemplo, a un seguro del activo.

Son opciones a la hora de tratar el riesgo

**Evitar o eliminar el riesgo**, por ejemplo, dejando de hacer esa actividad si el coste del tratamiento es superior al beneficio.

**Reducirlo o mitigarlo**, el coste del tratamiento es adecuado en función de los beneficios que obtenemos.

- Reducir la probabilidad o frecuencia de ocurrencia.
- Medidas preventivas.

**Reducir el impacto de la amenaza** o acotar el impacto, revisando medidas preventivas y funcionamiento.

**Transferirlo, compartirlo o asignarlo a terceros**, como por ejemplo un seguro o un servicio subcontratado, cuando esto es más beneficioso o menos costoso que el tratamiento directo.

**Aceptarlo**, a veces se hace necesario asumir algunos riesgos, cuando por ejemplo no compensa económicamente el tratamiento del riesgo, o por ejemplo en activos legacy (obsoleto), bien sea porque tenemos alguna aplicación cuyo coste de migración sería muy elevado o por otras razones, en este caso no implementamos medidas correctoras, pero sí se debe monitorizar el activo para confirmar que no aumenta el riesgo.

**Gestión de riesgos**

La gestión de riesgos es la suma del análisis de riesgos y el tratamiento del riesgo.

**Plan de tratamiento de riesgos**

Documento donde vienen reflejados la selección y justificación de las medidas a aplicar a cada riesgo que hayamos identificado.

**Riesgo residual**

Es el riesgo que sigue existiendo a pesar de haber aplicado medidas correctivas.

# METODOLOGÍAS DE ANÁLISIS DE RIESGOS Y GUÍAS DE BUENAS PRÁCTICAS

Los análisis de riesgos también llevan un procedimiento y atienden a leyes normas y procedimientos como son los siguientes:

**COSO (Committee of Sponsoring Organizations of the Treadway Commission)**

Creación de guías y marcos de trabajo en el ámbito de la gestión de riesgos empresariales.

**ISO 31000:2009**

Es una familia de normas que incluyen metodología, principios y directrices en materia de gestión de riesgos.

ISO/IEC 31010 - gestión de riesgos - evaluación del riesgo evaluación técnicas del riesgo.

ISO Guide 73:2009 - gestión de riesgos--vocabulario Gestión.

ISO 31000:2018 - Gestión del riesgo. Principios y directrices.

**MAGERIT**

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información creada por el Ministerio de Administraciones Públicas español.

**ISO / IEC 27005:2011**

Norma que aporta directrices para la gestión de riesgos de seguridad de la información.

**NIST SP - 800-30**

Metodología creada por el gobierno norteamericano.

Cada empresa tiene la capacidad de elegir una metodología o guía de buenas prácticas a seguir o incluso definir una propia.

Debes conocer INCIBE, Instituto de ciberseguridad español, donde también puedes encontrar muchas otras guías, entre ellas una de muy fácil comprensión de la gestión de riesgos.

# VULNERABILIDADES, MALWARE, ATAQUES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y CRITERIOS DE PROGRAMACIÓN SEGURA

En este apartado vamos a revisar las diferentes causas de vulnerabilidad, malware, y problemas en las aplicaciones que pueden ser causa de vulnerabilidad.

**Ingeniería social**

La ingeniería social es el arte del engaño o persuasión para obtener información confidencial mediante la manipulación de sesgos cognitivos de las personas, haciendo por ejemplo que pinchen en enlaces que les redireccionan a webs maliciosas con la apariencia de ser webs legítimas e infectas sus equipos.

El ser humano tiende a confiar en otras personas, de forma que podemos aprovechar este sesgo por ejemplo para hacernos pasar por el administrador de sistemas y solicitar al usuario que nos de sus credenciales haciéndoles ver que es necesario para solucionar un problema grave en su equipo.

Algunas de las técnicas usadas son:

- **Suplantación:** es un ataque en el cual el atacante suplanta a una persona de la empresa, por ejemplo, al administrador de sistemas, o llamando a personal de la empresa haciéndose pasar por un usuario de la misma.
- **Phishing:** en un ataque phishing, el atacante suele enviar un email al usuario haciéndose pasar por un servicio como un banco, o empresas como Amazon, Ebay, Correos, etc., donde el usuario pincha en un enlace donde se le solicitan sus credenciales de acceso. En ese email se suele provocar cierta preocupación y urgencia al usuario, diciéndole por ejemplo que, si no hace eso, se bloquearán sus cuentas.

  Estas acciones de phishing pueden ser dirigidas o masivas, cuando son dirigidas, se suelen enviar a personas concretas, por ejemplo, el CEO de una empresa, en ese caso se denomina **Whaling.**
- **Shoulder sourfing:** en este tipo de ataque, el atacante trata de extraer información confidencial mirando por encima del hombro a espaldas del usuario o echa una ojeada al escritorio, es por eso que muchos usuarios, que manejan información sensible utilizan filtros de pantalla.
- **Dumpster diving:** esta técnica se trata de mirar literalmente en la basura, en busca de información sensible con la que poder realizar un posterior ataque, por ejemplo, si tiras tus facturas del teléfono sin destruir adecuadamente el documento podrían saber tu nº de teléfono, tal vez tu DNI, o tu cuenta bancaria, etc.

- **Hoax:** se trata de emails que cuentan una falsa historia y hacen que el usuario tenga que tomar algún tipo de acción como pinchar en un enlace con las consecuencias que esto pueda entrañar.
- **Tailgating:** es otra técnica de ingeniería social que consiste en acceder a un edificio al que no se tiene permiso de acceso siguiendo de cerca a alguien que sí que tiene autorización para entrar y por ejemplo con su tarjeta ha desbloqueado una puerta de acceso, la atacante conversa con esa persona, y, por ejemplo, para tratar de entrar le puede decir que tiene una reunión muy importante y que, si no le importa que pase, que se va a llevar una regañina si llega tarde. Por ello, es importante formar en materia de seguridad a los empleados para que no se dejen llevar por el sesgo de confianza que comentábamos antes. Una contramedida para evitar esto pueden ser los mantrap, que son áreas entre dos puertas cerradas donde solo puede haber una persona y que una puerta no se abre hasta que no se cierra la otra.
- **Vishing:** es un phishing, pero realizado a través de una llamada telefónica.
  La razón por la que estos ataques suelen funcionar es porque tienen las siguientes características, autoridad, intimidación, prueba social, crean sensación de miedo a las consecuencias y urgencia de tomar una acción, además nos pueden hacer creer que provienen de alguien conocido, o en el caso de los ataques por teléfono darnos conversación de forma que se genere cierta confianza previa.

**Ataques de red**

Los ataques a las redes ocurren a diario, estos son algunos de ellos:

**Ataque de denegación de servicio (DoS: Denial of service):** en un ataque de denegación de servicio, el atacante suele inundar de peticiones un servidor o equipo de forma que lo deja fuera de servicio o hace que vaya mucho más lento.

**Ataque de denegación de servicio distribuido (DDoS: Distributed denial of service):** el resultado es el mismo que en un ataque DoS, solo que se hace desde múltiples equipos a la vez, el atacante primero compromete una serie de equipos que llamamos zombies y que sin saberlo son los que están realizando la denegación de servicios en el servidor o en la red.

**Spoofing o suplantación:** el atacante suplanta bien el correo electrónico de una persona o entidad (E-mail Spoofing) o la MAC de un equipo (MAC Spoofing) o su dirección IP (IP Spoofing), de forma que, a la hora de analizar el ataque, es otro equipo el que aparece como el origen del ataque.

**Replay Attack:** en este ataque, se comienza analizando el tráfico mediante un snniffer de red, el atacante captura el tráfico que quiere replicar y lo vuelve a enviar modificado a la red.

**Man-in-the-Middle (MITM):** ataque de hombre en el medio, donde el atacante logra ponerse en medio de dos sistemas de comunicación, haciendo que toda la información transmitida pase por él.

**DNS Poisoning:** envenenamiento DNS, donde el atacante compromete las entradas del servidor DNS, modificando los registros DNS y alterando la caché DNS, de forma que es capaz de redireccionar el tráfico web a otro sitio (Pharming).

**Eavesdropping/Snnifing:** existen herramientas que permiten capturar el tráfico de red, como por ejemplo Wireshark, de forma que podemos capturar paquetes que contengan información sensible, o simplemente información como puede ser alguna aplicación y su versión, o direcciones IP, MACs, que pueden resultar de interés para el atacante, por ejemplo, para realizar un envenenamiento de la caché ARP.

**Ataques Pass the hash:** es una técnica de ataque usada para tener acceso a redes que usan Microsoft NT LAN manager (NTLM) como protocolo de autenticación. El atacante accede al servidor remoto usando los hash NTLM en lugar de las contraseñas en texto plano. Obtiene estos hash del registro de Windows que puede convertir mediante herramientas como L0pthCrack.

**ARP Poisoning**: el envenenamiento de caché ARP, consiste precisamente en envenenar la caché ARP para una dirección IP en particular, por ejemplo, la puerta de enlace del router, de forma que esa dirección IP apunte a la MAC del atacante, lo que le asegura que siempre que envíes información al router esta pasará por la máquina atacante, esta es la forma en que se realiza un ataque de hombre en el medio, tanto en redes cableadas como inalámbricas.

**Ataque de amplificación:** es el proceso de incrementar la señal de la antena de WIFI para que alcance mayores distancias, de forma que el atacante pueda captar la señal sin necesidad de estar en la misma ubicación.

**Spam:** recepción de mensajes de email no solicitados, generalmente publicidad, pero pueden ser también maliciosos.

**Privilege Escalation o escalada de privilegios:** un atacante que ha conseguido acceder a un equipo con privilegios de usuario tratará de elevar sus privilegios para ser administrador, esto ocurre debido a alguna vulnerabilidad del software o del sistema operativo, por eso es imperativo realizar las correspondientes actualizaciones del sistema (patches).

**Port Scanning Attack o escaneo de puertos**: un escaneo de puertos, pretende conocer los puertos que están abiertos en un equipo remoto, conocer los servicios que corren detrás de esos puertos y sus versiones para posteriormente buscar sus vulnerabilidades y posibles Exploits, además podemos obtener la versión del sistema operativo o ejecutar scripts que me permitan conocer si ese equipo remoto tiene alguna vulnerabilidad específica, también podemos realizar un escaneo suplantando la IP o la MAC del equipo atacante, para no ser reconocido como origen del escaneo, entre otras cosas. La aplicación más conocida que se usa con este fin en NMAP.

Algunos de los escaneos más conocidos que se pueden hacer con esta herramienta son:

**TCP Connect Scan (-sT):** que trata de establecer una conexión con el equipo remoto mediante el three way handshake, enviando una flag TCP SYN a 1, y según la respuesta obtenida del equipo remoto establece si el puerto está abierto o no, si recibe el SYN-ACK, es que el puerto está abierto, si recibe un RST, está cerrado, tras recibir la respuesta nmap no completa el three way handshake con el ACK.

**SYN Scan o half open scan (-sS):** también llamado escaneo sigiloso.

**XMAS Scan:** se envía un paquete con las flags TCP de FIN, PSH y URG a 1.

**Protocolos anticuados:** se trata de protocolos que no se deberían usar precisamente porque son inseguros y ya tienen una versión que los sustituye que aporta seguridad al protocolo, como puede ser el protocolo HTTP que ofrece su versión segura con HTTPS, donde se añade el cifrado de la información mediante TLS. Por ejemplo, si rellenamos un formulario en una web con HTTP y estamos capturando con Wireshark, podríamos capturar en texto plano lo que hemos insertado en el formulario, por ejemplo, un usuario y contraseña, los números de una tarjeta de crédito, etc.

**Insiders:** son personas que desde dentro de la empresa pueden realizar un ataque.

**Session Hijacking:** este ataque consiste en un secuestro de sesión.

**Null sesión o sesiones nulas:** una sesión nula permite el acceso al sistema sin necesidad de poner una contraseña. Podemos crear una sesión nula mediante el comando de Windows Net use.

## Ataques por contraseña

Un ataque de contraseña es cuando el atacante trata de conocer la contraseña de acceso al sistema del usuario. Hay tres tipos de ataques por contraseña por excelencia:

- Ataque por diccionario.
- Ataques por fuerza bruta (Force Brute Attack).
- Ataques híbridos.

Otros ataques por contraseña son:

- Ataque de cumpleaños (Birthday Attack).
- Rainbow Tables.
- Ataques de texto plano (KPA).

## Ataques a aplicaciones

Muchos de los ataques a día de hoy ocurren porque se compromete un sistema a través de una aplicación que se está ejecutando en el mismo y que puede tener vulnerabilidades, los atacantes estudian las aplicaciones y la forma de encontrar en ellas un bug (fallo de seguridad), entre los ataques más habituales tenemos:

- **SQL Injection:** inyección de código SQL
- **Buffer overflow:** desbordamiento de buffer.
- **Cross-Site Scripting y Cross Site Request Forgery:** CSFR o XSFR o falsificación de petición en sitios cruzados.
- **Directory transversal/Comand Injection:** salto de directorio o cruce de directorio, permite al atacante acceder a cualquier tipo directorio sin ningunas credenciales.
- **Zero day Attack:** ataque de día cero, una vulnerabilidad desconocida que ha sido explotada.
- **Add ons maliciosos.**
- **Ejecución de código remoto arbitrario**: el atacante accede al sistema pudiendo ejecutar código.
- **Clickjacking:** también conocido como "ataque de compensación de UI", donde el atacante haciendo uso de capas transparentes trata de que el usuario haga click en un botón, secuestrando sus clics para redireccionarle a otro lugar o hacer que descargue o ejecute malware.
- **Typo squatting /URL hijacking:** es la posibilidad de abrir una web maliciosa cuando escribimos la URL de una web conocida, pero cometemos errores al escribirla, por ejemplo, en lugar de escribir Google, escribes gooogle.

**Amenazas físicas**

Algunas de las amenazas que experimentan las empresas son las relacionadas con amenazas físicas a los sistemas y dispositivos algunos de ellos son:

- **Snooping:** es el acto de fisgonear entre los papeles que se encuentran en la mesa o buscar información dentro de los archivadores, es por ello que hay que establecer una política de “mesas limpias” que especifica que los documentos deben está a buen recaudo cuando no se están usando.
- **Robo o pérdida de activos:** especialmente en los trabajadores móviles se puede dar el caso de robo de los activos, por ejemplo, una Tablet, equipo portátil o teléfono, es por ello por lo que también se deben adoptar las medidas adecuadas mediante políticas de la empresa donde se especifica por ejemplo que los discos deben estar cifrados, o que en caso de robo se pueda hacer un borrado remoto del dispositivo.
- **Error humano:** es muy común la ocurrencia de incidentes por error humano, generalmente por desconocimiento o falta de formación adecuada.
- **Sabotaje:** un empleado enfadado podría generar un incidente de seguridad a propósito, aunque no siempre tiene porque ser un empleado.

**Software malicioso**

Actualmente casi todos los tipos de virus y ataques se engloban dentro del término malware, de ahí que ahora a las soluciones de antivirus se las llame soluciones antimalware. Veamos algunos de los diferentes tipos de malware.

- **Virus:** un virus es una pieza de software malicioso que tiene la capacidad de infectar un sistema pudiendo eliminar datos o corromperlos, hacer que el equipo vaya más

lento o incluso que no sea capaz de iniciar el sistema operativo. Existen diferentes tipos de virus.

  - **Virus ejecutable:** virus que vienen junto a un archivo ejecutable, que se activan cuando se trata de abrir el archivo. Por eso se hace necesario desactivar la opción de Windows de "Reproducción automática" para dispositivos como unidades ópticas, dispositivos USB o discos de red.
  - **Virus de sector de arranque:** este virus ataca al sector de arranque y sobrescribe su código, lo que hace que el sistema operativo no pueda iniciar correctamente.
  - **Virus de Macro:** aplicaciones como las incluidas en el paquete ofimático Office permiten macros usando Visual Basic for Applications (VBA) que es un lenguaje de programación que permite modificar tanto la aplicación como el sistema operativo, ejecutando acciones como borrar archivos, o enviar emails masivos entre otras.

- **Bomba lógica:** es un tipo de virus que está programado para ejecutarse o bien en una fecha y hora concretos o ante una determinada acción (trigger) del usuario.
- **Escalada de privilegios:** ocurre cuando un atacante accede a un sistema y trata de adquirir privilegios de administrador para poder realizar todos los cambios que necesite en el sistema, como por ejemplo instalar una puerta trasera. Existen 3 tipos:
  - **Escalada de privilegios vertical**: un atacante con permisos de usuario eleva sus privilegios a administrador.

  - **Escalada de privilegios horizontal:** el atacante tiene los mismos permisos con los que accedió al sistema, pero con ellos es capaz de atacar otro equipo o recurso diferente.
  - **Desescalada de privilegios**: el atacante con privilegios es capaz de volver a adquirir privilegios de un nivel inferior para poder acceder a los recursos que tenía asignados ese usuario.
- **Gusano:** es un virus que tiene como característica replicarse a si mismo y de propagarse bien por la red, dispositivos USB o por email.
- **Troyano:** es un programa que trata de engañar al usuario que aparentemente tiene una funcionalidad, como por ejemplo ser un antivirus, pero que dentro contiene el malware que infecta el sistema, típicamente abriendo puertas traseras a través de puertos TCP/IP, o keyloggers.

  En la historia han sido muy famosos troyanos como Netbus, Kuang, Subseven o BackOrifice entre otros. Troyanos como Netbus permiten acceder al equipo remoto y ejecutar una serie de acciones controladas por el atacante como puedes ver en la imagen a continuación.
- **Spyware:** software malicioso que infecta el equipo o dispositivo móvil y recopila información sobre los sitios por los que navegamos, nuestros gustos, hábitos de navegación, así como otros datos. Datos que las empresas venden para entre otras cosas ofrecernos publicidad basada en nuestros gustos y deseos.

- **Adware**: típicos anuncios que se cargan y aparecen en nuestra pantalla sin solicitarlos por medio de una ventana pop-up, pidiéndonos acciones como suscribirnos o adquirir un producto o servicio.
- Spam: correos comerciales con publicidad no deseada.
- **Rootkits:** Malware oculto que permite a los atacantes acceder al equipo sin conocimiento por parte del usuario, proporcionando un control remoto del equipo con permisos administrativos. Existen 5 tipos diferentes:
  - **Nivel de aplicación**
  - **Nivel de Kernel**
  - **Nivel de librerías**
  - **Virtualizados**
  - **De Firmware**
- **Botnets:** redes de ordenadores infectados por el atacante cuya misión es atacar de forma conjunta a otro equipo.
- **RAT:** Remote Access trojan o troyano de acceso remoto.
- **Keylogger:** malware que captura las pulsaciones del teclado que guarda en un archivo de texto que posteriormente envía al atacante a través de una puerta trasera.
- **Backdoors:** También conocidas como puertas traseras, que no son más que puertos abiertos a través de los cuales el atacante se puede comunicar con nuestro equipo y ejercer un control remoto.

- **Ransomware:** malware que secuestra archivos, sistemas operativos o dispositivos móviles enteros mediante el cual los atacantes cifran la información del usuario y solicitan el pago de un rescate a cambio de descifrar sus archivos para devolverle el acceso a la información. Muy conocidos últimamente por ser ataque dirigidos a grandes empresas o entidades públicas como hospitales o gubernamentales.
- **Malware polimórfico:** malware que cambia constantemente sus características identificables para evadir la detección, de forma que es capaz de ocultarse, cifrarse así mismo, comprimirse, etc.

**Amenazas al hardware**

NO sólo nos deben preocupar ataque y malware, sino también las características del Hardware que permitan bien el acceso a los discos duros del equipo, o la exfiltración de datos, veamos unos ejemplos.

- **BIOS:** Basic Input Output System, la BIOS es el firmware de nuestra placa base que permite entre otras cosas la comunicación entre Software y Hardware, podemos configurar en ellas aspectos relacionados con el Hardware, dispositivos de almacenamiento, voltajes, velocidades, revoluciones de los ventiladores, dispositivos de arranque del sistema operativo, acceso permitido o no a diferentes dispositivos, etc. Podemos incluso proteger mediante contraseña la propia BIOS y los dispositivos de almacenamiento.

Por ejemplo, alguien podría acceder a la BIOS si esta no está protegida con contraseña y permitir el arranque desde una unidad USB booteable o un CD Live, pudiendo acceder a la información de los discos duros.
Podemos proteger con contraseña puertos USB, unidades ópticas para que no se puedan usar, o incluso deshabilitarlos totalmente con el fin de evitar la exfiltración de datos, lo mismo con la tarjeta de red, si ese equipo no necesita conexión a la red o a internet.
La BIOS es un entorno muy potente que permite cambiar opciones del sistema a muy bajo nivel, como hemos visto, podremos modificar cosas como el orden de arranque de los discos duros, pero también voltajes, protecciones y velocidades del propio procesador y de otros componentes que, configuradas de manera incorrecta, podrían dañar los componentes del ordenador. Por ello es muy común que un usuario inexperto acceda a la BIOS, la modifique sin tener el conocimiento suficiente y dañe el equipo, por eso, antes de cambiar cualquier parámetro de la BIOS, tenemos que informarnos de sus funciones y el impacto que tendrán.

- **Dispositivos USB:** relacionado con lo anterior, podemos deshabilitar los puertos USB del equipo para impedir la exfiltración de datos, así mismo para evitar infecciones por malware deshabilitar la reproducción automática sobre estos dispositivos que podría hacer que al insertar el USB se ejecutase directamente el malware.
  Así mismo se pueden tomar medidas como son los DLP, que evitan la exfiltración de datos sensibles, evitando su copia en dispositivos USB.

Hay que hacer especial mención a los dispositivos USB que incorporan una rutina programada para poder extraer datos y a los USB Killer, que al insertarlos generan un pulso de alto voltaje que literalmente “deja frita” a la placa base, y que fácilmente se pueden comprar por internet a precios irrisorios.

- **Smartphones y tablets:** este tipo de dispositivos son cada vez más usados y disponen de más funciones y capacidad de almacenamiento, por lo que es importante mantenerlos seguros para que en caso de robo no puedan acceder a la información contenida, que va desde contactos, emails, documentos, información personal y laboral, etc. En este caso, se hace especialmente importante tener contraseñas de acceso robustas, cifradas las unidades de almacenamiento, copias de seguridad de la información y poder realizar un borrado remoto del dispositivo en caso de pérdida o robo.

  Además, estos dispositivos disponen de tecnologías que de por sí son vulnerables como WIFI y Bluetooth con lo que, si las comunicaciones no están correctamente aseguradas, un atacante podría esnifar el tráfico que enviamos o recibimos y obtener información sensible. Algunas de estas técnicas usadas por los atacantes son:
  - **Bluesnarfing:** exploit que permite al atacante conectarse mediante bluetooth a otro dispositivo.
  - **Bluejacking:** consiste en el envió de mensajes no solicitados a través de bluetooth.

  - **Bluebuggin:** exploit que permite al atacante ganar acceso al teléfono pudiendo usarlo por ejemplo para hacer llamadas entre otras cosas.
  - **Snnifing WIFI:** esnifar el tráfico de la red WIFI.
- **NAS:** Network Attached Storage, es un dispositivo conectado a la red que dispone de una matriz redundante de discos (RAID) que permite el acceso a la información por parte de los usuarios conectados a la red, a parte de las vulnerabilidades que puedan tener a nivel de Hardware estos dispositivos, por ejemplo firmware no actualizado, también incorporan sistemas operativos y aplicaciones con sus propias vulnerabilidades, y una interfaz de configuración que permite gestionar a los usuarios que podrán acceder al dispositivo y sus permisos a los recursos compartidos.

**Vulnerabilidades en aplicaciones**

Muchas de las vulnerabilidades existentes se deben a la mala configuración de las aplicaciones (missconfiguration), a la falta de actualizaciones para parchear las mismas o a errores de programación.

- **OSINT:** open source intelligence, o inteligencia de fuentes abiertas, que permite obtener información acerca de las tecnologías y aplicaciones usadas por la empresa, así como versiones de esos productos, con los que posteriormente conformar un vector de ataque comprobando sus vulnerabilidades.
- **Improper input handling:** es tarea de los programadores asegurarse de que no hay errores en la programación de las aplicaciones o de su correcto tratamiento para que

la aplicación no deje de funcionar, se utiliza para describir funciones como la validación, desinfección, filtrado o codificación y/o decodificación de datos de entrada. El manejo inadecuado de entradas es una de las principales causas de vulnerabilidades críticas que existen en los sistemas y aplicaciones actuales.

- **Race conditions**: vulnerabilidad relacionada con los programas, cuando uno o más hilos (threads) acceden a recursos compartidos y son forzados a hacer 2 o más operaciones de forma simultánea, sin los controles adecuados estos procesos pueden interferir entre sí ocurriendo eventos fuera de la secuencia normal de la aplicación lo que como resultado hace que la aplicación se comporte de forma anómala.
- **MIsconfiguration:** configuración nula o inapropiada de las aplicaciones.
- **Configuraciones por defecto:** en cualquier aplicación siempre debemos modificar los valores por defecto, un ejemplo, sería la interfaz de entrada a nuestro router que tiene usuario y contraseña por defecto, en algunos casos, usuario admin y contraseña admin, debemos modificar esta configuración ya que estos datos son conocidos, además hay listados en internet que nos ofrecen usuarios y contraseñas por defecto de todas las marcas y modelos existentes.
- **Resource exhaustion:** el equipo no tiene suficientes recursos o no los maneja de forma adecuada para realizar correctamente sus funciones.
- **Usuarios sin formación**: ya hemos comentado que un usuario que maneja un equipo sin la formación adecuada, puede ocasionar muchos problemas de seguridad.
- **Configuración inapropiada de usuarios, contraseñas y permisos.**

- **Uso de cifrado inseguro:** un ejemplo podría ser cifrar las comunicaciones WIFI con WEP, que es inseguro, vulnerable y fácilmente descifrable.
- **Vulnerabilidades de memoria y buffer:**
    - **Memory Leak**: error de software que ocurre cuando una aplicación consume casi toda la memoria porque no se puede liberar un bloque de memoria reservada.
    - **Integer overflow:** cuando se guarda información en la memoria RAM, se le asigna un espacio específico, el integer overflow ocurre cuando las operaciones realizadas por la aplicación exceden ese espacio.
    - **Buffer overflow:** ocurre cuando las aplicaciones escriben en áreas fuera de las asignadas en memoria.
    - **Punteros sin referencia:** cuando se programan las aplicaciones se usan punteros para referenciar áreas de la memoria. Se utiliza para acceder o manipular los datos contenidos en la ubicación de la memoria a la que apunta un puntero. *(asterisco) se usa con una variable de puntero cuando se elimina la referencia de la variable de puntero, se refiere a la variable que se apunta, por lo que se denomina eliminación de referencia de punteros.
    - **Inyección DLL:** ocurre cuando un programa se ve obligado a cargar librerías dinámicas (DLL) en su espacio de direcciones y ejecutan código de las DLL que puede ser malicioso.
    - **Certificados y manejo de claves inadecuado:** la administración de claves en los entornos que utilizan criptografía, como por ejemplo las infraestructuras de clave

pública es crítico, de forma que hay que garantizar que las claves privadas se mantienen en lugar seguro.

# GESTIÓN DE RIESGOS

Se hace importante seguir un proceso cuando realizamos un análisis de riesgos de forma que nos aseguremos de identificar todas las amenazas y riesgos asociados a nuestros activos, lo que nos va a permitir planear las medidas necesarias y técnicas de mitigación para reducir el riesgo. Veamos el proceso de un análisis de riesgos.

**Identificar los activos**

Inicialmente tenemos que identificar, inventariar y conocer el valor de los activos, esta fase se conoce como la fase de identificación de activos. A continuación, vemos una lista de activos comunes:

- Hardware y software.
- Datos.
- Instalaciones físicas.
- Personal.
- Branding y reputación de la empresa.
- Equipos.
- Infraestructura de red.
- Servicios y aplicaciones, etc

## Identificar las amenazas (Threat assessment)

En esta fase identificamos las amenazas para cada activo identificado en la primera fase, por ejemplo, si tenemos una web un ejemplo de amenaza potencial sería un ataque de inyección de SQL, o por ejemplo, un fallo en el disco duro del servidor que cause la indisponibilidad del servidor causando un gran impacto económico.

Cuando realizamos un análisis de las amenazas, es importante saber que estas pueden provenir de diferentes fuentes:

- **Amenazas ambientales:** esto incluye, terremotos, tsunamis, huracanes, inundaciones, tormentas eléctricas, etc.
- **Amenaza humana:** amenaza que resulta de las acciones humanas que puede ser intencionada o no intencionada, ejemplos de esto pueden ser, un usuario que inserta un pendrive con un virus, robo, vandalismo, sabotaje, desconocimiento o falta de formación del usuario que utiliza el activo, etc.
- **Amenazas internas o externas:** las amenazas pueden ser internas, por ejemplo, un empleado descontento que decide de forma intencionada borrar datos importantes de la empresa, o amenazas externas como pudiera ser un intento de ataque por parte de un hacker.

Es importante saber que muchas de las amenazas provienen de la falta de conocimiento, debilidad en las contraseñas, no se ha realizado el hardening de los sistemas, no hay controles administrativos, no existen controles en el acceso a los datos, falta de

configuraciones adecuadas (missconfiguration) o que no se hacen las actualizaciones del software o el firmware, entre otros.

**Análisis del impacto**

El objetivo del análisis de impacto es identificar el resultado que provocará en el negocio la materialización de una amenaza. Por ejemplo, si una web de venta de billetes de avión sufre una denegación de servicio DoS, dependiendo del tiempo que esté fuera de servicio generará una gran pérdida económica y de reputación.

El impacto puede ser tangible cuando se conoce bien la pérdida económica que genera o intangible como es la pérdida de reputación, que no se puede estimar concretamente.

**Priorización de las amenazas**

Una vez identificadas las amenazas que pueden ocurrir, tenemos que priorizar el impacto y la probabilidad de ocurrencia (likelihood of occurrence), para solucionar primero los riesgos más graves o con mayor probabilidad de ocurrencia e impacto.

La forma de priorizar las amenazas depende del tipo de análisis de riesgos que estemos realizando, si este es cualitativo, asignaremos una escala de valor como bajo, medio y alto, y nos enfocaremos primerio en solucionar el riesgo alto, si usamos las métricas CVSS en su versión actual, los riesgos son crítico, alto, medio y bajo. Es común el uso de CVSS en bases de datos de vulnerabilidades conocidas como National Vulnerability Database (NVDB),

Common Vulnerabilities and Exposures (CVE) u Open Source Vulnerability Database (OSVDB).

**Identificar las técnicas de mitigación del riesgo**

Una vez hemos identificado las amenazas y las hemos priorizado, buscamos las soluciones adecuadas para reducir o mitigar el riesgo, lo que ya implica un gasto económico en la solución que vamos a implementar para proteger nuestro activo, por ejemplo, implementar firewalls, cifrado, sistemas de control de acceso, sistemas de prevención de intrusos (IPS), por nombrar algunos.

**Evaluar el riesgo residual**

Una vez completadas las fases anteriores y aplicadas las medidas que mitigan el riesgo tenemos que reevaluar el activo y comprobar que la amenaza ya no existe, si aún existe alguna amenaza, eso es lo que conocemos como riesgo residual, y esto es crítico a la hora de tomar nuevas decisiones, como puede ser aplicar medidas adicionales o decidir si asumimos el riesgo.

## ESTRATEGIAS DE MITIGACIÓN DEL RIESGO

Como ya hemos mencionado podemos gestionar el riesgo de diferentes formas, mitigarlo, minimizarlo, transferirlo o asumirlo, en cualquier caso, podemos adoptar por diversas opciones para mitigar los riesgos como son:

- **Forzar el uso de controles de seguridad:** implementando medidas como por ejemplo, RAID, soluciones de alta disponibilidad, firewalls, cifrado, IDS, IPS, actualizaciones, honeypots, software antimalware, o el uso de sistemas DLP (Data Loss prevention) donde el administrador de sistemas puede definir diferentes reglas para la información en función de si es considerada confidencial o sensible de forma que no se permita que la información se pueda compartir o copiar o transferir a un USB o cualquier otro medio extraíble, de forma que se evite la exfiltración de la información.
- **Control de cambios:** tenemos que asegurarnos de implementar procedimientos de control de cambios y de educar y formar a los empleados en la metodología adecuada a la hora de implementar cambios en los sistemas, como es documentarlos, e informar de los cambios.
- **Gestión de incidentes:** tenemos que contar con un equipo de gestión de incidentes y de procedimientos que puedan usar en caso de que ocurra un incidente.
- **Revisión de permisos:** hay que revisar regularmente los privilegios asignados a los usuarios, para asegurar el principio del mínimo privilegio, por ejemplo, es posible que uno de nuestros empleados haya necesitado acceder a un recurso de la empresa que bien porque ha cambiado de puesto, o por otras razones ya no necesite, con lo que debemos de asegurarnos de retirarle esos privilegios, esto ayuda a evitar la ocurrencia de incidentes de seguridad. Otro ejemplo sería si vamos a despedir a un empleado quitarle sus privilegios de acceso a los recursos antes de que sepa que va a ser despedido para evitar que con el enfado pueda borrar o robar información de la empresa.

- **Realizar auditorías rutinarias:** se pueden realizar auditorías de forma regular desde por ejemplo una revisión de los derechos, o de configuraciones, actualizaciones o análisis de vulnerabilidades.
- **Forzar el uso de políticas y procedimientos:** podemos decir que la seguridad dentro de la empresa comienza cuando tenemos definido nuestro plan de seguridad y nuestras políticas y procedimientos que deben seguir los empleados.

# METODOLOGÍA NIST SP 800-30

Como ya vimos, existen diferentes metodologías para la gestión de riesgos, una de las más importantes e implementadas tanto en empresas como en organismos gubernamentales es la metodología **NIST SP800-30.**

Se basa en el uso de categorías para clasificar la información en función del nivel de riesgo y proporciona estándares para asegurar la información de forma adecuada según su nivel. Esta metodología surge en el Instituto Nacional de Estándares y Tecnología, para evaluar los riesgos de seguridad de la información en sistemas TI.

Sus objetivos son:

- Asegurar los sistemas de información que almacenan, procesan y transmiten información.
- Gestión de Riesgos.
- Mejorar la administración y gestión de riesgos en base al resultado del análisis.
- Proporcionar una base para el desarrollo de la gestión del riesgo.
- Dar información sobre los controles de seguridad necesarios en base a la rentabilidad del negocio.
- Identificación de amenazas y vulnerabilidades.
- Identificar el impacto que generan la materialización de una amenaza.
- Evaluar la probabilidad de ocurrencia.

Esta metodología se compone de 9 fases:

1. Caracterización de los sistemas.
2. Identificación de amenazas.
3. Identificación de vulnerabilidades.
4. Análisis de controles tanto actuales como planificados.
5. Determinación de la probabilidad de ocurrencia que nos permite elaborar un ranking de las amenazas más probables y que requieren medidas inmediatas.
6. Análisis del impacto.
7. Determinación del riesgo: crítico, alto, medio y bajo usando métricas como el CVSS
8. Determinar la matriz del nivel de riesgo.
9. Recomendación de controles.
10. Documentación de los resultados: informe detallado de la valoración de riesgos.

En cuanto a la propia gestión del riesgo, una vez este ha sido determinado debemos.

- Priorizar acciones en función del nivel de riego, los más críticos primero.
- Evaluar los controles recomendados, analizando cuál es su viabilidad y eficacia y si se adecúan correctamente a nuestro entorno de trabajo, o incluso si requieren de formación adicional al personal y los costes que eso también implicaría.
- Análisis coste-beneficio, nos permite conocer el impacto derivado de la aplicación o no de esos controles.
- Selección de los controles necesarios para mitigar el riesgo.

- Asignación de responsabilidades de las personas encargadas de llevar a cabo la implementación y control de las medidas aplicadas.
- Desarrollar un plan de salvaguarda.

Web NIST SP 800-30

web Guía NIST 800-30

## METODOLOGÍA MAGERIT

**MAGERIT** es la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, elaborada por el Consejo Superior de Administración Electrónica. Actualmente se encuentra en su versión 3 (MAGERIT V3 (2019)).

Dicho método cubre la fase AGR (Análisis y Gestión de Riesgos) y su objetivo es la evaluación, homologación y certificación de Seguridad de Sistemas de Información (SGSI) según la **ISO 27001**.

MAGERIT analiza el impacto que puede tener para la empresa un incidente de seguridad, tratando de identificar las amenazas que pueden llegar a afectar a la empresa y las vulnerabilidades explotadas por estas amenazas, teniendo así una idea de las medidas preventivas y correctivas adecuadas para cada caso.

Se organiza en tres volúmenes

- Libro I : Método: Libro I : Método
- Libro II: Catálogo de Elementos: Libro II: Catálogo de Elementos
- Libro III: : Guía de Técnicas

**FASES**

- **Análisis de riesgos:**
  - Determinar **activos** y su valoración CIA.
  - Activo= recursos del sistema, información, datos.
    - Servicios (S).
    - Aplicaciones (SW).
    - Equipos (HW).
    - Soportes de almacenamiento de datos (SI).
    - Equipamiento auxiliar (AUX).
    - Redes de comunicaciones (COM).
    - Instalaciones (L).
    - Personas (P).
  - **Organización de los activos por capas:**
    - **CAPA 4: funciones y procesos de la organización.**
    - **CAPA 3: Información y datos**

    - **CAPA 2: Sistema de información**
        - Aplicaciones.
        - Equipos.
        - Soportes.
        - Redes.
    - **CAPA 1: Entorno**
        - Suministros eléctricos.
        - Climatización.
        - Comunicaciones.
        - Personal.
        - Edificio, mobiliario, etc.
  - Determinar **amenazas.** Cómo degradan CIA de un activo y probabilidad y frecuencia de aparición.
  - Determinar **salvaguardas.**
  - Determinar **impacto**.
  - Determinar el **riesgo** o medida del daño probable.
- Valoración de activos en las dimensiones CIA.
  - **Autenticidad:** medir el perjuicio que causaría no saber exactamente quién ha hecho cada cosa.
  - **Trazabilidad:** quién hace qué y cuándo.

- Posibilidad de identificar el origen y las diferentes etapas de un proceso de producción y distribución de bienes de consumo.
    - LOGS
- Determinar factores como:
    - Coste de reposición (adquisición e instalación).
    - Coste mano de obra para recuperar un activo.
    - Pérdida de ingresos.
    - Capacidad de operar (confianza de usuarios y proveedores).
    - Sanciones por incumplir leyes.
    - Daño a otros activos propios o ajenos.
    - Daño a personas.
    - Daños medioambientales.
- **Determinar análisis de amenazas.**
    - No hay un listado completo de amenazas.
    - Existen catálogos de amenazas.
        - Catálogo amenazas **MAGERIT**
        - **ISO 13335-4:2000** (amenazas y salvaguardas).
        - **ISF** (Information Security Forum).
        - **BSI** (Federal Office for information security)
    - Determinar la frecuencia de ocurrencia de las amenazas.
    - **Degradación**: mide el daño causado por un incidente de seguridad si este ocurre.

- **Impacto**: Medida del daño sobre el activo por materialización de amenaza. Cálculo en porcentaje para cada activo y para cada dimensión.
- **Impacto acumulado**: producido sobre el valor acumulado de un activo, a raíz de sus amenazas y frecuencia de las mismas.
    - Facilita selección de salvaguardas.
- **Impacto repercutido**: impacto en un activo a consecuencia de su valor propio (no del acumulado), y de las amenazas a las que están expuestos sus activos inferiores.
    - Consecuencias de incidencias técnicas

Extraído de Auditoría de la seguridad informática. Silvia Clara Menéndez Arante. Editorial RAMA