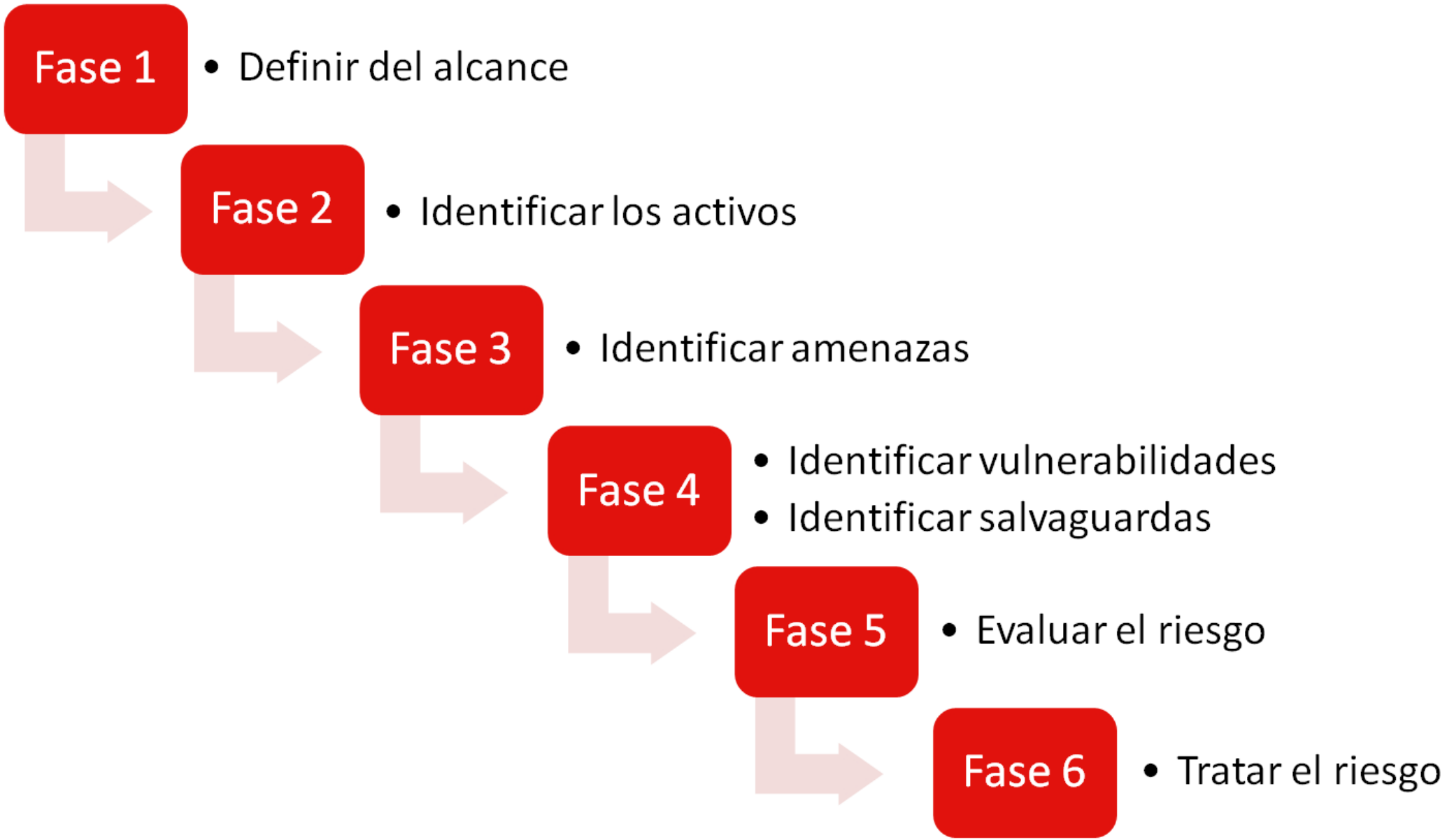
ANALISIS DE RIESGOS DE SISTEMAS DE INFORMACION

Metodologías

- **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.
- Enlace a Web COSO: *http://www.coso.org/guidance.htm*
- **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.
- Enlace a Web ISO 31000: *http://www.iso.org/iso/ES/home/standards/iso31000.htm*

Metodologías

- **MAGERIT**: metodología de Análisis y Gestión de Riesgos de los Sistemas de Información creada por el Ministerio de Administraciones Públicas español.
- Enlace a Web MAGERIT: *http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html*
- **ISO / IEC 27005:2011:** norma que aporta directrices para la gestión de riesgos de seguridad de la información.
- Enlace a Web ISO 27005: *http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=56742*
- **NIST SP - 800-30**: metodología creada por el gobierno norteamericano.
- Enlace a Web NIST: *http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf*


Fase 1
• Definir del alcance
Fase 2
• Identificar los activos
Fase 3
• Identificar amenazas
Fase 4
• Identificar vulnerabilidades
• Identificar salvaguardas
Fase 5
• Evaluar el riesgo
Fase 6
• Tratar el riesgo

Fase 1. Definir el alcance

- El primer paso a la hora de llevar a cabo el análisis de riesgos, es establecer el alcance del estudio. Vamos a considerar que este análisis de riesgos forma parte del Plan Director de Seguridad. Por lo tanto, recomendamos que el análisis de riesgos cubra la totalidad del alcance del PDS, dónde se han seleccionado las áreas estratégicas sobre las que mejorar la seguridad. Por otra parte, también es posible definir un alcance más limitado atendiendo a departamentos, procesos o sistemas.
- *Por ejemplo*, análisis de riesgos sobre los procesos del departamento Administración, análisis de riesgos sobre los procesos de producción y gestión de almacén o análisis de riesgos sobre los sistemas TIC relacionados con la página web de la empresa, etc. En este caso práctico consideramos que el alcance escogido para el análisis de riesgos es “Los servicios y sistemas del Departamento Informática

Fase 2. Identificar los activos

ID	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
ID_01	Servidor 01	Servidor de contabilidad.	Director Financiero	Servidor (Físico)	Sala de CPD1	Sí
ID_02	RouterWifi	Router para la red WiFi de cortesía a los clientes.	Dept. Informática	Router (Físico)	Sala de CPD1	No
ID_03	Servidor 02	Servidor para la página web corporativa.	Dept. Informática	Servidor (Físico)	CPD externo	Sí
…						

Fase 3. Identificar / seleccionar las amenazas

- Habiendo identificado los principales activos, el siguiente paso consiste en identificar las amenazas a las que estos están expuestos. Tal y como imaginamos, el conjunto de amenazas es amplio y diverso por lo que debemos hacer un esfuerzo en mantener un enfoque práctico y aplicado. *Por ejemplo*, si nuestra intención es evaluar el riesgo que corremos frente a la destrucción de nuestro servidor de ficheros, es conveniente, considerar las averías del servidor, la posibilidad de daños por agua (rotura de una cañería) o los daños por fuego, en lugar de plantearnos el riesgo de que el CPD sea destruido por un meteorito.
-

¿Cuáles son los vectores de ataque más frecuentes?

- **Correo electrónico y mensajería instantánea,** por ejemplo los correos y SMS de *phishing* que suplantan a organizaciones conocidas por el receptor, como bancos, empresas de paquetería, la Agencia Tributaria, nuestros proveedores y clientes, o nuestro soporte técnico, para engañarle con diversos señuelos, a seguir enlaces a páginas web falsas donde le pedirán introducir sus credenciales o descargar adjuntos maliciosos que instalan ***malware***. Es muy frecuente que se trate de ***ransomware***, es decir, el *malware* que bloquea los datos a cambio de un rescate. En otros casos, el *malware* convierte a nuestros dispositivos en zombis a su servicio para lanzar ataques a terceros o para otros fines poco éticos.

- **Navegación web**, bien por falta de actualización de los navegadores o por instalación de *plugins* maliciosos, bien por visitar páginas fraudulentas. Ante navegadores no actualizados, los ciberdelincuentes podrían explotar vulnerabilidades con técnicas como:
  - *drive-by download*, que permite la descarga de *malware* sólo con visitar una página maliciosa o ver un correo html;
  - *browser in the browser*, que simula una ventana emergente de autenticación, donde nos pedirán las credenciales.
-

- ***Endpoints*** o terminales y otros dispositivos en los que no se han configurado las opciones de seguridad lo que los deja vulnerables. Las configuraciones de los fabricantes por defecto son, en muchos casos, poco seguras. Por ejemplo, si usan contraseñas débiles o si permiten que se conecten USB o discos extraíbles, estos podrían llevar *malware*. Otras veces son configuraciones incompletas o insuficientes de las redes a las que pertenecen esos dispositivos y permiten el acceso a ellos y su manipulación. Un caso particular son los dispositivos IoT.

- **Aplicaciones web, portales corporativos, intranets y redes sociales** con configuraciones defectuosas o si están desactualizados pueden suponer una vía de entrada o bien una forma de dar información al ciberdelincuente para posteriores ataques.
-

- ***Software* de redes y sistemas mal configurado, desactualizado o no parcheado**, es decir, no se han seguido procedimientos adecuados en su configuración y no se han aplicado las actualizaciones o no existen por estar ya el *software* fuera de su vida útil. Un ejemplo de uso de esta vía de entrada por los ciberdelincuentes son los ataques contra el *router*, como *DNS hijacking* o los ataques de DoS o Denegación de servicio, como le pasó a esta empresa en esta historia real.
-

- **Credenciales de usuario comprometidas** bien porque están en fugas de datos y se reutilizan en otros sistemas, bien porque han sido obtenidas por fuerza bruta o por ataques de ingeniería social. En otros casos son obtenidas mediante *software* o *hardware* que registra las pulsaciones o *keyloggers* o *software* que espía redes wifi abiertas o con configuraciones de cifrado obsoletas.
-

- **Contraseñas y credenciales predecibles o por defecto** bien porque no se han cambiado, las típicas ´*admin/admin*´ o las que pone el fabricante y se pueden encontrar en la web; o si se han cambiado se ha hecho por otras de uso común o fácilmente predecibles por el entorno de usuario; bien porque están ´*hardcodeadas*´, es decir, incluidas en la electrónica de los dispositivos.
-

- ***Insiders*** o personas con acceso que pueden exfiltrar información. Pueden ser empleados insatisfechos por despecho, exempleados que conservan por fallos de procedimiento credenciales de acceso o bien los que pudieran haberse dejado sobornar por ciberdelincuentes.
-

- **Carencias del cifrado** bien por su debilidad, al usar claves simples y deducibles o protocolos obsoletos, o por no aplicarse correctamente las políticas al respecto, por ejemplo en dispositivos móviles o portátiles o por olvido de cifrar documentos en la nube. Este vector puede llevar a fugas de información.
-

- **Debilidades de la cadena de suministro**, como proveedores tecnológicos o empresas colaboradoras. Si sus sistemas sufren un incidente, nuestros datos pueden verse comprometidos. Por ello hemos de revisar las cláusulas de seguridad de los Acuerdos de Nivel de Servicio. Un caso particular son los proveedores de servicios en la nube.
-

Fase 4. Identificar vulnerabilidades y salvaguardas

- La siguiente fase consiste en estudiar las características de nuestros activos para identificar puntos débiles o vulnerabilidades. *Por ejemplo,* una posible vulnerabilidad puede ser identificar un conjunto de ordenadores o servidores cuyo sistemas antivirus no están actualizados o una serie de activos para los que no existe soporte ni mantenimiento por parte del fabricante. Posteriormente, a la hora de evaluar el riesgo aplicaremos penalizaciones para reflejar las vulnerabilidades identificadas.
-

- **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.

- **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

- **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.
- **Vishing**: es un phishing, pero realizado a través de una llamada telefónica.

Ataques de red

- **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

- **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.

Ataques al sistema

- **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

Nmap:

- **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
-
- 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.

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 (evitar algoritmos obsoletos: SHA1 o MD5 - usar: **SHA-2** y su variante más conocida, **SHA-256)**.
  - Ataques de texto plano (KPA).

Ataques a aplicaciones

- **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.

Ataques a aplicaciones

- **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

- **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 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,

Software malicioso

- **Virus:** un virus es una pieza de software malicioso que tiene la capacidad de infectar un sistema pudiendo eliminar datos o corromperlos
  - **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.

- **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

- **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

- **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.

- **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.

- **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.

Tecnicas de dispositivos moviles

- 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 dispositivo

- **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

- **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
- **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.

TÉCNICAS

CRITERIOS DE PROGRAMACIÓN SEGURA

- Como implementar apps mas seguras

- **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)

- **Control de cambios:** tenemos que asegurarnos de implementar procedimientos de control de 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,

- **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

Páginas para encontrar bases de datos de vulnerabilidades

- **CIRCL**
- Sus siglas vienen de Computer Incident Response Center Luxembourg. Se trata de una organización de seguridad diseñada para detectar y solucionar amenazas cibernéticas. En su **página** podemos ver diferentes informes y trabajos de investigación de este ámbito.
-

- **VulDB**
- ofrece una gran base de datos con **más de 124.000 CVE**. Cada día añaden cientos de vulnerabilidades nuevas. Además, las califican según el riesgo del exploit encontrado: bajo, medio o alto.
- Esta **plataforma** se ha coordinado con diferentes comunidades de seguridad. El objetivo es ofrecer una gran variedad de información de seguridad a los usuarios.

- **SecurityFocus**
- Otra base de datos más es **SecurityFocus**. Cuenta con **datos recopilados desde 1999**. Ofrece un rastreo constante de errores y vulnerabilidades de software.
- Podemos acceder a su base de datos en su **página web**.
-

- **Rapid7**
- Cuenta también con una base de datos amplia, pero en esta ocasión rara vez informa del código de explotación real. Lo que sí hace es ofrecer avisos que contienen referencias útiles a la documentación sobre esa explotación.
- Podemos acceder a la base de datos actualizada desde este **link**.

- **MITRE**
- es una organización que pertenece al gobierno de Estados Unidos. Es quien administra diferentes centros de investigación de seguridad y cuenta con una **base de datos de vulnerabilidades CVE muy amplia**, actualizada y con muchas referencias.
-

Fase 5. Evaluar el riesgo

Tabla para el cálculo de la probabilidad

Cualitativo	Cuantitativo	Descripción
Baja	1	La amenaza se materializa a lo sumo una vez cada año.
Media	2	La amenaza se materializa a lo sumo una vez cada mes.
Alta	3	La amenaza se materializa a lo sumo una vez cada semana.

Tabla para el cálculo del impacto

Cualitativo	Cuantitativo	Descripción
Bajo	1	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Medio	2	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
Alto	3	El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.

		IMPACTO		
		Bajo	Medio	Alto
PROBABILIDAD	Baja	Muy bajo	Bajo	Medio
	Media	Bajo	Medio	Alto
	Alta	Medio	Alto	Muy alto

Fase 6. Tratar el riesgo

- **Transferir** el riesgo a un tercero. *Por ejemplo*, contratando un seguro que cubra los daños a terceros ocasionados por fugas de información.
- **Eliminar** el riesgo. *Por ejemplo,* eliminando un proceso o sistema que está sujeto a un riesgo elevado. En el caso práctico que hemos expuesto, podríamos eliminar la wifi de cortesía para dar servicio a los clientes si no es estrictamente necesario.
- **Asumir** el riesgo, siempre justificadamente. *Por ejemplo,* el coste de instalar un grupo electrógeno puede ser demasiado alto y por tanto, la organización puede optar por asumir.
- **Implantar** medidas para mitigarlo. *Por ejemplo,* contratando un acceso a internet de respaldo para poder acceder a los servicios en la nube en caso de que la línea principal haya caído.

¿Qué podemos hacer para controlar esas vías de ataque?

- facilidad humana para cometer errores o fallos y las carencias organizativas podemos:
- Formarnos y sensibilizarnos. Accede al apartado de Formación.
- Aplicar políticas de uso, con restricciones y usos permitidos, y si fuera necesario con sanciones. Echa un vistazo a las Políticas de seguridad para la pyme.
- Establecer acuerdos y compromisos desde el comienzo como te contamos en el apartado contratación de servicios.
- Identificar a los responsables de la seguridad de cada servicio que utilice las TIC. Asegurar su formación y competencia.

- Fallos técnicos y de configuración podemos:
- Conocer todos nuestros activos, en nuestras instalaciones y en las de nuestros proveedores TI. Elaborar un inventario que incluya sus posibles vulnerabilidades. Si es necesario contrataremos una auditoría.
- Revisar las amenazas que pueden afectar a nuestros activos, valorar el daño que podrían causar y cuál es nuestra preparación ante ellas con un análisis de riesgos.

- Establecer una política de actualizaciones para mantener los activos actualizados y bien configurados. Valorar si es posible cambiarlos si no se pueden actualizar o bien dejarlos de utilizar.
- Proteger las comunicaciones y las redes wifi.
- Monitorizar continuamente los accesos a redes y servicios. Utilizar herramientas para detectar intrusiones.
- Gestionar los permisos de acceso, exigir doble factor de autenticación en los servicios críticos. Aplicar procedimientos de cambio de contraseña con frecuencia suficiente.