AES FUNDACIÓN

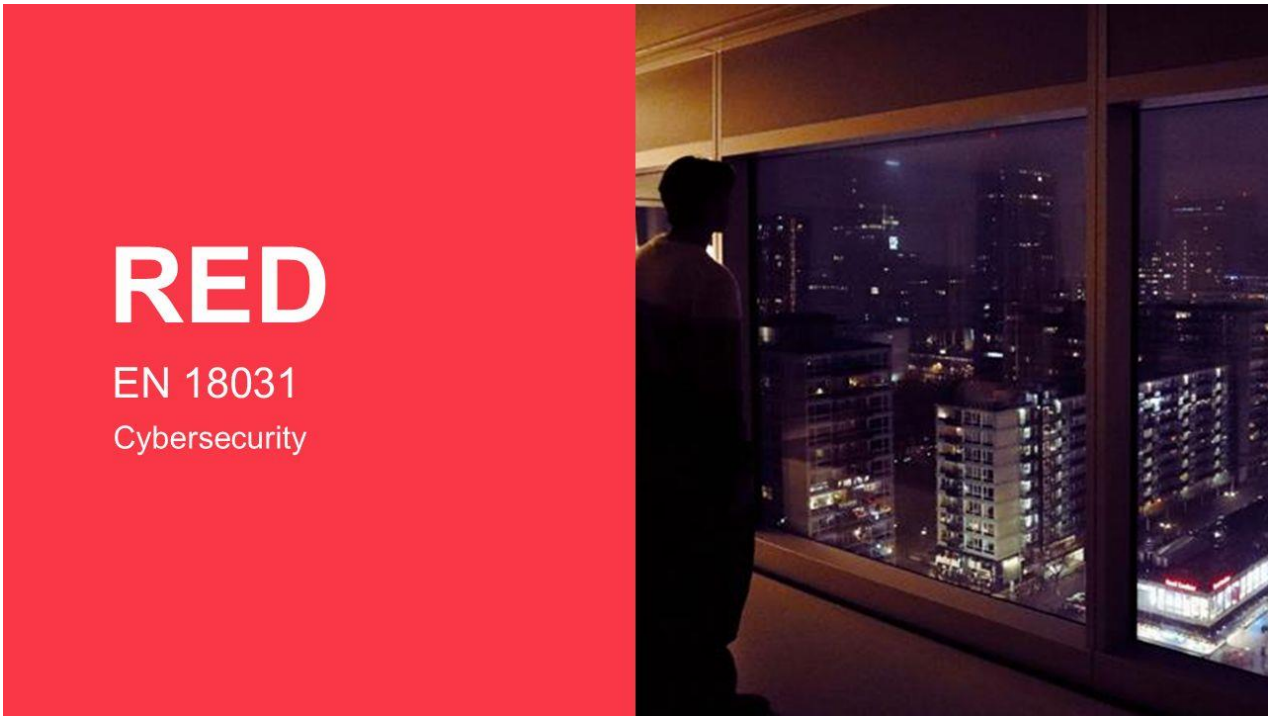
Guía de buenas prácticas en las tecnologías de la comunicación

INDICE

Guía de buenas prácticas en las tecnologías de la comunicación

Elaborada por el Área de Trabajo de Ciberseguridad de AES

Nombre	Empresa	Papel en la elaboración de la guía
Pablo Carmona Rebollo	ELECNOR SISTEMAS	Coordinador / Redactor
Laura Alcazar	IQSIGHT	Redactora
Alberto Alonso	AXIS	Redactor
Ricardo Cañizares	AES FUNDACION	Redactor
Antonio Gómez	ILUNION Seguridad	Redactor / Revisor
Jorge Noguerales	PROSEGUR	Redactor
Oscar Téllez	PYCSECA	Redactor



Presentación

En la Industria de la Seguridad en España y como asociación decana, AES siempre ha desarrollado un papel vital. Representamos a nuestro país tanto en los Comités Nacionales y Europeos donde se crean las normas como en las dos principales asociaciones europeas como son Eurosafe y Euralarm. Todo ello es posible gracias a la dedicación y conocimiento de nuestros expertos pertenecientes a las diferentes Áreas de Trabajo que disponemos. La información es poder y por supuesto vital para la competitividad de nuestras empresas asociadas. El compromiso social es parte de nuestro ADN y para ello creamos continuamente guías, recomendaciones y publicaciones desde donde transmitimos nuestro conocimiento. En nombre de toda la Junta Directiva de AES esperamos que disfrutes de este trabajo que con tanto cariño hemos realizado.

Iñigo Ugalde Blanco –Presidente de AES.

Después de muchos meses de trabajo y dedicación, el 27 de junio de 2024 quedó registrada AES FUNDACIÓN en el Registro Nacional de Fundaciones. Uno de los objetivos establecidos para la Fundación es la difusión de los documentos elaborados por las áreas de trabajo de AES.

Es por ello por lo que todas las publicaciones de nuestras áreas de trabajo (ya tenemos incorporadas varias guías que puedes consultar sin coste en Publicaciones AES Fundación así como la Newsletter y el Boletín, han empezado a aparecer con el color naranja distintivo de la Fundación, y en el caso de Newsletter y Boletín, con una nueva numeración de segunda época.

Todo ello forma parte del desarrollo #UniversoAES y #HaciendoIndustria. Espero que esta nueva publicación que os traemos hoy sirva de ayuda y siga contribuyendo con nuestra propuesta de valor **“dinamizando la seguridad ciudadana**”

Antonio Escamilla Recio –Presidente de AES FUNDACIÓN.

Presentación

El área de trabajo de ciberseguridad de la Asociación Española de Empresas de Seguridad (AES) viene desarrollando de forma continuada iniciativas orientadas a reforzar la protección de los sistemas de información y comunicaciones utilizados por las organizaciones del sector, así como de aquellos sistemas electrónicos que diseñan, implantan y mantienen para la prestación de servicios de seguridad.

En un contexto marcado por la creciente digitalización y la interconexión de los sistemas, la seguridad de las comunicaciones se ha convertido en un elemento estratégico y esencial. La transformación de los sistemas tradicionales hacia entornos basados en redes IP y plataformas digitales ha incrementado significativamente la superficie de exposición a los riesgos cibernéticos, haciendo necesario adoptar un enfoque integral de protección.

Como parte de este compromiso con la seguridad de la sociedad, y en línea con los principios recogidos en los diferentes manifiestos y líneas de actuación de AES, se presenta esta “Guía de buenas prácticas en las tecnologías de la comunicación”, elaborada por el área de trabajo de ciberseguridad.

Este documento pretende establecer un marco de referencia común que permita a las organizaciones mejorar la protección de sus comunicaciones técnicas, garantizando la confidencialidad, la integridad y la disponibilidad de la información crítica.

Esta guía aborda de forma estructurada los principales aspectos que condicionan la seguridad de las comunicaciones en los sistemas electrónicos de seguridad, incluyendo el análisis del flujo de información y los riesgos asociados, la aplicación de buenas prácticas tecnológicas, el uso de herramientas avanzadas como la inteligencia artificial, la relevancia del factor humano, así como la necesidad de implantar procesos de auditoría y mejora continua.

Merece especial atención el papel de las personas dentro de la seguridad de las comunicaciones. Tal y como se destaca en esta publicación, el factor humano constituye uno de los elementos más determinantes en la gestión de los ciberriesgos, por lo que la formación, la concienciación y el establecimiento de procedimientos claros resultan fundamentales para fortalecer la resiliencia de las organizaciones.

Asimismo, la guía incide en la importancia de adoptar medidas técnicas robustas, tales como el cifrado de las comunicaciones, la correcta gestión de identidades y accesos, el bastionado de dispositivos, la segmentación de redes y la implantación de arquitecturas resilientes que permitan garantizar la continuidad operativa frente a incidentes.

Presentación

Este documento es fruto del trabajo colaborativo de profesionales de diferentes organizaciones del sector, aportando una visión práctica, actualizada y alineada con las necesidades reales de las empresas de seguridad. Su objetivo es servir como herramienta de apoyo para la toma de decisiones, facilitando la implantación de medidas efectivas que contribuyan a la protección de las personas, los bienes y la información.

Desde el área de trabajo de ciberseguridad de AES, se continuará impulsando iniciativas de divulgación, formación y desarrollo de guías específicas que ayuden a las organizaciones a adaptarse a un entorno cada vez más complejo, marcado por la evolución constante de las amenazas y por la exigencia de cumplimiento normativo.

La ciberseguridad de las comunicaciones no es únicamente una cuestión técnica, sino un compromiso colectivo que requiere la implicación de todos los niveles de la organización ya que, solo mediante la combinación de tecnología, procesos y personas será posible construir entornos digitales seguros y resilientes.

Porque, en definitiva, la seguridad de las comunicaciones es responsabilidad de todos.

Antonio Jesús Gómez Pérez

Coordinador del área de trabajo de ciberseguridad

1. Objeto de la Guía

El presente documento tiene como propósito fundamental establecer un marco de referencia unificado que defina los principios, criterios y procedimientos necesarios para mitigar los riesgos cibernéticos en las comunicaciones técnicas de las empresas.

En un contexto donde la convergencia digital es absoluta, esta guía busca dotar a las organizaciones de las herramientas necesarias para proteger el flujo de información crítico, garantizando la seguridad no solo de la infraestructura física, sino de todo el ecosistema digital que la sustenta.

Los objetivos específicos que persigue esta guía son:

- Garantizar la Tríada de la Ciberseguridad: Asegurar que todas las comunicaciones técnicas cumplan con los principios de Confidencialidad (evitando interceptaciones), Integridad (previniendo la alteración de datos) y Disponibilidad (asegurando la continuidad operativa).
- Estandarización de la Protección Técnica: Proveer directrices claras para la implementación de medidas robustas, incluyendo protocolos de cifrado, gestión segura de credenciales y estrategias de recuperación ante desastres.
- Aseguramiento de Dispositivos (Hardening): Establecer prácticas de bastionado para reducir la superficie de ataque en equipos y sistemas, enfatizando la eliminación de servicios innecesarios y la actualización constante de firmware y software.
- Adaptación a Nuevas Tecnologías: Orientar sobre el uso seguro de plataformas de gestión centralizada (PSIM), herramientas en la nube y la integración responsable de la Inteligencia Artificial para la detección y gestión automatizada de amenazas.

- Fortalecimiento del Factor Humano y la Mejora Continua: Concienciar sobre el rol crítico de las personas en la cadena de seguridad, promoviendo la formación contra la ingeniería social y estableciendo una cultura de auditoría constante y simulacros de incidentes.

En definitiva, el objeto de esta guía es transformar la seguridad de las comunicaciones en un activo estratégico, reduciendo la vulnerabilidad ante amenazas como la interceptación de datos o el robo de credenciales, y asegurando la resiliencia operativa de los servicios de seguridad privada.

2. El flujo de información y los riesgos cibernéticos

La transformación digital ha convertido a los sistemas de seguridad física en dispositivos de red interconectados. Entender cómo fluyen los datos entre sensores, cámaras, paneles de control y centros de monitoreo es el primer paso para protegerlos. Este capítulo analiza la exposición de estas infraestructuras y define los pilares fundamentales para su protección1.

2.1. El panorama de amenazas en las comunicaciones

En el entorno actual, la seguridad de la información no es un añadido, sino un requisito funcional. El flujo de información entre los dispositivos de campo (cámaras, sensores, …) y los centros de control transita a menudo por redes compartidas o públicas, exponiendo a las empresas de seguridad a riesgos que van más allá del sabotaje físico.

Para proteger eficazmente estas comunicaciones, es imperativo identificar y comprender los tres vectores de ataque principales que comprometen la operativa de seguridad: la interceptación de datos, el robo de credenciales y la ingeniería social.

Interceptación de Datos (Sniffing y Man-in-the-Middle)

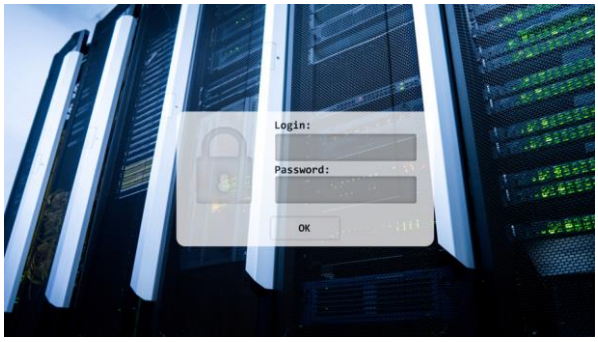
La interceptación ocurre cuando un actor malicioso se infiltra en el canal de comunicación para "escuchar" o capturar la información que se transmite entre dos puntos.

- En qué consiste: Mediante técnicas de sniffing (rastreo de paquetes), un atacante conectado a la misma red puede leer datos que viajan sin cifrar (texto plano). En ataques más sofisticados, como el Man-in-the-Middle (MitM), el atacante se interpone activamente entre el dispositivo de seguridad y el servidor, pudiendo no solo leer, sino modificar los datos.
- Impacto en Sistemas de Seguridad:
    - Visualización no autorizada: Acceso a transmisiones de vídeo en tiempo real de cámaras IP no cifradas, comprometiendo la privacidad del cliente.
    - Lectura de tramas: Obtención de códigos de usuario o estados de alarma transmitidos por paneles de intrusión antiguos o mal configurados.

Robo de Credenciales

El compromiso de las claves de acceso representa una de las vías más directas para que los ciberdelincuentes tomen el control de los sistemas de seguridad.

- En qué consiste: Los atacantes obtienen nombres de usuario y contraseñas legítimas. Esto suele lograrse mediante ataques de fuerza bruta (probar combinaciones masivamente), el uso de keyloggers (software que registra pulsaciones de teclado) o, frecuentemente, explotando la mala práctica de mantener las contraseñas predeterminadas de fábrica.



- Impacto en Sistemas de Seguridad:
  - Sabotaje remoto: Un atacante con credenciales de administrador en un VMS o una CRA puede desactivar grabaciones, silenciar alarmas o borrar registros de auditoría para ocultar actividades delictivas físicas.
  - Secuestro de dispositivos: Incorporación de cámaras y grabadores a botnets (redes de equipos zombies) para lanzar ataques masivos a terceros.

Ingeniería Social

A diferencia de los ataques técnicos, la ingeniería social se dirige al "factor humano", explotando la confianza o el error de los empleados para vulnerar la seguridad.

- En qué consiste: Se basa en la manipulación psicológica. Los métodos más comunes incluyen el phishing (correos electrónicos fraudulentos que suplantan a proveedores o directivos) y el vishing (llamadas telefónicas engañosas). El objetivo es inducir al personal a revelar información confidencial o ejecutar acciones inseguras.
- Impacto en Sistemas de Seguridad:
  - Acceso indebido: Un operador de CRA o un técnico de campo podría ser engañado para facilitar el acceso remoto a una instalación crítica bajo el pretexto de una "urgencia técnica" o "soporte del fabricante".
  - Infección de la red: Descarga de malware o ransomware en la red corporativa al abrir adjuntos infectados (ej. "Factura_Pendiente.pdf"), paralizando la capacidad de respuesta de la empresa.

2.2. Confidencialidad, Integridad y Disponibilidad: La Tríada de la Ciberseguridad

Para gestionar con eficacia los riesgos descritos anteriormente, la industria de la seguridad adopta el modelo de referencia universalmente conocido como la Tríada CID (Confidencialidad, Integridad y Disponibilidad). Estos tres principios no son conceptos abstractos, sino requisitos funcionales que deben cumplirse en cualquier

transmisión de señales técnicas, desde un salto de alarma hasta una secuencia de videovigilancia.

La aplicación de estos principios a las comunicaciones técnicas se define de la siguiente manera:

Confidencialidad

Garantiza que la información solo sea accesible y legible por personas o sistemas debidamente autorizados. En el contexto de la seguridad privada, la confidencialidad es sinónimo de privacidad y secreto profesional.

- El Riesgo: Si la comunicación no es confidencial, un tercero podría visualizar las cámaras de un cliente, obtener planos de la instalación descargados de la nube o acceder a listas de códigos de usuario.
- Aplicación Técnica: Se logra principalmente mediante el cifrado de datos en tránsito (VPNs, HTTPS) y en reposo. Esto asegura que, aunque un atacante intercepte los paquetes de datos de un sistema de CCTV, no podrá visualizar las imágenes sin la clave de descifrado correspondiente.

Integridad

Asegura que la información es veraz y no ha sido alterada, modificada o corrompida (ni de forma accidental ni malintencionada) durante su transmisión o almacenamiento.

- El Riesgo: La falta de integridad pone en duda la evidencia. Un atacante podría interceptar una señal de vídeo y reemplazarla por un bucle de imágenes pregrabadas (ataque de replay) para ocultar una intrusión en tiempo real, o modificar los registros (logs) de un control de accesos para borrar su rastro.
- Aplicación Técnica: Se implementa mediante el uso de firmas digitales y funciones hash que validan la autenticidad del origen de los datos. En videovigilancia, el watermarking (marca de agua digital) es esencial para garantizar la validez legal de las imágenes ante un tribunal, demostrando que no han sido manipuladas.

Disponibilidad

Garantiza que los sistemas, la red y la información estén operativos y accesibles en el momento en que se necesitan. En seguridad electrónica, este es a menudo el factor más crítico: de nada sirve una cámara de alta resolución si la señal no llega a la CRA durante un robo.

- El Riesgo: La interrupción del servicio. Los ataques de Denegación de Servicio (DDoS), el corte físico de cables, el jamming (inhibición de radiofrecuencia) o simplemente un fallo en un router, pueden dejar una instalación "ciega" y "sorda", impidiendo la comunicación de eventos de alarma.
- Aplicación Técnica: Se asegura mediante la redundancia (doble vía de comunicación: Ethernet + 4G/5G), sistemas de alimentación ininterrumpida (SAI/UPS), segmentación de redes para evitar saturaciones y planes de recuperación ante desastres.

2.3. La red como esqueleto de la comunicación

En la era de la seguridad IP, la red de datos ya no es un mero accesorio, sino el esqueleto que sostiene y da vida a toda la infraestructura de seguridad. Sin una red robusta y segura, los dispositivos más avanzados de CCTV o control de accesos pierden su eficacia.

Este apartado analiza la exposición inherente a las infraestructuras de comunicación actuales y la necesidad crítica de estructurarlas adecuadamente mediante la segmentación y el monitoreo.

Análisis de la exposición de las redes corporativas

Tradicionalmente, los sistemas de seguridad operaban en circuitos cerrados aislados (CCTV analógico). Hoy en día, la convergencia tecnológica ha llevado a que cámaras, grabadores y paneles de control compartan a menudo la misma infraestructura de red que los ordenadores de administración, impresoras y el Wi-Fi de empleados.

Esta red plana (sin divisiones) genera una superficie de exposición crítica:

- Movimiento Lateral: Si un atacante infecta un ordenador de recepción a través de un correo de phishing, y la red no está segmentada, el malware puede desplazarse lateralmente hasta alcanzar el servidor de vídeo o la central de alarmas conectada al mismo switch.
- Saturación de Tráfico: El tráfico masivo de datos no críticos (descargas, streaming de empleados) puede saturar el ancho de banda, provocando latencia o pérdida de paquetes en las transmisiones de vídeo de seguridad o señales de alarma prioritarias.

La necesidad de Segmentación

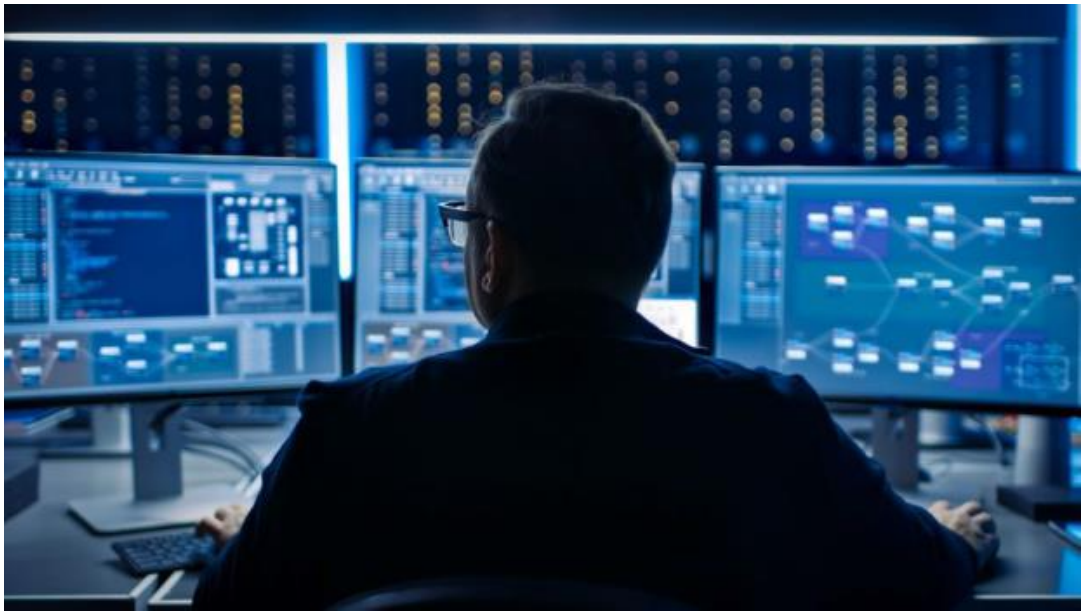
Para mitigar la exposición, es imperativo implementar una arquitectura de red segmentada. La segmentación consiste en dividir la red física en múltiples redes lógicas (VLANs - Virtual Local Area Networks) que actúan como compartimentos estancos.

- Aislamiento de Tráfico: Los sistemas de seguridad deben residir en una VLAN exclusiva, separada lógica y funcionalmente de la red corporativa y de las redes de invitados. De este modo, un incidente de seguridad en la red de oficinas no comprometerá la integridad de los sistemas de seguridad física.
- Control de Acceso (ACLs): La segmentación permite aplicar Listas de Control de Acceso, definiendo reglas estrictas sobre quién puede hablar con quién (por ejemplo, permitir que el VMS vea las cámaras, pero bloquear que las cámaras intenten conectarse a internet o a otros servidores).

La necesidad de Monitoreo

La seguridad de la red no es estática; requiere una vigilancia continua. Implementar herramientas de monitoreo es esencial para detectar comportamientos anómalos antes de que se conviertan en incidentes críticos.

- Visibilidad de la Red: Los administradores deben tener capacidad para visualizar qué dispositivos están conectados y cuánto ancho de banda consumen.
- Detección de Anomalías: El monitoreo permite identificar patrones sospechosos, como una cámara IP que intenta comunicarse con una dirección IP externa desconocida en horario nocturno, lo cual podría indicar una infección o un intento de exfiltración de datos.



3. Buenas prácticas en el uso de tecnologías de comunicación

Protección de la información y los datos: principios, riesgos y soluciones

3.1. Introducción

La información es uno de los activos más valiosos en la era digital. Desde datos personales hasta secretos empresariales, su protección es fundamental para garantizar la privacidad, la confianza y la continuidad operativa.

La protección de datos no solo implica evitar accesos no autorizados, sino también asegurar su integridad, disponibilidad y correcto uso a lo largo de todo su ciclo de vida.

¿Qué entendemos por protección de la información?

La protección de la información consiste en aplicar medidas técnicas y organizativas para evitar accesos no autorizados, alteraciones indebidas y pérdida o destrucción de datos

Este concepto abarca tanto datos digitales como físicos, e incluye procesos de almacenamiento, transmisión y procesamiento.

3.2. Principios fundamentales

La seguridad de la información se basa en tres principios clave:

- Confidencialidad: Garantiza que solo las personas autorizadas puedan acceder a la información.
- Integridad: Asegura que los datos no han sido modificados sin autorización.
- Disponibilidad: Permite que la información esté accesible cuando se necesita.

3.3. Riesgos y amenazas más comunes

Las organizaciones se enfrentan a una variedad de riesgos y amenazas que pueden comprometer la integridad, confidencialidad y disponibilidad de los datos. Uno de los riesgos más importantes son las fugas de datos, que ocurren cuando información sensible es expuesta, ya sea de forma accidental o intencionada.

La ingeniería social se ha convertido en una de las técnicas más empleadas por ciberdelincuentes. Consiste en manipular a personas para obtener información

confidencial, utilizando estrategias como el phishing, el pretexting o el spoofing. Estos métodos aprovechan la vulnerabilidad humana, ya que muchas veces los atacantes se hacen pasar por entidades legítimas para ganarse la confianza y acceder a recursos sensibles.

Por otro lado, el malware y el ransomware representan amenazas tecnológicas especialmente peligrosas. El malware abarca una amplia variedad de programas maliciosos diseñados para infiltrarse en sistemas informáticos, robar información, o causar daños. El ransomware, en particular, cifra los datos de la víctima y exige un rescate para su liberación, lo que puede interrumpir operaciones críticas y generar pérdidas económicas significativas. La evolución constante de estas amenazas exige una protección proactiva y actualizada.

Finalmente, los errores humanos siguen siendo una de las principales causas de incidentes de seguridad. Acciones como el uso de contraseñas poco seguras, la divulgación involuntaria de datos por correo electrónico, o la falta de atención al abrir enlaces sospechosos, facilitan la tarea de los atacantes. La formación continua y la concienciación sobre buenas prácticas de seguridad resultan esenciales para reducir estos riesgos y fortalecer la protección de los sistemas y la información.

3.4. Técnicas y herramientas de protección

Existen diversas técnicas y herramientas, como el cifrado y el control de accesos, que garantizan la seguridad de la información, asegurando que solo personas autorizadas puedan acceder o modificar los datos.

Cifrado de datos: El cifrado transforma la información en un formato ilegible para cualquier persona que no disponga de la clave adecuada. Esta técnica puede aplicarse tanto a los datos almacenados (en reposo) como a los datos que se transmiten a través de redes (en tránsito), garantizando así la confidencialidad y seguridad de la información frente a accesos no autorizados.

Control de accesos: El control de accesos determina quién puede consultar o modificar determinada información. Para ello, se utilizan mecanismos de autenticación, que verifican la identidad de los usuarios, y de autorización, que establecen los permisos necesarios para acceder a recursos específicos. De este modo, se asegura que solo las personas autorizadas puedan realizar determinadas acciones sobre los datos.

3.5. Protocolos de cifrado en comunicaciones

El cifrado se basa en una combinación de criptografía simétrica y asimétrica, optimizada para garantizar confidencialidad, integridad y autenticación en entornos distribuidos.

Arquitectura criptográfica en tránsito

En protocolos como TLS 1.3, en el establecimiento de sesión se utiliza un modelo híbrido:

- Intercambio de claves: basado en ECDHE (Elliptic Curve Diffie-Hellman Ephemeral), proporcionando *Perfect Forward Secrecy (PFS)*.
- Autenticación: mediante certificados X.509 emitidos por autoridades de certificación (CA).
- Cifrado simétrico: algoritmos como AES-GCM o ChaCha20-Poly1305 para eficiencia y seguridad.

Este enfoque reduce la exposición frente a ataques de descifrado retroactivo, incluso si se comprometen claves a largo plazo.

VPN y encapsulación segura

Las VPN utilizan protocolos robustos como los siguientes:

- IPsec (ESP mode): cifrado y autenticación a nivel de red, con IKEv2 para negociación segura de claves.
- WireGuard: protocolo basado en criptografía de última generación (Curve25519, ChaCha20), con menor superficie de ataque.
- OpenVPN: basado en TLS, altamente configurable pero más complejo.

El cifrado se aplica mediante encapsulación de paquetes, evitando inspección profunda (DPI) por actores no autorizados.

Cifrado en entornos cloud

Los proveedores de servicios de almacenamiento y procesamiento en la nube como Amazon Web Services, Microsoft Azure y Google Cloud Platform implementan modelos avanzados:

- Envelope Encryption: claves de datos cifradas con claves maestras (KMS/HSM).
- Customer Managed Keys (CMK) vs Provider Managed Keys (PMK)
- Hardware Security Modules (HSM): almacenamiento seguro de claves con certificación FIPS 140-2/3.

Además, se integran mecanismos de confidential computing, donde los datos permanecen cifrados incluso en memoria.

3.6. Gestión de credenciales: autenticación fuerte e identidad digital

La gestión de identidades se basa en el paradigma IAM (Identity and Access Management) y en modelos de confianza cero (*Zero Trust Architecture*).

Autenticación multifactor avanzada

La autenticación multifactor avanzada (MFA) se encuentra en proceso de evolución hacia modelos resistentes al phishing como los siguientes:

- TOTP (Time-Based One-Time Password): basado en RFC 6238
- FIDO2 / WebAuthn: autenticación sin contraseña (*passwordless*), basada en criptografía asimétrica
- Push authentication: validación contextual en dispositivos confiables

Aplicaciones como Google Authenticator o Microsoft Authenticator implementan TOTP, mientras que llaves físicas (YubiKey) usan FIDO2.

3.7. Gestión de identidades y control de acceso

Los sistemas de gestión de identidades y control de acceso (IAM) implementan protocolos como los siguientes:

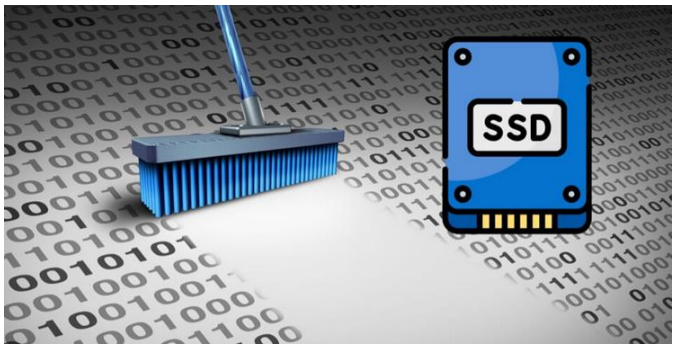
- RBAC (Role-Based Access Control)
- ABAC (Attribute-Based Access Control)
- Principio de mínimo privilegio (PoLP)
- Just-In-Time Access (JIT)

En conjunción con protocolos de federación, que permiten delegar el proceso de autenticación entre sistemas distribuidos, de estos protocolos podemos citar los siguientes:

- SAML 2.0
- OAuth 2.0
- OpenID Connect (OIDC)

3.8. Protección contra amenazas emergentes

Las amenazas emergentes representan un desafío constante, ya que evolucionan rápidamente y adoptan nuevas formas para vulnerar sistemas y datos. Es fundamental anticipar estos riesgos y desplegar mecanismos de defensa que permitan proteger de manera



proactiva la infraestructura y las cuentas de personas usuarias. Entre las amenazas más relevantes se encuentran aquellas que explotan credenciales filtradas, técnicas avanzadas de phishing y el secuestro de sesiones, cada una con características propias que requieren estrategias específicas de mitigación

- **Credential stuffing:** Esta amenaza consiste en el uso masivo de combinaciones de usuario y contraseña obtenidas de filtraciones previas para intentar acceder a sistemas de forma automatizada. Para mitigar este riesgo se ha implementado la autenticación multifactor (MFA), que añade una capa adicional de seguridad, y técnicas de rate limiting que restringen la frecuencia de intentos de acceso, dificultando los ataques automatizados.
- **Phishing avanzado:** Los atacantes emplean métodos sofisticados para engañar a las personas usuarias y obtener credenciales o información sensible. La adopción de soluciones como FIDO2 permite una autenticación sin contraseña, eliminando la vulnerabilidad asociada al robo de credenciales vía phishing y reforzando la protección contra intentos de suplantación.
- **Session hijacking:** El secuestro de sesiones implica la captura o manipulación de tokens de sesión para acceder a cuentas legítimas. Para contrarrestar este tipo de ataques se utilizan tokens firmados, que garantizan la integridad y autenticidad de la sesión, así como mecanismos de rotación periódica de sesiones, dificultando la explotación de sesiones robadas y limitando el tiempo de exposición ante posibles incidentes.

3.9. Copias de seguridad (backups) y recuperación ante desastres (DR/BCP)

Permiten recuperar datos ante pérdidas o ataques, para ello se deben realizar copias periódicas y utilizar almacenamiento externo o en la nube

La resiliencia de los sistemas depende de arquitecturas diseñadas bajo principios de tolerancia a fallos y continuidad operativa.

Estrategias avanzadas de backup

Más allá del modelo 3-2-1, se adoptan enfoques como:

- Backups inmutables (immutable backups): protegidos contra modificación (WORM storage)
- Snapshots incrementales: optimización de almacenamiento
- Air-gapped backups: aislados físicamente o lógicamente de la red

Esto es crítico frente a ransomware que intenta cifrar o eliminar copias de seguridad.

Arquitecturas de alta disponibilidad

- Active-Active: múltiples nodos operativos simultáneamente
- Active-Passive: failover automático ante fallo
- Geo-redundancia: replicación entre regiones

Proveedores cloud como AWS y Azure ofrecen:

- Replicación síncrona y asíncrona
- Multi-AZ (Availability Zones)
- Cross-region disaster recovery

Métricas críticas a tener en cuenta

- **RTO** (Recovery Time Objective): tiempo máximo de recuperación
- **RPO** (Recovery Point Objective): pérdida máxima de datos tolerable

En entornos críticos (finanzas, salud), estos valores tienden a ser cercanos a cero.

Planificación y automatización

Un Disaster Recovery Plan (DRP) efectivo debe incluir, procedimientos documentados y testados regularmente, automatización mediante infraestructura como código (IaC) y simulaciones de desastre (*chaos engineering*).

En los entornos actuales, la protección de datos no puede abordarse de forma aislada. La convergencia entre criptografía avanzada, gestión de identidades y resiliencia operativa define el estado del arte en ciberseguridad.

El enfoque actual se basa en asumir compromiso (*assume breach*) y diseñar sistemas capaces de resistir ataques, detectar anomalías y recuperarse sin pérdida crítica

Buenas prácticas esenciales

- Usar contraseñas robustas y únicas
- Activar autenticación multifactor
- Mantener sistemas actualizados
- Minimizar los datos recolectados
- Aplicar el principio de “mínimo privilegio”
- Cifrar información sensible

3.10. Seguridad de los dispositivos y sistemas:

3.10.1. **Hardening (bastionado) de equipos:** eliminación de servicios innecesarios y uso de protocolos seguros**.**

El bastionado o endurecimiento (hardening) de dispositivos de seguridad electrónica es un proceso clave para proteger la infraestructura de una organización frente a amenazas internas y externas. Los equipos como cámaras de vigilancia (CCTV, tanto IP como analógicas), NVR/DVR, paneles de alarmas, controladores de acceso, intercomunicadores IP y sistemas de intrusión, entre otros, requieren controles específicos para garantizar su integridad y disponibilidad.

A continuación, se detallan una serie de recomendaciones de bastionad, estructuradas por áreas clave, orientadas a reducir riesgos y fortalecer la seguridad de dispositivos de seguridad electrónica.

Gestión de credenciales y autenticación

- Deshabilitar cuentas de fábrica o servicios de soporte que no se utilicen, para evitar accesos no autorizados.
- Eliminar o deshabilitar cuentas por defecto (admin, root, 888888, etc.) siempre que el fabricante lo permita, minimizando la superficie de ataque.
- Implantar políticas de contraseñas robustas: longitud mínima de 12 caracteres, combinación de letras, números y símbolos, y caducidad periódica para prevenir el uso de credenciales comprometidas.
- Activar autenticación multifactor (MFA) si el dispositivo lo soporta, añadiendo una capa adicional de protección.
- Limitar el número de usuarios y asignar privilegios mínimos necesarios, evitando la proliferación de cuentas con altos permisos.
- Configurar el bloqueo de cuentas tras varios intentos fallidos y limitar las sesiones simultáneas para reducir el riesgo de ataques por fuerza bruta.
- Deshabilitar el acceso anónimo a servicios como ONVIF, RTSP u otros, asegurando que solo usuarios autenticados puedan acceder.
- En sistemas que usan aplicaciones móviles, exigir registros seguros y prohibir el uso compartido de credenciales, garantizando trazabilidad y control.

Actualización y gestión del firmware

- Mantener el firmware actualizado con los parches y actualizaciones proporcionados por el fabricante, para corregir vulnerabilidades conocidas.
- Descargar firmware únicamente desde fuentes oficiales, evitando riesgos asociados a software malicioso.
- Desactivar actualizaciones automáticas sin control, pero implantar un proceso regular de revisión y actualización para mantener la seguridad.
- Gestionar el ciclo de vulnerabilidades revisando mensualmente los boletines del fabricante y suscribiéndose a servicios de notificación si están disponibles.
- Verificar el hash del firmware antes de instalarlo, asegurando la autenticidad e integridad del software.
- Documentar fechas, versiones y responsables de cada actualización para mantener un historial detallado y facilitar auditorías.
- Programar ventanas de mantenimiento que minimicen la indisponibilidad de sistemas críticos durante las actualizaciones.

3 Buenas prácticas en el uso de tecnologías de la comunicación

Segmentación y arquitectura de red

- Evitar exponer dispositivos directamente a Internet, reduciendo la posibilidad de ataques remotos.
- Colocar los dispositivos en redes segmentadas, utilizando VLAN específicas para sistemas de seguridad.
- Restringir la comunicación únicamente a servidores de grabación, sistemas de monitorización, servidores de autenticación y plataformas de gestión autorizadas

Configuración de red segura

- Deshabilitar protocolos inseguros como Telnet, HTTP, SNMPv1/v2, FTP y ONVIF no seguro.
- Activar protocolos seguros: HTTPS con certificados (preferentemente generados por la CA corporativa), SSH y SNMPv3 para monitorización.
- Forzar el uso de TLS 1.2 o superior donde sea posible, asegurando la protección de datos en tránsito.
- Establecer listas de control de acceso (ACLs) en switches y firewalls para limitar el acceso solo a IPs de administración autorizadas.
- Deshabilitar funciones automáticas como UPnP, NAT transversal y P2P cloud, salvo que sean imprescindibles y seguras.

Bastionado de servicios y funciones

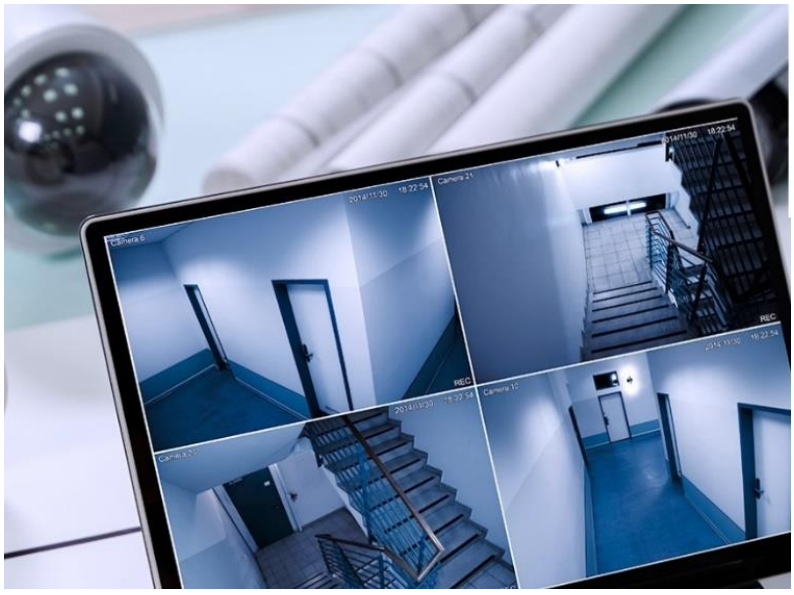
- Deshabilitar funciones innecesarias como audio, P2P, Wi-Fi o cloud propietario si no se utilizan, eliminando posibles vectores de ataque.
- Activar alarmas o alertas ante intentos de acceso no autorizado, permitiendo una respuesta rápida ante incidentes.
- Revisar y desactivar puertos físicos no necesarios (USB, microSD, audio) para evitar la manipulación directa.
- Deshabilitar el envío automático de datos a servicios en la nube del fabricante, la gestión remota no controlada y servicios broadcast innecesarios como LLDP o ONVIF discovery si no se usan.
- Configurar retención limitada de logs, cumpliendo con la normativa de privacidad y protección de datos.
- Habilitar notificaciones de alertas ante reinicios inesperados, pérdida de comunicación, cambios de configuración y accesos administrativos.

Monitorización, auditoría y registros

- Logs de eventos de seguridad: registrar intentos fallidos, accesos exitosos y cambios de usuarios para detectar posibles brechas.
- Logs de integridad: monitorizar reinicios, cambios en firmware y restauraciones de configuración.
- Logs de red: documentar desconexiones de dispositivos, fallas de enlace y errores de autenticación en SNMP.
- Logs operativos: registrar fallas en discos duros, saturación de almacenamiento y caídas de cámaras.
- Integrar los equipos con un SIEM o plataforma de monitorización central, como Syslog, para centralizar la gestión de eventos.
- Configurar la hora mediante NTP seguro (NTS), preferiblemente interno, para mantener la sincronización y trazabilidad de los registros.
- Activar una retención mínima de 90 días de logs, según la normativa aplicable y las necesidades de auditoría.

Seguridad física de los dispositivos

- Ubicar grabadores, paneles o controladores en racks cerrados con control de acceso físico para dificultar el acceso no autorizado.
- Utilizar anclajes anti-manipulación o domos antivandálicos en cámaras accesibles, protegiendo los equipos ante intentos de sabotaje.
- Desactivar botones físicos de reset o protegerlos bajo cubierta mecánica si el fabricante ofrece esa opción.
- Proteger rutas de cableado para evitar sabotaje o extracción de información.
- Deshabilitar puertos USB o tarjetas si no son necesarios, evitando la introducción de dispositivos externos.



Respaldo, recuperación y continuidad

- Realizar backups automáticos de la configuración de cada dispositivo al menos una vez por semana para garantizar la recuperación ante incidentes.
- Probar la restauración regularmente, asegurando la funcionalidad de los procedimientos de emergencia.
- Cifrar las copias de seguridad y almacenarlas en un repositorio seguro con control de acceso restringido.
- Conservar un inventario de versiones para poder revertir cambios fallidos rápidamente.
- Documentar procedimientos de recuperación rápida ante fallos de hardware, corrupción de firmware o pérdida de comunicación.

Inventario, documentación y gobernanza

- Mantener un inventario centralizado que incluya modelo, serie, versión de firmware, dirección IP, ubicación física, nivel de criticidad y responsable de cada dispositivo.
- Documentar parámetros clave como la topología de red, puertos y protocolos utilizados, y políticas de retención de video o auditorías.
- Establecer un procedimiento formal de alta y baja de dispositivos, asegurando el control durante todo el ciclo de vida.

Evaluación de proveedores y cadena de suministro

- Verificar que el fabricante indique la fecha de fin de soporte del dispositivo, ciclos regulares de parches, SBOM (lista de software de terceros incluido en el dispositivo), certificaciones de seguridad y transparencia en la gestión de vulnerabilidades (PSIRT).
- Evitar equipos sin soporte o con firmware obsoleto, priorizando la adquisición de dispositivos actualizados.

- Revisar contratos para garantizar actualizaciones durante la vida útil del dispositivo, protegiendo la inversión y la seguridad de la infraestructura.

La aplicación de estas recomendaciones de bastionado contribuye a una protección integral de los dispositivos de seguridad electrónica, minimizando riesgos y reforzando la resiliencia de la infraestructura. Es fundamental adaptar estas medidas a la realidad de cada organización, realizar revisiones periódicas y mantener una cultura de seguridad activa entre las personas responsables técnicas y operativas.

3.10.2. Actualización de sistemas: la importancia de mantener el software y el firmware al día para corregir vulnerabilidades.

Una de las acciones más eficaces a la hora de proteger los sistemas de comunicaciones consiste en la actualización periódica del software y el firmware. Esta práctica no solo mejora el rendimiento, sino que también es clave para prevenir riesgos derivados de posibles vulnerabilidades.

Para facilitar la implementación de buenas prácticas, se adjunta un checklist de ejemplo que puede servir como guía para verificar y asegurar la correcta actualización de los sistemas.

Checklist para dispositivos de Seguridad Electrónica	
Credenciales y Autenticación	
☐	Se cambiaron todas las contraseñas por defecto.
☐	Se eliminaron o deshabilitaron cuentas predeterminadas del fabricante.
☐	Las contraseñas cumplen con políticas de complejidad (≥12 caracteres).
☐	MFA habilitado (si aplica).
☐	Límite de intentos fallidos configurado.
☐	Sin acceso anónimo en ONVIF, RTSP u otros servicios.
☐	Usuarios con privilegios mínimos requeridos.
Firmware y Actualizaciones	
☐	El firmware está actualizado.
☐	Se verifica integridad (hash) antes de actualizar.
☐	Solo se usan firmwares oficiales del fabricante.
☐	Hay un registro de versiones y fechas de actualización.
☐	Existe un proceso periódico de revisión de vulnerabilidades.
Seguridad de Red	
☐	Dispositivos aislados en VLAN dedicada.
☐	No hay exposición directa a Internet.

Checklist para dispositivos de Seguridad Electrónica	
☐	Se deshabilitaron protocolos inseguros (Telnet, HTTP, FTP, SNMP v1/v2).
☐	Se usa HTTPS/TLS 1.2+, SSH y/o SNMPv3.
☐	Se aplican ACLs para acceso desde IPs autorizadas.
☐	UPnP, NAT transversal y P2P están deshabilitados (si no se usan).
☐	NTP configurado con servidor seguro interno.
Bastionado del Dispositivo	
☐	Servicios innecesarios desactivados (audio, cloud, Wi-Fi, ONVIF discovery, etc.).
☐	Puertos físicos no usados deshabilitados (USB, microSD, audio).
☐	Logs configurados (tiempo de retención, nivel de detalle).
☐	Alertas habilitadas para cambios críticos y fallos.
☐	Certificados actualizados y válidos (si aplica).
Monitorización y Auditoría	
☐	Integración con SIEM o Syslog
☐	Revisión periódica de logs de seguridad.
☐	Sincronización horaria correcta (NTP).
☐	Se monitorizan fallos de red, almacenamiento, reinicios y cambios de configuración.
Seguridad Física	
☐	Equipos ubicados en rack o gabinete cerrado.
☐	Protección contra manipulación en cámaras accesibles.
☐	Botones de reset inaccesibles o protegidos.
☐	Cableado protegido contra sabotaje.
Respaldo y Continuidad	
☐	Configuraciones respaldadas periódicamente.
☐	Backups cifrados y almacenados de forma segura.
☐	Procedimientos de restauración documentados y probados.

Checklist para dispositivos de Seguridad Electrónica	
☐	Inventario de versiones para revertir cambios fallidos.
Inventario y Documentación	
☐	Inventario actualizado de todos los dispositivos (modelo, IP, firmware, SBOM, fecha límite de soporte, ubicación, responsable).
☐	Topología documentada.
☐	Parámetros de configuración documentados.
☐	Procedimientos formales de alta y baja de dispositivos.
Proveedor y Cadena de Suministro	
☐	El fabricante publica parches de forma regular.
☐	El fabricante publica o facilita la fecha límite de soporte de actualizaciones.
☐	Los dispositivos no están al final de su vida útil (EOL, fecha límite de soporte).
☐	Revisión de seguridad del fabricante (PSIRT, historial de vulnerabilidades).
☐	El fabricante facilita el SBOM de los dispositivos
☐	Garantía y soporte de actualizaciones vigentes.

3.11. Uso de plataformas y herramientas seguras

La eficacia de un sistema de video vigilancia moderno no depende únicamente de la calidad de las cámaras o de la infraestructura de red. La verdadera fortaleza del sistema reside en su capacidad para integrarse, gestionarse y operar de forma segura dentro de un ecosistema tecnológico más amplio. En este contexto, las plataformas de gestión centralizada y las herramientas de colaboración en la nube desempeñan un papel fundamental para garantizar una operación coordinada, eficiente y resiliente.

3.11.1. Sistemas de gestión centralizada (PSIM): interoperabilidad de sistemas de seguridad para una respuesta coordinada.

Los **PSIM (Physical Security Information Management)** son plataformas diseñadas para unificar, en una sola interfaz, múltiples sistemas de seguridad física: CCTV, control de accesos, alarmas, sensores perimetrales, sistemas contra incendios, analítica de vídeo y más. Su objetivo es proporcionar una visión global y facilitar la toma de decisiones en situaciones críticas.

Funciones clave de un PSIM aplicado a CCTV

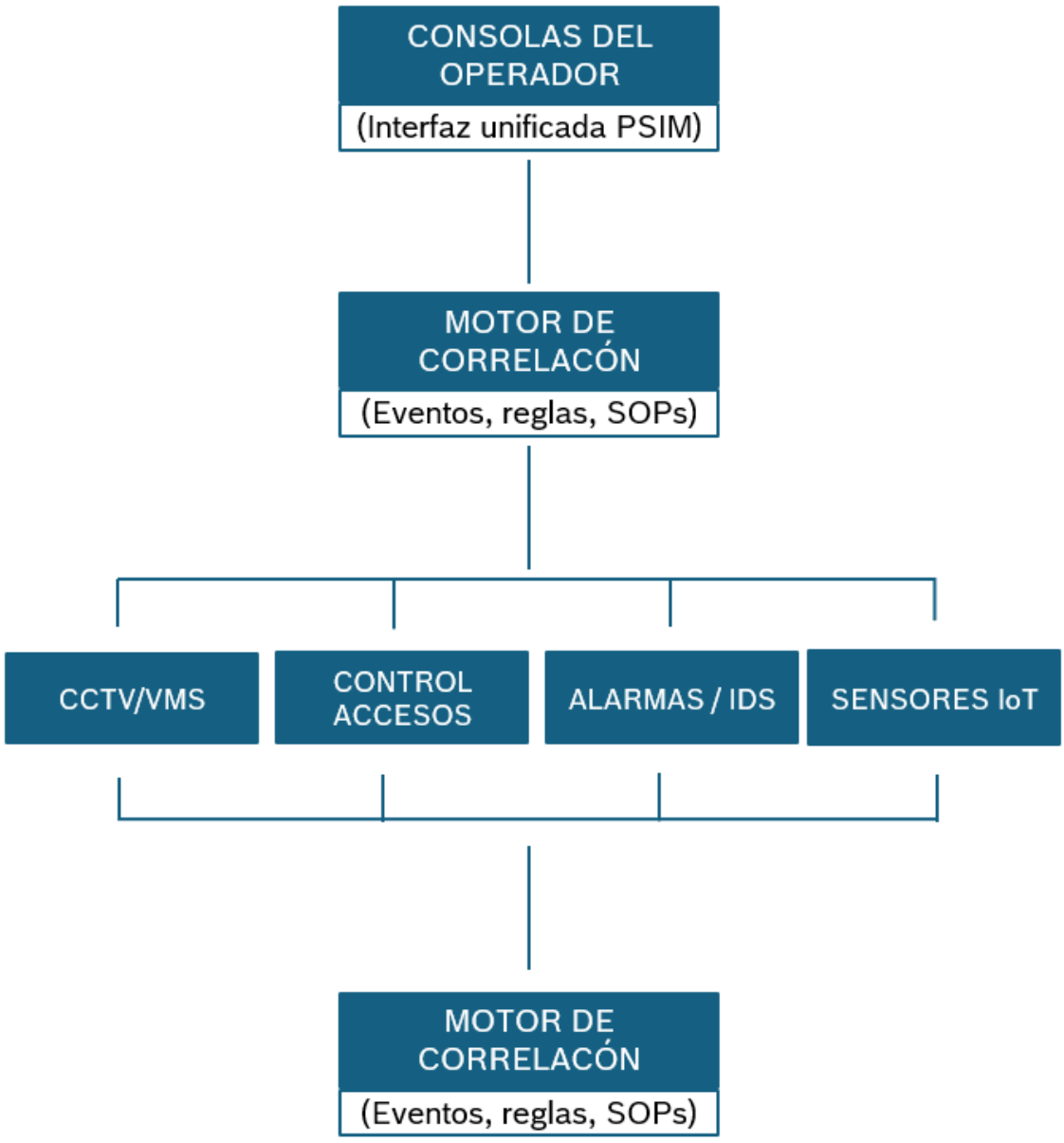
- **Integración de múltiples fuentes de vídeo**: permite visualizar cámaras de distintos fabricantes y tecnologías sin depender de un único proveedor.
- **Correlación automática de eventos**: el sistema puede vincular una alarma de intrusión con la cámara más cercana, generando una respuesta inmediata.
- **Gestión centralizada de incidentes**: los operadores reciben procedimientos guiados (SOPs) que estandarizan la respuesta ante eventos.
- **Registro y auditoría**: todas las acciones quedan documentadas, lo que facilita el cumplimiento normativo y la trazabilidad.
- **Escalabilidad**: permite gestionar desde instalaciones pequeñas hasta infraestructuras críticas distribuidas geográficamente.

Beneficios para la seguridad

- **Respuesta más rápida y precisa** gracias a la automatización y correlación de datos.
- **Reducción de errores humanos** mediante flujos de trabajo guiados.
- **Mayor resiliencia operativa** al centralizar la supervisión y permitir redundancia.
- **Interoperabilidad real** entre sistemas heterogéneos, evitando silos tecnológicos.

Aplicación Técnica, pasos para su correcta implementación

- Seleccionar plataformas compatibles con estándares abiertos (ONVIF, PSIA).
- Asegurar que el PSIM soporte cifrado de extremo a extremo en comunicaciones.
- Integrar el sistema con políticas de ciberseguridad corporativas.
- Realizar pruebas periódicas de interoperabilidad y simulacros de incidentes.



Esquema básico de un PSIM

3.11.2. Software de colaboración: criterios para la selección y el uso seguro de plataformas en la nube.

El trabajo colaborativo es esencial en la gestión de sistemas de videovigilancia, especialmente cuando participan múltiples equipos como operadores, técnicos, responsables de seguridad, proveedores externos de comunicación y alojamiento, así como autoridades. La coordinación efectiva entre estos grupos permite optimizar la vigilancia, mejorar la respuesta ante incidentes y garantizar la protección integral de las instalaciones. En este sentido, **las plataformas de colaboración en la nube se han convertido en herramientas fundamentales**, ya que facilitan el intercambio de información, la coordinación de acciones y la documentación de incidentes en tiempo real. La capacidad de acceder a datos y registros desde cualquier ubicación agiliza la toma de decisiones y permite una gestión más eficiente de los recursos.

No obstante, **el uso de estas plataformas introduce una serie de riesgos que deben ser gestionados de manera rigurosa para evitar vulnerabilidades** que puedan afectar la seguridad de la información. Es imprescindible seleccionar soluciones tecnológicas que sean seguras y que cumplan con criterios estrictos de protección y privacidad de datos. Entre los requisitos fundamentales se encuentran:

- El **cumplimiento normativo**, que implica la alineación con el Reglamento General de Protección de Datos (GDPR), la certificación ISO 27001 y otras regulaciones aplicables a la gestión de datos sensibles.
- El **cifrado robusto** tanto en tránsito como en reposo es esencial para prevenir accesos no autorizados, siendo recomendable que las claves sean gestionadas directamente por la organización para mantener el control sobre la información.
- El **control de acceso granular**, que debe establecer roles, permisos específicos y sistemas de autenticación multifactor (MFA) para garantizar que solo las personas autorizadas puedan acceder a los datos y funcionalidades de la plataforma.

Asimismo, la integración con sistemas de seguridad existentes, como los sistemas de gestión de vídeo (VMS), plataformas de integración de seguridad física (PSIM) y herramientas de ticketing, permite una operativa más fluida y una visión unificada de la seguridad. El registro de actividad y auditoría es imprescindible para facilitar investigaciones internas y asegurar el cumplimiento de los requisitos legales, permitiendo rastrear cualquier acción realizada dentro del sistema. Por último, la ubicación de los datos debe ser preferiblemente en regiones autorizadas por la organización, lo que ayuda a cumplir con las políticas de soberanía de datos y regulaciones locales.

En cuanto a la aplicación técnica y los pasos para un uso seguro de estas plataformas, **es fundamental evitar compartir grabaciones sensibles por canales no autorizados, como correos personales o aplicaciones de mensajería no corporativas**, ya que esto puede exponer información crítica a riesgos innecesarios. Resulta igualmente **importante configurar políticas de retención y eliminación de archivos**, evitando la acumulación de datos que puedan suponer un peligro en caso de brechas de seguridad. La implementación de MFA y contraseñas robustas a todos los usuarios es una medida básica pero muy efectiva para prevenir accesos fraudulentos. El acceso a terceros debe limitarse mediante permisos temporales y supervisados, garantizando que solo se concedan cuando sea estrictamente necesario y bajo control. Además, **la capacitación continua de los equipos en el uso seguro de la plataforma y en la gestión de incidentes contribuye a minimizar errores humanos** y a fortalecer la cultura de seguridad dentro de la organización.

Las ventajas operativas que se derivan de la adopción de plataformas seguras y colaborativas son notables:

- Se logra una comunicación más fluida entre equipos distribuidos, lo que favorece la coordinación y la eficiencia en la gestión de incidentes.
- Se incrementa la rapidez en la toma de decisiones, ya que la información se encuentra disponible en tiempo real y puede ser evaluada por todos los implicados.
- La documentación centralizada de incidentes y acciones facilita el seguimiento histórico y la elaboración de informes, mientras que la reducción de tiempos de respuesta y la mejora en la coordinación contribuyen a elevar el nivel de seguridad general y a optimizar los recursos disponibles.

4. El uso de la inteligencia artificial en la seguridad de las comunicaciones

En el ámbito que nos ocupa, que no es otro que el de la seguridad y fiabilidad de las comunicaciones / telecomunicaciones y su relación con la emergente figura de la denominada inteligencia como herramienta adicional de trabajo o análisis, esta última hace posible la detección proactiva de amenazas, siempre a través de tareas y acciones de análisis de comportamiento y el procesamiento de lenguaje natural para identificar phishing y anomalías en tiempo real.

A su vez, sirve también de ayuda y desarrollo en las tareas o acciones de análisis forense, así como en la automatización en la gestión de alertas, mejorando la eficiencia operativa.

4.1. Detección de amenazas en tiempo real: cómo la IA analiza patrones de comunicación para identificar anomalías, ataques de *phishing* y actividad maliciosa.

Hemos de tener bien presente que las IAs utilizan algoritmos de aprendizaje profundo y automático (*machine learning*) con la finalidad de analizar el tráfico y los patrones de comunicación en tiempo real, superando las limitaciones de los sistemas tradicionales.

- **Seguridad Endpoints:** protegiendo equipos, portátiles, servidores y móviles que se conectan a redes empresariales, actuando como un escudo contra malware, ransomware y accesos no autorizados. Funciona examinando archivos y comportamientos sospechosos, esencial ya que el 70% de las filtraciones inician en estos dispositivos.
- **Detección de Phishing:** identificación de correos electrónicos o sitios web falsos que buscan robar información sensible. Las señales clave incluyen remitentes inusuales, ortografía deficiente, sentido de urgencia y enlaces sospechosos.
- **Análisis de Anomalías:** Identificando comportamientos inusuales en la red (accesos fuera de horario, volúmenes de datos extraños o cambios en los patrones de comunicación de un usuario), lo cual permite a la IA detectar intrusiones sofisticadas.

4.2. Automatización y eficiencia operacional: la IA para automatizar la gestión de alertas, la clasificación de amenazas y el análisis forense.

Sin duda alguna, la IA colabora y ayuda en el ámbito de la seguridad permitiendo a los equipos de seguridad manejar un volumen elevado de alertas, mejorando la precisión, diligencia y rapidez en la resolución. Lo que facilita:

- **Gestión de Alertas y Clasificación:** Mediante algoritmos avanzados, la inteligencia artificial puede identificar patrones sospechosos y priorizar las alertas según su nivel de riesgo. Esto permite que los equipos se centren en los incidentes más críticos, optimizando el tiempo y los recursos disponibles.
- **Análisis Forense:** La IA es capaz de analizar grandes cantidades de datos en tiempo real, ayudando a detectar la causa raíz de los incidentes de seguridad. Gracias a su capacidad para correlacionar información de distintas fuentes, se puede reconstruir el escenario de una brecha de seguridad de manera más eficiente y precisa.
- **Respuesta Automatizada (SOAR):** Las plataformas SOAR impulsadas por IA permiten automatizar procesos de respuesta ante incidentes, ejecutando acciones predefinidas como el aislamiento de sistemas afectados o la recopilación de evidencias. Esto no solo agiliza la reacción ante amenazas, sino que también reduce el margen de error humano.

En definitiva, la integración de la inteligencia artificial proporciona una ventaja significativa, ya que mejora la capacidad de anticipar, detectar y responder ante amenazas, contribuyendo a un entorno más seguro y resiliente.

4.3. Desafíos y futuro de la IA en la ciberseguridad: consideraciones sobre la ética, la privacidad de los datos y la necesidad de supervisión humana para evitar decisiones erróneas.

No obstante, todo lo enumerado anteriormente, el uso de la inteligencia artificial presenta una serie de puntos delicados y riesgos críticos que abarcan desde aspectos técnicos hasta dilemas éticos y sociales tales como sesgo algorítmico y discriminación, privacidad de datos y seguridad, falta de veracidad, falta de transparencia, dependencia tecnológica, daño ambiental.

- **Privacidad de Datos:** El uso de grandes volúmenes de datos para entrenar modelos de IA implica riesgos de privacidad si no se gestionan adecuadamente, obligando a cumplir estrictamente con regulaciones como el RGPD.
- **Sesgo y Ética:** Los sistemas de IA pueden heredar sesgos de sus datos de entrenamiento, provocando discriminación o decisiones erróneas.
- **Necesidad de Supervisión Humana:** La IA puede fallar, por lo que es esencial mantener modelos de supervisión como *Human-in-the-Loop* (HITL - validación directa) o *Human-on-the-Loop* (HOTL - monitoreo) para asegurar decisiones éticas y evitar daños.
- **Amenaza Adversaria:** Los ciberdelincuentes también utilizan IA para crear ataques más convincentes, lo que genera una carrera armamentista tecnológica.

5. El factor humano en la seguridad de las comunicaciones

Los sistemas de comunicaciones constituyen la columna vertebral de los Sistemas Electrónicos de Seguridad, permiten la transmisión de datos, voz y la prestación de servicios esenciales para la protección de personas y bienes. El incremento de la digitalización y de la conectividad de estos sistemas a redes públicas y privadas, ha incrementado los riesgos asociados a su uso y gestión, especialmente los ciberriesgos derivados del factor humano.

Cuando hablamos de ciberriesgos estamos hablando de las amenazas y vulnerabilidades que pueden comprometer la confidencialidad, integridad y disponibilidad de la información, en el caso que nos atañe, de la información que procesan, almacenan y trasmiten los Sistemas Electrónicos de Seguridad. En el En el sector de la Seguridad Privada, el factor humano representa uno de los elementos más críticos, ya que la interacción del personal con la tecnología puede convertirse en un vector de ataque, tanto de forma intencionada como accidental. La falta de formación adecuada, la presión laboral o la desinformación pueden desencadenar incidentes de seguridad graves.

El personal técnico encargado de la instalación y mantenimiento de los sistemas de telecomunicaciones desempeña un rol esencial en la seguridad de la infraestructura. Sin embargo, la falta de formación adecuada, la negligencia o los errores no intencionados pueden dar lugar a vulnerabilidades críticas que ponen en riesgo la integridad y disponibilidad de los servicios. A continuación, se detallan algunos de los principales ciberriesgos asociados:

Entre los principales ciberriesgos con origen en el factor humano podemos citar los siguientes:

- Errores de configuración: La incorrecta configuración de routers, switches, firewalls y otros dispositivos de red puede abrir puertas traseras inadvertidas, permitiendo accesos no autorizados o exponiendo información sensible a internet.
- Aplicación inadecuada de parches y actualizaciones: No instalar o actualizar adecuadamente el software y firmware de los equipos incrementa el riesgo de explotación de vulnerabilidades conocidas, facilitando, entre otros ataques de ransomware o intrusiones externas.

- Gestión deficiente de contraseñas y credenciales: El uso de contraseñas por defecto, credenciales compartidas o la falta de rotación periódica puede permitir a atacantes internos o externos tomar control de sistemas críticos.
- Desconocimiento de políticas de seguridad: Cuando el personal técnico no está al tanto de los procedimientos y políticas internas, se incrementa la probabilidad de omitir controles esenciales, como la segmentación de redes, el cifrado de datos o la monitorización de accesos.
- Falta de documentación y registro de cambios: La ausencia de un seguimiento riguroso de las modificaciones en la infraestructura puede dificultar la identificación y resolución de incidentes, prolongando la exposición a amenazas.
- Nivel insuficiente de concienciación en ciberseguridad: Técnicos que no han sido formados en amenazas actuales pueden caer fácilmente en trampas de ingeniería social o no identificar comportamientos anómalos, actuando sin el debido escepticismo ante solicitudes o accesos sospechosos.
- Manipulación inadecuada de equipos retirados o en desuso: No aplicar procesos seguros para el borrado de datos o la eliminación física de dispositivos puede derivar en la filtración de información confidencial.
- Errores durante la gestión de incidencias: Actuar bajo presión o sin procedimientos claros puede llevar a respuestas impulsivas, empeorando la situación o generando nuevas brechas de seguridad.

La suma de estos factores convierte a la falta de formación, la negligencia y los errores técnicos en un vector de riesgo tan relevante como el de los ataques sofisticados provenientes del exterior.

5 El factor humano en la seguridad de las comunicaciones

5.1. Formación y concienciación: capacitación del personal para identificar y evitar amenazas como el phishing y la ingeniería social**.**

La formación y la concienciación del personal son una de las estrategias más eficaces para reducir la incidencia de ciberriesgos derivados del factor humano.

La principal diferencia entre formación y concienciación es que la formación trata sobre el "cómo" (técnicas, habilidades, conocimientos prácticos), mientras que la concienciación hace foco en el "porqué" (motivación, cambio de mentalidad, interiorización de riesgos). Con la formación se busca proporcionar conocimientos técnicos y con la concienciación se pretende crear una cultura que ayude a conocer los riesgos y a que la formación recibida se aplique. En resumen:

- La formación está centrada en proporcionar competencias específicas. Se enfoca en la teoría y práctica para saber actuar ante situaciones concretas.
- La concienciación busca que las personas sean conscientes de los riesgos y su responsabilidad, e interioricen la necesidad de actuar correctamente.

La formación y la concienciación son complementarias, ambas son imprescindibles: sin concienciación, la formación no se aplica, y sin formación, la concienciación no sabe cómo aplicarse.

Los programas de formación deben ser integrales, continuos y adaptados a los distintos perfiles profesionales.

Para alcanzar un adecuado nivel de capacitación debe impartirse tanto formación presencial como online, combinando sesiones teóricas con talleres prácticos y simulacros. Utilizando métodos que faciliten el aprendizaje como lo siguientes:

- Microlearning: Impartir contenidos breves y focalizados para facilitar la asimilación y retención de conceptos clave.
- Gamificación: Utilizar dinámicas de juego para motivar la participación y el aprendizaje activo del personal.

Todo el personal de seguridad debe recibir formación que contemple, entre otros, los siguientes contenidos: la gestión segura de contraseñas, el reconocimiento de intentos de ingeniería social, la protección de dispositivos móviles y la cultura de ciberseguridad.

Adicionalmente, la formación de los técnicos de Sistemas Electrónicos de Seguridad debe incluir temas específicos sobre:

- Configuración segura de dispositivos y redes.
- Actualizaciones y parches críticos.
- Buenas prácticas de documentación y registro de cambios.
- Gestión segura de contraseñas y credenciales de acceso.
- Seguridad en la manipulación y desecho de equipos.
- Protocolos de respuesta ante incidentes.

La concienciación centra en la creación de una actitud proactiva hacia la seguridad, en su sentido más, amplio va un paso más adelante de la formación formal y se centra en la creación de una actitud proactiva hacia la seguridad. Algunas acciones clave incluyen:

- Campañas informativas: Difusión regular de mensajes y materiales visuales sobre buenas prácticas y riesgos emergentes.
- Comunicación interna efectiva: Establecer canales de comunicación directos entre el departamento de seguridad y el resto de la organización para resolver dudas y reportar incidentes.
- Fomento de la cultura de seguridad: Reconocer y premiar comportamientos seguros, involucrar a la alta dirección y promover el liderazgo en seguridad.
- Simulacros y ejercicios de concienciación: Organizar simulaciones de ataques de ingeniería social para sensibilizar al personal sobre la importancia de la vigilancia y la responsabilidad individual.

5 El factor humano en la seguridad de las comunicaciones

La implicación de todos los niveles de la organización es esencial para consolidar una cultura de seguridad robusta y sostenible.

Para evaluar la eficacia y eficiencia de las acciones de formación y concienciación es necesario realizar un seguimiento de estas y realizar ejercicios prácticos y simulacros para medir el grado de concienciación y de adquisición de conocimientos y habilidades. Estableciendo una serie de indicadores y métricas que nos van a permitir implantar un ciclo de mejora continua de las actividades de formación y concienciación. Entre los indicadores que debemos tener en cuenta están los siguientes:

- Tasa de participación: Porcentaje de empleados que completan las actividades formativas y de concienciación.
- Resultados de evaluaciones: Nivel de conocimiento adquirido y capacidad de aplicación práctica.
- Número de incidentes reportados: Incremento en la detección y comunicación de posibles amenazas por parte del personal.
- Reducción de incidentes: Disminución de eventos de seguridad relacionados con el factor humano.

El seguimiento de estos indicadores permite ajustar las acciones implementadas y fomentar la mejora continua en la gestión de ciberriesgos.

La protección de los sistemas de telecomunicaciones frente a los ciberriesgos derivados del factor humano requiere una estrategia integral basada en la formación, concienciación y el uso de herramientas tecnológicas. Por ello es necesario

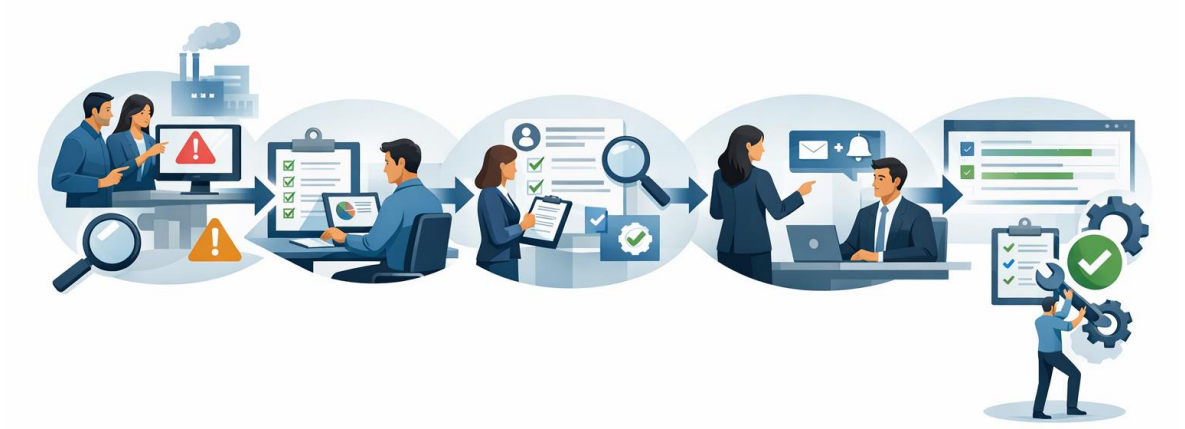
- Implantar programas de formación adaptados a todos los perfiles profesionales.
- Desarrollar campañas de concienciación periódicas y accesibles.

- Fomentar la cultura de seguridad corporativa desde la dirección hasta el último de los empleados.
- Utilizar plataformas tecnológicas para facilitar el aprendizaje y la evaluación continua.
- Establecer indicadores claros para medir la eficacia de las acciones y ajustar las estrategias según los resultados.
- Prestar especial atención a la formación y supervisión del personal técnico encargado de la instalación y mantenimiento de los Sistemas Electrónicos de Seguridad, dotándoles de conocimientos actualizados y de protocolos claros para la gestión segura de los sistemas.

La gestión proactiva del factor humano, conjugada con una sólida estrategia de formación y concienciación, es esencial para minimizar los ciberriesgos, garantizar el correcto funcionamiento de los Sistemas Electrónicos de Seguridad y por lo tanto la seguridad de las personas y bienes.

5.2. Procedimientos de reporte: establecer canales claros para la notificación de incidentes y vulnerabilidades a través de medios seguros.

Los procedimientos de reporte de ciberincidentes son fundamentales para garantizar la ciberseguridad de los Sistemas Electrónicos de Seguridad. La detección temprana y la comunicación de los ciberincidentes, junto con una y la respuesta permiten minimizar el impacto de las ciberamenazas y de las propias vulnerabilidades de los sistemas. Para lograr este objetivo deben establecerse procedimientos y canales



seguros para la notificación de ciberincidentes y vulnerabilidades.

Cuando hablamos de ciberincidente se refiere a cualquier evento que comprometa la confidencialidad, integridad o disponibilidad de la información que almacena, procesa o trasmite cualquier sistema de información. La correcta identificación y clasificación de estos eventos es el primer paso para su reporte y gestión.

Entre los tipos más comunes de ciberincidentes podemos citar:

- Accesos no autorizados
- Software malicioso
- Ataques de phishing
- Exfiltración de datos
- Ataques de denegación de servicio
- Vulnerabilidades explotadas
- Errores de configuración
- Incidentes internos accidentales
- Sabotajes

Un procedimiento de reporte de ciberincidentes debe estar perfectamente estructurado y detallado, para permitir y facilitar la realización de las siguientes tareas:

- Identificación del incidente
- Clasificación del tipo y severidad
- Registro en el sistema de gestión de incidentes
- Notificación a la dirección
- Activación del protocolo de respuesta
- Documentación de acciones tomadas
- Cierre del incidente
- Análisis del incidente y de la respuesta

Para garantizar la confidencialidad y autenticidad de la información relativa al ciberincidente, se deben establecer canales seguros de comunicación, como pueden ser:

- Sistemas de ticketing con autenticación multifactor
- Correo electrónico cifrado
- Plataformas de reporte en línea con acceso restringido
- Aplicaciones móviles seguras para notificación en tiempo real
- Integración con sistemas SIEM, PSIM y otras herramientas de gestión y supervisión

Estos canales de comunicación deben estar disponibles para todo el personal y ser objeto de auditorías periódicas.

Un procedimiento de reporte de ciberincidentes debe establecer los roles y responsabilidades de todo el personal:

- Usuarios: Identificar y reportar incidentes
- Técnicos de Sistemas Electrónicos de Seguridad: Identificar y reportar incidentes
- Equipo de respuesta a incidentes: Validar, clasificar y responder
- Responsable de Seguridad: Coordinar la gestión de incidentes
- Dirección: Aportar recursos y tomar decisiones estratégicas
- Equipo de Auditoría: Verificar el cumplimiento de procedimientos

Los procedimientos de reporte deben facilitar el cumplimiento de la legislación vigente y estar alineados con los principales estándares del mercado.

El establecimiento de procedimientos claros y canales seguros para el reporte de ciberincidentes es esencial para garantizar el correcto funcionamiento de los Sistemas Electrónicos de Seguridad y por tanto la seguridad de las personas y bienes que estos protegen.

No hay que olvidar que la formación continua y la concienciación son pilares fundamentales para mejorar la capacidad de detección y reporte de ciberincidentes, y que junto con el uso de tecnologías adecuadas permiten una respuesta eficaz ante las ciberamenazas.

6. Auditoría y mejora continua en la ciberseguridad

Para garantizar la eficacia, la eficiencia y la resiliencia de los Sistemas Electrónicos de Seguridad y, por lo tanto, la seguridad de las personas y los bienes que estos protegen es necesario realizar auditorías e implantar procesos de mejora continua.

Una auditoría de ciberseguridad consiste en evaluar de manera sistemática las políticas, los controles y los procedimientos implementados en el sistema. Este proceso permite identificar vulnerabilidades, verificar el cumplimiento normativo y asegurar que los mecanismos de protección funcionan correctamente. Las auditorías pueden ser tanto internas, realizadas por el propio personal de la organización, o externas, llevadas a cabo por entidades especializadas.

Durante el proceso de auditoria se debe realizar una evaluación de riesgos para identificar las vulnerabilidades, las ciberamenazas potenciales y el análisis del posible impacto sobre el sistema, en caso de materialización de las mismas. Para identificar las posibles vulnerabilidades es necesario, entre otras acciones, efectuar una revisión de los controles de acceso al sistema, verificando la gestión de las credenciales y permisos, así como una inspección de la infraestructura, redes, dispositivos y protocolos utilizados. También es necesario analizar todo lo relativo al cumplimiento normativo, para asegurar que el sistema cumple con la legislación vigente y los estándares aplicables.

6 Auditoría y mejora continua en la ciberseguridad

Un proceso de mejora continua implica el establecimiento de un ciclo continuo de revisión y actualización de las medidas de ciberseguridad en el Sistema Electrónico de Seguridad. Al utilizar metodologías de mejora continua, como puede ser el ciclo PDCA (Planificar, Hacer, Verificar, Actuar), con este proceso de mejora continua las organizaciones pueden adaptarse rápidamente a los nuevos riesgos y tecnologías. Este enfoque fomenta una cultura de prevención y respuesta proactiva ante ciberincidentes.

Planificar: Definir objetivos y políticas de ciberseguridad basados en los resultados de las auditorías previas.

Hacer: Aplicar políticas, implementar controles, soluciones tecnológicas y formación al personal.

Verificar: Monitorizar y medir el rendimiento de las medidas adoptadas.

Actuar: Realizar ajustes y mejoras en función de los resultados obtenidos y de las nuevas ciberamenazas detectadas.

La mejora continua es imprescindible para mantener la eficacia y eficiencia de los Sistemas Electrónicos de Seguridad a la hora de garantizar la seguridad de las personas y bines que protegen. Para ello es necesario:

- Realizar auditorías periódicas de forma anual o semestral, ajustando la frecuencia según el nivel de exposición y criticidad de los activos protegidos.
- Mantener los sistemas, aplicaciones y dispositivos actualizados, aplicando los parches y mejoras propuestos por los fabricantes.
- Una política de capacitación continua, proporcionando formación periódica al personal sobre buenas prácticas, políticas de seguridad y amenazas emergentes, promoviendo una cultura de protección proactiva.
- Implantar procesos de documentación y seguimiento, para registrar los hallazgos, recomendaciones y acciones tomadas durante cada auditoría, y realizar revisiones de seguimiento para verificar la implementación de las mejoras.
- Integrar nuevas tecnologías, evaluando y adoptando herramientas innovadoras como sistemas de inteligencia artificial para detección de anomalías, análisis de comportamiento y respuesta automática ante incidentes.

La realización de auditorías y la aplicación de procesos de mejora continua permite una respuesta ágil ante los cambios tecnológicos y las ciberamenazas emergentes, una reducción de las vulnerabilidades y de la exposición a los ciberriesgos, lo que se traduce en una mayor confianza en los Sistemas Electrónicos de Seguridad y en una

optimización de los procesos internos y el uso de recursos, lo que facilita el cumplimiento normativo.

La auditoría y la mejora continua en la ciberseguridad de los Sistemas Electrónicos de Seguridad son procesos imprescindibles para garantizar una protección eficaz, eficiente y sostenible.

6.1. Auditorías periódicas: realización de revisiones para identificar vulnerabilidades en las tecnologías de comunicación**.**

Las auditorías periódicas, no deben ser una simple formalidad, son un proceso estructurado y minucioso para evaluar el estado real de los Sistemas Electrónicos de Seguridad. Su objetivo principal es identificar vulnerabilidades, anticipar amenazas emergentes y garantizar la resiliencia frente a los posibles incidentes que puedan suponer un impacto sobre la integridad, disponibilidad y confidencialidad de la información gestionada por los Sistemas Electrónicos de Seguridad

Metodología de las revisiones

El proceso de auditoría comprende diversas etapas, cada una de ellas orientada a detectar vulnerabilidades, evaluar riesgos y proponer controles efectivos:

- Evaluación de la infraestructura: Se debe realizar una inspección detallada de todos los dispositivos, redes y componentes asociados a comunicaciones: servidores, switches, routers, sistemas inalámbricos, terminales y aplicaciones.

Se debe verificar la configuración de cada elemento, el cumplimiento de los estándares de seguridad y la existencia de controles de acceso adecuados. Asimismo, se deben analizan las políticas de actualización, la segmentación de redes y la gestión de activos críticos.

- Identificación de vulnerabilidades: mediante el uso de herramientas automatizadas y técnicas manuales, se deben buscar puntos débiles en el software, firmware y hardware. Se deben efectuar escaneos en busca de errores de configuración, versiones obsoletas, falta de parches de seguridad o presencia de puertas traseras. Además, se deben evaluar los protocolos de comunicación para verificar que emplean métodos de cifrado robustos y están protegidos contra ataques como sniffing, spoofing y man-in-the-middle.
- Pruebas de penetración: se deben realizar simulacros de ataques por parte de especialistas, utilizando técnicas de hacking ético para medir la respuesta de los sistemas frente a intentos de explotación. Se deben evaluar la resistencia a la infiltración, la capacidad de detección de anomalías y la efectividad de las medidas de remediación. Los resultados nos van a ofrecer una imagen clara de los riesgos y de los posibles escenarios de impacto.
- Revisión de políticas y procedimientos: se deben analizar las políticas internas, manuales de seguridad, procedimientos de respuesta ante incidentes y protocolos de comunicación para asegurarse de que están actualizados, cubren toda la casuística posible y se aplican correctamente. Se debe verificar la existencia de planes de formación para el personal, la asignación de responsabilidades y la documentación de cambios y mejoras.

Las tecnologías de comunicación utilizadas en los Sistemas Electrónicos de Seguridad pueden tener una serie de vulnerabilidades, que pueden ser explotadas si no se gestionan de manera proactiva, entre ellas citaremos:

- Falta de cifrado: La transmisión de datos sin cifrado puede facilitar el acceso no autorizado y la interceptación de información sensible.
- Configuraciones incorrectas: Errores en la configuración de redes, dispositivos o aplicaciones pueden abrir puertas a actores malintencionados. Por ejemplo, contraseñas por defecto o puertos abiertos innecesarios.
- Software desactualizado: Aplicaciones y sistemas que no se actualizan regularmente son vulnerables a amenazas conocidas, ya que los parches de seguridad no se aplican.
- Ausencia de controles de acceso robustos: La falta de autenticación multifactor, políticas de gestión de contraseñas o segmentación de usuarios incrementa el riesgo de accesos indebidos.
- Exposición a amenazas externas: Conexiones remotas mal protegidas, uso de redes públicas o dispositivos móviles poco seguros pueden ser puntos de entrada para ataques.

6 Auditoría y mejora continua en la ciberseguridad

Las auditorías periódicas de los sistemas electrónicos de seguridad son una práctica esencial para anticipar riesgos y fortalecer la protección de las tecnologías de comunicación utilizadas en los Sistemas Electrónicos de Seguridad.

6.2. Análisis de riesgos y simulacros: implementación de ejercicios de ciberataques para evaluar la efectividad de los protocolos**.**

El análisis de riesgos es un proceso sistemático que permite identificar, evaluar y priorizar las ciberamenazas a las que está expuesta un sistema, en nuestro caso un Sistema Electrónico de Seguridad. El objetivo es determinar el nivel de riesgo y establecer los controles adecuados.

Las fases de un análisis de riesgos son las siguientes:

- Identificación de activos y amenazas: El primer paso consiste en identificar los activos críticos (cámaras, servidores, redes, etc.) y las amenazas potenciales, tanto internas como externas. Es fundamental considerar la posibilidad de amenazas persistentes avanzadas (APT), que pueden permanecer ocultas durante largos periodos de tiempo.
- Evaluación de vulnerabilidades: Se deben analizar las vulnerabilidades presentes en el hardware, el software y la configuración de los sistemas. Las actualizaciones no aplicadas, contraseñas débiles o configuraciones por defecto son puntos de entrada habituales para los atacantes.
- Estimación de impacto y probabilidad: Se evalúa el impacto potencial de cada amenaza sobre los activos, así como la probabilidad de que esta se materialice. Esto permite priorizar los riesgos y enfocar los recursos en aquellos más críticos.
- Diseño de medidas de mitigación: En función de los riesgos identificados, se diseñan controles técnicos y organizativos para reducir la exposición: segmentación de redes, autenticación robusta, protocolos de cifrado, formación del personal y procedimientos de respuesta ante incidentes.

Algunas de las buenas prácticas a la hora diseñar medidas de mitigación e implantar controles de son:

- Actualizar regularmente el software y firmware de todos los dispositivos.
- Implementar autenticación multifactor en el acceso a los sistemas.
- Segregar las redes de los Sistemas Electrónicos de Seguridad del resto de la red corporativa.
- Utilizar protocolos cifrados para la transmisión de datos.
- Formar a los usuarios en ciberseguridad y concienciar sobre los riesgos.
- Realizar auditorías y pruebas de penetración periódicas.

6 Auditoría y mejora continua en la ciberseguridad

Una forma de detectar vulnerabilidades tanto técnicas como procedimentales es la realización de simulacros y de ejercicios de ciberataques, también conocidos como pruebas de penetración, son actividades controladas en las que se simulan ataques reales contra un Sistema Electrónico de Seguridad con el objetivo de identificar vulnerabilidades y medir la capacidad de respuesta de los equipos de seguridad. Los simulacros, por su parte, reproducen situaciones de crisis o incidentes de seguridad para poner a prueba los procedimientos, la coordinación y la toma de decisiones bajo presión.

Los principales objetivos que se persiguen con la realización de simulacros y ejercicios son:

- Detectar vulnerabilidades en los sistemas y protocolos de seguridad.
- Evaluar la capacidad de respuesta y recuperación ante incidentes.
- Mejorar la formación y concienciación del personal involucrado.
- Actualizar y optimizar las medidas de ciberseguridad existentes.

Fases para la implementación de ejercicios y simulacros

- Planificación: Definir los objetivos, el alcance y los escenarios a simular. Seleccionar los equipos participantes y establecer los criterios de evaluación.
- Diseño del ejercicio: Crear guiones realistas que contemplen diferentes tipos de amenazas (phishing, malware, acceso no autorizado, etc.) y que pongan a prueba tanto los sistemas como los procedimientos.
- Ejecución: Realizar el ejercicio en un entorno controlado, monitorizando en tiempo real las acciones y respuestas.
- Análisis de resultados: Recopilar y analizar la información obtenida, identificando puntos fuertes y áreas de mejora.
- Informe y retroalimentación: Elaborar un informe detallado y proponer acciones correctivas o de refuerzo según los hallazgos.
- Revisión periódica: Programar ejercicios y simulacros de forma regular para fomentar la mejora continua.

La realización de simulacros y de ejercicios nos va a proporcionar un incremento de la resiliencia frente a ataques reales, una reducción del tiempo de respuesta, tanto en la detección como en la mitigación y recuperación, así como una mayor concienciación y capacitación del personal en materia de ciberseguridad.

Para maximizar la efectividad de estos simulacros y ejercicios, es imprescindible contar con el apoyo de la dirección y fomentar una cultura de ciberseguridad en toda la organización. Se deben documentar todos los simulacros y ejercicios, y utilizar los resultados para actualizar los protocolos y las medidas técnicas, dentro del proceso de mejora continua.

7. Glosario de términos

- **Acceso No Autorizado**: Entrada a un sistema o recurso sin el permiso adecuado, lo que puede comprometer la seguridad de la información.
- **Acceso Remoto**: Capacidad de acceder a un sistema o red desde una ubicación fuera de la red local, a menudo a través de Internet.
- **Análisis de Riesgos**: Proceso de identificar, evaluar y priorizar riesgos potenciales que pueden afectar la seguridad de un sistema o información.
- **Antivirus**: Software diseñado para detectar, prevenir y eliminar malware de un sistema informático.
- **Autenticación**: Proceso de verificar la identidad de un usuario o sistema, generalmente mediante contraseñas, tokens o biometría.
- **Autenticación Multifactor (MFA)**: Método de seguridad que requiere dos o más formas de verificación para acceder a un sistema, aumentando la protección contra accesos no autorizados.
- **Backdoor**: Método oculto para eludir la autenticación normal y obtener acceso no autorizado a un sistema.
- **Botnet**: Red de dispositivos infectados por malware que pueden ser controlados de forma remota por un atacante para realizar ataques coordinados.
- **Ciberespionaje**: Actividades de espionaje realizadas a través de medios digitales para obtener información confidencial de organizaciones o gobiernos.
- **Ciberincidente**: Evento que compromete la confidencialidad, integridad o disponibilidad de la información en un sistema de información.
- **Ciberseguridad**: Prácticas y tecnologías diseñadas para proteger sistemas, redes y datos de ataques, daños o accesos no autorizados.
- **Cifrado**: Proceso de convertir datos en un formato ilegible para proteger la información durante su almacenamiento o transmisión.
- **Confidencialidad**: Principio de la ciberseguridad que asegura que la información solo sea accesible por personas o sistemas autorizados.
- **Denegación de Servicio (DoS)**: Ataque que busca hacer que un servicio no esté disponible al inundarlo con tráfico o solicitudes.
- **DDoS (Distributed Denial of Service)**: Variante del ataque DoS que utiliza múltiples sistemas para sobrecargar un servicio, dificultando su disponibilidad.
- **Escaneo de Puertos**: Técnica utilizada para identificar puertos abiertos en un sistema, que pueden ser vulnerables a ataques.
- **Escaneo de Vulnerabilidades**: Proceso de identificar debilidades en un sistema o red que podrían ser explotadas por atacantes.
- **Exfiltración de Datos**: Proceso de transferir datos de un sistema a un lugar no autorizado, a menudo como resultado de un ataque.

7 Glosario de términos

- **Firewall**: Dispositivo o software que controla el tráfico de red entrante y saliente, permitiendo o bloqueando datos según reglas de seguridad predefinidas.
- **Gestión de Identidades y Accesos (IAM)**: Conjunto de políticas y tecnologías que aseguran que las personas adecuadas tengan acceso a los recursos correctos en el momento adecuado.
- **Gestión de Parcheo**: Proceso de aplicar actualizaciones y parches de seguridad a software y sistemas para corregir vulnerabilidades.
- **HTTPS (Hypertext Transfer Protocol Secure):** es un protocolo seguro para proteger la conexión de un navegador y un sitio web.
- **Ingeniería Social**: Técnica utilizada para manipular a las personas y obtener información confidencial, como contraseñas o datos personales, a través de engaños.
- **Integridad**: Garantía de que la información no ha sido alterada de manera no autorizada, asegurando su exactitud y consistencia.
- **Malware**: Software malicioso diseñado para infiltrarse o dañar un sistema, incluyendo virus, gusanos, troyanos y ransomware.
- **Malware Ransomware**: Tipo de malware que cifra los archivos de un sistema y exige un rescate para su recuperación.
- **Mitigación**: Estrategias y acciones implementadas para reducir la probabilidad o impacto de un riesgo o amenaza.
- **Phishing**: Técnica de fraude en línea que intenta engañar a las personas para que revelen información confidencial, como contraseñas o datos bancarios, a través de correos electrónicos o sitios web falsos.
- **Phishing Dirigido (Spear Phishing)**: Variante de phishing que se dirige a individuos o empresas específicas, utilizando información personal para aumentar la probabilidad de éxito.
- **Red de Área Amplia (WAN)**: Red que conecta dispositivos en áreas geográficas más extensas, como ciudades o países.
- **Red de Área Local (LAN)**: Red que conecta dispositivos dentro de un área geográfica limitada, como una oficina o un edificio.
- **Redundancia**: Estrategia de seguridad que implica tener copias de seguridad o sistemas alternativos para asegurar la continuidad operativa en caso de fallos.
- **Seguridad en la Nube**: Conjunto de políticas, tecnologías y controles diseñados para proteger datos, aplicaciones y servicios en entornos de computación en la nube.
- **Seguridad de Aplicaciones**: Prácticas y tecnologías que protegen aplicaciones de software contra amenazas y vulnerabilidades.
- **Sistemas de Detección de Intrusos (IDS)**: Herramientas que monitorean redes o sistemas en busca de actividades maliciosas o violaciones de políticas.

7 Glosario de términos

- **Sniffing**: Técnica de interceptación de datos en tránsito, donde un atacante puede capturar información que no está cifrada.
- **Spoofing**: Técnica utilizada para engañar a un sistema o usuario haciéndose pasar por otra entidad, como un sitio web o dirección de correo electrónico legítima.
- **Token de Seguridad**: Dispositivo o software que genera un código único para la autenticación de usuarios, a menudo utilizado en MFA.
- **Tríada de la Ciberseguridad (CID)**: Modelo que se basa en tres principios fundamentales: Confidencialidad, Integridad y Disponibilidad, que deben ser garantizados en cualquier sistema de información.
- **VMS (Video Management System)**: Sistema de gestión de video.
- **VPN (Virtual Private Network)**: (Red Privada Virtual) es una herramienta que cifra las conexione en internet**.**
- **Vulnerabilidad**: Debilidad en un sistema, aplicación o red que puede ser explotada por un atacante para comprometer la seguridad.
- **Whaling**: Tipo de phishing que se dirige a altos ejecutivos o personas influyentes dentro de una organización, buscando obtener información crítica.
- **Zero Trust Architecture**: Modelo de seguridad que asume que las amenazas pueden estar tanto dentro como fuera de la red, y que, por lo tanto, no confía en ningún usuario o dispositivo por defecto.

Elaborado por el Área de
Trabajo de ciberseguridad de:

AES
ASOCIACIÓN ESPAÑOLA
EMPRESAS DE SEGURIDAD

C/Alcalá, 99 2ºA - 28009 Madrid
Telf. 915 765 225

www.aesfundacion.es
patronato@aesfundacion.es

@FundacionAES AES Fundación