UNIDAD DE TRABAJO 1. Protección y seguridad informática en la empresa. Concepto de seguridad y autodiagnóstico.

Principios de la ciberseguridad, conceptos básicos, datos de seguridad de la información, mecanismos de seguridad, normas y SGSI, seguridad física y lógica, nuevos entornos, Modelo PDCA, autodiagnóstico.

OBJETIVO: En esta unidad el alumnado conocerá los principales conceptos de ciberseguridad, sus categorías, clasificación, impacto y dimensión dentro del área empresarial. Conocerá e identificará el marco normativo a utilizar durante el presente módulo. Conocerá la importancia de hacer la evaluación de riesgos, así como los principales puntos de la seguridad física y lógica donde deberán aplicarse políticas y procedimientos de prevención. Conocerá los principales riesgos y vectores de ataque realizados por los diferentes actores de la industria del cibercrimen, así mismo será capaz de conocer el nivel de seguridad informática en su organización (Autodiagnóstico), así como la importancia de formar al personal.

Contenido del documento.

Elementos a ser protegidos y mecanismos de seguridad

Antes de exponer los elementos a ser protegidos hay que tener en cuenta varios conceptos, la vulnerabilidad, amenaza y riesgo.

Vulnerabilidad: Debilidad o f**allo de un sistema que puede ser aprovechado con fines maliciosos** (normalmente mediante un programa que se denomina exploit). Cuando se descubre el desarrollador del software o hardware lo solucionará publicando una actualización de seguridad del producto.
Sinónimo: Agujero de seguridad
Vulnerabilidades CVE o Common Vulnerabilities and Exposures
• Estándar desarrollado por la corporación no gubernamental: MITRE
• Incluye las vulnerabilidades que se descubren
• Y dota de una nomenclatura común a las vulnerabilidades.
• Esta información está disponible en la web: https://cve.mitre.org/

Amenaza: Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede **tener causas naturales, ser accidental o intencionada.** Si esta circunstancia desfavorable **acontece a la vez que existe una vulnerabilidad o debilidad** de los sistemas o aprovechando su existencia, puede derivar en un **incidente de seguridad.**

Riesgo: Es la posibilidad de que una **amenaza o vulnerabilidad se convierta en un daño real** para la empresa, que resulte en una pérdida o robo de información o en una detención de su actividad como consecuencia del daño ocasionado. El riesgo puede ser **mitigado mediante políticas de seguridad y continuidad del negocio** que suelen prever posibles ataques y **proponen soluciones** de actuación ante situaciones cuyo riesgo pueda ser elevado.

Es muy importante tener estos conceptos claros debido a que será necesario evaluar los porcentajes de riesgo de los elementos a proteger según su importancia en la empresa y sus posibles vulnerabilidades y amenazas (análisis de riesgos), esto nos **permitirá definir de manera congruente las políticas y mecanismos de protección** para cada uno de ellos sin que sean exagerados o insuficientes.

Seguridad física.

Controles Físicos

La seguridad física es la disciplina que diseña, despliega y mantiene controles de seguridad aplicables al mundo físico con el objeto de proteger diferentes tipos de activos:

- Áreas y espacios.
- Equipamiento.
- Personas.

Si bien las personas son el bien más valioso y el fin último de la seguridad en las organizaciones, generalmente las medidas para proteger a las mismas están incluidas en las otras dos **(especialmente la protección de áreas y espacios).**

Si alguien que desea atacar un sistema tiene acceso físico al mismo, todo el resto de medidas de seguridad implantadas se convierten en inútiles. Muchos ataques son entonces

triviales, **como por ejemplo los de denegación de servicio; si apagamos una máquina** que proporciona un servicio es evidente que nadie podrá utilizarlo.

Otros ataques **se simplifican enormemente**, p. ej. si deseamos obtener datos podemos copiar los ficheros o robar directamente los discos que los contienen. Incluso dependiendo el grado de vulnerabilidad del sistema es posible tomar el control total del mismo, por ejemplo r**einiciándolo con un disco de recuperación que nos permita cambiar las claves de los usuarios.**

Por lo tanto las **principales amenazas para la seguridad física** son: acceso físico (acceso a nuestros dispositivos), integridad física (de nuestro equipo ante golpes, caídas, etc), fugas de información (escribir datos, post it, una libreta expuestas con nuestras notas y credenciales etc).

A continuación se listan los **controles específicos y medidas de prevención** para crear y mantener áreas seguras y mitigar estas amenazas:

- **Perímetro de seguridad física**: Control orientado a proveer protección contra la entrada no autorizada.
    - **Seguridad perimetral**: Los requisitos para la seguridad física deben tener en cuenta los niveles de protección del perímetro de las instalaciones o elementos que contienen la información a proteger con controles como muros, vallas, alarmas, protección de ventanas, cerraduras, etc.
    - **Áreas atendidas**: las áreas restringidas a personal autorizado deberían contar con un área de recepción atendida o medios de control adecuados para limitar el acceso físico.
    - **Barreras:** Si es aplicable deberían considerarse barreras físicas que impidan el acceso no autorizado y protejan el área de agentes ambientales adversos.
    - **Sistemas Anti-incendios:** Contar con sistemas de protección contra el fuego cumpliendo con la legislación vigente.
    - **Detección de intrusión:** Se deben considerar sistemas de detección de intrusos (p ej. Alarmas).
    - **Segmentación de espacios:** Deberían separarse físicamente las áreas de proceso de información que van a ser gestionadas por personal externo de las propias de la organización.
- **Controles de acceso físico:** Aquellas áreas que se consideran seguras deben estar protegidas por controles de entrada que permitan solo personal autorizado incluyendo la asignación, modificación y eliminación de los permisos de acceso, sistemas de entrada como tornos, monitorización de los diferentes punto de entradas (sensores de movimiento, cámaras de vigilancia, etc), registro y análisis de las entradas y salidas (tanto personal interno como externo y visitas) gestión del personal externo, uso de identificadores (como tarjetas), etc. Otras soluciones son: Analizadores de retina, tarjetas inteligentes, videocámaras, vigilantes jurados etc.
- **Seguridad de oficinas, despachos e instalaciones:** Las instalaciones deben diseñarse para evitar al máximo posible el riesgo que la información confidencial sea accesible para los visitantes. Para ello se debe evitar siempre que sea posible que las áreas claves estén en sitios con paso público, evitar carteles y otros signos que aportan demasiada

información sobre el edificio y las áreas internas, que la información y las actividades realizadas en áreas sensibles puedan ser visibles/audibles desde fuera, etc.

- **Protección contra amenazas externas y medioambientales:** Se deben diseñar controles contra desastres naturales, ataques maliciosos y accidentes (como inundaciones, fuego, terremotos, explosiones, ataques terroristas, manifestaciones públicas, etc). Por ejemplo en el caso de terremotos se aconseja:
  - ☐ No situar equipos en sitios altos para evitar caídas,
  - ☐ No colocar elementos móviles sobre los equipos para evitar que caigan sobre ellos,
  - ☐ Separar los equipos de las ventanas para evitar que caigan por ellas o qué objetos lanzados desde el exterior los dañen,
  - ☐ Utilizar fijaciones para elementos críticos,
  - ☐ Colocar los equipos sobre plataformas de goma para que esta absorba las vibraciones.

Otro desastre natural importante son las **tormentas con aparato eléctrico**, especialmente frecuentes en verano, que generan subidas súbitas de tensión muy superiores a las que pueda generar un problema en la red eléctrica. A parte de la protección mediante el uso de **pararrayos, la única solución a este tipo de problemas es desconectar los equipos** antes de una tormenta (qué por fortuna suelen ser fácilmente predecibles).

En entornos normales es recomendable que haya un cierto grado de **humedad**, ya que en si el ambiente es extremadamente seco hay mucha electricidad estática. No obstante, tampoco interesa tener un nivel de humedad demasiado elevado, ya que puede producirse condensación en los circuitos integrados que den origen a un cortocircuito. En general no es necesario emplear ningún tipo de aparato para controlar la humedad, pero no está de más **disponer de alarmas que nos avisen cuando haya niveles anómalos.**

Otro tema distinto son las inundaciones, ya que casi cualquier medio (máquinas, cintas, routers ...) que entre en contacto con el agua queda automáticamente inutilizado, bien por el propio líquido o bien por los cortocircuitos que genera en los sistemas electrónicos. Contra ellas podemos **instalar sistemas de detección que apaguen los sistemas si se detecta agua y corten la corriente en cuanto estén apagados.** Hay que indicar que los equipos deben estar por encima del sistema de detección de agua, sino cuando se intente parar ya estará mojado.

Por último mencionaremos el **fuego** y los humos, que en general provendrán del incendio de equipos por sobrecarga eléctrica. Contra ellos emplearemos **sistemas de extinción, que aunque pueden dañar los equipos que apaguemos (aunque actualmente son más o menos inocuos),** nos evitarán males mayores. Además del fuego, también el humo es perjudicial para los equipos (incluso el del **tabaco**), al ser un abrasivo que ataca a todos los componentes, por lo que es recomendable **mantenerlo lo más alejado posible de los equipos.**

- **Trabajo en áreas seguras:** Se deben diseñar e implementar procesos para el trabajo en áreas seguras, teniendo en cuenta aspectos como que el personal sólo debería saber de

la existencia de, y los trabajos realizados en, áreas seguras según el criterio de necesidad de saber, evitar el trabajo no supervisado en áreas seguras, las áreas seguras vacías deberían quedar cerradas y protegidas o evitar cualquier tipo de grabación en estas áreas.

- **Áreas de entrega y carga:** Los puntos de carga y de entrega de mercancía suelen ser puntos sensibles para la seguridad física por lo se debería tomar en cuenta algunos aspectos como horarios definidos de apertura y cierre, control de apertura y cierre de puertas externas e internas, control de personal, realización de inventarios de materiales entregados, revisión de mercancías entregadas para detectar materiales peligrosos o separar entregas entrantes y salientes o barreras adicionales de seguridad.

Así mismo, es primordial asegurar que se proteja el equipamiento:

- **Ubicación y protección del equipamiento:** Se debe proteger el equipamiento de la organización dado que en el mismos e realiza el procesamiento y/o almacenamiento de la información, teniendo en cuenta controles como:
    - Colocación del equipamiento para minimizar el acceso innecesario a las áreas de trabajo.
    - Colocación de las áreas de procesamiento de información donde se gestione información sensible de forma que se minimice el riesgo de escuchas o vistas de dicha información.
    - Las instalaciones de almacenamiento estarán protegidas contra acceso indebido.
    - Los ítems que requieran de un mayor nivel de protección deberán ser protegidos especialmente y en áreas específicas para reducir el nivel general de protección necesario.
    - Se deben implantar controles para evitar daños al equipamiento como fuego, humo, sobrecargas eléctricas, agua, polvo, químicos, etc.
    - Se deben crear y mantener guías para comer, beber y fumar cerca del equipamiento para evitar su daño.
    - Se deben monitorizar las condiciones ambientales como humedad y temperatura para asegurar que están dentro de los límites seguros para el equipamiento.Para controlar la temperatura emplearemos aparatos de aire acondicionado.
    - Se debe aplicar protección contra electricidad en los edificios y desplegar filtros de protección de electricidad en todas las líneas eléctricas y de comunicaciones.
    - El equipamiento que maneje información sensible deberá estar protegido contra fugas electromagnéticas o ruido eléctrico intentando no situarlo cerca de elementos que puedan causar esta pérdida. En caso de que fuese necesario podemos instalar filtros o apantallar las cajas de los equipos.
- **Elementos de soporte:** El equipamiento será protegido contra fallos en el suministro eléctrico y otras disrupciones causadas por los elementos de soporte (electricidad, comunicaciones, agua, gas, alcantarillado, etc). Para los cortes podemos emplear *Sistemas de Alimentación Ininterrumpida* (SAI), que además de proteger ante cortes eléctricos mantienen el flujo de corriente constante, evitando las subidas y bajadas de tensión. Estos equipos disponen de baterías que permiten mantener varios minutos los

aparatos conectados a ellos, permitiendo que los sistemas se apaguen de forma ordenada (generalmente disponen de algún mecanismo para comunicarse con los servidores y avisar de que ha caído la línea o de que se ha restaurado después de una caída).

Por último indicar que además de los problemas del sistema eléctrico también debemos preocuparnos de la corriente estática, que puede dañar los equipos. Para evitar problemas se pueden emplear sprays antiestáticos o ionizadores y tener cuidado de no tocar componentes metálicos, evitar que el ambiente esté excesivamente seco, etc.

- **Seguridad en el cableado:** Todo el cableado de comunicaciones y suministro de electricidad será protegido contra intercepción, interferencias o daño. Se deberán tener en cuenta como el enterramiento o protección adecuada de los cables, segregación de cables de comunicación y electricidad para evitar interferencias y para cableado de sistemas críticos aspectos como el uso de conductos blindados y puntos de acceso protegidos, uso de apantallado electromagnético, acceso controlado a las salas de cableado o paneles de acceso, etc.
- **Mantenimiento del equipamiento:** El equipamiento deberá ser mantenido siguiendo todas las indicaciones de los fabricantes con el fin de optimizar su vida útil y evitar fallos en la integridad y disponibilidad de la información.
- **Retirada de bienes:** El equipamiento, información y software no será retirado sin la correspondiente autorización y asegurando que quede un registro de la salida y entrada de los mismos.
- **Seguridad del equipamiento y de los activos fuera de las instalaciones:** Se deben proteger los activos fuera de la organización tomando en cuenta los diferentes riesgos externos, teniendo en cuenta aspectos como dejar ningún equipamiento desatendido, tener elementos específicos de protección como cables y candados, etc.
- **Seguridad en la reutilización o eliminación de equipos:** Todos los equipos que contengan medios de almacenamiento deberán ser verificados para asegurar que todos los datos sensibles y el software licenciado han sido eliminados sobrescritos de forma segura antes de su eliminación o reutilización (puede ser tanto destrucción física como cifrado, reescritura segura, uso de medios de desmagnetizado, etc).
- **Equipamiento desatendido por el usuario:** Los usuarios no deben dejar las sesiones abiertas mientras el equipo no esté atendido. Además de los procedimientos de bloqueo de pantalla, la sesión de la aplicación y de la red debe cerrarse cuando las conexiones no se utilizan. Esto debería aplicarse tanto a los dispositivos móviles como a los equipos fijos.

No hay que descuidar a las **personas** que integran la organización, si no se controla el acceso a las instalaciones, nunca se podrá hablar de estar en una situación adecuada de seguridad. En estos días, todo el mundo está cada vez más ocupado y las listas de tareas pendientes son cada vez más largas. Parece que nunca hay suficiente tiempo en el día y es fácil distraerse cuando hay poco tiempo. Lo hemos escuchado todo antes, la seguridad siempre debe estar en la parte superior de su lista de tareas pendientes, pero sabemos que no siempre es así.

El eslabón más débil e importante de cualquier sistema de seguridad es siempre el mismo: las personas. No importa cuán completas, efectivas o costosas sean las herramientas de seguridad, todas pueden colapsar si un solo usuario descuidado comete un simple error.

Independientemente de la comprensión que tengan los usuarios de los principios básicos de seguridad de los datos como elegir contraseñas seguras o no abrir archivos adjuntos de correos electrónicos desconocidos.

Cada vez que alguien decide hacer clic en un enlace desconocido o abrir un archivo adjunto de correo electrónico sospechoso, una organización podría estar enfrentando una pérdida masiva de datos y una interrupción significativa en su negocio.

A **nivel personal,** es imprescindible cumplir con las **siguientes orientaciones como medidas de prevención** para conseguir un índice mínimo de seguridad en el tratamiento de los datos:

1. Se debe tener en cuenta que un objetivo vulnerable es un objetivo atractivo para los atacantes y que le puede pasar a cualquiera, en cualquier momento, en **cualquier lugar y en cualquier dispositivo.**
2. Se ha de practicar una buena gestión de contraseñas, utilizando una combinación sólida de caracteres y sin utilizar la misma contraseña para varios sitios. Es necesario no compartir las contraseñas personales con otras **personas y evitar escribirlas**. Por supuesto, no hay que escribirlas en una nota adhesiva pegada en el monitor. Si se tiene problemas para recordar las contraseñas, la utilización de un gestor de contraseñas solvente, como Keepass es una buena alternativa, teniendo que recordar una única contraseña (muy segura).
3. Nunca se debe dejar los **dispositivos desatendidos.** Si se necesita dejar el ordenador, teléfono o tablet durante un determinado período de tiempo, sin importar cuán corto sea, se ha de bloquear la pantalla para que nadie pueda usarla.
4. Si se guarda información confidencial en una unidad de almacenamiento USB, tendrá que ser bloqueada también. Para facilitar dicho bloqueo, existen programas como BitLocker (para Windows 10) o Dislocker (para Linux o macOS), que proveen funcionalidades para el cifrado de unidades de almacenamiento y proteger los datos contenidos mediante una contraseña.
5. Se deberá tener cuidado al hacer **clic en archivos adjuntos o enlaces en un correo** electrónico. Si un correo electrónico es inesperado o sospechoso por algún motivo, la acción recomendable es no abrirlo. Los estafadores pueden buscar esa información en línea y utilizarla para dirigirse a las personas de su empresa. Una a**ctuación recomendada es la verificación de la URL del sitio web** de origen para ver si parece legítimo.
6. Para minimizar el riesgo de filtración de información sensible (correo electrónico) al agente equivocado, en el caso de tener que enviar un correo electrónico a un grupo numeroso de colaboradores, se puede **optar por incluir a todos los destinatarios en la sección de copia oculta (CCO).** De esta forma, ningún destinatario conocerá el email del resto.

7. La navegación sensible, como la banca o las compras, solo debe realizarse en un **dispositivo que le pertenezca, en una red en la que se confíe.** La utilización del teléfono de un amigo, una computadora pública o la Wi-Fi gratis en una cafetería son vectores de exposición perfectos para el robo o copia de nuestros datos.
8. **Realizar copias de seguridad** de sus datos con regularidad.
9. El software antivirus tendrá que estar **siempre encendido y actualizado.**
10. Se tiene que ser consciente de **lo que se conecta al equipo.** El malware se puede propagar a través de unidades USB infectadas, discos duros externos e incluso teléfonos inteligentes.
11. Los delincuentes pueden extraer una **cantidad asombrosa de información de todo aquello compartido en las redes sociales** como cuál es nuestro lugar de estudio o trabajo, cuando estamos de vacaciones... que podría ayudarles a obtener acceso a nuestros datos o incluso a nuestra casa.
12. Tener cuidado con la **ingeniería social,** donde alguien intenta obtener información de la persona objetivo mediante la manipulación. Si alguien llama o envía un correo electrónico pidiendo información confidencial, como información de inicio de sesión o contraseñas, se puede decir que no. **Siempre puede llamar a la empresa directamente** para verificar las credenciales antes de dar cualquier información.
13. **Controlar nuestras cuentas** para detectar cualquier actividad sospechosa. Si se ve algo inusual, podría ser una señal de que se ha visto comprometida nuestra seguridad. Ante dicha situación, lo ideal es informar al responsable de la seguridad informática en nuestra empresa.

Compartir la presente lista con quien estime oportuno, **la ciberseguridad es un "deporte de equipo",** si un compañero o colaborador son vulnerables a un ataque todo el hogar u organización es vulnerable al mismo ataque.

Tampoco se ha de descuidar el mantenimiento regular y los controles ambientales apropiados para los equipos y las instalaciones físicas, **como limpieza, reparación o refrigeración, para asegurar la continuidad de las operaciones.** Por ejemplo, en zonas donde exista una posibilidad real de situaciones climatológicas o ambientales catastróficas (tornados, monzones, terremotos), es adecuado plantearse deslocalizar recursos o la información mediante aplicaciones e información alojada en la nube, cuyos servidores podrán estar situados incluso en otro continente.

El apoyo normativo a la seguridad física

Todas las normativas y guías de buenas prácticas de seguridad en ICS recogen, de alguna manera, los requerimientos de seguridad física. Las más representativas podrían ser:

- El estándar internacional IEC 62443-2-1 '*Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program*'. Punto 4.3.3.
- NERC CIP-005-5 '*Cyber Security - Electronic Security Perimeter(s)*'.
- NERC CIP-014-2 '*Physical Security*'.

Otra que no es específica del entorno industrial, pero que podría considerarse referente a la hora de implementar controles de seguridad tanto a nivel físico como especialmente al lógico es:

- ISO/IEC 27001:2013 '*Information technology -- Security techniques -- Information security management systems – Requirements*'. Puntos A.11.1, A.11.2, A.11.4.

https://www.incibe-cert.es/blog/el-punto-el-seguridad-y-ciberseguridad-convergen

Seguridad lógica.

Además proteger el *hardware* nuestra política de seguridad debe incluir medidas de protección de los datos, ya que en realidad la mayoría de ataques tienen como objetivo la obtención de información, no la destrucción del medio físico que la contiene.

Dentro de la seguridad lógica podemos abarcar muchos aspectos según los activos presentes en la empresa, no obstante atenderemos primero al nexo de unión entre las personas y la tecnología, los procesos. Las organizaciones deben tener un **marco de actuación para gestionar tanto los ataques cibernéticos** intentados como los exitosos.

Un proceso explicará **cómo identificar ataques, proteger sistemas, detectar y responder** a amenazas y recuperarse de ataques exitosos.

La empresa o entidad deberá saber cuales **son los riesgos**, especialmente aquellos con severidad crítica, y poder tomar las medidas adecuadas para manejarlos.

La **anticipación** a potenciales amenazas mediante la investigación y planificación de medidas de mitigación y contingencia específicas, permiten una adecuada y pronta respuesta ante dichos posibles incidentes. Es decir, **siempre hay que procurar evitar llegar al punto de tener que ejecutar medidas de contingencia,** por ello, hay que realizar un esfuerzo continuado en la prevención de amenazas, lo cual, siempre redundará un ahorro de recursos, tiempo y dinero. Identificaremos los puntos más importantes de la **seguridad lógica,** siempre adaptándolas al tipo y operación de la empresa a proteger.

- ☐ Gestión de identidades y Control de Acceso
- ☐ Requisitos del negocio para el Control de Acceso
- ☐ Gestión del acceso de usuarios y Responsabilidad de usuarios
- ☐ Control de Acceso a sistemas y aplicaciones
- ☐ Protección de la información y Criptografía
- ☐ Copias de seguridad, seguridad en el correo y monitorización
- ☐ Seguridad en el punto final
- ☐ Seguridad en red
- ☐ Gestión de incidentes

- Gestión de la identidad y el control de acceso

La gestión de identidades y accesos, es un término genérico para los procesos internos de una organización que se enfocan en administrar cuentas de usuario y recursos de red corporativa, incluidos los derechos de acceso para las organizaciones, usuarios, aplicaciones y sistemas.

Junto a estos procesos, podemos encontrar una disciplina dentro del software que busca crear productos para automatizar estos procesos y hacerlos más efectivos y homogéneos.

Terminología de Gestión de Identidades y Control de Accesos:

- Gestión de accesos: El proceso de **configurar el nivel de acceso** para cada usuario y grupo dentro de un sistema. A través de este proceso, los administradores, conceden acceso a usuarios autorizados y restringen el acceso a los usuarios no autorizados. Esto se puede realizar de forma jerárquica a través del uso de grupos de usuarios. La gestión de accesos requiere de **auditoría periódica y mantenimiento** para mantenerse al día con el negocio en continua evolución y los roles de los empleados.
- Necesidad de saber / Menor privilegio: Se trata de dos principios que regulan las buenas prácticas de la gestión de accesos y la provisión de permisos. El primero regula que los usuarios sólo deberían tener acceso a aquella información que sea imprescindible para realizar su trabajo y a nada más. El segundo dice que los usuarios deberían tener los privilegios mínimos que les permitan realizar su trabajo.
- Aprovisionamiento / Desaprovisionamiento: El primero es el proceso de establecer una identidad y su acceso asociado en un sistema. El segundo es el proceso de eliminar dicho acceso y las identidades asociadas cuando un usuario se va, es despedido, cambia de área o puesto (y por tanto requiere de nuevos accesos y permisos) o su contrato finaliza.
- Identificación, autenticación y autorización: Estos términos son la **triada del control de acceso,** mostrando el flujo en el que un usuario accede a un sistema. La identificación es el proceso por el que un usuario establece cual es su identidad. La autenticación es el proceso por el cual el sistema verifica de alguna manera que el usuario tiene realmente la identidad proclamada (que nadie le está usurpando). Y por fin, la autorización, es una vez identificado y autenticado al usuario, el sistema comprueba los permisos de acceso que tiene a dicho sistema.
- Factores de Autenticación / 2FA / MFA: Existen diferentes esquemas de autenticación de usuarios, basados en la propiedad del factor utilizado para verificar la identidad. El primero es **“algo que sabes”,** basado generalmente en el uso de un usuario y contraseña. El Segundo factor es **“algo que eres”** o autenticación biométrica, en el que el Sistema comprueba alguna característica física del usuario como su huella digital, el iris, la palma de la mano, su huella de voz, etc. Finalmente **“algo que tienes”,** en el cual la autenticación se basa en la posesión de un objeto como una smartcard, token que genera contraseñas aleatorias de forma temporal o smartphone al que llegan contraseñas temporales. Para mejorar la seguridad del acceso, se recomienda, al menos para sistemas críticos, el uso de más de un factor de autenticación (2FA o doble factor de autenticación o MFA o multifactor de autenticación).

- Acceso basado en roles (RBAC): Se trata de un paradigma de gestión del acceso y el privilegio en el cual se definen roles empresariales de acceso a los cuales se les conceden acceso a diferentes sistemas (cada uno de ellos con un conjunto de permisos). Así, a **cada usuario, de acuerdo a su puesto de trabajo se le asignan uno o más roles**. Este modelo es el más utilizado actualmente, si bien existen otros modelos como el Control de Acceso discrecional o DAC (método de restricción de acceso a objetos que se basa en la identidad de los sujetos que pretenden operar o acceder sobre ellos, es decir, se concede a cada individuo un conjunto de permisos personalizado) y el Control de Acceso Obligatorio o **MAC (Este mecanismo de acceso es complementario y añade una capa adicional. Se basa en un "etiquetado"** de todo elemento del sistema y sobre las cuales se aplicarán las políticas de control de acceso configuradas. Así, cualquier operación de un sujeto sobre un objeto será **comprobado las etiquetas y aplicando las políticas MAC establecidas** para determinar si la operación está permitida, aún incluso cuando se hayan cumplido otros controles de seguridad. Este sistema viene de sistemas militares y aún se aplica a sistemas gubernamentales, de inteligencia, etc).
- Flujos de trabajo Altas, Bajas y Modificaciones: Cada vez que se quiere aprovisionar (alta), desaprovisionar (baja) o modificar los permisos o rol de un usuario, se debe contar con un **flujo de trabajo en el que los roles involucrados y los pasos a dar estén claramente definidos.** Quién puede solicitarlo, quién/es debe/n aprobarlo, quién lo audita/monitoriza, etc.
- Inicio de Sesión Único (SSO): Se trata de un mecanismo de control de acceso que permite que un usuario se autentique una vez ante un sistema maestro y éste gestione sus credenciales contra otros sistemas de forma que no sea necesario volverse a autenticar **(generalmente durante un periodo definido o bien hasta el cierre de sesión)**.
- Contraseña de un solo uso (OTP): Mecanismo de acceso basado en una contraseña es válida una sola vez. Esto puede ser mediante **sistemas que generan contraseñas de forma aleatoria y regular en el tiempo (cliente y servidor la misma contraseña)** o bien mediante el envío de la contraseña a un **dispositivo de usuario como teléfono** (bien por SMS o más seguro, disponiendo de una aplicación desplegada).

● Requisitos del negocio para el control de accesos

- Política de control de acceso: Una política de control de acceso debe ser e**stablecida, documentada y revisada** basada en los **requisitos de seguridad del negocio** y de la información. Los **propietarios de los activos** deberán determinar las **reglas de control de acceso apropiadas, los derechos de acceso y restricciones** para determinados roles de usuarios, con el **nivel de detalle y de dureza** de los controles que reflejen los riesgos de seguridad asociados. Los controles de acceso pueden ser tanto **físicos como lógicos y se deberían considerar en conjunto**. Tanto a los usuarios como a los proveedores de servicios se les debería dar una declaración clara de los requisitos de negocio que los controles deben alcanzar. La política debería tener en cuenta los siguientes aspectos:

- ➢ **Requisitos de seguridad** para las aplicaciones de negocio.
- ➢ **Políticas** para la diseminación de la información y autorización (p.e la necesidad de saber los niveles de seguridad y clasificación de la información).
- ➢ La consistencia entre los **derechos de acceso y las políticas** de clasificación de la información de sistemas y redes.
- ➢ La legislación **relevante y cualquier obligación contractual** respecto de la limitación de acceso a datos o servicios.
- ➢ La **gestión de derechos de acceso** en un entorno distribuido y en red que reconozca todos los tipos de conexiones existentes.
- ➢ **Segregación de los roles** de control de acceso (p.e petición de acceso, autorización, administración del acceso, etc).
- ➢ **Requisitos para la autorización forma**l de las peticiones de acceso.
- ➢ **Requisitos para la revisión periódica** de los derechos de acceso.
- ➢ **Eliminación** de los derechos de acceso.
- ➢ Archivado de los **registros de todos los eventos** significativos relacionados con el uso y gestión de las identidades de usuario y la información secreta de autenticación.
- ➢ Roles con **acceso privilegiado.**

❖ Acceso a las redes y a los servicios de red: Se trata de un **requisito para gestionar la autorización de los usuarios que acceden a los recursos de red**. Para ello se exige como requisito elaborar una **política específica para el uso de los recursos de red.** Aunque este está cubierto en gran parte por el anterior, la política de "gestión de acceso de usuarios de red" debe **determinar a qué información** se puede acceder, los procedimientos de autorización, los controles de gestión para la protección de las redes, las conexiones de red permitidas (p. Ej., No mediante wifi), los requisitos de autenticación y la supervisión del uso. La política debe identificar:

- ➢ La red y servicios a los cuales se accede.
- ➢ Los procedimientos de autorización.
- ➢ Los controles que tienen estos procedimientos.
- ➢ Los medios por los cuales se accede (VPN, Wifi etc.).
- ➢ Los requisitos de autenticación.
- ➢ Como se supervisa (monitorización) el uso de los servicios de red.

● Gestión del acceso de usuarios

❖ Registro de usuarios y cancelación del registro: Se trata de un control para el **alta y baja de los usuarios**. Este control exige establecer un proceso de altas y bajas que permite los derechos de acceso teniendo en cuenta:

- ➢ Un registro de IDs o cuentas de usuario donde se vincula o **identifica** al usuario.
- ➢ Los IDs deben **desactivarse automáticamente** o de forma inmediata cuando el usuario abandona la organización.
- ➢ **Eliminación** periódica de usuarios **redundantes**.
- ➢ Los IDs redundantes **nunca pueden ser asignados** a otros usuarios.

- ➢ El proceso de cancelación debería tener en cuenta:
  - La revocación del ID del usuario.
  - La revocación de los permisos del ID de usuario.

❖ Gestión de acceso a los usuarios: Se debe establecer un proceso formal para asignar y revocar los accesos a sistemas y servicios que:

- ➢ Incluya la **aprobación del propietario del servicio o sistema.**
- ➢ Verifique si el acceso cumple con las **políticas de acceso** definidas.
- ➢ **Se garantice que el acceso** no se da hasta finalizar el **proceso de autorización**.
- ➢ Asegure que se mantiene un **registro de los accesos concedidos**.
- ➢ Asegure que se **eliminen los accesos** de usuarios que han abandonado la organización.
- ➢ Asegure que se m**odifican los accesos de usuarios** que han cambiado de función o puesto de trabajo si procede.
- ➢ Asegure que se **revisen periódicamente los derechos** de acceso.

❖ Gestión de derechos de acceso privilegiados: El control de los derechos de acceso privilegiados debe realizarse de forma independiente mediante un proceso específico que:

- ➢ Tenga en cuenta las **políticas de acceso privilegiado** definidas.
- ➢ Se identifican **accesos privilegiados de cada sistema o proceso**.
- ➢ Se tengan en cuenta las reglas generales de **mínimos privilegios.**
- ➢ Se establezca una **norma de caducidad** de los permisos privilegiados.
- ➢ Se definen **IDs especiales o distintos** para las cuentas de uso normales o no privilegiadas.
- ➢ Se definan procedimientos para **evitar el uso no autorizado** de cuentas con derechos de acceso privilegiados.
- ➢ Se verifican periódicamente las **competencias de los usuarios.**
- ➢ Considere mecanismos para mantener la **confidencialidad** de los datos de acceso de usuarios genéricos para los usuarios privilegiados o **mecanismos** para forzar el cambio de contraseñas cuando un usuario privilegiado abandona o cambia de puesto de trabajo.

❖ Gestión de la información de autenticación secreta de los usuarios: Control para garantizar que se mantiene la confidencialidad de la información secreta de acceso (p. ejemplo contraseñas, tokens, smartcards, etc). Gestionar la información de autenticación supone controlar:

- ➢ Incluir **cláusulas en contratos y condiciones de puesto de trabajo** sobre el mantenimiento del secreto de las contraseñas o información de autenticación.
- ➢ **Obligación de cambiar contraseñas iniciales** después de su primer uso.
- ➢ **Identificar** al **usuario** antes de entregar las contraseñas y **obtener acuse de recibo.**
- ➢ Uso de contraseñas seguras, **no compartidas.**
- ➢ Uso de **medios seguros de comunicación** (Correos cifrados etc.).
- ➢ **Cambiar contraseñas a personal externo** después de que han realizado sus trabajos (instalaciones de software etc.).

- Revisión de derechos de acceso de usuario: Control para establecer una revisión periódica de los permisos de accesos de los usuarios que tenga en cuenta aspectos como:
  - **Revisar derechos de acceso** a la terminación de empleo o cambios en la organización (cambios de empleo o promociones).
  - **Limitar en el tiempo los derechos de acceso con privilegios** especiales.
  - **Revisar las cuentas con privilegios especiales** periódicamente y registrar los cambios que se realicen.
- **Eliminación o ajuste** de los derechos de acceso: Control para garantizar que se modifican los derechos de acceso al finalizar el empleo o cambiar de puesto de trabajo dentro de la organización.
- **Responsabilidades** del usuario:
- Uso de la información de autenticación secreta: Cada organización debe establecer **normas para la utilización de contraseñas** teniendo en cuenta aspectos como:
  - Asegurar que las contraseñas no se divulguen.
  - Evitar el uso de registros de contraseñas (papel, archivos etc.).
  - Políticas para cambiar las contraseñas ante amenazas.
  - Políticas para la calidad de las contraseñas, teniendo en cuenta aspectos como:
    - Tamaño (Menos de 10 caracteres se consideran triviales hoy en día, y eso si se cumplen las reglas de complejidad).
    - Complejidad (regla 3 de 4, utilizar al menos un carácter de tres grupos de entre 4 posibles, minúsculas, mayúsculas, numéricos y caracteres especiales como @¿?.
    - Validez temporal (cambiarla cada cuánto tiempo).
    - Se deberán tener criterios más o menos estrictos dependiendo de si la cuenta es de usuario normal, servicio, privilegiada, compartida, etc.
  - Evitar el almacenamiento de contraseñas de forma insegura.
  - Forzar cambios de contraseñas iniciales.
  - Evitar compartir contraseñas para distintos usos.

Control de acceso a sistemas y aplicaciones

- Restricción de acceso a la información: Las funciones de una aplicación o sistema deben considerar las restricciones de control de acceso determinadas por la **política de control definida**. Se deben tener en cuenta aspectos como:
  - Utilizar menús para controlar el acceso a las distintas funciones.
  - Ocultar las funciones de administración a los usuarios habituales.
  - Determinar los datos accesibles, determinando los datos que pueden estar disponibles para cada ID de usuario.
  - Restringir de forma selectiva derechos de lectura / escritura / eliminación / ejecución etc.
  - Limitar el tipo de información de salida.

- ➢ Considerar accesos físicos o lógicos adicionales para sistemas o información altamente clasificados.

❖ Procedimientos de conexión (log-on) seguros: Donde se requiera por la política de control de accesos, el acceso a los sistemas y aplicaciones debería estar controlado por un proceso de **acceso (log-on)** seguro. El nivel de rigor para establecer la identidad del usuario dependerá de la criticidad del sistema y la información gestionada. Puede ser desde **1 factor de autenticación a un doble factor con usuario y contraseña y una smartcard o aplicación en el móvil.** El método de acceso debe mostrar la información mínima sobre el sistema o aplicación para evitar ofrecer a un usuario no autorizado información que podría ayudar en un ataque. En general se deben tener en cuenta **aspectos como no mostrar identificadores hasta haber pasado el proceso exitósamente, no mostrar mensajes de ayuda, validar la información sólo cuando esta esté completa, y en caso de error, no mostrar donde ocurrió este, proteger contra intentos de fuerza bruta, generar eventos de los intentos exitosos y fallidos de acceso, no mostrar las contraseñas en claro ni enviarlas sin cifrar por la red, etc.**

❖ Sistema de gestión de contraseñas: Se debe automatizar en los sistemas y aplicaciones, cuando esto sea técnicamente posible, la seguridad de las contraseñas, filtrando aquellas que no cumplan los requisitos establecidos. Un sistema así debe tener en cuenta aspectos como:

- ➢ Reforzar el uso de IDs individuales así como contraseñas para mantener la responsabilidad individual (accountability).
- ➢ Permitir a los usuarios seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación para permitir errores de entrada.
- ➢ Reforzar la selección de contraseñas de calidad.
- ➢ Forzar a los usuarios a cambiar sus contraseñas cuando entren por primera vez.
- ➢ Forzar el cambio regular de contraseñas y cuando sea necesario (p.e sospecha de intrusión en la cuenta).
- ➢ Mantener un registro de las contraseñas utilizadas y prevenir su reuso.
- ➢ No mostrar contraseñas en la pantalla mientras se entra.
- ➢ Almacenar los ficheros de contraseñas separados de los datos de la aplicación.
- ➢ Almacenar y transmitir las contraseñas de forma protegida (p.e cifradas).

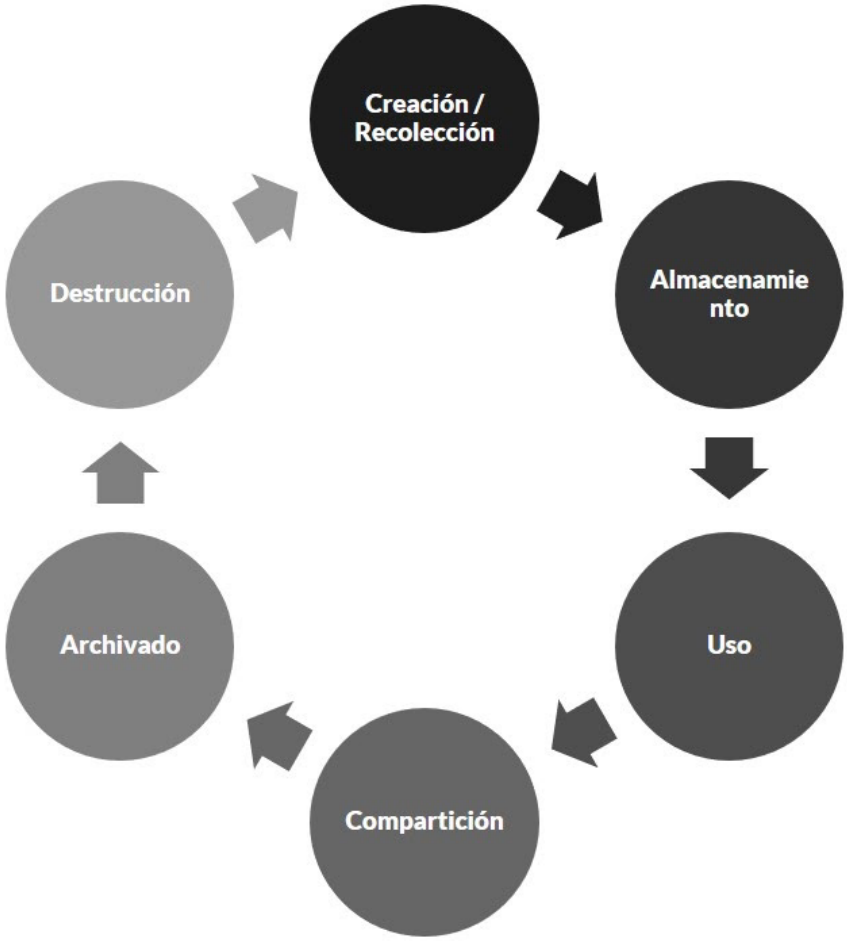
❖ Uso de programas de utilidad privilegiados: Aquellos programas con capacidades de anulación del sistema o sus controles deben ser restringidos y supervisados de manera especial. Los programas con funciones privilegiadas deberían requerir autenticación por separado y estar segregados de las aplicaciones del sistema. Todas las actividades realizadas deben registrarse. Se debe considerar nuevamente la segregación de funciones cuando sea posible.

❖ Control de acceso al código fuente de programas: El acceso al código fuente y elementos asociados (como diagramas, diseños, especificaciones, etc) deberá ser estrictamente controlado para evitar cambios no controlados y el acceso a partes sensibles que podrían dar a un potencial atacante una ventaja.

- Protección de la información y criptografía.

La protección de la información es el proceso de **salvaguardar la información importante para una organización contra corrupción, compromiso o pérdida.** La importancia de esta disciplina es cada vez mayor, toda vez que cada vez se genera más información en las organizaciones, la tolerancia a la indisponibilidad de la misma.

Para la protección de la misma se debe tener en cuenta su ciclo de vida y los posibles estados dentro de la misma en que los datos se pueden encontrar:



El ciclo de vida de los datos sigue los siguientes pasos:

- En la creación y recolección de información es cuando la información es creada o bien se transforma mediante su modificación y/o añadido de nuevos registros.
- En la fase de almacenamiento la información es cuando la información se guarda en reposo en espera de su uso.
- En el uso la información es consumida, aunque no modificada. Este segundo caso conllevaría la vuelta a la fase de creación o recolección.
- Compartición. La información se hace disponible para otras personas, mediante su envío por email, creación de nuevos usuarios en un sistema, etc.
- Archivado: Almacenamiento a largo plazo de la información con el objeto de dar cumplimiento a obligaciones legales, requisitos internos, etc.

- Eliminación completa de la información cuando ya no es necesaria.

Este ciclo no se basa en pasos secuenciales, sino que cada paso puede llevar a otros, dado que desde su uso se puede pasar a creación y de ahí a almacenamiento y de ahí a compartición, por ejemplo.

Principios de criptografía

La criptografía es un conjunto de técnicas, que originalmente tratan sobre la protección o el ocultamiento de la información frente a observadores no autorizados. A través de la criptografía la información puede ser protegida contra el acceso no autorizado, su interceptación, su modificación y la inserción de información extra.

- Funciones dentro de la seguridad: Con la criptografía se intenta garantizar las siguientes propiedades deseables en la comunicación de información de forma segura (a estas propiedades se las conoce como funciones o servicios de seguridad):
  - Confidencialidad: solamente los usuarios autorizados tienen acceso a la información.
  - Integridad de la información: garantía ofrecida a los usuarios de que la información original no será alterada, ni intencional ni accidentalmente.
  - Autenticación de usuario: es un proceso que permite al sistema verificar si el usuario que pretende acceder o hacer uso del sistema es quien dice ser.
  - Autenticación de remitente: es el proceso que permite a un usuario certificar que el mensaje recibido fue de hecho enviado por el remitente y no por un suplantador.
  - Autenticación del destinatario: es el proceso que permite garantizar la identidad del usuario destinatario.
  - No repudio en origen: que cuando se reciba un mensaje, el remitente no pueda negar haber enviado dicho mensaje.
  - No repudio en destino: que cuando se envía un mensaje, el destinatario no pueda negar haberlo recibido cuando le llegue.
  - Autenticación de actualidad (no replay): consiste en probar que el mensaje es actual, y que no se trata de un mensaje antiguo reenviado.
- Criptosistemas de clave pública y privada: Existen dos tipos fundamentales de criptosistemas o sistemas de cifrado:
  - Criptosistemas simétricos o de clave privada. Son aquellos que emplean una misma clave k tanto para cifrar como para descifrar. Presentan el inconveniente de que para ser empleados en comunicaciones la clave k debe estar en posesión tanto en el emisor como en el receptor, lo cual nos lleva a preguntarnos cómo transmitirles a los participantes en la comunicación esa clave de forma segura.
  - Criptosistemas asimétricos o de clave pública, que emplean una doble clave (kp,kP). kp se la conoce como clave privada y kP se la conoce como clave pública. Una de ellas sirve para la transformación o función E de cifrado y la otra para la transformación D de descifrado. En muchos casos son intercambiables, esto es, si empleamos una para cifrar la otra sirve para descifrar y viceversa. Estos

criptosistemas deben cumplir además que el conocimiento de la clave pública kP no permite calcular la clave privada kp. Ofrecen un abanico superior de posibilidades, pudiendo emplearse para establecer comunicaciones seguras por canales inseguros puesto que únicamente viaja por el canal la clave pública, que sólo sirve para cifrar, o para llevar a cabo autenticaciones. Sin la clave privada (que no es deducible a partir de la clave pública) un observador no autorizado del canal de comunicación será incapaz de descifrar el mensaje cifrado.

- Protección de la confidencialidad en información almacenada y en tránsito: En términos generales, hay dos circunstancias en las que se debe usar el usar el cifrado: cuando los datos están **"en tránsito" o cuando están "en reposo"**. "En tránsito", en este contexto, es cuando envías información a través de Internet, por correo electrónico, o cuando necesitas almacenarla en otro lugar que no sea tu propio dispositivo. Los datos se consideran "en reposo" cuando se encuentran almacenados en tu dispositivo, ya sea en una parte integrada como un disco rígido, o en un medio extraíble, como una unidad USB. Respecto de este último punto, hay que tener en cuenta varios modelos:
  - Cifrado de disco duro (full disk encryption) o dispositivo: El cifrado de disco duro permite que si el portátil o equipo se pierde por ejemplo, la información contenida en él no pueda ser accedida simplemente montando el disco duro o dispositivo en otra máquina. Tienen la ventaja de ser "transparentes" para el usuario en la medida de que si se ha hecho login correctamente el usuario accede a los documentos de la misma forma que lo haría en un equipo no cifrado. Sin embargo, si se ha hecho login en el equipo o el servidor de ficheros es accesible por el administrador, nada impide a un usuario deshonesto acceder a los datos, copiarlos, reenviarlos, etc. Los datos están protegidos mientras residen en el dispositivo o disco duro, pero dejan de estarlo una vez son extraídos del mismo (copiados a otro dispositivo, reenviarlos, etc.).
  - Cifrado a nivel de fichero: No se cifra una partición o disco duro sino sólo ficheros individuales. Los ficheros cifrados no sólo lo están cuando se encuentran almacenados en el disco, sino que también pueden estar protegidos en tránsito, cuando son enviados por ejemplo como adjuntos en un email. En este caso se pierde el acceso transparente por parte de un usuario y también la protección transparente del mismo. Es decir por ejemplo con **PGP,** es necesario disponer de la clave pública de la persona con la que quiero compartir el fichero protegido, y por otro lado, ella deberá tener mi clave pública para poder descifrarlo. Por otro lado, una vez que el documento ha sido descifrado por el receptor, puede almacenarse desprotegido, reenviar desprotegido, etc.
  - Cifrado de base de datos: Sistemas de base de datos como SQL Server u Oracle utilizan **TDE – Transparent Data Encryption** para proteger los datos almacenados en bases de datos. Las tecnologías de TDE realizan operaciones de cifrado y descifrado de datos en tiempo real. Esto permite a los desarrolladores de aplicaciones, por ejemplo, trabajar con datos sin necesitar modificar las aplicaciones existentes. Este tipo de cifrado protege los datos en reposo en base de datos, pero no cuando estos han sido ya accedidos por la aplicación correspondiente y han podido ser extraídos. Respecto de los administradores, no

serán capaces de ver la información si los certificados utilizados para el cifrado son gestionados por otro grupo. Por lo general se cifran columnas concretas con datos sensibles, no toda la tabla (DNI, número de tarjeta, etc).

- ➢ Cifrado a nivel de aplicación. En este caso es la aplicación la que se encarga de cifrar los datos que se almacenarán, en bases de datos, repositorios, etc. Si bien es la técnica más potente y segura, a la vez es la más compleja al tener que añadir funcionalidades de cifrado en el desarrollo de la aplicación, asegurando su implementación correcta. En este caso, sólo los gestores de las claves utilizadas por la aplicación serán capaces de ver todos los datos descifrados. Los usuarios, de acuerdo a sus permisos, serán capaces de acceder a un subconjunto de información. Así mismo, tienen otro problema, y es que no se podrá realizar indexación a nivel de BBDD, búsquedas, etc al estar la información cifrada.

- ❖ Firmas digitales: autenticación, no repudio y protección de la integridad: La firma digital consta de dos “claves” o secuencias de caracteres separadas. Consiste en aplicar mecanismos criptográficos al contenido de un mensaje o documento con el objetivo de demostrar al receptor del mensaje que el emisor del mensaje es real (autenticación), que éste no puede negar que envió el mensaje (no repudio) y que el mensaje no ha sido alterado desde su emisión (integridad). El primer paso es crear un resumen o hash del mensaje. Los funciones de resumen o hash son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija, que representa un resumen de toda la información que se le ha dado (crea una cadena que solo puede volverse a crear con esos mismos datos). Para crear una firma digital, el software de firma crea un hash unidireccional de los datos electrónicos que se deben firmar. La clave privada se usa para encriptar el hash. El hash cifrado junto con otra información es la firma digital. Cualquier cambio en los datos, incluso cambiando o eliminando un solo carácter, da como resultado un valor diferente. Este atributo permite a otros validar la integridad de los datos mediante el uso de la clave pública del firmante para descifrar el hash. Si el hash descifrado coincide con un segundo hash calculado de los mismos datos, prueba que los datos no han cambiado desde que se firmó. Así mismo, al usar la clave privada del emisor, podemos asegurar el no repudio y la autenticación. La única manera de que se pueda descifrar el hash del mensaje con la clave pública de una persona es que se haya usado su clave privada.

● Copias de seguridad, seguridad en el correo y monitorización

Copias de seguridad

Una copia de seguridad es un proceso mediante el cual se duplica la información existente de un soporte a otro, con el fin de poder recuperarlos en caso de fallo del primer alojamiento de los datos (tanto a nivel completo en caso de desastre, como parcial en caso de corrupción o pérdida de unos ficheros).

- Para determinar la frecuencia con la que debemos realizar copias de seguridad, será necesario realizar un análisis en el que se tengan en cuenta los siguientes factores:
  - Número de datos o archivos generados y/o modificados en la organización.
  - Impacto para el negocio de la pérdida de datos por unidad de tiempo (una hora, un día, una semana, un mes, etc).
  - Coste de almacenamiento.
  - Obligaciones legales y normativas.
- Otro tema a tener en cuenta es el periodo de retención de los datos, cuánto tiempo debemos mantener las copias de seguridad, a decidir en base a requisitos legales y necesidades de la organización.
- También es crítico decidir el tipo de copia de seguridad a realizar:
  - Copia de seguridad completa: Cuando se realiza una copia de seguridad completa todos los archivos y carpetas del sistema se copian. Por lo tanto, tu sistema de copias de seguridad almacena una copia completa que es igual a la fuente de datos del día y hora en que se hace la copia de seguridad. Aunque el tiempo que se necesita para hacer esta copia de seguridad es mayor y requiere más espacio de almacenamiento, tiene la ventaja de que con una copia de seguridad completa la restauración es más rápida y más simple.
  - Copia de seguridad incremental: En este caso, la única copia completa es la primera. A partir de ahí, las copias de seguridad posteriores sólo almacenan los cambios realizados desde la copia de seguridad anterior. En este caso el proceso de restauración es más largo porque tienes que utilizar varias copias diferentes para restaurar completamente el sistema, pero a cambio el proceso de hacer la copia de seguridad es mucho más rápido y ocupa menos espacio de almacenamiento.
  - Copia de seguridad diferencial: Igual que las incrementales, la primera copia de seguridad es la única completa. La diferencia con la incremental viene del hecho de que aquí cada copia de seguridad posterior tiene todos los cambios respecto a la primera copia completa, y no respecto a la copia de seguridad anterior, como era el caso de la incremental. Por lo tanto en este caso la copia de seguridad requiere más espacio de almacenamiento que las incrementales, pero con la ventaja de que el tiempo de restauración es menor.
  - Copia espejo (mirroring): Con una copia de seguridad en espejo se realiza una copia exacta de los datos originales. Se suele hacer “en directo”, es decir, a la vez que trabajas con los datos reales, se hace una copia espejo en un disco alternativo. La ventaja de una copia en espejo es que la copia de seguridad no contiene archivos antiguos o en desuso. Pero esto también puede ser un problema ya que si un archivo se elimina accidentalmente en el sistema original, el sistema espejo lo elimina también. Generalmente se utiliza en sistemas con requisitos de disponibilidad elevados y que cuentan con sitios espejos (sistemas en activo que pueden tomar el lugar de los sistemas originales en cuestión de segundos).
- Se deben contar con procedimientos de recuperación y probar de forma regular tanto los procedimientos como las copias con el fin de asegurar que en caso de necesidad no existirá problema, como que las copias de seguridad no se habían realizado

correctamente y no es posible recuperarlas o que en el procedimiento se han olvidado incluir pasos críticos.

- Por último, pero no menos importante, hay que tener muy presente que se deberán proteger las copias de seguridad con el mismo nivel de controles que la información original (con el objeto de evitar que se conviertan en un agujero), y tener en cuenta que es necesario disponer de copias en sitios geográficamente alejados del sitio donde se alojan los datos originales en caso de desastre (otra ubicación de la organización, un tercero contratado específicamente o la nube).

Data Loss Prevention e Information Rights Management

Un aspecto crítico en la protección de datos es la gestión del nivel de acceso de los ficheros no estructurados (aquellos que no se encuentran en una base de datos) y su compartición dentro y fuera de la organización. Para ello se disponen de 2 tipos de soluciones principalmente que pueden complementarse:

- Data Loss Prevention (DLP): Una solución de prevención de pérdida de datos (DLP) es un sistema que está diseñado para **detectar potenciales brechas de datos/ transmisiones de datos y prevenirlos a través de monitorización, detección y bloqueo de información sensible mientras está en uso (acciones de extremos), en movimiento (tráfico de red) y en reposo (almacenamiento de datos)**. La solución no cifra los ficheros, sino que les aplica etiquetas en su descripción de metadatos, y son los agentes desplegados en los equipos/servidores o bien los nodos en red quienes se encargan de bloquear cualquier acción peligrosa. Así, se pueden conceder permisos de grano fino, como leer y editar, pero no copiar/pegar o enviar por mail. En caso de su extracción a disco externo (como USB) se puede bien bloquear, permitir sin problemas (perdiendo el control) o bien aplicando cifrado para que sólo sea posible verlo en otro equipo controlado por la organización (que disponga del agente). Las políticas generalmente se aplican por roles y/o departamentos y a nivel de repositorios, información con características similares (por ejemplo que contengan la palabra confidencial o números de la seguridad social).
- Information Rights Management: Las tecnologías de IRM (Information Rights Management) **permiten el cifrado de documentación aplicando una protección persistente a los mismos.** La documentación en reposo se encuentra cifrada y sólo está accesible a los usuarios que tengan derechos de acceso a la misma. Los derechos por lo general se dan de forma granular y se asignan usuario a usuario, por lo que es más recomendable de cara a la compartición de ficheros con terceras partes. Así, se puede compartir un fichero con sólo permisos de lectura, o también de modificación, pero por ejemplo no de compartición, copia o impresión. Así mismo, los permisos pueden ser cambiados o eliminados en tiempo casi real. Para el acceso a la información por sus receptores, se requiere de un cliente que accede al servidor de permisos cada vez que se abra el fichero para comprobar qué se puede hacer (algunas soluciones permiten su acceso online sin modificación y sólo para cierto tipo de ficheros como PDF u office).

Seguridad en el correo electrónico

El correo electrónico es uno de los principales medios de compartición de información, tanto a nivel interno de la organización como externa, a la vez que uno de los principales vectores de entrada para amenazas (correos phishing). Por ello, se deben contar con sistemas que permitan obtener las siguientes funcionalidades:

- Detección de phishing: Mediante técnicas como detección de orígenes, inteligencia artificial aplicada al análisis del contenido, etc, detectar que se trata de un posible caso de phishing.
- Detonación de ficheros y enlaces: Capacidad de poder analizar enlaces y adjuntos en correos electrónicos mediante el uso de sandboxes para validar su comportamiento.
- Análisis de malware: Capaz de poder utilizar técnicas de firmas y de inteligencia artificial para validar si un fichero adjunto es un malware.
- Control de información saliente (DLP): Análisis del contenido de los correos y los adjuntos para, sólo o en conjunción con una solución DLP. Poder evitar fugas de información. En su caso, se puede utilizar cifrado, de forma que solo el receptor esperado pueda descifrarlo.
- Detección de fraudes y buzones comprometidos: Capacidad de detectar actividad anómala en buzones y posibles casos de fraude como el fraude del CEO.
- Detección de exploits: Análisis de comportamiento al abrir enlaces y/o adjuntos para detectar posibles explotaciones del sistema para desplegar malware, tomar el control del sistema, etc.

Monitorización de actividad en BBDD y almacenes de datos

Las bases de datos y los repositorios de ficheros son objetivos primordiales para los atacantes debido a la sensibilidad de la información contenida de manera general. Por ello, u**n método de proteger los datos es monitorizar la actividad realizada en los mismos a bajo nivel** con el objeto de descubrir posibles comportamientos sospechosos o directamente delictivos. Una solución de este tipo debería ofrecer la siguiente funcionalidad:

- Automatizar el descubrimiento y la clasificación de datos sensibles: Es vital que una solución de este tipo permita analizar el tráfico y los repositorios/bases de datos a las que tiene acceso con el objeto de encontrar tanto nuevos repositorios como nueva información susceptible de protección.
- Monitorización en tiempo real de la actividad de los usuarios: Debe ser capaz de poder analizar la actividad a nivel granular y auditarla para diferentes repositorios, bases de datos SQL y no SQL, data warehouses, etc.
- Soporte al cumplimiento legal y normativo (plantillas predefinidas): Debe incluir plantillas para auditar y reportar el cumplimiento legal y normativo para diferentes de estas como RGPD, PCI-DSS, HIPAA, SOX, etc.
- Políticas predefinidas y adaptables: Debe incluir por defecto multitud de políticas adaptables para auditar y bloquear actividades sospechosas y/o potencialmente peligrosas.

- ❖ Bloqueo de acciones y enmascaramiento de datos: Debe permitir actuar como un cortafuegos de capa 7 (de aplicación) con el objeto de bloquear acciones que se hayan definido previamente, a la vez que permite otras acciones enmascarando los datos (cubriendo una parte de los mismos por protección, por ejemplo para la protección de datos personales.

● Seguridad en punto final

La protección del punto final se basa en proteger la infraestructura final (como sistemas y servidores) así como las aplicaciones desplegadas en los mismos con el objeto de evitar un punto de entrada a la información almacenada (o bien que sirvan como un punto de salto a otros sistemas con información más interesante para el atacante, se puedan robar credenciales que se reutilicen, se pueda utilizar el correo del afectado para un fraude, etc)

Protección contra malware

Los antivirus son programas cuyo objetivo es detectar y eliminar virus informáticos. Con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e internet, los antivirus han evolucionado hacia programas más avanzados que además de buscar y detectar virus informáticos consiguen bloquearlos, desinfectar archivos y prevenir una infección de los mismos.

Actualmente son capaces de reconocer otros tipos de malware como spyware, gusanos, troyanos, rootkits, RATs, etc. Históricamente se basaban en firmas, de manera que se necesitaba en los fabricantes hubiesen creado (o recibido de otros, dado que compartían), dicha firma. Esto ya no es válido, dado que es fácil modificar un virus para que su firma no genere una alarma, además de que muchas veces cuando se tiene una firma ya es tarde (p.e wannacry).

Los nuevos sistemas se basan en aprendizaje máquina o aprendizaje profundo de forma que se entrena a los sistemas para que detecten características que comparten los malware, de forma que son capaces de detectarlos sin firmas, aunque sean nuevos (si bien ya comienzan a encontrarse ficheros con modificaciones suficientes para engañar a estos sistemas).

Otros sistemas se basan en detectar las características de una explotación, de forma que prevengan que el malware pueda tomar control del sistema, cifrar el disco duro, elevar privilegios, etc.

Detección de intrusiones (Endpoint Detection & Response)

Este tipo de soluciones se encargan de monitorizar los sistemas donde están desplegados los agentes, analizando los procesos que se crean, trazas de memoria, conexiones de red entrantes y salientes, etc, para detectar posibles ataques hacia o desde el sistema. Aborda la necesidad de una supervisión en tiempo real, centrarse en los análisis de seguridad y en la respuesta al incidente.

Ofrece una visibilidad completa de extremo a extremo sobre la actividad de cada equipo, administrada desde una única consola, junto con una valiosa inteligencia de seguridad que podría usar un experto de seguridad informática para una investigación y respuesta mayores.

El objetivo principal de EDR es la **detección proactiva de amenazas nuevas o desconocidas**, **infecciones previamente no identificadas que penetran en la organización directamente a través de endpoints y servidores**. Ofrecen las siguientes capacidades:

- Modelo preventivo (pre-infección) y detectivo (post-infección) basado en análisis sobre patrones de comportamiento.
- Enfoque reactivo (post-incidente) apoyado en capacidades de contención y remediación rápida frente incidentes (segundos o minutos).
- Capacidades forenses, basadas en análisis sobre el registro de actividades del endpoint (tráfico de red, procesos, etc.).
- Inteligencia agregada, a través de un proceso continuo de investigación e innovación gracias a laboratorios y analistas expertos mediante la compartición de información de la consola con el fabricante.

Configuración segura o hardening

El hardening o **configuración segura es el proceso de configuración sistemática de los sistemas y aplicaciones (firmware, SO, BBDD, aplicaciones de negocio, etc) con el objeto de reducir la superficie de ataque potencial así como seleccionar opciones que aumenten la seguridad** general del sistema y la información.

Existen multitud de guías de fabricantes para realizar dicha tarea, así como guías de organizaciones internacionales como el Center for Internet Security.

En general, este **proceso se centra en aspectos como cerrar puertos innecesarios en los sistemas, asegurar las políticas de acceso de usuarios (como contraseñas seguras o los factores de autenticación necesarios), la habilitación de cifrado, configuración de las capacidades de seguridad nativas de cada sistema/aplicación, permisos de seguridad en archivos y carpetas, acceso remoto, etc.**

Gestión de vulnerabilidades

La gestión de vulnerabilidades es un proceso continuo de TI consistente en la identificación, evaluación y corrección de vulnerabilidades en los sistemas de información y las aplicaciones de una organización, **categorizando los activos según su importancia/valor y clasificando las vulnerabilidades según el nivel de riesgo,** de forma que se puedan priorizar las vulnerabilidades a corregir (por lo general existen más vulnerabilidades que capacidad de mitigarlas/corregirlas).

El proceso de gestión de vulnerabilidades suele incluir las siguientes acciones:

- Obtención de un inventario (y categorización por nivel de criticidad) de los activos de TI de una empresa, lo que incluye servidores, infraestructura de redes, estaciones de trabajo, impresoras y aplicaciones.
- Detección de las vulnerabilidades existentes mediante escáneres de redes, escáneres de vulnerabilidades en host y software de pruebas de penetración automáticas (o pruebas manuales) y determinación de los niveles de riesgo. Generalmente, los escaneos en red suelen dar más falsos positivos que los realizados con agentes (puesto que no pueden probar determinados aspectos o bien no tienen acceso al sistema para validar condiciones necesarias para explotar una vulnerabilidad).
- Reparación de sistemas y dispositivos vulnerables y presentación de informes sobre las medidas correctivas adoptadas. Este subproceso debe alinearse con la gestión del cambio para evitar impactar en los sistemas y contar con procedimientos específicos como contar con un plan de vuelta atrás antes de aplicar cambios en prueba en entornos de pre-producción antes de su despliegue definitivo.

Otras tecnologías de protección de punto final

- FIM: La monitorización de integridad de fichero o FIM emplea uno o varios algoritmos de hash para extraer los «message digest» o resúmenes de un archivo o archivos críticos del sistema y se almacenan en una base de datos o archivo maestro («línea base»). De forma regular, se ejecutan extracciones de «resúmenes y se comparan contra la línea base» con el fin de detectar posibles modificaciones, generando alertas a los administradores si esto ocurre. Esta es una forma fácil y confiable de garantizar la integridad de la configuración y los datos en sistemas informáticos y complementar los controles asociados a la gestión de cambios («Change Management») y trazabilidad. Esto por ejemplo es importante en los ficheros de configuración, ficheros críticos de DLL, etc para poder detectar modificaciones indebidas que denotaban una posible brecha (como instalación de una puerta trasera).
- Protección de móviles: Los smartphones, ya sean corporativos, o personales a los que se les permite acceso a la información corporativa, deben ser protegidos. Esta tipo de soluciones deben contar con protección antivirus (no para iPhone a día de hoy), cifrado de datos, correo electrónico seguro, creación de espacios de trabajo separados (el personal, y el de trabajo con el calendario, datos y correo cifrado), gestión remota (actualizaciones, cambio de políticas, borrado/bloqueo en caso de robo), etc.
- Tecnología de señuelos: Este tipo de tecnología es capaz de crear sistemas señuelo en la red incluyendo información falsa adaptada al tipo de información gestionada por la organización. Esto sirve tanto para detectar de manera inequívoca que se está produciendo un ataque (al no ser un sistema de negocio, nadie debe entrar al mismo) como para poder analizar el ataque realizado y aprender del adversario. Hoy en día existe tecnología que despliega sistemas tontos, y en caso de ataque permite levantar un sistema completo para engañar al atacante (anteriormente los sistemas tontos eran fáciles de detectar, pero disponer de una infraestructura de sistemas completa era inviable por el costo de licencias. Aquí se tiene lo mejor de ambos mundos).

- ❖ Seguridad en la virtualización: La tecnología de virtualización, tanto la clásica (como VMWare) como la basada en contenedores (como Kubernetes), supone un nuevo paradigma, de forma que se debe proteger no solo la máquina física, sino las máquinas virtuales/contenedores que dependen de ella. Por ello, la tecnología de seguridad debe adaptarse a este nuevo entorno, teniendo en cuenta aspectos como la monitorización de tráfico en redes virtuales (en algunos casos, el tráfico entre máquinas virtuales nunca pasa por interfaces de red físicas, por lo que diferentes soluciones tradicionales están ciegas).
- ❖ RASP: Las aplicaciones Runtime Application Self-Protection o aplicaciones de autoprotección en tiempo de ejecución se integran dentro de las aplicaciones web, siendo capaz de conocer sus puntos vulnerables y de proteger las peticiones de entrada con datos de entrada maliciosos que se dirijan a estos puntos. Trabaja de manera autónoma y es capaz de inferir la lógica de negocio de la propia aplicación y conocer lo que debe proteger. Esto evita los problemas de administración y gestión de reglas que ocurren en los cortafuegos a nivel de aplicación.

● Seguridad en red

Los sistemas, aplicaciones e información de las organizaciones se encuentran desplegadas en redes informáticas que facilitan su comunicación, tanto a nivel interno como externo. Así, en la red se pueden originar nuevas amenazas que deben ser paradas, a la vez que aporta información que puede ayudar a detectar un ataque en curso.

Segmentación y microsegmentación de la red

La segmentación de la red consiste en dividir una gran red (como puede ser la intranet, una extranet, etc) en segmentos más pequeños, filtrando por cada uno de ellos las entradas y salidas de tráfico de red, de forma que se facilite minimizar la superficie de exposición de los sistemas en el interior. Los criterios para la selección de sistemas a incluir en un segmento puede tomar en cuenta aplicaciones con un nivel de criticidad mayor que su entorno, sistemas con funcionalidades complementarias, entornos de un sistema, etc. Esta segmentación se suele realizar de manera física o bien lógica (siendo el mecanismo más utilizado en uso de VLANs o redes virtuales), si bien tiene una limitación sobre el número de subredes que se pueden tener (al gestionarse mediante electrónica de red que se acaba saturando.

Para poder llegar a un nivel superior de segmentación, se creó el término micro-segmentación, donde el objetivo es llegar a segmentar por servicios dentro de una misma aplicación, de forma que casi cada sistema cuenta con su propio segmento y reglas de filtrado. Para poder llegar a tal nivel, se introdujo un nuevo tipo de tecnología, Red Definida por Software (SDN), un conjunto de técnicas relacionadas con el área de redes computacionales, cuyo objetivo es facilitar la implementación e implantación de servicios de red de una manera determinista, dinámica y escalable, evitando al administrador de red gestionar dichos servicios a bajo nivel (mediante la separación del plano de control, software del plano de datos, hardware).

Por lo general este tipo de productos cuentan con sistemas de análisis que permiten poner la red en modo escucha para que ofrezcan un posible mapa de segmentos y reglas de filtrado que a continuación podrá ser refinado por la organización (en lugar de comenzar desde cero que sería un trabajo enorme dado el número de sistemas en empresas grandes y multinacionales).

IDS/IPS (Detección/Prevención de intrusiones en red)

Un sistema de detección de intrusiones (IDS) **es un programa de detección de accesos no autorizados a una red.** Se basa en el análisis pormenorizado del tráfico de red, el cual al entrar al analizador es comparado con firmas de ataques conocidos, o comportamientos sospechosos, como puede ser el escaneo de puertos, paquetes malformados, etc. **El IDS no sólo analiza qué tipo de tráfico es, sino que también revisa el contenido y su comportamiento. Un IPS (prevención) añade capacidad de bloqueo del tráfico de acuerdo a reglas predefinidas.**

En el caso de tráfico cifrado, para analizarlo (como en otras soluciones como cortafuegos), se puede utilizar técnicas de **man in the middle (el dispositivo se coloca en la mitad suplantando al otro miembro en cada conversación, de forma que ambos utilicen sus certificados)** o bien cargar los certificados de cifrado de todos los sistemas a analizar su tráfico.

Dado que los sistemas de firmas tienen los mismos problemas que los antivirus, un nuevo modelo basado en aprendizaje máquina y aprendizaje profundo ha surgido para poder detectar ataques en la red mediante análisis de anomalías y características similares de ataques.

Cortafuegos (FWs)

Un cortafuegos (FW) es la parte de una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas, todo mediante reglas definidas. En base a este principio, se recomienda definir qué está permitido y bloquear el resto (whitelisting) que definir lo que no está permitido y permitir el resto (blacklisting).

Los FW han evolucionado en los siguientes modelos:

- A nivel de paquetes: En este caso se crean reglas para paquetes de datos, debiendo crear reglas en ambos sentidos, lo cual era un problema de seguridad (se puede permitir el acceso en la dirección contraria del flujo de datos).
- Con estado: En este caso se mantenía una tabla dentro del FW que controlaba las sesiones creadas, de forma que sólo era necesario crear una regla del origen al destino, permitiendo el paso al resto de paquetes que fuesen parte de la sesión.
- A nivel de aplicación: Son aquellos que actúan sobre la capa de aplicación pudiendo entender entender ciertas aplicaciones y protocolos (por ejemplo FTP, DNS o HTTP), y permite detectar si un protocolo no deseado se coló a través de un puerto no estándar o si se está abusando de un protocolo de forma perjudicial. El ejemplo más claro es el WAF que permite proteger aplicaciones web frente a ataques como SQL Injection o XSS.
- Con inspección profunda de paquetes (DPI): El DPI combina las funciones de un sistema de detección/prevención de Intrusiones (IDS/IPS) con un tradicional cortafuegos de

estado permitiendo detectar ciertos ataques que ni los sistemas de detección de intrusiones ni los sistemas de prevención de intrusiones ni los cortafuegos de estado pueden detectar por sí solos. Así por ejemplo, es capaz de asociar sesiones a usuarios y a protocolos (sin importar el puerto utilizado) y filtrar por estos aspectos.

- Software Defined Firewall: Con el advenimiento de las redes definidas por software, un nuevo tipo de cortafuegos nació definido a través de las reglas de control del SDN, de forma que se libera el cortafuegos del plano de datos.

SIEM (Security Information and Events Management)

Se trata de un tipo de herramienta de seguridad que permite **recolectar eventos de seguridad desde diferentes fuentes (SO, FWs, IDS, AV, etc) en un formato unificado con el objeto de poder correlacionarlos y poder analizar posibles intrusiones o problemas de seguridad** que afecten a diferentes tipos de sistema y de forma centralizada. Su principal funcionalidad es la siguiente:

- Disponer de reglas de alerta y correlación para notificar posibles intrusiones y el cumplimiento normativo.
- Disponer de un sistema de análisis avanzado de los eventos para los gestores de incidentes.
- Capacidad de análisis de comportamiento de usuarios y entidades (UEBA) que permite establecer patrones estadísticos avanzados del comportamiento de usuarios y dispositivos con el objeto de alertar de anomalías que podrían ser indicadores de un ataque.
- Capacidad de análisis de comportamiento y análisis forense en red (NBA) para establecer patrones estadísticos avanzados del tráfico general de la red y poder detectar anomalías.
- Permitir la integración u ofrecer un sistema de orquestación, automatización y respuesta de seguridad (SOAR) para definir pasos de respuesta ante tipologías de incidentes así como la automatización de determinados pasos (detonación de ficheros, recopilación de información, bloqueo en un cortafuegos, aislamiento en la red de un sistema o conjunto de sistemas, etc).