U1 - Fundamentos de ciberseguridad

La ciberseguridad es una disciplina que protege los sistemas informáticos, las redes, los datos y la información de las amenazas cibernéticas que pueden afectar su confidencialidad, integridad y disponibilidad. Esta disciplina es crucial en la era digital, ya que las empresas buscan evolucionar e innovar tecnológicamente para ser competitivas, eficientes y adaptables, pero también se enfrentan a nuevos desafíos y riesgos para su seguridad.

1. ¿Qué es la ciberseguridad?

La ciberseguridad se puede definir en **cinco dimensiones**: la seguridad de las comunicaciones, la seguridad de las operaciones, la seguridad de la información, la seguridad física y la seguridad pública/nacional.

A su vez, la protección de la información cuenta con **tres principios fundamentales** que orientan las acciones y decisiones a tomar en el ámbito de la ciberseguridad: confidencialidad, integridad y disponibilidad.

Transformación digital de la empresa

La empresa debe adaptarse al entorno digital para alcanzar una mayor eficiencia y competitividad. La posibilidad de acceder y procesar datos desde cualquier lugar y en cualquier momento requiere **asumir ciertos retos** en el diseño y seguridad de la red.

Este proceso de digitalización tiene un impacto y requiere una transformación en todos los aspectos de la actividad empresarial, desde la operatividad hasta la gestión e innovación, siempre en función del tipo de organización.

Definición de ciberseguridad

La ciberseguridad es el conjunto de medidas y acciones que tienen como objetivo **proteger la información y los sistemas** que la procesan, almacenan y transmiten de las amenazas que existen en el entorno digital.

De acuerdo con Information Systems Audit and Control Association (ISACA), la ciberseguridad se centra en la **protección de los activos de información** mediante el tratamiento de amenazas que ponen en peligro su confidencialidad, integridad y disponibilidad.

Según la Agencia de la Unión Europea para la Ciberseguridad (ENISA), la ciberseguridad se centra en la **seguridad del ciberespacio**, que se conoce como el espacio de interacción entre individuos, servicios y dispositivos que utilizan una red global de telecomunicaciones.

La ciberseguridad se centra en **cinco ámbitos o dimensiones**, en base a qué se enfrentan:

- **Seguridad de las comunicaciones**: protección contra amenazas que pueden impactar en la infraestructura técnica de un sistema o red informática y puedan provocar una alteración o mal funcionamiento del sistema o red.
- **Seguridad de las operaciones**: protección contra la corrupción intencionada de los procesos desarrollados en un sistema o red informática que puedan ocasionar resultados no previstos .
- **Seguridad de la información**: protección contra la amenaza de robo, borrado o alteración de los datos que se almacenan o transmiten en un sistema o red informática.
- **Seguridad física**: protección contra las amenazas físicas que puedan influir o afectar al bienestar de un sistema o red informática, como el acceso físico a los servidores, un incendio o inundación y la coerción de los usuarios.
- **Seguridad pública/nacional**: protección contra amenazas originadas en el ámbito cibernético pero que pueden tener consecuencias graves en la seguridad física o digital de una nación u organización que puedan afectar a servicios públicos esenciales, sistemas financieros, etc.

2. ¿Qué buscamos proteger?

Se busca la protección de los tres principios fundamentales de la **tríada CID**, que se ajustan a los requisitos específicos de cada empresa:

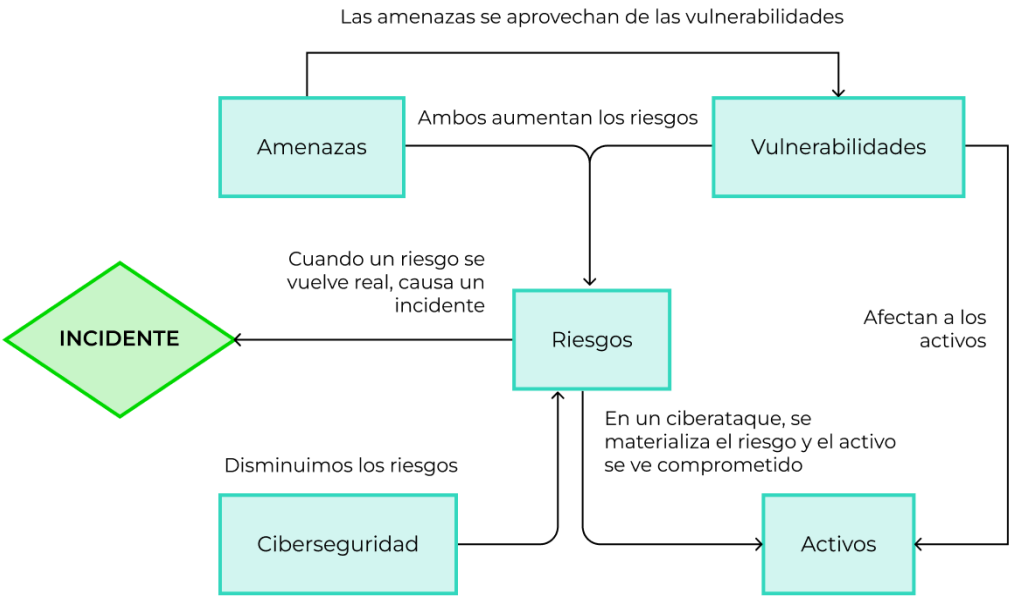
- **Confidencialidad**: sólo las personas autorizadas podrán acceder a la información, facilitando la protección de datos estratégicos o sensibles.
- **Integridad**: asegurar que la información sea completa, precisa y libre de modificaciones no autorizadas, crucial en entornos donde los datos deben reflejar fielmente la realidad.
- **Disponibilidad**: la información y los sistemas deberán estar accesibles y operativos cuando se necesiten, evitando interrupciones innecesarias.

A veces se establecen algunos principios complementarios, como la **autenticación** o la **trazabilidad**. La **privacidad** se muestra en la actualidad como un factor adicional similar a la confidencialidad, pero desde la perspectiva individual.

3. Gestión del riesgo en ciberseguridad

La ciberseguridad ha pasado de buscar la seguridad total al enfoque de la administración del riesgo. Para entender el riesgo, es necesario conocer algunos de sus conceptos clave:

- **Amenazas**: acción potencial que puede causar daño.
- **Vulnerabilidad**: debilidad técnica u organizativa de nuestro sistema. La Base Nacional de Vulnerabilidades (NVD) rastrea las que se han divulgado públicamente.
- **Activos**: recursos valiosos que debemos proteger.
- **Incidente**: acontecimiento que ocurre cuando una amenaza se aprovecha de una vulnerabilidad.
- **Riesgos**: combinación de la probabilidad de que ocurra un suceso y su impacto en los activos. El riesgo de una vulnerabilidad se cuantifica por la probabilidad de que sea explotada y su posible impacto.



Identificación y protección de activos críticos

Los activos tienen valor relevante para la organización, por lo que es indispensable entender cómo se relacionan entre sí. Esto nos permitirá identificar los riesgos y las vulnerabilidades de manera correcta, basándonos en la dependencia entre activos y cómo interactúan entre sí dentro del sistema.

Dentro de los activos, existe la categoría de **activos de alto valor** (high value asset o HVA), cuya protección es esencial para la continuidad del negocio. Muchas estrategias de ciberseguridad se centran en ellos, pero esto presenta un riesgo adicional: es posible que un atacante acceda a estos HVA mediante la explotación de activos secundarios, que aparentemente son menos críticos y están menos protegidos. Por ello, es esencial adoptar una visión integral que no deje nada de lado.

Catálogo y tratamiento de vulnerabilidades

La documentación de las vulnerabilidades se suele hacer con un CVE o Common Vulnerabilities and Exposures, que es un identificador único coordinado por MITRE. Una de las fuentes más importantes para consultar estas vulnerabilidades documentadas es la NVD o National Vulnerability Database, gestionada por el NIST.

El CVS otorga un número identificador a la vulnerabilidad, que necesitará ser evaluado por el estándar CVSS (Common Vulnerability Scoring System) para medir su gravedad. Esta medición se realiza mediante dos grupos de métricas: de explotabilidad y de impacto.

Vulnerabilidades Zero-day

Las vulnerabilidades Zero-day son las más críticas, ya que no han sido descubiertas ni por desarrolladores ni reveladas públicamente, por lo que no cuentan con parches o medidas de mitigación, por lo que son codiciadas por los agentes maliciosos.

Para hacer frente a este riesgo, han surgido programas como Project Zero (Google) o Zerodium, que fomentan el descubrimiento de fallos de seguridad de manera ética.

La importancia de gestionar el riesgo

Una gestión adecuada permite la toma de decisiones informadas y sostenibles, ofreciendo beneficios como una correcta priorización de recursos, la reducción de la exposición, respuestas eficaces y el cumplimiento de normativas.

4. Panorama global de la Ciberseguridad

Los **ciberataques** dirigidos a **infraestructuras críticas** son cada vez más comunes, y el mercado global de ciberseguridad está experimentando un rápido crecimiento. La inversión en ciberseguridad ha aumentado y las normas y regulaciones evolucionan de forma constante, tratando de adaptarse a los nuevos ciberataques y ciberdelincuentes.

Tendencias globales en TIC

Hay tres tendencias principales que cuentan con un efecto significativo:

- Inteligencia Artificial (AI) y Big Data
- Cloud Computing
- Internet de las Cosas (IoT) y la tecnología 5G

Muchas tecnologías se desarrollan sin tener en cuenta las posibles amenazas cibernéticas, aumentando el riesgo de que las medidas de seguridad sean insuficientes.

Panorama global de riesgos

Los **ciberataques** sobre infraestructuras críticas son el riesgo en 5º lugar por impacto sobre la economía global en 2023, según el Foro Económico Mundial.

Debido a la interconexión digital a nivel global, mantener un estado de ciberseguridad satisfactorio se complica cada vez más, por lo que se pueden aprovechar nuevas herramientas. El aprendizaje automático y la inteligencia artificial son dos grandes ejemplos de estas nuevas ayudas, que serán imprescindibles para medir e informar mejor sobre el ciberriesgo.

Las características y la evolución del ciberespacio que contribuyen al **aumento de los ciberataques** son:

- La naturaleza distribuida de Internet.
- La capacidad de los ciberdelincuentes de atacar objetivos fuera de su jurisdicción.
- La creciente rentabilidad y facilidad de comercio en la Dark Web.
- La proliferación de dispositivos móviles y del Internet de las Cosas (IoT) en el mundo.

5. Impacto de los ciberataques en las organizaciones

Algunas de las formas en las que los ciberataques afectan a una organización son:

- **Costes económicos**: por robos de propiedad intelectual o los costes de reparación para volver al panorama anterior al ataque.
- **Coste de reputación**: un ataque puede resultar en una reducción de la confianza por parte de inversores o clientes o un menor número de clientes.
- **Costes normativos**: no cumplir con regulaciones y normativas puede acarrear multas o sanciones significativas.

U2 - Amenazas, actores y estrategias de protección

1. Grupos de actores, amenazas y dominios de la ciberseguridad

La ciberseguridad es un campo que involucra a diversos **actores** y se encuentra en varios ámbitos, como son la gestión de la seguridad de la información, la arquitectura de la seguridad de la información y los servicios de seguridad gestionados. En el centro están las **ciberamenazas**. Para prevenirlas, se emplean estrategias como el análisis de riesgos, la defensa en profundidad y la comunicación de incidentes.

Atacantes, defensores y víctimas

Los actores de las ciberamenazas son muy variados:

- **Hacktivismo**: cuenta con motivaciones variadas que suelen ser políticas, sociales o ideológicas.
- **Ciberespionaje**: es muy común en entornos industriales para obtener ventajas competitivas frente a las empresas que operan en el mismo mercado.
- **Insiders**: realizan ataques desde dentro de la empresa, ya sea por motivos financieros o de venganza.

- **Cibercrimen**: realizan ataques de forma indiscriminada con una motivación económica.
- **Ciberguerra**: con motivación política y militar, roban información estratégica, de inteligencia o buscan desestabilizar a gobiernos.
- **Ciberterrorismo**: buscan causar el pánico, por lo general con una motivación política, ideológica o propagandística.
- **Desastres naturales**: estos eventos no cuentan con un objetivo concreto por su naturaleza, pero se debe contar con estrategias para protegerse de ellos y recuperarse si ocurren.

Los vectores de ataque son las formas o medios que usan los ciberatacantes, y se clasifican en:

- Los **ataques pasivos** no modifican la información del sistema que obtienen o utilizan y suelen ser difíciles de detectar. Algunos ejemplos son:
    - Typosquatting: registro de dominios similares para engañar al usuario.
    - Phishing: envío de correos electrónicos falsos.
    - Ingeniería social: manipulación o persuasión de personas.
- Los **ataques activos** buscan alterar, degradar o destruir el sistema o sus recursos. Son más visibles, ya que provocan daños o interrupciones. Algunos ejemplos son:
    - Malware: se emplean programas maliciosos.
    - Explotación de vulnerabilidades no parcheadas: se aprovechan debilidades que no se han protegido o solucionado.
    - Suplantación del correo electrónico: se envían correos falsos desde direcciones legítimas.
    - Ataques de persona-en-el-medio (man-in-the-middle): interceptan o modifican la comunicación entre dos partes.
    - Secuestro de dominios: se redirige un dominio legítimo a otro malicioso.
    - Ransomware: se cifran datos del sistema y se pide un rescate.

Los ciberataques tienden a combinar ambos tipos de vectores para alcanzar sus objetivos. El cibercrimen usa una amplia variedad de estrategias, pero hay algunos patrones y estructuras de funcionamiento establecidas, como las **Tácticas, Técnicas y Procedimientos (TTP)**:

- Tácticas: vector con el que se busca desarrollar la actividad y alcanzar el objetivo.
- Técnicas: métodos usados para alcanzar el objetivo táctico.
- Procedimientos: pasos establecidos y preconfigurados para desplegar las técnicas y lograr el éxito.

Un **ciberataque** sigue varios pasos. Primero, el atacante identifica un objetivo potencial. Después reúne información sobre el mismo y la emplea para identificar los posibles vectores de ataque que puede emplear. Procede a acceder de forma no autorizada para obtener la información que busca o instalar código malicioso y, por último, vigila la red de la víctima para tener un flujo continuo de información o usar sus recursos informáticos.

Dominios básicos

Los esfuerzos de ciberseguridad suelen agruparse en tres dominios complementarios:

- **Gestión de la seguridad de la información**: diseña, implementa y revisa el marco de políticas, procesos y controles que garantizan la tríada CID de los datos.
- **Arquitectura de seguridad**: define la infraestructura y los mecanismos técnicos que protegen los sistemas y las redes.
- **Servicios de seguridad gestionados (MSSP)**: analizan el monitoreo y la respuesta a incidentes. aprovechando la experiencia y la escala de un proveedor especializado.

2. Procesos básicos de seguridad y gestión del riesgo

La eficacia de la ciberseguridad se basa en la interacción entre cuatro pilares fundamentales: tecnología, seguridad, operaciones y personas. Su combinación permite la construcción de una defensa sólida, proactiva y resiliente frente a ciberataques.

Procesos básicos

La ciberseguridad se estructura en una serie de **procedimientos** que garantizan la seguridad digital. Entre otros, podemos encontrar:

- **Gestión de riesgos**: evalúa los riesgos y los mantiene bajo control.
- **Control de acceso lógico a los sistemas**: asegura que sólo aquellos que deben tener acceso lo tienen, y únicamente con los permisos necesarios.
- **Ciclo de vida de seguridad del software**: se incluyen criterios de seguridad en el software desde el inicio de su desarrollo para hacerlo seguro desde el principio.
- **Monitorización y gestión de incidentes**: incluye la dirección de hackers y la obligación de trazabilidad establecida por las normativas.
- **Continuidad de negocio y contingencias tecnológicas**: estudia los procesos de negocio para seguir funcionando a pesar de sufrir un incidente.
- **Concienciación y formación**: crea una cultura de seguridad en el personal, mediante cursos, ejercicios, etc.

La **gestión de riesgos** se centra en minimizar dichos riesgos a un nivel aceptable. El primer paso es realizar un análisis de riesgos para identificarlos y cuantificarlos. Una vez completado, se estudia la mejor forma para lidiar con el riesgo que se haya encontrado, en función de las características que muestre: reducirlo, transferirlo, asumirlo o eliminarlo.

Los **ciberseguros** son una herramienta cada vez más empleada por las organizaciones y se adaptan a sus necesidades. El Instituto Nacional de Estándares y Tecnología (NIST) ha concebido un marco de ciberseguridad aceptado y validado por expertos para proporcionar una variedad de regulaciones, directrices y prácticas adecuadas. Este marco propone **cinco funciones** que cualquier organización puede adaptar para satisfacer sus necesidades:

- **Identificar (identify)**: desarrolla una comprensión organizativa de la gestión de riesgos para los diferentes elementos de la empresa.
- **Proteger (protect)**: limita o contiene el impacto de los eventos de ciberseguridad y describe las salvaguardias para prestar servicios críticos.
- **Detectar (detect)**: identifica la ocurrencia de un evento de manera oportuna.
- **Responder (respond)**: busca la minimización del impacto mediante las medidas apropiadas.

- **Recuperar (recover)**: busca mantener los planes de resiliencia y restaurar los servicios que se hayan dañado durante el incidente.

Por su parte, Gartner ha propuesto una de las mejores segmentaciones del mercado de la ciberseguridad por tecnología:

- Gestión de identidad y accesos (IAM)
- Protección de endpoints
- Seguridad de red
- Seguridad en la nube
- Gestión de vulnerabilidades y parches
- Monitorización y respuesta ante incidentes
- Protección de datos
- Ciberinteligencia

Del riesgo a la respuesta

El ecosistema tecnológico de la ciberseguridad es amplio y complejo, en respuesta a la necesidad de proteger múltiples capas. Las diversas herramientas y soluciones están diseñadas para cubrir distintas funciones y áreas, y se agrupan en dos grandes fases:

- **Pre-compromiso**: identificación y protección.
- **Post-compromiso**: detección, respuesta y recuperación.

Esta estructura funcional permite la construcción de arquitecturas de seguridad más coherentes y eficaces, alineando las tecnologías con objetivos específicos.

3. Estrategia de defensa en profundidad

La infraestructura de TI se divide en siete capas de defensa, en un intento de incrementar la resiliencia global de la organización, ya que distribuye los controles en diferentes niveles. En cada una de estas capas se aplican una serie de medidas de protección integral para mitigar los peligros asociados, así como asegurar la seguridad y el rendimiento adecuado del sistema. Las capas trabajan en conjunto: si una amenaza penetra una capa, el resto trabaja para detenerla antes de que produzca daño.

Las capas son:

- **Políticas y procedimientos**: son la base para controlar riesgos y amenazas. Se reúnen en un documento de acuerdo con la Norma ISO 27001.
- **Seguridad física**: se estructuran en tres categorías de subsistemas
    - Sistemas de control de acceso y vigilancia
    - Sistemas de videovigilancia
    - Sistemas de detección de intrusos y notificaciones.
- **Defensas perimetrales**: el perímetro es el espacio de la red interna de confianza en contacto con redes externas no fiables. Para su defensa, se emplean cortafuegos, antivirus o dispositivos debidamente protegidos, entre otros. Es la primera línea de protección entre la red interna y el exterior.
- **Defensa de red**: emplea sistemas de detección y prevención de intrusiones, segmentación de redes, cifrado de datos y protección de redes inalámbricas.
- **Defensas de host**: las tres tareas fundamentales que implica son la actualización de los parches de seguridad, la desactivación de servicios innecesarios y el mantenimiento del antivirus activo y actualizado.
- **Defensas de aplicación**: usan controles de acceso rigurosos a través de mecanismos de autenticación y autorización robustos.
- **Defensas de datos**: si una amenaza supera todo lo anterior, la autenticación y autorización, junto al cifrado, son una salvaguarda adicional.

Estrategia de confianza cero

La confianza zero o Zero Trust es un enfoque que elimina la confianza implícita, tanto dentro como fuera del perímetro de red. Se basa en el principio clave de “nunca confíes, siempre verifica”, asumiendo que toda identidad, dispositivo o conexión puede estar comprometida. Esto le lleva a exigir una validación continua antes de conceder cualquier acceso.

Un despliegue eficaz de una estrategia Zero Trust exige la integración de datos de seguridad contextuales para poder tomar decisiones informadas y contar con visibilidad permanente de todos los recursos, garantizando una detección temprana y una respuesta rápida.