ACERCA DE LOS AUTORES

DAVID GIMÉNEZ MUÑOZ

Ingeniero Técnico en Informática de Gestión por la Universidad Politécnica de Valencia. Master Universitario en Ingeniería de Sistemas e Informática por la Universidad de Zaragoza. Experto Universitario en la Gestión y Repuesta a Ciberincidentes, por la Universidad de Zaragoza. Certified Ethical Hacker (CEH) y Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) por el Centro Criptológico Nacional.

Técnico Medio Informático de Ciberseguridad, en el Área de Sistemas del Servicio de Informática y Comunicaciones de la Universidad de Zaragoza. Profesor de la asignatura de Bastionado de Redes y Sistemas del Curso de Especialización "Ciberseguridad en entornos de las Tecnologías de la Información" del Centro de FP Campus Digital y Perito Informático Judicial.

ANTONIO J. MANERO CANTÍN

Ingeniero Técnico en Informática de Sistemas por la Universidad de Zaragoza, con una sólida trayectoria como empresario y profesional en el ámbito tecnológico. A lo largo de su carrera, ha combinado roles como docente, auditor de formación y administrador de sistemas, destacando por su versatilidad y capacidad de adaptación en diversos entornos profesionales. Su experiencia abarca tanto el sector público como el privado, trabajando para la administración pública, grandes empresas de telecomunicaciones y multinacionales en áreas clave como administración de sistemas, comunicaciones, seguridad informática y formación.

Como docente, ha impartido formación técnica especializada en sistemas, transmitiendo conocimientos avanzados en informática y tecnologías de la información a centenares de personas. En su rol de auditor en formación, ha realizado evaluaciones exhaustivas de infraestructuras tecnológicas, garantizando la correcta formación a sus usuarios. Como administrador de sistemas, ha gestionado redes y servidores de alto rendimiento, implementando soluciones innovadoras para mejorar la eficiencia y la fiabilidad de las operaciones.

1

INTRODUCCIÓN AL BASTIONADO DE REDES Y SISTEMAS

1.1 CONCEPTOS BÁSICOS DE CIBERSEGURIDAD

1.1.1 Definición de ciberseguridad

La ciberseguridad se enfoca en la protección de sistemas informáticos, redes y datos impidiendo el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados. Implementando medidas de seguridad, garantizando la confidencialidad, integridad y disponibilidad de los datos. La ciberseguridad es imprescindible para reducir las amenazas, desde ataques de malware o phishing hasta ransomware.

Este objetivo se logra empleando técnicas y tecnologías diversas, como pueden ser, firewalls, sistemas de detección de intrusos (IDS/IPS), cifrado de datos o dispositivos, control de accesos, y análisis de vulnerabilidades. El desarrollo de nuevas tácticas y herramientas por parte de los ciberdelincuentes es continuo, por lo que, las organizaciones han de adoptar sistemas de defensa proactivos y adaptativos para garantizar la protección de sus activos digitales.

1.1.1.1 DIFERENCIA ENTRE SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD

En los años 60, la seguridad informática se caracterizaba por la rigidez y enfocada en la protección perimetral de un sistema monolítico. Un sistema seguro era aquel completamente aislado y desconectado del entorno, almacenado bajo múltiples capas de protección física.

En los 90, la seguridad se centraba en identificar y neutralizar amenazas conocidas aunque empezó a desarrollarse un modelo más dinámico, anticipándose y reaccionando a nuevas amenazas.

Hoy en día, se basa en enfocar de manera adaptativa y proactiva, usando tecnologías avanzadas de detección, protección y respuesta ante ataques. Siendo capaces de identificar y reducir la cantidad de amenazas en tiempo real.

La seguridad informática protege los sistemas y datos dentro de una organización mediante el uso de defensas internas. Sus herramientas son firewalls, antivirus, sistemas de detección de intrusiones (IDS). Control de acceso, uso de estándares como ISO/IEC 27001 o similares.

La ciberseguridad incluye más aspectos como es la detección temprana de amenazas en redes externas, añadiendo al análisis métodos como el uso de la inteligencia artificial, big data, técnicas de threat hunting y apoyándose en frameworks como el NIST Cybersecurity Framework, IPS, NIS2, etc.

La seguridad se centra en proteger la integridad y privacidad de la información almacenada en sistemas informáticos dentro de una organización.

La ciberseguridad abarca un espectro más amplio, protegiendo sistemas, redes y programas de ataques digitales en el ciberespacio interconectado.

La seguridad informática evoluciona hacia la "Zero Trust Architecture", mientras que la ciberseguridad se dirige hacia la "Seguridad Cuántica" y la "Inteligencia Artificial Autónoma en Ciberseguridad".

En la actualidad (año 2025), las grandes organizaciones ya sean empresariales o gubernamentales implementan una seguridad informática que elimina la diferencia entre redes internas (intranet) y redes externas (internet o acceso a otras redes de diferentes corporaciones) y simultáneamente aplican sistemas de ciberseguridad para protegerse de distintos tipos de ataques y vulnerabilidades.

- La seguridad informática se enfoca en la protección de sistemas individuales.
- La ciberseguridad abarca un enfoque más amplio, incluyendo la protección de redes y datos en el entorno digital.
- Ambas disciplinas utilizan tecnologías y herramientas complementarias.
- La ciberseguridad es una evolución de la seguridad informática, adaptada a las amenazas del mundo digital actual.

Ejemplo

- **Seguridad Informática:** instalar un antivirus en un ordenador personal, configurar un firewall en un router doméstico, realizar copias de seguridad periódicas de datos importantes.
- **Ciberseguridad:** implementar un sistema para la de detección de intrusos en una red, utilizar certificados digitales para encriptar las comunicaciones y realizar pruebas de penetración para identificar vulnerabilidades.

1.1.1.2 DETECCIÓN DE INTRUSIONES

La detección de intrusiones forma parte tanto de la seguridad informática como de la ciberseguridad, pero se asocia más directamente con la ciberseguridad.

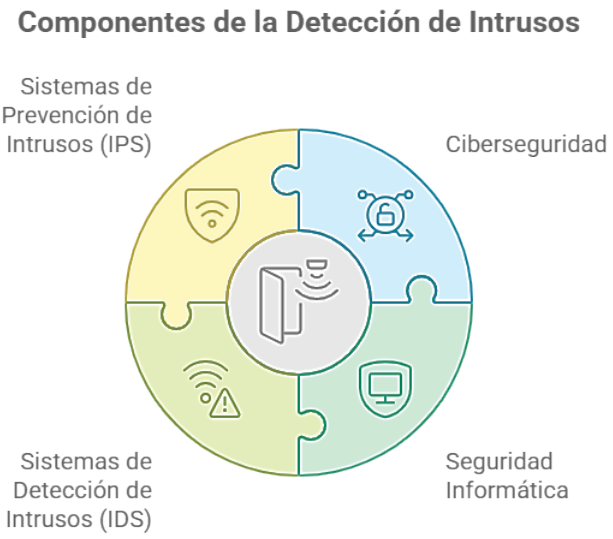
La detección de intrusiones se realiza mediante sistemas de detección de intrusos (IDS) y sistemas de prevención de intrusos (IPS), que monitorizan la red y los sistemas, identificando comportamientos sospechosos o no autorizados.

La detección de intrusos es considerada una función de la ciberseguridad, porque identifica y responde a las amenazas digitales y los ataques cibernéticos. Por contra, dado que la ciberseguridad es parte de la seguridad informática, la detección de intrusos también está incluida en la seguridad informática.

En resumen, la detección de intrusos está más estrechamente relacionada con la ciberseguridad, pero forma parte de la seguridad informática en su conjunto.

Aspecto	Seguridad Informática	Ciberseguridad
Enfoque	Sistemas y datos internos	Ecosistema digital global
Alcance	Limitado a la organización	Abarca Internet y redes interconectadas
Metodología	Reactiva, basada en reglas	Proactiva, basada en inteligencia
Tecnologías clave	Firewalls, Antivirus, IDS	AI, Big Data, Threat Intelligence
Perspectiva	Micro (sistemas individuales)	Macro (interconexiones y patrones)
Estándares	ISO/IEC 27001	NIST Cybersecurity Framework

Tabla 1.1. Tabla de diferencias entre seguridad informática y ciberseguridad



ASPECTO	SINERGIA DE SEGURIDAD INFORMÁTICA
Objetivo común	Protección de activos digitales
Evolución	Se complementan en estrategias de defensa en profundidad
Implementación	Se complementan en estrategias de defensa en profundidad
Respuesta a incidentes	Colaboración para una respuesta integral
Cumplimiento normativo	Ambas contribuyen al cumplimiento de regulaciones
Innovación	Avances en una disciplina benefician a la otra

Tabla 1.2. Tabla de sinergias entre seguridad informática y ciberseguridad

1.1.1.3 EL HACKER

Un hacker es una persona con conocimientos avanzados en programación y sistemas informáticos que explora y manipula redes y dispositivos con el fin de entender su funcionamiento interno. En el contexto de la ciberseguridad, el término puede dividirse en varias categorías, que incluyen hackers éticos, hackers maliciosos y hackers de sombrero gris. Cada uno de estos grupos actúan con diferentes intenciones y métodos, lo que subraya la complejidad y la dualidad del término.

Tipo de Hacker	Descripción	Intención
White Hat (Sombrero Blanco)	Hackers éticos que trabajan con empresas y organizaciones para mejorar su seguridad. Utilizan sus habilidades para identificar vulnerabilidades y corregirlas.	Proteger sistemas, mejorar seguridad, y realizar hacking ético.
Black Hat (Sombrero Negro)	Hackers maliciosos que buscan explotar vulnerabilidades de sistemas para obtener acceso no autorizado, robar datos o causar daños.	Robar información, dañar sistemas, o ganar dinero ilegalmente.
Grey Hat (Sombrero Gris)	Hackers que operan en un área intermedia. A veces acceden a sistemas sin autorización, pero con la intención de informar las vulnerabilidades encontradas.	Mezcla de intenciones éticas y no éticas.
Script Kiddie	Personas con pocos conocimientos técnicos que utilizan herramientas y scripts desarrollados por otros para realizar ataques básicos o vandalismos en línea.	Ganar notoriedad, realizar ataques simples o por diversión.
Hacktivista	Hackers que realizan ataques con fines políticos o sociales, buscando promover una causa o ideología mediante actos de hacking.	Promover causas políticas, sociales o ideológicas.
Cracker	Hackers especializados en romper protecciones de software, como la eliminación de protecciones de derechos de autor (DRM) o la piratería de programas.	Eliminar restricciones de software, piratería.
Phreaker	Hackers especializados en vulnerabilidades en redes de telecomunicaciones, especialmente en los sistemas telefónicos tradicionales.	Explorar y explotar sistemas de telecomunicaciones.

Tipo de Hacker	Descripción	Intención
State-Sponsored Hacker (Patrocinado por el Estado)	Hackers que trabajan para gobiernos o agencias de inteligencia para realizar ciberataques con fines de espionaje, sabotaje o defensa nacional.	Espionaje, sabotaje, o defensa a nivel estatal.
Cyberterrorista	Hackers que utilizan ciberataques como medio para causar terror o desestabilización política, social o económica.	Causar terror, desestabilización o destrucción.
Lamer	Hackers inexpertos que fingen tener habilidades avanzadas pero carecen de conocimientos técnicos profundos.	Impresionar a otros sin tener habilidades reales.
Elite Hacker	Hackers con habilidades avanzadas y conocimientos técnicos profundos, respetados dentro de la comunidad hacker por su expertise.	Avanzar en el conocimiento de la ciberseguridad o causar impacto.
Blue Hat	Hackers externos contratados por empresas para encontrar vulnerabilidades en sistemas antes de que se implementen públicamente.	Probar la seguridad de sistemas como contratista externo.
Red Hat	Hackers que actúan como "vigilantes", atacando a hackers maliciosos (Black Hat) mediante métodos agresivos para detener sus actividades.	Ataques a infraestructuras de hackers maliciosos utilizando tácticas ofensivas.
Green Hat	Novatos que buscan aprender.	Aprender y adquirir habilidades en ciberseguridad o ciberataques.

Tabla 1.3. Tabla de tipos de hacker

1.2 AMENAZA, VULNERABILIDAD, RIESGO E IMPACTO

Es fundamental comprender las diferencias y las interrelaciones entre los conceptos de amenaza, vulnerabilidad, riesgo e impacto para poder adentrarse en el estudio del bastionado de sistemas y comunicaciones.

1.2.1 Amenaza

Una amenaza es cualquier evento capaz de explotar una vulnerabilidad y causar daño a un sistema informático. Pueden manifestarse de varias formas, ataques digitales externos, fallos en la autoprotección digital, o eventos físicos como incendios o robos.

Las amenazas cibernéticas son complejas y están en constante evolución. Los ataques usan sofisticadas técnicas para explorar cualquier vulnerabilidad, conocida o no, para inutilizar, modificar y/o robar datos e información sensible.

Algunas de las amenazas o técnicas más comunes son:

- **Malware**: programas maliciosos como virus, troyanos y ransomware diseñados para infiltrarse en los sistemas y causar daños, corrupción o robo de datos que pueden incluso interrumpir el funcionamiento normal de sistemas y redes.
- **Phishing**: técnicas de ingeniería social diseñada para engañar a los usuarios para obtener información sensible, como contraseñas y datos de tarjetas de crédito, generalmente a través de correos electrónicos, mensajes de texto a los teléfonos o sitios web falsos o con poca seguridad.
- **Ingeniería social:** técnica que suele requerir de conocimientos psicológicos con el objetivo de manipular a las personas para que revelen información confidencial o realicen determinadas acciones con el fin de comprometer la seguridad de los sistemas.
- **Ataques de denegación de servicio DDoS (Distributed Denial of Service)**: Ataques que sobrecargan un sistema con tráfico en sus comunicaciones, haciéndolo inaccesible para los usuarios legítimos o haciendo que los sistemas funcionen tan lentamente que no sea viable su uso.
- **Ransomware:** es un tipo de malware que cifra los archivos de un sistema y exige un rescate para su descifrado.
- **Ataques de día cero:** explotación de vulnerabilidades en software antes de que se haya desarrollado un parche para solucionarla.
- **Ataques internos:** amenazas provenientes de empleados o contratistas con acceso a sistemas y datos de la organización.

1.2.2 Vulnerabilidad

Una vulnerabilidad es una debilidad o deficiencia en un sistema que puede ser explotada por una amenaza, comprometiendo la integridad, disponibilidad o confidencialidad de los datos.

Una vez detectadas, pueden ser mitigadas rápidamente mediante acciones correctivas. Sin embargo, mientras permanezcan activas, estas brechas aumentan el riesgo de un ciberataque.

Las vulnerabilidades son brechas en los sistemas explotadas por los ciberdelincuentes.

Las más comunes son:

- **Vulnerabilidades de software:** debilidades o errores de código de aplicaciones o sistemas operativos que los ciberdelincuentes explotan
  - Desbordamiento de búfer: cuando un programa escribe más datos en un búfer de lo que puede manejar, permitiendo la ejecución de código malicioso.
  - Inyección SQL: ejecutar consultas SQL no autorizadas que manipulan las bases de datos.
  - Cross-Site Scripting (XSS): inyección de scripts maliciosos en páginas web vistas por otros usuarios, lo que compromete la información del usuario y permite realizar acciones en su nombre.
  - Fallos de autenticación y autorización: permitiendo a usuarios no autorizados acceder a recursos restringidos.
- **Vulnerabilidades de configuración:** si los sistemas, aplicaciones o dispositivos no están correctamente programados o configurados pueden dejar expuestos ventanas de ataque.
  - Puertos abiertos innecesarios: puertos que no son necesarios para la operación de un sistema pero que están abiertos y pueden ser explotados para ataques.
  - Configuraciones predeterminadas que no se han cambiado: el uso de las contraseñas predeterminadas o que vienen de fábrica por defecto o configuraciones iniciales que son conocidas y fácilmente explotables.
  - Permisos excesivos: accesos no restringidos que permiten a cualquier usuarios poder realizar acciones no autorizadas.
  - Falta de cifrado: transmisión o almacenamiento de datos sin un cifrado, lo que facilita el robo de información.
- **Vulnerabilidades de red:** explotando errores en la infraestructura de red o en su configuración hace que los atacantes puedan manipular el tráfico de red.
  - Ataques de intermediario (Man-in-the-Middle): Interceptación de la comunicación entre dos partes para espiar, modificar o robar datos transmitidos.
  - Sniffing de redes: captura de tráfico de red para obtener información confidencial como credenciales de usuario o datos sensibles.
  - Ataques de denegación de servicio (DoS/DDoS): Saturación de un servicio con tráfico malicioso para hacerlo inaccesible a usuarios legítimos.

- **Vulnerabilidades de seguridad física:**
  - Vulnerabilidades que permiten el acceso físico no autorizado a equipos o instalaciones, comprometiendo la seguridad de los sistemas y datos.
  - Acceso físico no autorizado a servidores: Personas no autorizadas que logran acceder físicamente a los servidores, pudiendo manipular o extraer datos directamente.
  - Dispositivos: Pérdida o robo de dispositivos que contienen información, como laptops o discos duros no cifrados.
  - Falta de controles de acceso físico: El no tener mecanismos que restringir el acceso no autorizado a determinadas áreas, salas o centros de datos.
- **Vulnerabilidades de recursos humanos:** errores humanos, negligencias o acciones de sabotaje por parte de los empleados.
  - Ingeniería social: técnicas para manipular a personas y obtener información sensible o accesos no autorizados.
  - Phishing: envío de correos electrónicos fraudulentos.
  - Contraseñas débiles o compartidas: fáciles de adivinar o que se comparten entre empleados.
- **Vulnerabilidades de gestión de seguridad:** falta de políticas, procedimientos y controles que gestionen la seguridad de los datos.
  - Ausencia de un plan de respuesta a incidentes
  - Políticas de seguridad desactualizadas.
  - Falta de auditorías de seguridad.
- **Vulnerabilidades de terceros y suministro:** riesgos asociados con el uso de servicios, software o hardware de terceros.
  - Dependencia de software de terceros con vulnerabilidades conocidas
  - Ataques en la cadena de suministro
  - Proveedores que no cumplen con los protocolos de seguridad

1.2.3 Riesgo

El riesgo es la probabilidad de que una amenaza aproveche una vulnerabilidad para atacar un sistema. En otras palabras, el riesgo es la posibilidad de que una amenaza se materialice y cause daño, aprovechando una vulnerabilidad no detectada o no resuelta.

La gestión de riesgos implica identificar, evaluar y mitigar las vulnerabilidades de un sistema para reducir la probabilidad de un ataque exitoso.

1.2.4 Impacto

Son las consecuencias o efectos que un incidente de seguridad, vulnerabilidad o ataque tiene sobre los activos, la confidencialidad, integridad y disponibilidad de la información, además de su operativa, reputación.

Su evaluación puede ser en términos cualitativos y cuantitativos, dependiendo de las métricas que se usen para medir las pérdidas o daños.

Concepto	Definición	Ejemplos
Amenaza	Posibilidad de que un evento o acción pueda explotar una vulnerabilidad.	Malware, Phishing, DoS, APT, errores humanos, desastres naturales.
Vulnerabilidad	Debilidad o falla en un sistema que puede ser explotada por una amenaza, comprometiendo la seguridad.	Fallos de diseño, configuraciones incorrectas, errores en el software, falta de actualizaciones.
Riesgo	Probabilidad de que una amenaza se materialice y cause daño, aprovechando una vulnerabilidad.	Riesgo de un ataque ransomware debido a sistemas no parcheados, riesgo de phishing por falta de formación.
Impacto	Consecuencias de un incidente de seguridad.	Financiero en caso de ransomware, Confidencialidad y reputación

Tabla 1.4. Tabla resumen de conceptos

1.3 PRINCIPIOS FUNDAMENTALES DE LA CIBERSEGURIDAD

Los principios fundamentales de la ciberseguridad son:

1.3.1 Confidencialidad

Garantiza que los datos son accesibles únicamente por las personas o dispositivos autorizados. Se basa en el control riguroso del acceso y la implementación de mecanismos de autenticación y autorización. De esta forma se protege la información sensible a la exposición no autorizada y se asegura que sólo individuos o entidades con autorización puedan acceder a ellos.

1.3.2 Integridad

Garantiza que la información y los sistemas no son modificados sin autorización, empleando técnicas de control de versiones, sumas de verificación y mecanismos de auditoría que detectan y previenen manipulaciones o alteraciones no autorizadas o controles de cambio. Asegura que la información y los sistemas no sean alterados por partes no autorizadas. De esta forma garantizamos que dicha información no ha sido manipulada.

1.3.3 Disponibilidad

Los sistemas y los datos siempre han de ser accesibles para los usuarios autorizados. Hay que asegurar que los recursos estén operativos y accesibles sin interrupciones inesperadas.

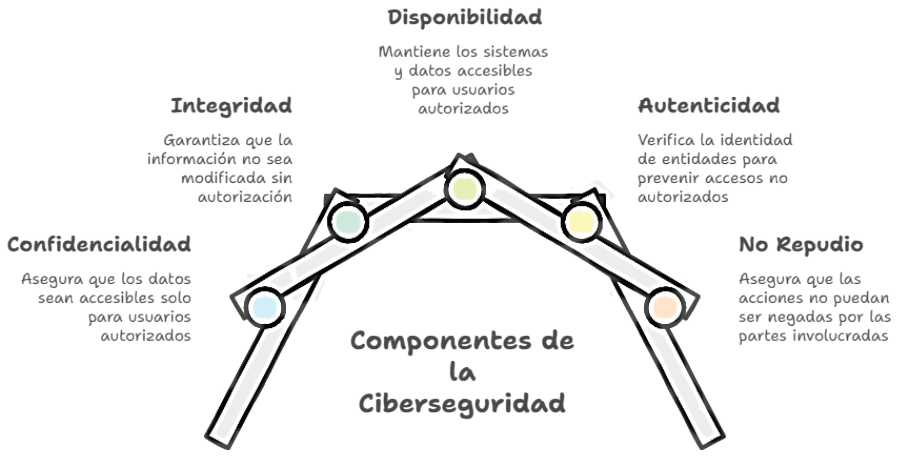
Los principios de confidencialidad, integridad y disponibilidad son la base de la ciberseguridad.

1.3.4 Autenticidad

La autenticidad garantiza que una entidad (persona, dispositivo o sistema) es quien dice ser, verificando su identidad de manera confiable. En el contexto de ciberseguridad, se logra mediante mecanismos como contraseñas, certificados digitales, tokens, autenticación multifactor (MFA) o biometría. Este principio asegura que solo las entidades legítimas y autorizadas puedan interactuar con los sistemas o datos, previniendo accesos fraudulentos o suplantaciones de identidad. Por ejemplo, en el bastionado de redes, un sistema de autenticación robusto (como un firewall con autenticación de usuarios) asegura que solo los usuarios verificados puedan acceder a recursos protegidos.

1.3.5 No repudio

El no repudio asegura que una acción, transacción o comunicación no pueda ser negada por las partes involucradas, garantizando que se pueda probar quién realizó una acción y qué acción se llevó a cabo. En ciberseguridad, se implementa mediante mecanismos como firmas digitales, registros de auditoría (logs) y certificados electrónicos que vinculan de forma inequívoca una acción a una entidad específica. Por ejemplo, en el bastionado de sistemas, el no repudio es clave para rastrear accesos o cambios en la red, asegurando que un usuario no pueda negar haber realizado una operación, como la modificación de un archivo o el acceso a un sistema crítico.



1.4 TIPOS DE ATAQUES CIBERNÉTICOS

Existen varios tipos de ataques, cada uno con métodos y objetivos diferentes. Algunos ejemplos incluyen:

- **Ataques de fuerza bruta**: intentos repetidos de adivinar contraseñas mediante combinaciones posibles.
- **Ataques de inyección SQL**: explotan vulnerabilidades en aplicaciones web para ejecutar comandos SQL maliciosos.
- **Ataques de hombre en el medio (MitM)**: interceptan y alteran la comunicación entre dos partes sin que estas se den cuenta.
- **Cross-Site Scripting (XSS):** inyecta scripts maliciosos en sitios web confiables, que luego se ejecutan en el navegador de la víctima.
- **Ataque de intermediario (Evil Twin)**: crea un punto de acceso Wi-Fi falso para interceptar el tráfico de red de las víctimas.

Ejemplos:

El ataque de ransomware WannaCry en 2017 afectó a miles de organizaciones en todo el mundo, cifrando datos y demandando pagos para su liberación.

En 2018 un ataque a las infraestructuras de la red eléctrica de Ucrania dejó sin servicio de luz a gran parte de la población.

En septiembre de 2024 en el contexto de un enfrentamiento bélico se hizo explotar simultáneamente miles de buscapersonas y walkie talkie.

1.5 IMPORTANCIA DEL BASTIONADO

1.5.1 Bastionado o “hardening”

Proviene del ámbito militar y hace referencia al refuerzo o fortificación de una estructura defensiva. En el contexto de la seguridad informática, se refiere a fortalecer sistemas, redes y dispositivos para reducir su vulnerabilidad ante ataques y amenazas externas. Es un proceso diseñado para fortalecer y proteger accesos no autorizados y ataques. Su objetivo principal es establecer una barrera defensiva robusta que impida la explotación de vulnerabilidades minimizando los riesgos que comprometen sistemas, comunicaciones y datos.

Contiene una serie de medidas que buscan reducir la exposición a amenazas al eliminar o mitigar las debilidades potenciales en la infraestructura tecnológica. Contribuye a crear un entorno más seguro.

1.5.2 Bastionado de sistemas

Es la implementación de medidas de seguridad específicas de sistemas hardware, sistemas operativos y aplicaciones para protegerlos contra accesos no autorizados, malware y otras amenazas. Esto incluye la configuración segura de servidores, estaciones de trabajo.

Ejemplos de prácticas en el bastionado de sistemas:

- Acceso a configuraciones hardware.
- Aplicación de parches y actualizaciones de seguridad.
- Deshabilitación de servicios y puertos innecesarios.
- Configuración de políticas de contraseñas seguras y autenticación multifactor.
- Monitorización y registro de actividades del sistema.
- Formación de los usuarios finales.

1.5.3 Bastionado de redes

Protección y securización de la infraestructura de red, lo que incluye routers, switches, firewalls, particionados de redes, uso de VLAN y otros dispositivos de comunicación, controlando y asegurando el flujo de tráfico de datos y previniendo los accesos no autorizados.

Ejemplos de prácticas en el bastionado de redes:

- Configuración de firewalls y otros dispositivos que filtran el tráfico no autorizado.
- Utilización de redes privadas virtuales (VPN) para asegurar las comunicaciones.
- Segmentación de la red para limitar el acceso a recursos críticos.
- Implementación de sistemas de detección y prevención de intrusiones (IDS/IPS).

1.5.4 Bastionado de dispositivos

El bastionado de dispositivos se centra en asegurar dispositivos individuales, como computadoras portátiles, smartphones, y dispositivos IoT. La idea es configurar estos dispositivos de manera que se minimicen sus vulnerabilidades, asegurando que solo ejecuten aplicaciones y servicios seguros.

Ejemplos de prácticas en el bastionado de dispositivos:

- Configuración segura y bloqueo de dispositivos no utilizados.
- Control de acceso mediante políticas de autenticación robustas.
- Cifrado de datos almacenados y en tránsito.
- Monitorización del comportamiento del dispositivo para detectar actividades sospechosas.

Aspecto	Bastionado de Sistemas	Bastionado de Redes	Bastionado de Dispositivos	Coincidencias
Objetivo Principal	Proteger sistemas operativos, datos y aplicaciones.	Proteger la infraestructura de red.	Proteger dispositivos individuales.	Reducir vulnerabilidades y proteger contra amenazas.
Ámbito de Aplicación	Servidores, estaciones de trabajo, software.	Routers, switches, firewalls, infraestructura de red.	Computadoras portátiles, smartphones, IoT, etc.	Involucra la configuración segura y control de acceso.
Técnicas y Herramientas	Parches, configuración de servicios, políticas de contraseñas.	Firewall, VPN, IDS/IPS, segmentación de red.	Encriptación, autenticación, monitoreo de dispositivos.	Todos utilizan herramientas de configuración y monitoreo.
Enfoque de Seguridad	Seguridad a nivel de sistema operativo y software.	Control del tráfico y acceso en la red.	Seguridad del hardware y software en dispositivos.	Prevención y detección de amenazas es fundamental.
Configuración y Mantenimiento	Actualización y revisión de sistemas y software.	Configuración y revisión de dispositivos de red.	Configuración y actualización de dispositivos.	Requieren mantenimiento continuo y monitoreo constante.

Tabla 1.5. Tabla de comparación: bastionado de sistemas, redes y dispositivos

Esta tabla muestra las diferencias y similitudes entre el bastionado de sistemas, redes y dispositivos, indicando que aunque se aplican en diferentes niveles, todos son esenciales para mantener la seguridad.

1.5.5 Beneficios del bastionado

- **Prevención de accesos no autorizados**: proteger sistemas y comunicaciones contra intrusiones y accesos no autorizados.
- **Protección de datos**: conservar la integridad y confidencialidad de la información.
- **Reducción del área de un posible ataque:** al minimizar los puntos de entrada potenciales, se disminuye el riesgo de un ataque exitoso y en el caso de que el ataque sea exitoso, este afecte al menor número de sistemas posible.
- **Detección temprana de amenazas:** usar sistemas de monitorización y alertas permiten la detección, identificación y respuesta rápida ante incidentes de seguridad.
- **Cumplimiento normativo:** cumplir con las regulaciones relacionadas con los datos ayuda a su seguridad.
- **Protección de la reputación:** sin incidentes de seguridad la organización protege y aumenta su reputación fortaleciendo la confianza entre socios y clientes.

Ejemplos de incidentes:

- En mayo del 2024 en España, una entidad bancaria emite un informe en el que reconoce que ha sufrido una filtración de datos de clientes y empleados, aunque asegura que no se trata de credenciales para acceder desde internet y operar en las cuentas de sus clientes.
- El FBI alerta a una empresa de logística de ser objetivo de un posible ataque cibernético a nivel mundial y concretamente a una de sus subcontratas por DDos. La subcontrata reacciona actualizando y mejorando sus sistemas de seguridad, colaborando además para poder localizar quiénes y desde donde se realizan el ciberataque.

1.5.5.1 IMPACTO ECONÓMICO Y REPUTACIONAL

La falta de bastionado lleva a pérdidas financieras significativas debido a robos de datos, fraudes y multas por incumplimiento. Además, este tipo de incidentes dañan gravemente la reputación de una organización, generando pérdida de confianza de clientes, socios y posibles inversores.

1.6 PRINCIPIOS DE LA ECONOMÍA CIRCULAR EN LA INDUSTRIA 4.0

1.6.1 Definición de economía circular

Es un modelo de producción y consumo que promueve la reutilización, recuperación, reciclaje y renovación de materiales y productos existentes, buscando maximizar la reutilización de los recursos naturales y reducir la generación de diferentes tipos de residuos.

Este modelo puede ampliarse en:

- **Aumento de la vida útil de los dispositivos**: haciendo el mantenimiento y realizando las actualizaciones continuas del software y del hardware.
- **Reducción del desperdicio electrónico**: reciclando y reutilizando los componentes tanto tecnológicos como electrónicos.
- **Virtualización:** consolidando sistemas físicos en servidores virtuales, reduciendo tanto el consumo de energía como el espacio físico utilizado.

Prácticas sostenibles

- **Reutilización de hardware**: reacondicionar equipos antiguos y no desecharlos.
- **Eficiencia energética**: optimizar el consumo de energía en los centros de datos y sistemas informáticos.
- **Reciclaje de componentes**: establecer programas de reciclaje de dispositivos electrónicos e intentar darles una segunda vida.

Legislación actual

- **Unión Europea**: la Directiva de Residuos de Aparatos Eléctricos y Electrónicos (WEEE) establece normas para la gestión de residuos electrónicos.
- **Internacional**: normas ISO como la ISO 14001 que establece un marco para la gestión ambiental efectiva.

1.7 LA SEGURIDAD "ZERO TRUST" (CONFIANZA CERO)

Este modelo de seguridad se basa en "nunca confiar, siempre verificar". Considera que todos los usuarios, tanto internos como externos son amenazas. Por eso cada intento de acceso a cualquier recurso ha de ser autenticado, autorizado y monitorizado continuamente.

- Verificación continua de la identidad y contexto de los usuarios y los dispositivos, independientemente de su ubicación.
- Asegurar el entorno mediante una segmentación de la red.
- Autenticación robusta.
- Control de acceso.

La implementación de Zero Trust permite una defensa proactiva, adaptativa y exhaustiva contra amenazas.

La adopción de la seguridad Zero Trust no constituye una tarea puntual, sino un trabajo constante.

Ejemplo:

- Para IBM es fundamental en entornos de nube híbrida. Incluye segmentación de la red, control de acceso basado en roles y autenticación multifactorial. Así no solo protege la red, sino que también proporciona una protección continua y adaptada a las amenazas emergentes.
- Palo Alto Networks amplía esta visión: se basa la identidad y contexto. Inspecciona y registra todo el tráfico, tanto interno como externo en tiempo real. También se centra en la microsegmentación, permitiendo un control granular de accesos y minimizando el número de sistemas que pueden ser atacados.

1.8 GHERRAMIENTAS WEB DE MONITORIZACIÓN DE ATAQUES CIBERNÉTICOS EN TIEMPO REAL

Revisar webs que monitorizan ciberataques en tiempo real, es una gran ayuda para mantener una seguridad robusta y proactiva.

Proporcionan una visión general y actualizada de ataques a nivel mundial que pueden permitir la identificación de patrones de ataque emergentes y evaluar las amenazas en tiempo real.

Con esta monitorización se puede detectar rápidamente intentos de intrusión, evaluar su impacto potencial y anticipar y ajustar las estrategias defensivas para mitigar los riesgos de un posible ataque.

No solo permite una respuesta rápida ante incidentes, también ayuda a prevenir ataques al fortalecer las medidas de seguridad preventivas.

La vigilancia, la monitorización constante y la información en tiempo real son necesarias para proteger los activos digitales y garantizar la integridad, confidencialidad y disponibilidad de los sistemas.

Nombre	URL	Descripción
Kaspersky Cybermap	cybermap.kaspersky.com	Muestra un mapa interactivo en tiempo real con datos sobre ataques cibernéticos globales detectados por Kaspersky.
Bitdefender Global Threat Map	https://threatmap.bitdefender.com/	Mapa interactivo que visualiza ataques cibernéticos detectados por Bitdefender en tiempo real.
Check Point ThreatCloud Map	https://threatmap.checkpoint.com/	Ofrece un mapa global de amenazas en tiempo real, con datos sobre ataques y actividades maliciosas detectadas por Check Point.
Javier Ripoll's Cyberattack Map	*javierripoll.es*	Proporciona enlaces a diversas herramientas y mapas que muestran ataques cibernéticos en tiempo real.

Tabla 1.6. Tabla de sistemas de monitorización global

1.9 LEGISLACIÓN Y NORMAS EUROPEA Y ESPAÑOLA EN CIBERSEGURIDAD

1.9.1 Legislación

Son conjunto de leyes, regulaciones y normas que establece la autoridad competente, como el poder legislativo de un país, una región o una entidad gubernamental. Tienen la función de regular la conducta y las relaciones de los individuos y organizaciones dentro de una jurisdicción específica. Cubren derechos y deberes de los ciudadanos y organizaciones, procedimientos judiciales, normas de seguridad, regulación de actividades económicas y sociales y un largo etcétera.

Características clave de la legislación:

- **Normativa obligatoria:** las leyes y regulaciones establecidas por la legislación son obligatorias y deben ser cumplidas por todos los sujetos a su jurisdicción.
- **Autoridad legal:** es creada y promulgada por entidades con autoridad legislativa, como parlamentos, congresos, asambleas legislativas o autoridades locales.
- **Protección y orden:** tiene como objetivo mantener el orden social, proteger los derechos individuales y colectivos, y establecer las normas para la convivencia en sociedad.
- **Procedimiento formal:** la creación y modificación de la legislación sigue un procedimiento formal y estructurado, que puede incluir debates, votaciones y revisiones.

- **Aplicación y cumplimiento:** las leyes son aplicadas y supervisadas por las autoridades competentes, como organismos judiciales y agencias gubernamentales, que se encargan de asegurar su cumplimiento.

La legislación es esencial para la estructura y funcionamiento de cualquier sociedad, proporciona un marco legal que regula el comportamiento de los individuos y organizaciones, protege los derechos, y mantiene el orden y la justicia.

Legislación / Código	Jurisdicción	Descripción
España: Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD)	España	Regula la protección de datos personales en España, incluyendo derechos digitales como el derecho al olvido.
España: Ley de Seguridad Nacional (LSN)	España	Establece el marco para la protección de la seguridad nacional, incluyendo la ciberseguridad.
Unión Europea: Reglamento General de Protección de Datos (GDPR)	UE	Regula la protección de datos personales en todos los países de la UE, estableciendo requisitos estrictos para la gestión de datos.
Unión Europea: Directiva NIS2 (Network and Information Systems Directive)	UE	Establece normas para la seguridad de las redes y sistemas de información en la UE, ampliando el alcance y los requisitos de la Directiva NIS original.

Tabla 1.7. Tabla ejemplo de legislaciones sobre seguridad IT

1.9.2 Normas

Regla o directriz indica cómo deben comportarse las personas y las organizaciones en una sociedad. Son principios fundamentales que regulan el comportamiento social y aseguran el orden, la justicia y la equidad dentro de una jurisdicción específica.

Características Clave de una Norma Legal:

- **Generalidad:** las normas legales se aplican a todas las personas o situaciones que se encuentren dentro de su ámbito de aplicación. No están dirigidas a individuos específicos sino a grupos o categorías de personas.
- **Obligatoriedad:** tienen carácter obligatorio. El incumplimiento puede resultar en sanciones o consecuencias legales.
- **Autoridad:** son emitidas por una autoridad con capacidad legal, como el legislativo (parlamentos o asambleas), el ejecutivo (gobernantes) o el judicial (tribunales).

- **Normativa:** definen derechos, deberes y procedimientos, estableciendo claramente lo que se permite, prohíbe o exige.
- **Sanciones:** medidas correctivas que se aplican en caso de incumplimiento.
- **Adaptabilidad:** pueden ser modificadas, derogadas o reemplazadas mediante procedimientos legales establecidos, permitiendo su adaptación a cambios en las condiciones sociales, económicas o tecnológicas.

Norma	Descripción	Ámbito de Aplicación
NIST SP 800-53	Recomendaciones para la gestión de riesgos de seguridad en sistemas de información.	Estados Unidos, aplicable a agencias federales y sus contratistas.
GDPR (Reglamento General de Protección de Datos)	Regulación de protección de datos personales en la Unión Europea.	Unión Europea, aplicable a todas las entidades que procesan datos personales de residentes en la UE.
CIS Controls	Conjunto de controles de seguridad recomendados para la protección de sistemas informáticos.	Global, adoptado por organizaciones para mejorar su postura de seguridad.

Tabla 1.8. Tabla ejemplo de normativas

1.9.3 Normas ISO

Una norma ISO (Organización Internacional de Normalización) es un estándar internacional que establece especificaciones, directrices y/o características para asegurar que los productos, servicios y/o sistemas sean seguros, eficientes y de calidad. Son desarrolladas por la Organización Internacional de Normalización, entidad no gubernamental y no vinculante que trabaja para establecer estándares internacionales aceptados globalmente.

Características**:**

- **Consenso internacional:** elaboradas mediante un consenso entre expertos y partes interesadas de diferentes países. Intenta que se reflejen las mejores prácticas y necesidades globales.
- **Requisitos técnicos:** definen especificaciones técnicas y requisitos para productos, servicios y o sistemas, abarcando distintos aspectos como la calidad, seguridad, eficiencia y rendimiento.
- **Mejora continua:** fomentan la mejora continua proporcionando directrices y mejores prácticas.

- **Aplicabilidad global:** pueden ser adaptadas a las regulaciones y requisitos locales.
- **Documentación y publicación:** son publicadas como documentos oficiales y se actualizan periódicamente.

Objetivos:

- **Uniformidad y compatibilidad:** aseguran que los productos y servicios cumplan con estándares internacionales.
- **Seguridad y protección:** establecen requisitos que garantizan la seguridad y protección en diversas áreas como la ciberseguridad.
- **Eficiencia y mejora:** promueven prácticas eficientes y efectivas que permiten a las organizaciones mejorar su desempeño y calidad.
- **Confianza del cliente:** mejora la confianza del cliente en los productos y servicios.

Una norma ISO proporciona un marco estandarizado para asegurar que los productos, servicios y/o sistemas sean de alta calidad y cumplan con requisitos internacionales, beneficiando tanto a las organizaciones como a los consumidores.

Norma ISO	Descripción	Objetivo
ISO/IEC 27001	Norma para sistemas de gestión de seguridad de la información (SGSI).	Establecer, implementar, mantener y mejorar un SGSI para proteger la confidencialidad, integridad y disponibilidad de la información.
ISO/IEC 27002	Directrices para la implementación de controles de seguridad de la información.	Proporcionar directrices para la selección, implementación y gestión de controles de seguridad de la información.
ISO/IEC 27005	Directrices para la gestión de riesgos de seguridad de la información.	Ofrecer un enfoque sistemático para la gestión de riesgos de seguridad de la información.
ISO/IEC 27017	Directrices para la seguridad de la información en la nube.	Proporcionar recomendaciones específicas para la seguridad en servicios de computación en la nube.
ISO/IEC 27018	Directrices para la protección de datos personales en la nube.	Establecer directrices para la protección de datos personales en servicios de computación en la nube.
ISO/IEC 27019	Seguridad de la información para los sistemas de control industrial.	Ofrecer directrices para la gestión de la seguridad de la información en sistemas de control industrial.

Norma ISO	Descripción	Objetivo
ISO/IEC 27032	Directrices para la ciberseguridad.	Proporcionar un marco para la gestión de la ciberseguridad, cubriendo aspectos técnicos, organizacionales y de protección.
ISO/IEC 27033	Seguridad en redes.	Ofrecer directrices para la implementación de medidas de seguridad para redes de comunicación.
ISO/IEC 27034	Seguridad de las aplicaciones.	Establecer un marco para integrar la seguridad en el ciclo de vida del desarrollo de aplicaciones.
ISO/IEC 27035	Gestión de incidentes de seguridad de la información.	Proporcionar directrices que detectan, reportan y responden a incidentes de seguridad de la información.
ISO/IEC 27037	Directrices para la identificación, recolección, adquisición y preservación de evidencias digitales.	Proporcionar directrices para la gestión forense de la evidencia digital en investigaciones de incidentes de seguridad.
ISO/IEC 27038	Técnicas de filtrado de datos para la protección de datos.	Ofrecer directrices para el uso de técnicas de filtrado de datos para proteger la información confidencial.
ISO/IEC 29100	Marco de privacidad de la información.	Proporcionar un marco para proteger la privacidad de la información personal y gestionar los riesgos asociados.
ISO/IEC 29101	Arquitectura de privacidad.	Establecer una arquitectura de privacidad para la gestión de la privacidad de la información en sistemas y servicios.
ISO/IEC 29134	Evaluación de impacto en la protección de datos personales.	Ofrecer directrices para realizar evaluaciones de impacto sobre la protección de datos personales y sus implicaciones.

Tabla 1.9. Tabla resumen de algunas normas orientadas a ciberseguridad