Introducción a la seguridad informática

Importancia de la seguridad informática

El espectacular auge de Internet y de los servicios telemáticos ha hecho que los equipos informáticos y las redes de comunicación de datos se conviertan en un elemento cotidiano en nuestras vidas.

Los sistemas de información se han convertido en un soporte fundamental para el funcionamiento de la gran mayoría de las empresas. El uso de las tecnologías de la información ha permitido a las empresas gestionar de forma eficiente su **información** y prestar **servicios** a través de Internet. Estos servicios se pueden usar para dar soporte operacional a la empresa o pueden ser el producto final que se venda a los clientes.

¿Por qué es necesaria la **gestión del riesgo** de estos sistemas de información? Si las empresas dependen de los sistemas de información para su funcionamiento, necesitan saber hasta qué punto pueden confiar en ellos, qué puede salir mal y estar preparadas para recuperar la situación operacional en un tiempo y coste aceptables cuando suceda un incidente.

El primer paso de la gestión del riesgo consistirá en valorar la situación actual de la empresa, para ello se realizará un **análisis de riesgos** para determinar los posibles problemas que pueden surgir. Se identificarán los activos de la empresa, sus vulnerabilidades, las amenazas a las que están expuestos y el riesgo que suponen estas amenazas para la empresa. En otras palabras se determinará el posible daño económico resultante en caso de producirse un incidente de seguridad así como la probabilidad de que ese incidente pueda llegar a producirse.

Una vez conocida al situación de la empresa mediante el análisis de riesgos, el siguiente paso es evaluar si la situación es aceptable o si es necesario **tratar los riesgos** detectados estableciendo medidas o controles para mitigar los posibles efectos de las amenazas. No es posible eliminar completamente todos los riesgos, pero se deben tomar las medidas razonables para que los daños potenciales sean aceptables para la organización. Se debe llegar a una situación de **equilibrio entre el coste de la protección y el valor del activo protegido**. No tiene sentido gastar más que el valor del activo que se protege, pero tampoco se puede dejar un activo desprotegido y sufrir los efectos de no haber invertido lo suficiente en su protección.

Se debe tener en cuenta que las amenazas son dinámicas: la empresa cambia y su entorno cambia. Este cambio constante hace imprescindible que el proceso de gestión de riesgos se realice usando un **ciclo de mejora continua**. Puesto que la empresa, los sistemas de información y las amenazas evolucionan, la gestión del riesgo tiene que ser una actividad que se realice cíclicamente para adaptarse a los cambios.

Definición de Seguridad de la información

La **seguridad de la información** se refiere a la protección de la información y de los sistemas que la procesan, almacenan y transmiten, contra cualquier tipo de amenaza que pueda comprometer su **confidencialidad, integridad y disponibilidad**. Estos tres principios forman la base de la seguridad de la

información y son comúnmente conocidos como la **tríada CIA** (por sus siglas en inglés: Confidentiality, Integrity, Availability).

{:class="center"}

Confidencialidad

La **confidencialidad** implica garantizar que la información sea accesible únicamente por las personas autorizadas, protegiendo los datos sensibles contra accesos no autorizados.

Según la norma ISO/IEC 27000, la confidencialidad es la "propiedad de que la información no esté disponible ni se divulgue a individuos, entidades o procesos no autorizados" (ISO/IEC 27000:2018).

Integridad

La **integridad** se refiere a la exactitud y completitud de la información, así como a la protección contra modificaciones no autorizadas.

La norma ISO/IEC 27000 define la integridad como la "propiedad de exactitud y completitud" de los activos de información (ISO/IEC 27000:2018).

Disponibilidad

La **Disponibilidad** asegura que la información esté disponible y accesible para su uso cuando sea necesario. La disponibilidad.

Según la ISO/IEC 27000, es la "propiedad de ser accesible y utilizable a demanda por una entidad autorizada" (ISO/IEC 27000:2018).

Definición de Seguridad de la Información Extendida

La tríada CIA (Confidencialidad, Integridad y Disponibilidad) constituye el núcleo de la seguridad de la información, pero en varias normas y marcos se amplía la definición de seguridad de la información con dos dimensiones adicionales: **Autenticidad** y **Trazabilidad**.

Reconociendo que la protección de los datos también depende de garantizar la legitimidad de la información y la capacidad de rastrear sus movimientos y modificaciones a lo largo del tiempo.

Autenticidad

La **autenticidad** se refiere a la garantía de que la información, así como sus fuentes y usuarios, son genuinos y pueden ser verificados. Asegurar la autenticidad implica que los datos no han sido alterados desde su creación y que provienen de una fuente confiable.

Según la norma ISO/IEC 27000, la autenticidad es definida como "la propiedad de que una entidad es lo que dice ser" (ISO/IEC 27000:2018). En el contexto de la seguridad de la información, la autenticidad es fundamental para prevenir fraudes y asegurar que tanto la información como las comunicaciones sean legítimas.

Trazabilidad

La **trazabilidad** se refiere a la capacidad de rastrear la historia, aplicación o localización de lo que se está considerando. En el ámbito de la seguridad de la información, la trazabilidad está relacionada con la capacidad de seguir el rastro de las actividades y transacciones que se realizan en un sistema, lo que incluye el seguimiento de accesos y modificaciones. Esto es crucial para la **auditoría** y la **responsabilidad**, permitiendo identificar quién hizo qué, cuándo y cómo. La trazabilidad está alineada con el principio de **no repudio**, que asegura que las acciones realizadas por un usuario o sistema puedan ser probadas, de modo que nadie pueda negar haber realizado una acción específica.

Estas dimensiones adicionales están reflejadas en varias normas y marcos, como la **ISO/IEC 27001**, que incluye controles relacionados con la autenticación, la gestión de registros y la auditoría, elementos esenciales para garantizar la autenticidad y la trazabilidad en los sistemas de información.

Conceptos Fundamentales: Activo, Vulnerabilidad, Amenaza, Riesgo y Controles

En la gestión de la seguridad de la información, es fundamental comprender varios conceptos clave que forman la base para identificar y mitigar los riesgos a los que están expuestos los recursos de una organización. Estos conceptos incluyen **activo**, **vulnerabilidad**, **amenaza**, **riesgo** y **controles**. A continuación, se explican estos términos y su interrelación.

Activo

Un **activo** es cualquier recurso de valor para la organización que necesita ser protegido. Los activos pueden ser tangibles o intangibles y abarcan desde la información misma hasta los sistemas que la procesan, almacenan y transmiten. Ejemplos de activos incluyen:

- **Datos y bases de datos**: Información crítica, como registros de clientes, propiedad intelectual, planes estratégicos, etc.
- **Sistemas de información**: Hardware, software, redes y servidores.
- **Recursos humanos**: Personal con conocimientos especializados.
- **Infraestructura física**: Edificios, centros de datos, instalaciones de telecomunicaciones.

El valor de un activo depende de su importancia para la operación y el éxito de la organización, así como del impacto que tendría su pérdida, daño o compromiso.

> **Activo**: Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. [UNE 71504:2008]

Vulnerabilidad

Una **vulnerabilidad** es una debilidad o deficiencia en un activo o en las medidas de seguridad que lo protegen, que podría ser explotada por una amenaza para causar daño. Las vulnerabilidades pueden ser de naturaleza técnica, física, o humana. Ejemplos de vulnerabilidades incluyen:

- **Fallos de software**: Bugs o configuraciones inseguras que pueden ser explotadas por un atacante.
- **Controles de acceso inadecuados**: Contraseñas débiles o mal gestionadas.
- **Deficiencias físicas**: Áreas no aseguradas o dispositivos sin protección física adecuada.
- **Errores humanos**: Falta de formación del personal o errores operacionales.

La existencia de una vulnerabilidad no implica necesariamente que se vaya a sufrir un daño, pero sí aumenta el potencial de que una amenaza se materialice.

> **Vulnerabilidad**: Debilidad de un activo o control que puede dar lugar a una o más amenazas.[ISO 27000]

Amenaza

Una **amenaza** es cualquier circunstancia o evento con el potencial de explotar una vulnerabilidad y causar daño a un activo. Las amenazas pueden ser intencionales, como los ataques cibernéticos, o no intencionales, como los desastres naturales. Ejemplos de amenazas incluyen:

- **Ciberataques**: Malware, phishing, ataques DDoS, etc.
- **Desastres naturales**: Inundaciones, terremotos, incendios.
- **Fallos técnicos**: Caídas de sistemas, fallos de hardware.
- **Errores humanos**: Borrado accidental de datos, divulgación no autorizada de información.

El impacto de una amenaza puede variar, dependiendo de la vulnerabilidad que explote y del valor del activo afectado.

> **Amenaza**: Causa potencial de un incidente indeseado, que puede resultar en daño a un sistema u organización.[ISO 27000]

Riesgo

El **riesgo** es la posibilidad de que una amenaza explote una vulnerabilidad y cause un impacto negativo sobre un activo. En términos simples, el riesgo puede ser entendido como la probabilidad de que ocurra un evento adverso y la magnitud de sus consecuencias. El riesgo se calcula generalmente como:

```
Riesgo = Probabilidad de la amenaza × Impacto del evento
```

Los riesgos pueden ser categorizados en función de su gravedad y la urgencia de mitigación, lo que ayuda a las organizaciones a priorizar sus esfuerzos de seguridad.

> **Riesgo**: efecto de incertidumbre en los objetivos. [ISO 27000]

- Un efecto es una desviación de lo esperado - positiva o negativa.
- Incertidumbre es el estado, incluso parcial, de deficiencia en la información relacionada con el entendimiento o el conocimiento de un evento, sus consecuencias o su probabilidad.
- El riesgo se caracteriza a menudo en relación a potenciales "eventos" y "consecuencias" (definidos en ISO 73:2003) o una combinación de ambos.
- El riesgo a menudo se expresa en términos de una combinación de consecuencias de un evento (incluyendo cambios en las circunstancias) y su probabilidad de ocurrencia asociada.
- En el contexto de sistemas de gestión de la seguridad de la información, los riesgos de la seguridad de la información pueden ser expresados como el efecto de incertidumbre sobre los objetivos de la seguridad de la información.
- Los riesgos de la seguridad de la información están asociados con el potencial de que amenazas exploten vulnerabilidades de activos de información o grupos de activos de información y consecuentemente cause daño a la organización.

Controles

Los **controles** son las medidas y procedimientos implementados para mitigar o eliminar los riesgos, reduciendo la probabilidad de que una amenaza explote una vulnerabilidad o minimizando el impacto si ocurre un incidente de seguridad. Los controles pueden ser de varios tipos, incluidos:

- **Controles preventivos**: Destinados a evitar que ocurran incidentes de seguridad (por ejemplo, firewalls, políticas de acceso, autenticación multifactor).
- **Controles detectivos**: Diseñados para identificar incidentes de seguridad cuando ocurren (por ejemplo, sistemas de detección de intrusiones, registros de auditoría).
- **Controles correctivos**: Orientados a mitigar el daño y recuperar la funcionalidad tras un incidente (por ejemplo, planes de recuperación ante desastres, copias de seguridad).

Los controles deben ser seleccionados y diseñados en función del análisis de riesgos y alineados con los objetivos de la organización, garantizando que sean adecuados para proteger los activos de forma eficaz y eficiente. Es posible que los controles no siempre consigan el efecto pretendido.

Los controles también son denominados **salvaguardas**, **medidas** de seguridad o contramedidas.

> Control: Medida que modifica el riesgo.

Interrelación de los Conceptos

La relación entre estos conceptos es fundamental para la gestión de la seguridad de la información. Un activo valioso que presenta una vulnerabilidad puede estar en riesgo si existe una amenaza que pueda explotarlo. Los controles se implementan para reducir estos riesgos, protegiendo así los activos de la organización. La evaluación continua de los riesgos y la actualización de los controles es esencial para mantener la seguridad en un entorno cambiante.

Seguridad Física y Seguridad Lógica

La **seguridad física** y la **seguridad lógica** son dos aspectos fundamentales de la seguridad de la información, cada uno con enfoques, objetivos y mecanismos distintos, pero complementarios. Ambos tipos de seguridad son esenciales para proteger los activos de una organización, pero lo hacen de maneras diferentes.

Seguridad Física

La **seguridad física** se refiere a las medidas diseñadas para proteger los elementos tangibles de una organización, tales como el hardware, las instalaciones, el personal y otros recursos físicos, contra amenazas físicas. El objetivo principal de la seguridad física es evitar el acceso no autorizado, el daño o la destrucción de estos activos.

Algunos ejemplos de medidas de seguridad física incluyen:

- **Control de acceso**: Uso de tarjetas de identificación, cerraduras electrónicas, guardias de seguridad, y sistemas de vigilancia para restringir el acceso a áreas sensibles.
- **Videovigilancia**: Cámaras de seguridad para monitorear y grabar actividades en áreas críticas.
- **Sistemas de detección y alarma**: Detectores de humo, sistemas contra incendios, alarmas de intrusión y sensores de movimiento.
- **Protección contra desastres**: Medidas para proteger las instalaciones contra incendios, inundaciones, terremotos, y otras amenazas naturales.

La seguridad física es esencial para evitar que personas no autorizadas accedan o dañen los recursos que contienen o procesan información crítica, como servidores, centros de datos, o dispositivos de almacenamiento.

Algunas medidas de seguridad física son el estudio de de la ubicación correcta, medidas preventivas contra incidentes como incendios o inundaciones o el controles de acceso físico.

Seguridad Lógica

La **seguridad lógica** se refiere a las medidas utilizadas para proteger los sistemas informáticos y la información que almacenan o procesan, mediante la implementación de controles en el software, datos, y procesos informáticos. Este tipo de seguridad se enfoca en proteger los activos digitales contra amenazas cibernéticas, como el acceso no autorizado, la modificación o destrucción de datos, y el robo de información.

Ejemplos de medidas de seguridad lógica incluyen:

- **Autenticación y control de acceso**: Uso de contraseñas, autenticación de múltiples factores, y sistemas de gestión de identidades para garantizar que solo los usuarios autorizados puedan acceder a los sistemas y datos.
- **Cifrado**: Protege la confidencialidad de los datos mediante la codificación de la información para que solo pueda ser leída por usuarios con la clave correcta.
- **Cortafuegos (firewalls) y sistemas de detección de intrusiones**: Monitorean y controlan el tráfico de red para bloquear accesos no autorizados y detectar actividades sospechosas.
- **Software antivirus y antimalware**: Protege los sistemas contra virus, spyware, ransomware, y otros tipos de software malicioso.
- **Políticas de seguridad y gestión de parches**: Definen las reglas para el uso seguro de los sistemas y aseguran que todos los componentes de software estén actualizados para prevenir vulnerabilidades.

Complementariedad entre Seguridad Física y Lógica

La seguridad física y la seguridad lógica deben trabajar en conjunto para proporcionar una protección integral de la información. Por ejemplo, aunque un servidor pueda estar protegido por cifrado (seguridad lógica), si un intruso puede acceder físicamente al dispositivo, podría extraer los datos directamente. Del mismo modo, si un centro de datos tiene controles de acceso físicos estrictos, pero carece de seguridad lógica adecuada, un atacante podría explotar vulnerabilidades de software para acceder a la información.

Por lo tanto, para garantizar la seguridad de la información de manera efectiva, es crucial que las organizaciones adopten un enfoque holístico que combine tanto medidas de seguridad física como lógica.

Clasificación de los controles según el momento de aplicación

Seguridad activa:

Son aquellas medidas que se utilizan para evitar las amenazas antes de que se produzcan. Son preventivas y evitan grandes daños a los sistemas informáticos, se consideran acciones previas a un ataque.

Seguridad pasiva:

Comprende el conjunto de medidas utilizadas para intentar minimizar los daños una vez que se produzca el ataque o fallo, activando los mecanismos de recuperación.
Son correctivas, minimizan el impacto y los efectos causados por accidentes, es decir, se consideran medidas o acciones posteriores a un ataque o un incidente. Un ejemplo son las copias de seguridad que permiten minimizar el efecto de un incidente producido.

Seguridad Activa y Seguridad Pasiva

En el ámbito de la seguridad de la información, las estrategias para proteger los activos de una organización pueden clasificarse en dos categorías principales: **seguridad activa** y **seguridad pasiva**. Ambas son complementarias y juegan un papel crucial en la defensa contra amenazas y en la mitigación de riesgos.

Seguridad Activa

La **seguridad activa** se refiere a las medidas y mecanismos que se implementan de manera proactiva para detectar, prevenir y responder a incidentes de seguridad en tiempo real. Estas acciones están diseñadas para intervenir activamente en la protección de los sistemas, haciendo frente a las amenazas antes o mientras ocurren.

Ejemplos comunes de seguridad activa:

- **Sistemas de detección y prevención de intrusiones (IDS/IPS)**: Estos sistemas monitorizan el tráfico de red y los sistemas en busca de actividades sospechosas o patrones de ataque, y pueden bloquear automáticamente las amenazas detectadas.
- **Firewalls**: Los firewalls filtran el tráfico entrante y saliente basado en reglas de seguridad predefinidas, evitando que el tráfico malicioso acceda a la red.
- **Antivirus y antimalware en tiempo real**: Estos programas escanean los archivos y actividades del sistema en busca de software malicioso y lo eliminan antes de que cause daño.

- **Autenticación multifactor (MFA)**: Al requerir múltiples formas de verificación (como contraseñas, tokens físicos, o datos biométricos) para acceder a un sistema, se reduce significativamente la posibilidad de acceso no autorizado.
- **Respuesta a incidentes**: Equipos dedicados y herramientas especializadas para gestionar y mitigar incidentes de seguridad a medida que ocurren, minimizando el impacto en la organización.

Seguridad Pasiva

La **seguridad pasiva** se refiere a las medidas que están diseñadas para resistir o mitigar los efectos de un ataque o incidente de seguridad sin requerir una intervención activa en tiempo real. Estas medidas no previenen activamente los ataques, pero aseguran que, si ocurre un incidente, el daño se minimice y la recuperación sea posible.

Ejemplos comunes de seguridad pasiva:

- **Cifrado de datos**: El cifrado protege la confidencialidad de la información almacenada o transmitida, de modo que, aunque los datos sean interceptados o robados, no puedan ser leídos sin la clave de descifrado.
- **Backups (copias de seguridad)**: La creación regular de copias de seguridad garantiza que la información crucial pueda ser restaurada en caso de pérdida, daño o corrupción de datos.
- **Políticas de control de acceso**: Estas políticas definen quién tiene acceso a qué información y recursos, limitando la exposición de datos sensibles.
- **Seguridad física**: Aunque no es proactiva contra ataques cibernéticos, la seguridad física, como las cerraduras, los sistemas de videovigilancia, y los controles de acceso a las instalaciones, previene el acceso no autorizado a los componentes físicos de los sistemas de información.
- **Redundancia de sistemas**: La implementación de sistemas y recursos redundantes asegura que si un componente falla, otro puede tomar su lugar sin interrupción del servicio.

Complementariedad entre Seguridad Activa y Pasiva

Ambas formas de seguridad son necesarias para una protección integral. La **seguridad activa** permite responder rápidamente a las amenazas y detener los ataques en curso, mientras que la **seguridad pasiva** asegura que, en caso de que una amenaza pase desapercibida o no pueda ser detenida, los daños sean mínimos y se pueda garantizar la continuidad del servicio y la recuperación de los datos.

Por ejemplo, un sistema que combina **cifrado de datos** (seguridad pasiva) con un **IDS/IPS** (seguridad activa) está mejor protegido contra una gama más amplia de amenazas que uno que solo utiliza una de estas estrategias. De este modo, se logra un enfoque más robusto y resiliente frente a los diversos riesgos que enfrenta la organización en el entorno digital actual.

Alta Disponibilidad

La **alta disponibilidad** es un enfoque estratégico en la arquitectura de sistemas que garantiza que un servicio o sistema esté operativo y accesible la mayor parte del tiempo, **minimizando las interrupciones y el tiempo de inactividad**. Esto es especialmente crítico para aplicaciones y servicios que requieren

funcionamiento continuo, como plataformas de comercio electrónico, sistemas financieros o infraestructuras críticas.

Para lograr alta disponibilidad, se utilizan diversas técnicas, como la redundancia de hardware y software, la replicación de datos, el uso de balanceadores de carga, y la implementación de mecanismos de failover que aseguren que, en caso de fallo de uno de los componentes, otro pueda tomar su lugar sin interrumpir el servicio.

Cálculo del nivel de disponibilidad

La disponibilidad se calcula como la proporción del tiempo en que un sistema está operativo respecto al tiempo total (sumando el tiempo de operación y el tiempo de reparación). La fórmula expresa la disponibilidad como el cociente entre el tiempo medio entre fallos y la suma del tiempo medio entre fallos y el tiempo medio de reparación.

$$D=\frac{MTBF}{MTTR + MTBF}$$

En este contexto, $$D$$ representa la disponibilidad de un sistema, $$MTBF$$ es el **Mean Time Between Failures** o **Tiempo Medio Entre Fallos**, y $$MTTR$$ es el **Mean Time To Repair** o **Tiempo Medio de Reparación**.

Los Nueves de la Alta Disponibilidad

Los "nueves" se refieren al porcentaje de tiempo que un sistema está disponible durante un año, y es una forma común de medir la **disponibilidad** de un sistema. Cuantos más "nueves" haya, mayor es la disponibilidad, y por lo tanto, menor el tiempo de inactividad.

- **99% de disponibilidad (dos nueves)**: Aproximadamente 3,65 días de inactividad al año.
- **99.9% de disponibilidad (tres nueves)**: Aproximadamente 8,76 horas de inactividad al año.
- **99.99% de disponibilidad (cuatro nueves)**: Aproximadamente 52,56 minutos de inactividad al año.
- **99.999% de disponibilidad (cinco nueves)**: Aproximadamente 5,26 minutos de inactividad al año.
- **99.9999% de disponibilidad (seis nueves)**: Aproximadamente 31,5 segundos de inactividad al año.

Ejemplos Relevantes

1. **Google Cloud y Amazon Web Services (AWS)**: Ambos ofrecen servicios con SLA (Service Level Agreement) que garantizan entre el 99.95% y el 99.99% de disponibilidad, dependiendo del servicio. Estos proveedores implementan alta disponibilidad a través de centros de datos distribuidos geográficamente, redundancia y sistemas automatizados de failover.

2. **Sistemas Financieros**: Las plataformas de transacciones financieras, como las redes de cajeros automáticos o las aplicaciones bancarias en línea, a menudo requieren cinco nueves de disponibilidad para asegurar que los clientes puedan acceder a sus fondos y realizar transacciones en cualquier momento.

3. **Servicios de Salud**: Los sistemas de información hospitalaria (HIS) y las aplicaciones de monitoreo de pacientes en tiempo real necesitan operar con alta disponibilidad para asegurar que los médicos tengan acceso continuo a la información crítica, incluso durante emergencias.

La alta disponibilidad es esencial para garantizar que los sistemas críticos continúen operando sin interrupciones, ofreciendo a los usuarios un servicio confiable y continuo, independientemente de las condiciones adversas que puedan presentarse.

Ejercicios

Análisis de riesgos en 5 minutos

El Instituto Nacional de Ciberseguridad de España (**INCIBE**) es una entidad pública dependiente del Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial. INCIBE se dedica a mejorar la ciberseguridad en España, tanto en el ámbito privado como en el público. Ofrece servicios de apoyo a empresas, ciudadanos, e instituciones, promoviendo la educación y concienciación en ciberseguridad, y actuando como centro de respuesta ante incidentes de seguridad informática. Su objetivo es fortalecer la confianza digital y proteger la información y los sistemas frente a amenazas cibernéticas.

https://www.incibe.es/

En este ejercicio se propone contestar el cuestionario de evaluación de riesgos de seguridad de la información que ofrece INCIBE y estudiar los resultados obtenidos. Se pueden usar datos d una empresa real o fictícia.

Una vez completado el cuestionario,se propone revisar los resultados.

- ¿Qué aspectos de la empresa son valorados al analizar el nivel de riesgo?
- ¿Qué legislaicón se propone revisar?
- ¿Qué medidas de seguridad se proponen?

Cuestionario: https://www.incibe.es/empresas/herramientas/conoces-tus-riesgos

Bibliografía

- ISO/IEC 27000: Descripción de las normas de la familia y definiciones de vocabulario https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip
- Instituto nacional de ciberseguridad (INCIBE): https://www.incibe.es/
    - INCIBE - Gestión de riesgos https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf

- Centro criptográfico nacional (CCN): https://www.ccn-cert.cni.es/
- Agencia española protección de datos (AEPD): Ahttps://www.aepd.es/es
    - Normativa protección de datos. https://www.aepd.es/es/informes-y-resoluciones/normativa-y-circulares
- European Union Agency for Cybersecurity (ENISA): https://www.enisa.europa.eu/
    - Gestión de riesgos ENISA: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management
- ALARP: https://www.sciencedirect.com/topics/engineering/as-low-as-reasonably-practicable-process-safety