Glosario de Términos

Jesús Temprano Gallego

DAW2

Ultima revisión: 19/11/2025

Contenido

1. Amenazas y vulnerabilidades informáticas.

Amenazas

Cualquier situación, acción o evento que **pueda causar daño** a los sistemas, datos o redes de un equipo u organización.

https://www.incibe.es/empresas/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Vulnerabilidades

Fallos o debilidades en sistemas, programas o redes **que pueden ser aprovechados** por atacantes para causar daño o acceder sin permiso.

https://www.incibe.es/empresas/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Confidencialidad

Principio de seguridad que asegura que la información solo sea accesible para **quienes tienen autorización**, evitando accesos no autorizados.

https://www.incibe.es/empresas/blog/sabes-proteger-informacion-tu-empresa

Disponibilidad

Principio de seguridad que garantiza que los sistemas, servicios y datos estén **accesibles** y **operativos** cuando los usuarios autorizados los necesiten.

https://www.incibe.es/empresas/blog/sabes-proteger-informacion-tu-empresa

Integridad

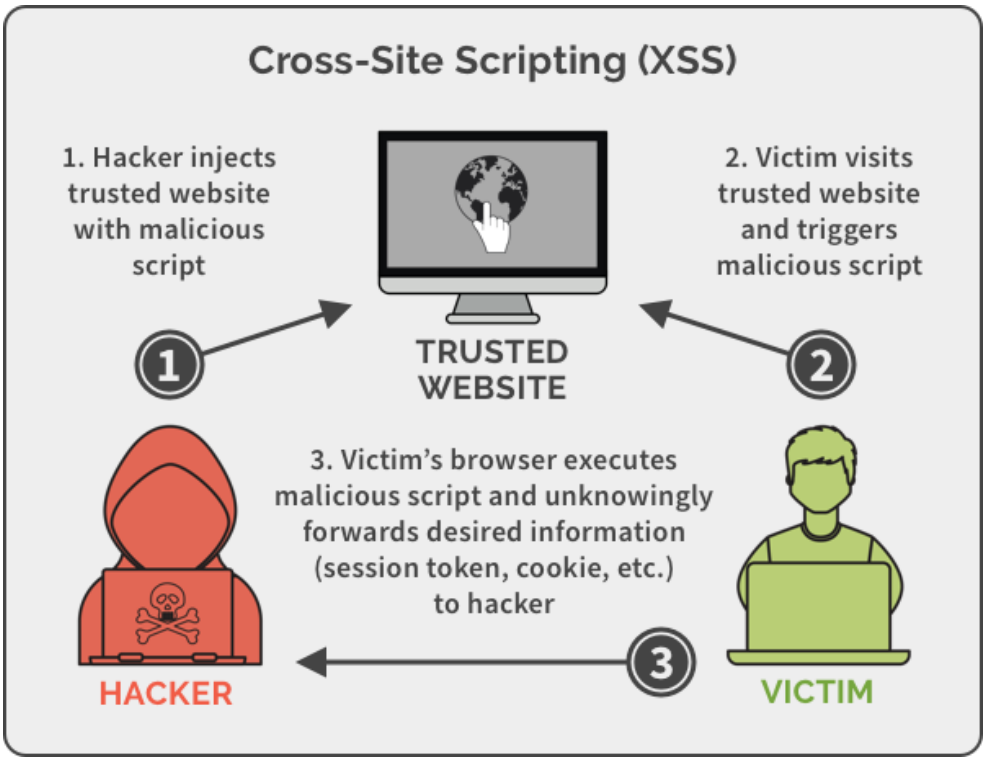
Principio de seguridad que asegura que la información no sea alterada, modificada o destruida de forma no autorizada.

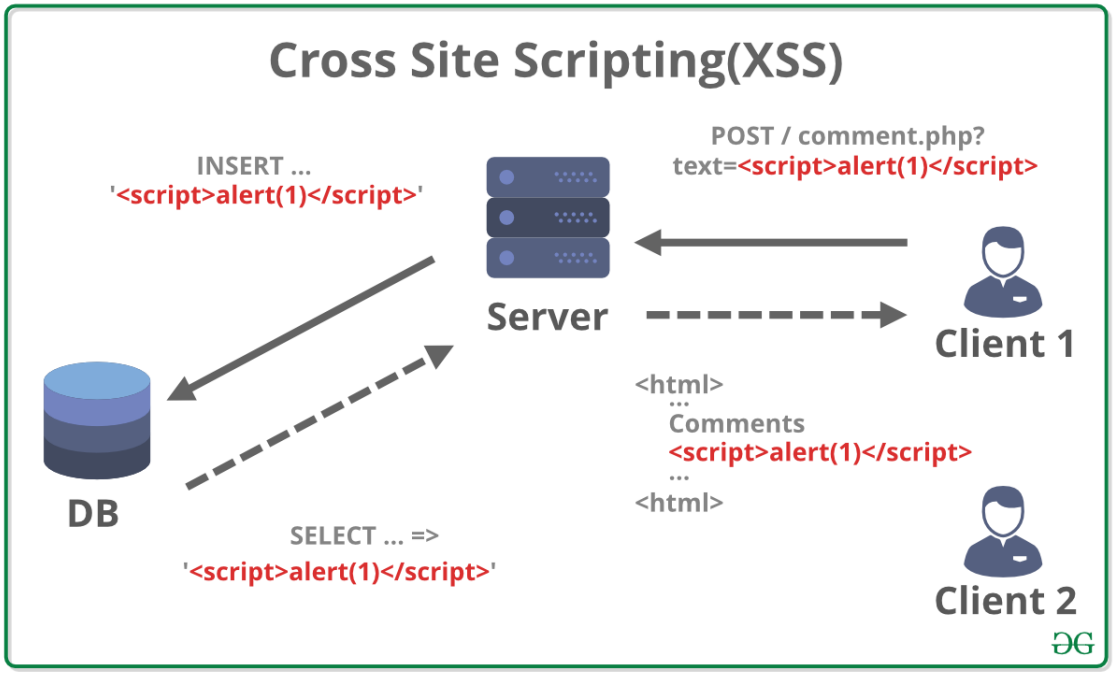
https://www.incibe.es/empresas/blog/sabes-proteger-informacion-tu-empresa

Cross-Site Scripting (XSS)

Vulnerabilidad de seguridad en aplicaciones web donde un atacante inserta código malicioso (normalmente JavaScript) que se ejecuta en el navegador de otros usuarios.

https://www.welivesecurity.com/la-es/2021/09/28/que-es-ataque-xss-cross-site-scripting/

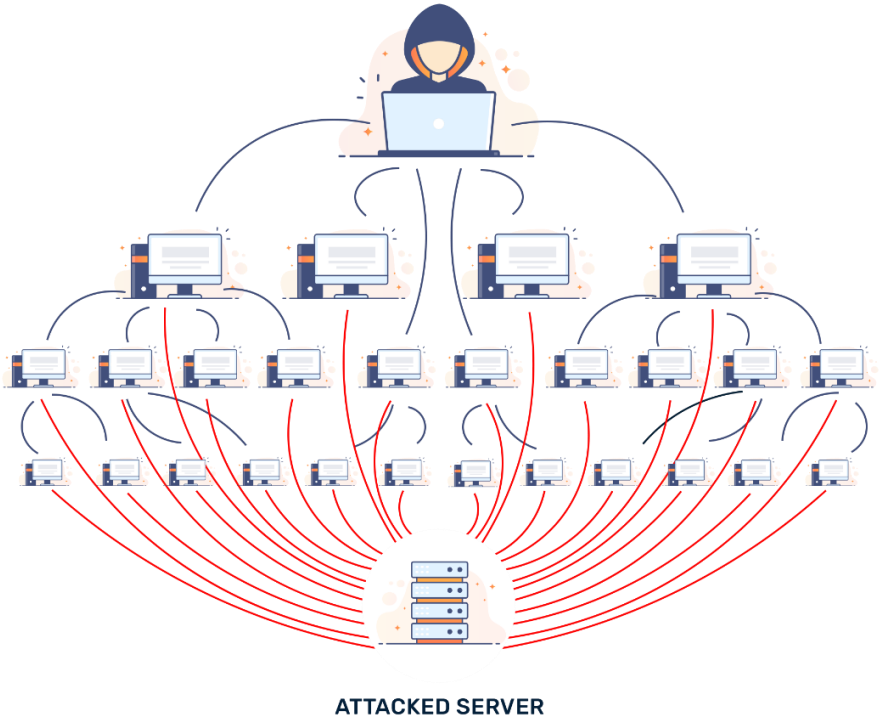




DDoS

Ataque que busca saturar un servidor o red enviando gran cantidad de tráfico **desde múltiples equipos**, provocando que deje de funcionar.

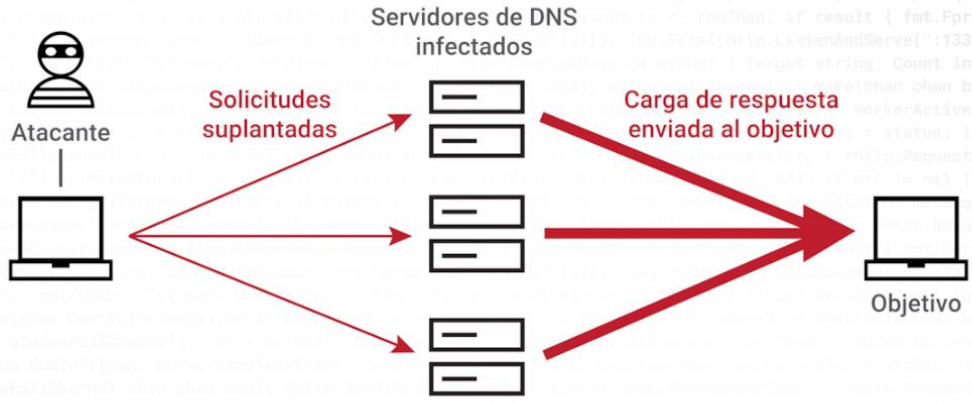
https://www.cloudflare.com/es-es/learning/ddos/what-is-a-ddos-attack/



DoS

Es un ataque que también busca saturar un servidor o red enviando gran cantidad de tráfico provocando que deje de funcionar, *pero a diferencia del DDoS*, este es **desde un solo equipo**.

https://www.cloudflare.com/es-es/learning/ddos/glossary/denial-of-service/



Exploits

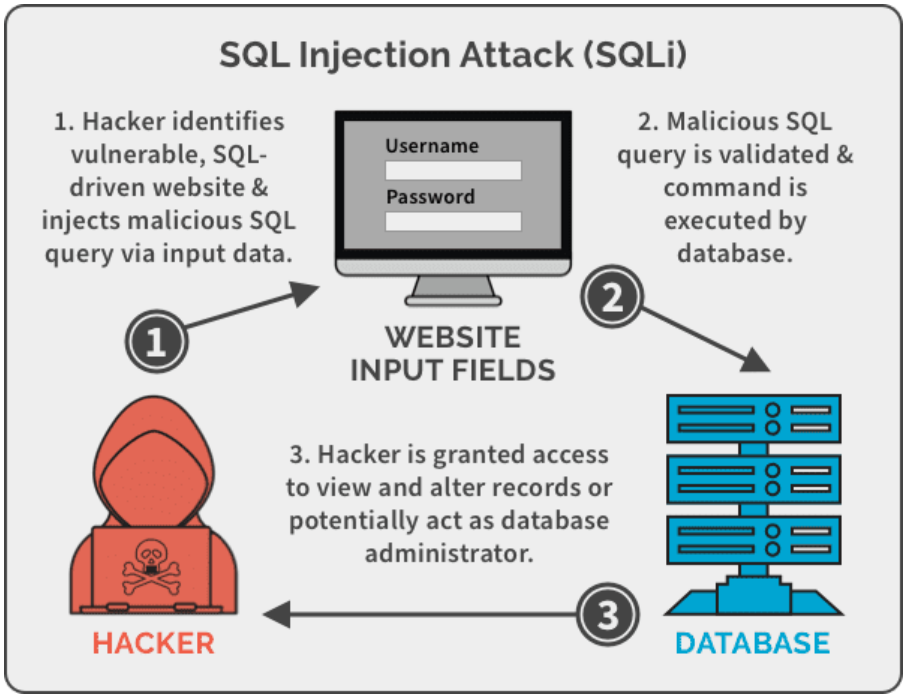
Programas, fragmentos de código o técnicas que aprovechan vulnerabilidades en sistemas, aplicaciones o redes para realizar acciones no autorizadas.

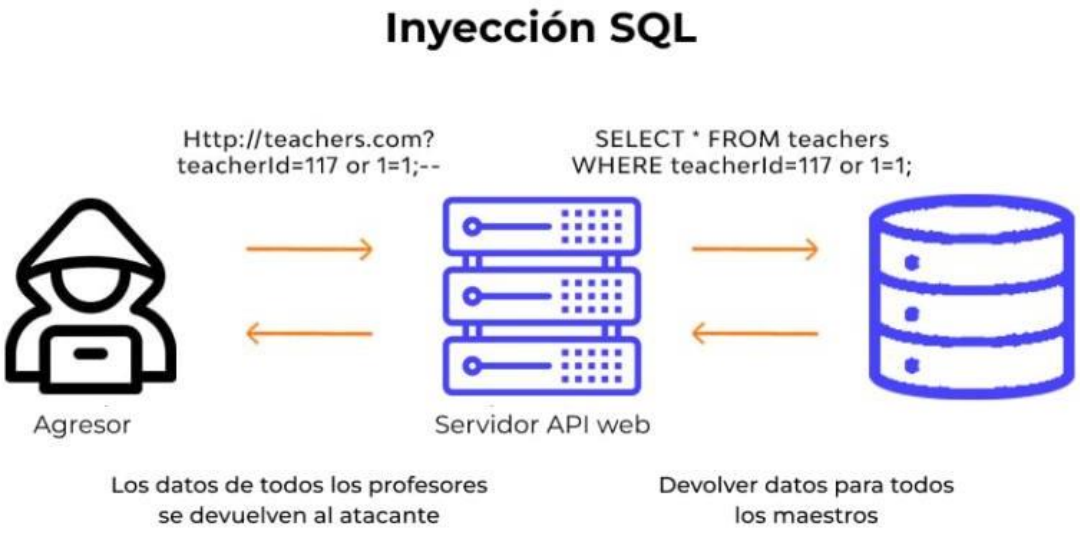
https://www.bitdefender.es/consumer/support/answer/22884/

Inyección SQL

Vulnerabilidad donde un atacante inserta código SQL malicioso en una aplicación para acceder o manipular la base de datos sin permiso.

https://www.incibe.es/empresas/blog/ataques-inyeccion-sql-amenaza-tu-web



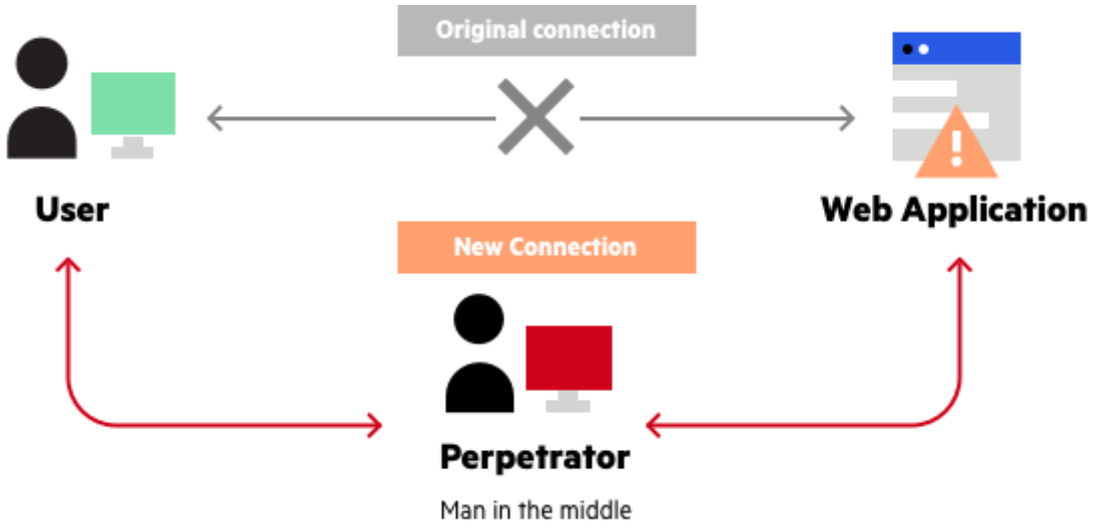


Man-in-the-Middle

Ataque en el que un atacante intercepta y, a veces, modifica la comunicación entre dos partes sin que ellas lo sepan.

https://www.incibe.es/empresas/blog/el-ataque-del-man-middle-empresa-riesgos-y-formas-evitarlo

https://www.youtube.com/watch?v=XigK57MTk7Y



2. Medidas de protección básicas.

Auditoría

Revisión sistemática de sistemas, redes y procedimientos de seguridad para verificar que cumplan con normas, políticas y buenas prácticas; para detectar posibles fallos o vulnerabilidades que podrían aprovechar los atacantes.

https://www.incibe.es/ed2026/talento-hacker/blog/auditoria-de-ciberseguridad-que-es-para-que-sirve-y-como-formarte-en-este-campo

https://www.piranirisk.com/es/academia/especiales/auditoria-de-ciberseguridad-empresas

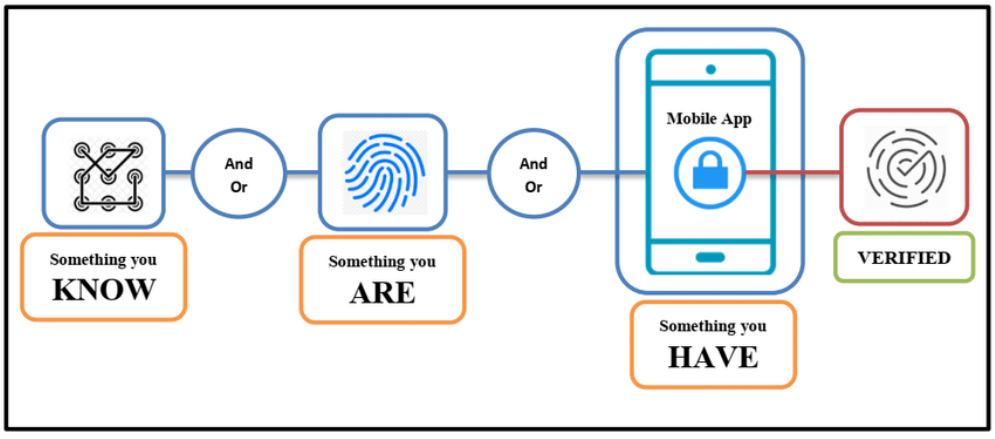
Autenticación Multifactor (MFA)

Método de seguridad que requiere más de un tipo de verificación para acceder a un sistema.

Combina algo que sabes (*contraseña o PIN*), algo que tienes (*móvil*, token) y algo que eres (huella, reconocimiento facial o voz).

https://aws.amazon.com/es/what-is/mfa/

https://www.cloudflare.com/es-es/learning/access-management/what-is-multi-factor-authentication/



Filtrado

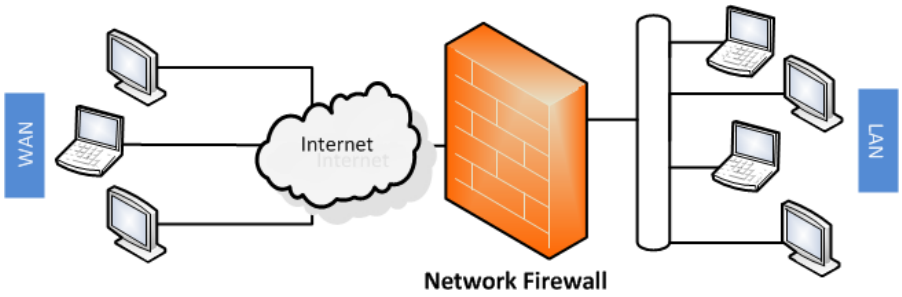
Proceso de examinar y controlar el tráfico de red o información según ciertas reglas para permitir o bloquear el acceso.

https://flashstart.com/es/optimiza-el-rendimiento-con-filtros-wifi/

Firewall

Dispositivo o software especializado en impedir la comunicación. Controla el tráfico de red entre diferentes redes, permitiendo o bloqueando el acceso según reglas de seguridad.

https://www.cloudflare.com/es-es/learning/security/what-is-a-firewall/



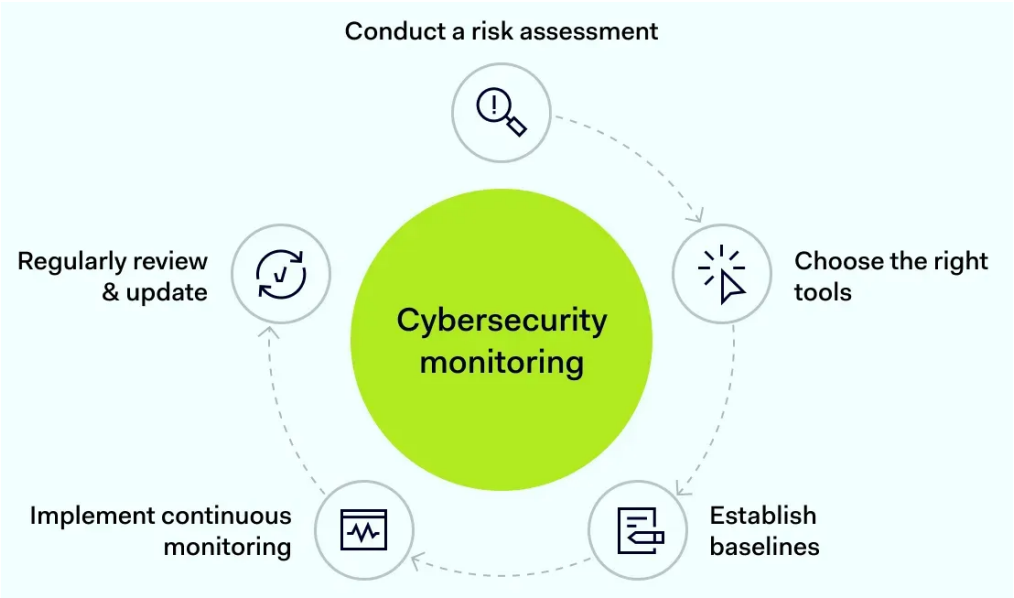
Monitoreo

Supervisión continua de sistemas, redes o aplicaciones para detectar problemas, anomalías o posibles ataques.

https://www.ibm.com/es-es/think/topics/network-monitoring

https://www.ibm.com/es-es/think/topics/infrastructure-monitoring

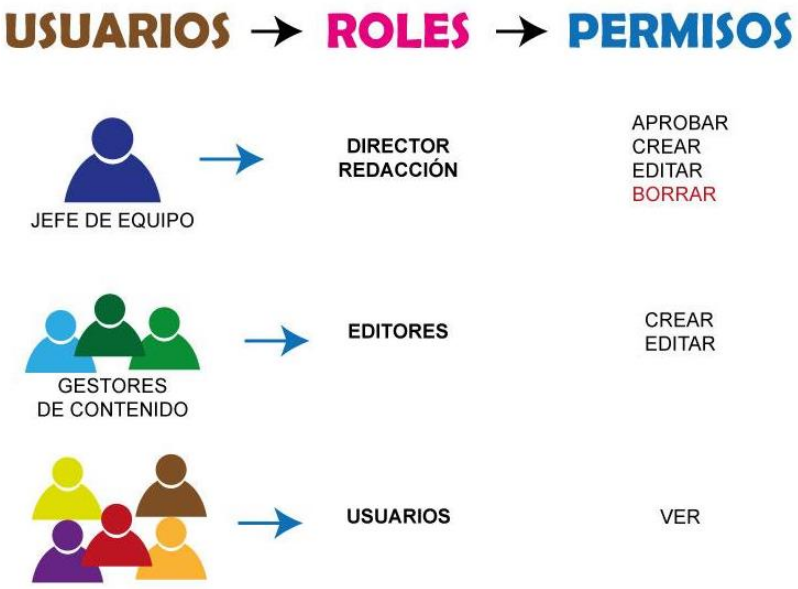
https://www.ibm.com/es-es/think/topics/condition-monitoring



Permisos

Derechos asignados a usuarios o programas que determinan qué acciones pueden realizar sobre archivos, carpetas o recursos del sistema.

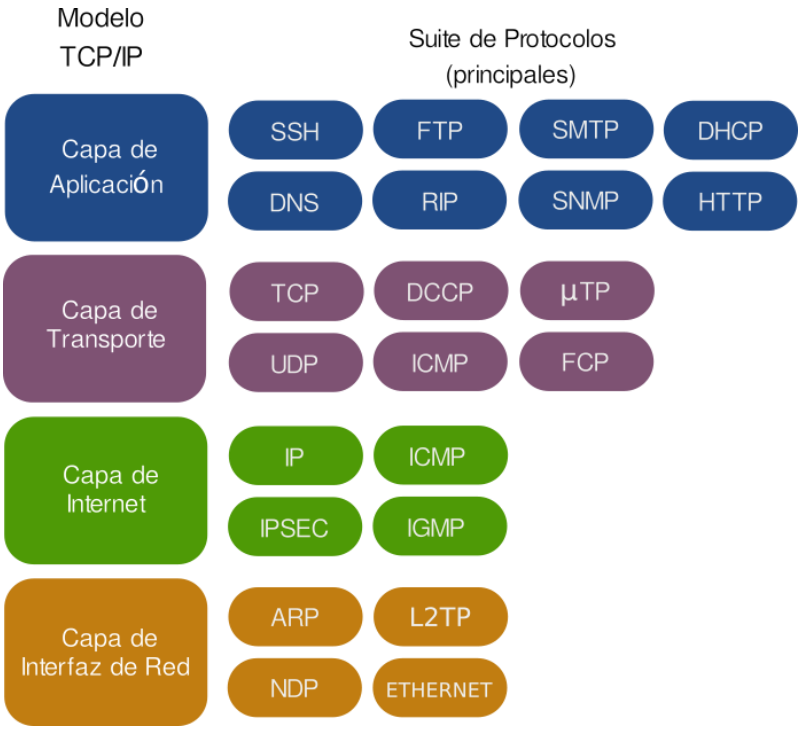
https://www.ibm.com/docs/es/gdp/12.x?topic=guardium-managing-roles-permissions



Protocolos

Conjuntos de reglas que determinan cómo se comunican los dispositivos en una red (por ejemplo, HTTP, TCP/IP, FTP).

https://es.wikipedia.org/wiki/Familia_de_protocolos_de_internet



Puertos

Puntos lógicos que permiten a un ordenador o servidor identificar y gestionar diferentes tipos de tráfico de red o servicios (por ejemplo, puerto 80 para HTTP).

https://achirou.com/guia-rapida-de-puertos-y-protocolos/

Reglas

Conjunto de **condiciones** o **instrucciones** que determinan cómo deben actuar los sistemas de seguridad, como cortafuegos o antivirus, para permitir o bloquear acciones.

https://help.eset.com/ees/10.1/es-CL/idh_dialog_epfw_app_tree_rules_page.html

Ejemplo de reglas de un cortafuegos

Regla	Acción	IP Origen	IP Destino	Proto-colo	Puerto Origen	Puerto Destino
1	Aceptar	172.16.0.0/16	192.168.0.4	tcp	cualquiera	25
2	Aceptar	cualquiera	192.168.10.8	tcp	cualquiera	80
3	Aceptar	172.16.0.0/16	192.168.0.2	tcp	cualquiera	80
4	Negar	cualquiera	cualquiera	cualquiera	cualquiera	cualquiera

Roles

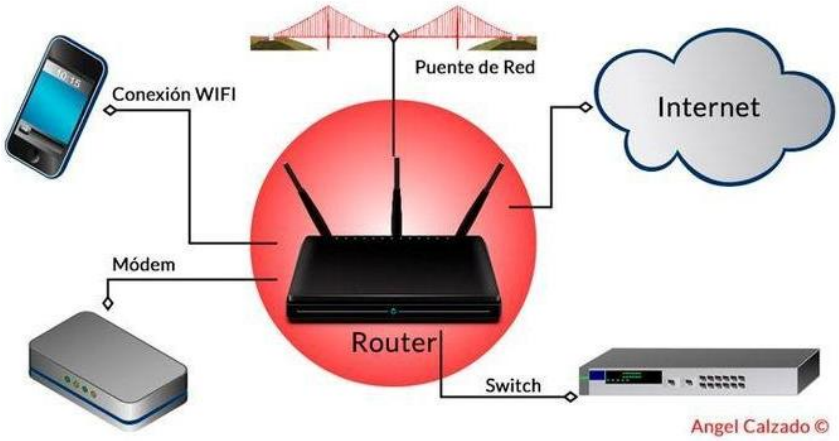
Conjuntos de **permisos** o **funciones** asignados a uno o varios usuarios dentro de un sistema, que determinan qué acciones puede realizar (por ejemplo: *administrador, usuario, invitado*).

https://www.ibm.com/docs/es/gdp/12.x?topic=guardium-managing-roles-permissions

Routers

Dispositivo o software especializados en comunicar. Dirigen el tráfico de datos entre diferentes redes, como entre una red local (LAN) y una conexión a Internet.

https://es.wikipedia.org/wiki/Rúter



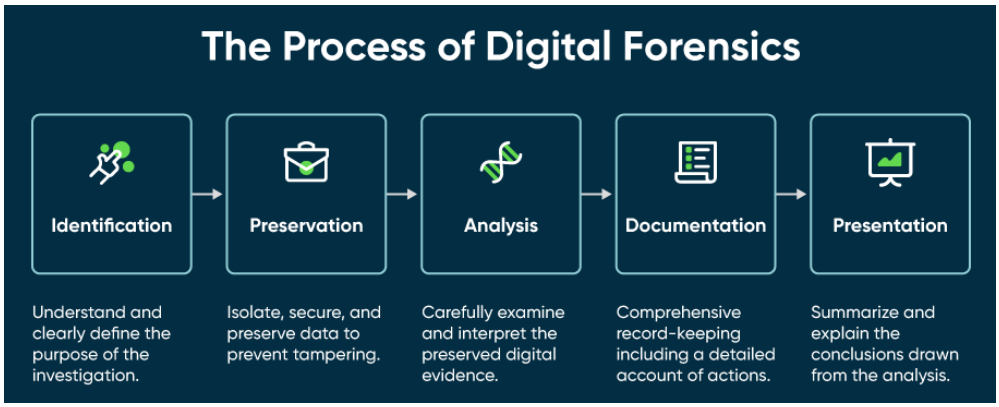
3. Análisis de los Incidentes de seguridad.

Análisis forense

Proceso de investigar incidentes de seguridad en un equipo o red para identificar qué ocurrió, cómo ocurrió y quién fue responsable, preservando evidencia digital.

https://www.ibm.com/es-es/think/topics/digital-forensics

https://www.bernanetwork.com/analisis-forense-informatico



Ciclo de vida de un incidente: detección, análisis, contención, erradicación, recuperación y aprendizaje

Proceso que sigue un equipo de seguridad para manejar un incidente:

- **Detección**: Identificar que ha ocurrido un incidente.
- **Análisis**: Determinar la causa y el alcance del incidente.
- **Contención**: Limitar el daño y evitar que se propague.
- **Erradicación**: Eliminar la amenaza de los sistemas afectados.
- **Recuperación**: Restaurar los sistemas y datos a un estado normal.
- **Aprendizaje**: Revisar el incidente para mejorar la seguridad y prevenir futuros problemas.

https://socprime.com/es/blog/what-is-the-vulnerability-management-lifecycle/

Estrategias proactivas

Medidas de seguridad que se toman antes de que ocurra un incidente para prevenir ataques o problemas, como análisis de vulnerabilidades o actualizaciones periódicas.

https://stefanini.com/es/tendencias/articulos/futuro-ciberseguridad-estrategias-proactivas-proteccion-negocios

https://enthec.com/seguridad-proactiva/

Incidentes de seguridad

Eventos que afectan la seguridad de la información o sistemas, como ataques, accesos no autorizados o fallos de software.

https://www.bancosantander.es/glosario/incidente-seguridad

https://blog.hackmetrix.com/incidentes-de-seguridad-que-son-y-como-protegerte/

Indicadores de compromiso (IoC)

Señales o evidencias que indican que un sistema o red ha sido comprometido por un ataque o malware.

https://www.cloudflare.com/es-es/learning/security/what-are-indicators-of-compromise/

https://www.fortinet.com/lat/resources/cyberglossary/indicators-of-compromise

4. Herramientas y tecnologías de aplicación.

Antimalware

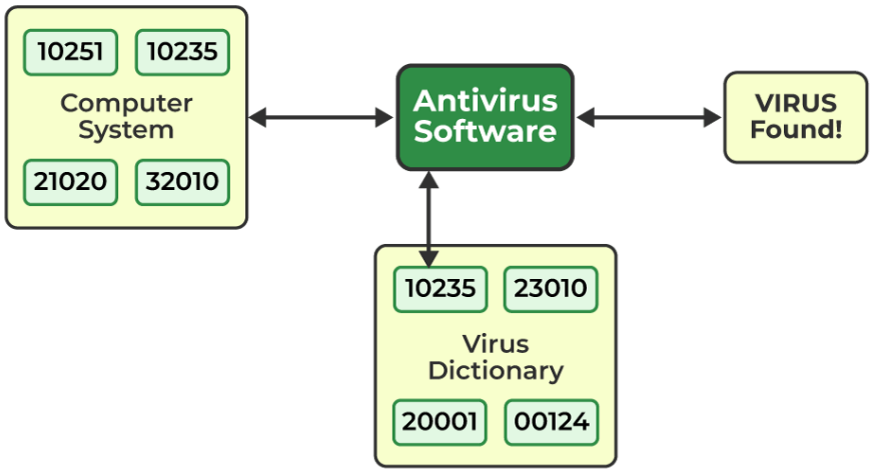
Software diseñado para detectar, prevenir y eliminar **programas maliciosos** como virus, troyanos, spyware, ransomware, etc.

https://lockbits.cl/blog/antivirus-y-antimalware-cual-es-la-diferencia/

Antivirus

Tipo de antimalware especializado en detectar y eliminar virus informáticos, aunque muchos antivirus modernos también protegen contra otros tipos de malware.

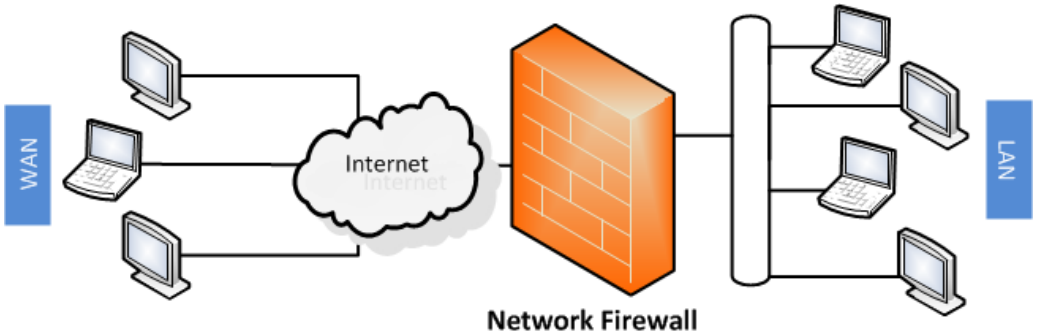
https://www.geeksforgeeks.org/computer-science-fundamentals/what-is-antivirus-software/



Cortafuegos

Dispositivo o software especializado en impedir la comunicación. Controla el tráfico de red entre diferentes redes, permitiendo o bloqueando el acceso según reglas de seguridad.

https://www.cloudflare.com/es-es/learning/security/what-is-a-firewall/

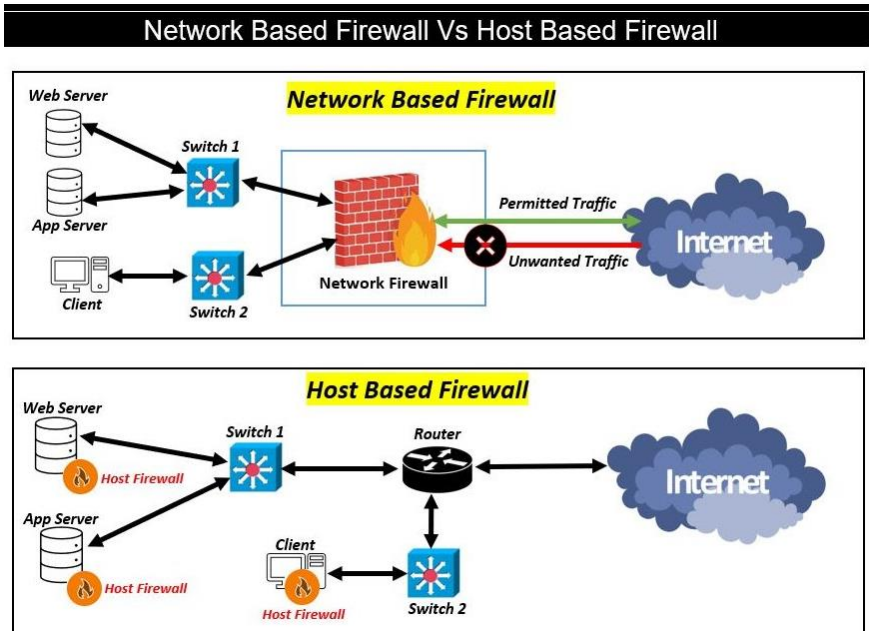


Cortafuegos: basados en red y basados en host

- **Basados en red**: Protegen toda una red, filtrando el tráfico que entra y sale a nivel de red.
  https://www.hpe.com/es/es/what-is/network-firewall.html

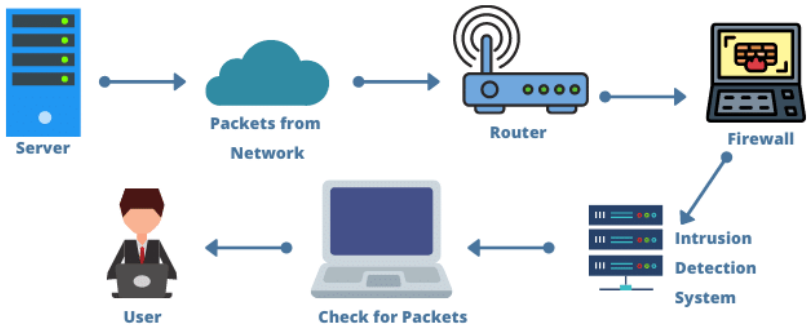
- **Basados en host**: Protegen un equipo específico, controlando el tráfico hacia y desde ese equipo.
  https://www.paloaltonetworks.com/cyberpedia/what-is-a-host-based-firewall

https://www.tufin.com/blog/host-based-firewall-vs-network-based-firewall-best-fit

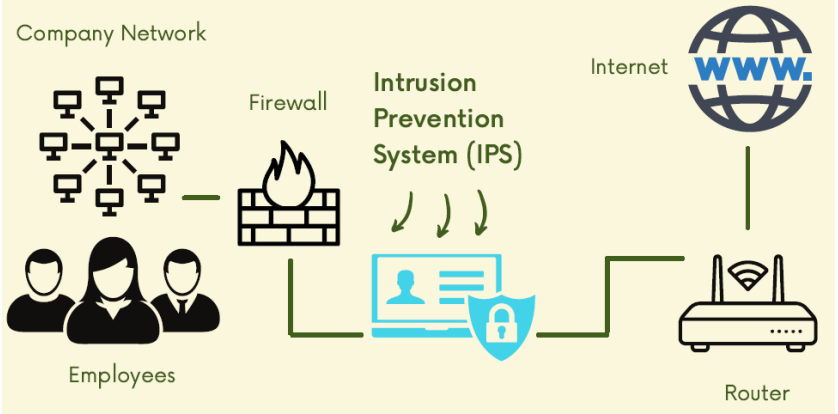


IDS/IPS

- **IDS (Intrusion Detection System)**: Sistema que detecta actividades sospechosas o intrusiones en una red o equipo.
  https://www.fortinet.com/lat/resources/cyberglossary/intrusion-detection-system



- **IPS (Intrusion Prevention System)**: Similar al IDS, pero además bloquea automáticamente las amenazas detectadas.
  https://www.ibm.com/think/topics/intrusion-prevention-system



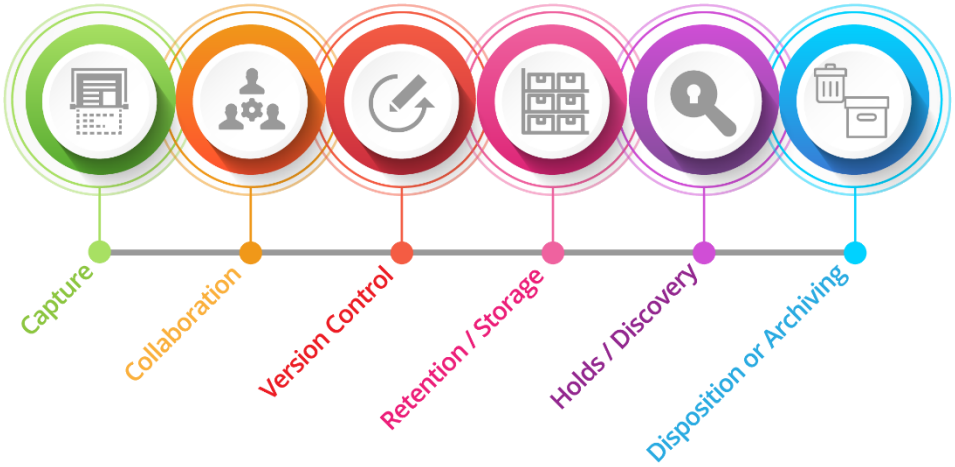
5. Normativas y buenas prácticas de uso.

Ciclo de vida de la información

Etapas por las que pasa la información desde que se crea hasta que se elimina, incluyendo creación, almacenamiento, uso, compartición, archivado y destrucción.

https://www.esic.edu/rethink/tecnologia/ciclo-vida-datos-c

https://www.athento.com/es/fases-del-ciclo-de-vida-de-la-informacion-desde-la-creacion-a-la-eliminacion/

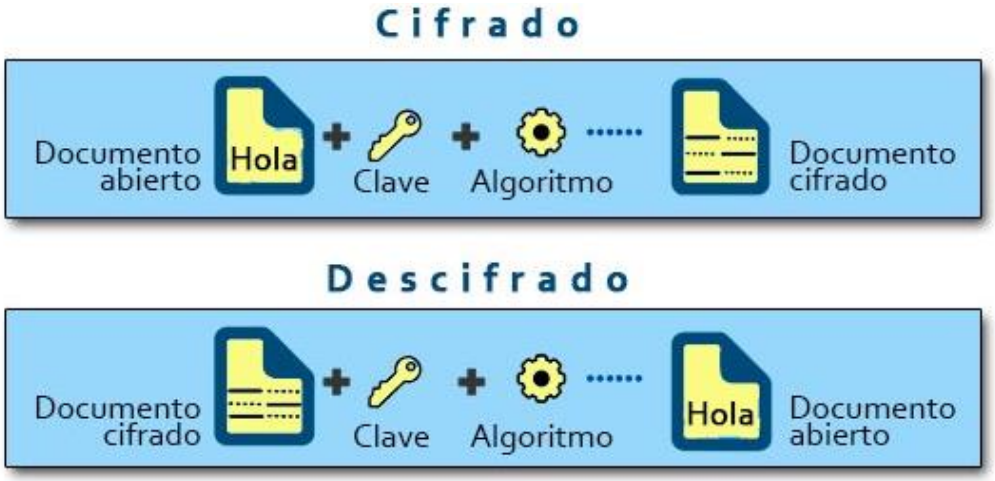


Cifrar

Transformar datos en un formato ilegible para que solo puedan ser leídos por personas autorizadas usando claves de descifrado.

https://www.ibm.com/es-es/think/topics/encryption

https://www.incibe.es/ciudadania/tematicas/cifrado



Datos sensibles

Información que requiere protección especial porque su divulgación puede causar daño, como datos personales, financieros o de salud.

https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_es

https://www.aepd.es/preguntas-frecuentes/0-conceptos-basicos/FAQ-0004-que-son-los-datos-sensibles

https://protecciondatos-lopd.com/empresas/datos-especialmente-protegidos-sensibles/

Diagnóstico de fallos

Proceso de identificar y analizar problemas en sistemas, redes o equipos para encontrar su causa y solucionarlos.

Esquema Nacional de Seguridad (ENS)

Conjunto de normas y medidas de seguridad que deben seguir las administraciones públicas en España para proteger la información y los sistemas.

ISO/IEC 27001

Norma internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI) en una organización.

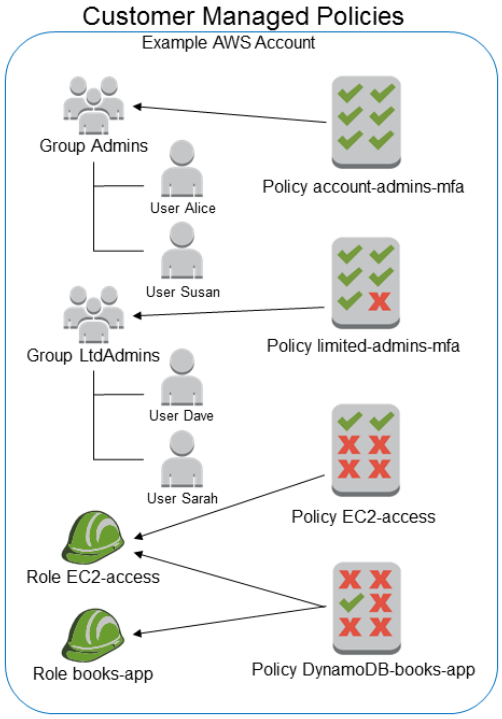
https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/#Centralizar_y_simplificar_la_gestion_de_la_seguridad_de_la_informacion

https://en.wikipedia.org/wiki/ISO/IEC_27001

Políticas de acceso

Conjunto de reglas que definen quién puede acceder a qué recursos, en qué condiciones y con qué nivel de privilegio.

https://www.datasunrise.com/es/centro-de-conocimiento/politica-de-control-de-acceso/



Propuestas de mejora

Sugerencias o acciones planificadas para aumentar la seguridad, eficiencia o rendimiento de los sistemas informáticos.

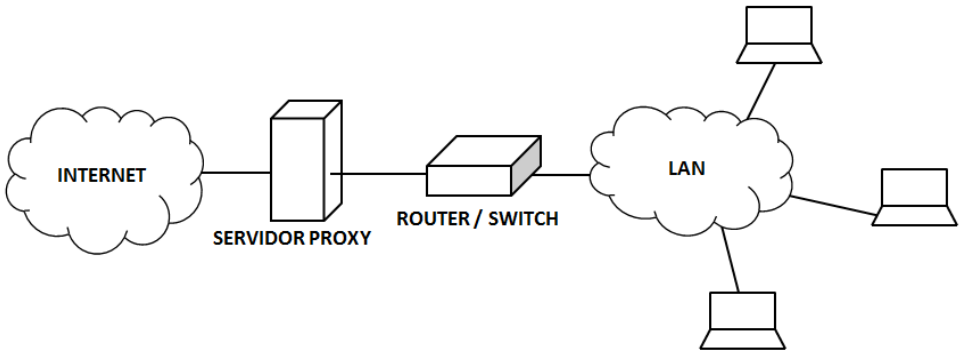
https://www.fundacionbankinter.org/noticias/10-propuestas-para-mejorar-la-seguridad-informatica/

Proxy

Dispositivo o software especializado en mediar la comunicación entre un equipo y otro servidor o Internet. Recibe las solicitudes de un equipo y las envía al destino final, permitiendo controlar el tráfico, filtrar contenido y proteger la identidad del usuario.

https://www.arsys.es/blog/que-es-un-proxy-y-para-que-sirve

https://es.wikipedia.org/wiki/Proxy https://es.wikipedia.org/wiki/Servidor_proxy



Ransomware

Tipo de malware que bloquea o cifra los archivos de un equipo y exige un pago (rescate) para recuperarlos.

https://www.docusign.com/es-mx/blog/desarrolladores/ramsomware

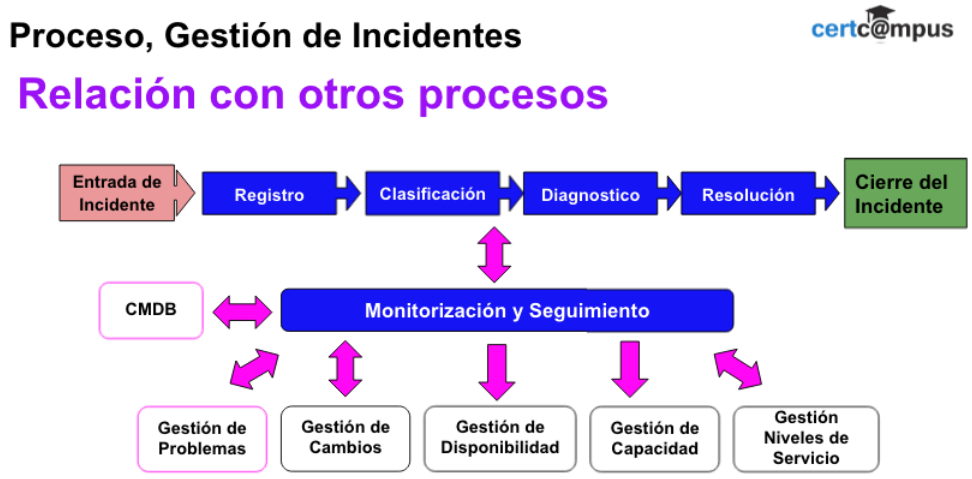
https://www.malwarebytes.com/es/ransomware

Registro de incidencias

Documento o sistema donde se anotan todos los incidentes de seguridad detectados, su causa, impacto y las acciones tomadas para resolverlos.

https://www.easyvista.com/es/blog/que-es-la-gestion-de-incidencias/

https://mesbook.com/control-de-incidencias/



Reglamento General de Protección de Datos (RGPD)

Ley europea que protege los datos personales de los ciudadanos, regulando cómo las organizaciones pueden recopilarlos, usarlos y almacenarlos.

https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm

https://es.wikipedia.org/wiki/Reglamento_General_de_Protección_de_Datos

https://protecciondatos-lopd.com/empresas/rgpd-reglamento-general-proteccion-datos/

https://www.hacienda.gob.es/es-ES/El%20Ministerio/Paginas/DPD/Normativa_PD.aspx

6. Mas recursos interesantes

https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

https://valide.redsara.es/valide/faqs.html

https://firmaelectronica.gob.es/ciudadanos/cosas-deberias-saber/certificados-electronicos

https://www.ccn-cert.cni.es/es/sobre-nosotros/mision-y-objetivos.html

https://www.dsn.gob.es/sites/default/files/documents/Estrategia_Nacional_de_Ciberseguridad2019.pdf

https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

https://es.wikipedia.org/wiki/Seguridad_informática

https://www.bureauveritasformacion.com/boletin/noticias_home/BVF-infografia-ciberseguridad-general

https://www.kaspersky.com/resource-center/preemptive-safety/how-to-prevent-cyberattacks