AES FUNDACIÓN

Concienciando a la industria en ciberseguridad 2025

Índice

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.

Introducción
Concienciando a la industria

El *área de trabajo de ciberseguridad* de la Asociación Española de empresas de Seguridad (AES) lleva años trabajando para concienciar a sus asociados sobre la necesidad de mejorar la ciberseguridad tanto de sus sistemas de información y comunicaciones (utilizados en su propia gestión empresarial o para la prestación de servicios a clientes), así como de los sistemas que diseñan, fabrican, implantan y mantienen.

Este compromiso con la ciberseguridad forma parte de la responsabilidad de AES para con la seguridad de la sociedad, como declara la asociación en su manifiesto 2020-2022:

> "*Una de las necesidades más básicas de la sociedad actual es la protección frente a las amenazas, en cualquiera de las formas en las que se produzcan. Sin las medidas de protección adecuadas, los ciudadanos que conforman la sociedad afrontan riesgos.*"

El fruto del trabajo del área de ciberseguridad de AES se ha plasmado en varios documentos y artículos disponibles para su descarga en las páginas web de la asociación, https://www.aesseguridad.es/, y de AES Fundación https://aesfundacion.es/.

Durante el año 2025 se han publicado en los boletines y en las newsletters de AES Fundación una serie de artículos sobre la importancia de la ciberseguridad en todos los ámbitos de las operaciones de las empresas, haciendo foco especialmente en la problemática asociada a los Sistemas Electrónicos de Seguridad. Todos estos contenidos se han recopilado en la presente publicación.

Además, el área de trabajo de ciberseguridad no solo ha estado trabajando en la divulgación y concienciación sobre la importancia de aplicar criterios de ciberseguridad en Sistemas Electrónicos de Seguridad, también ha colaborado con el resto de las áreas de trabajo de AES aportando la visión de la ciberseguridad como elemento transversal e imprescindible a la hora de garantizar la protección de personas y bienes.

Durante el próximo año seguiremos ampliando las actividades de divulgación y concienciación en ciberseguridad, aumentando su difusión utilizando todos los canales y formatos que puedan estar a nuestro alcance. Además, trabajaremos en el desarrollo de guías sectoriales específicas que complementen las guías que han elaborado otras áreas de trabajo de AES, y que ayuden al cumplimiento de la regulación actual y a la adecuación a lo establecido por las directivas NIS2 y CER.

Ricardo Cañizares Sales

La ciberseguridad es cosa de todos

Las personas son uno de los principales activos con los que cuenta una organización. No existe ninguna organización pública o privada que desarrolle sus actividades sin la participación de personas. Las organizaciones alcanzan sus objetivos de negocio gracias al esfuerzo y dedicación de las personas que forman parte de la misma, por ello, es obvio que las personas son un activo de la organización que es necesario proteger.

Otro de los más valiosos de cualquier organización es la información, y la ciberseguridad se ha convertido en un elemento clave a la hora de proteger la información para garantizar su confidencialidad, su integridad y su disponibilidad.

Cuando se compromete la confidencialidad, la integridad, o la disponibilidad de la información de una organización, se está comprometiendo la continuidad de sus operaciones, y por lo tanto su capacidad de alcanzar sus objetivos de negocio, lo que pone en riesgo su propia existencia.

Todas las normas y estándares de ciberseguridad que se han publicado incluyen requisitos específicos dedicados a tratar aspectos relativos al personal. Esto se debe a que las personas son el eslabón más importante, y en muchos casos el más débil, del conjunto de elementos y procesos que ayudan a garantizar la ciberseguridad de las organizaciones. Igualmente, en toda la legislación en vigor relativa a la ciberseguridad se contemplan requisitos de obligado cumplimiento relativos al personal.

La ciberseguridad es cosa de todos

La alta dirección de una organización es la responsable de establecer una política de ciberseguridad, de implantar un modelo organizativo, y de dotar de los recursos que permitan implementarla de forma eficaz y eficiente. Además, debe tener en cuenta que la ciberseguridad es una prioridad estratégica que afecta a todos los aspectos de la organización. Esta política de ciberseguridad debe contemplar las funciones y responsabilidades de todo el personal de la organización, en relación con la confidencialidad, la integridad, y la disponibilidad de la información.

La responsabilidad de la ciberseguridad no es solo de la alta dirección y de los técnicos, existen funciones y responsabilidades relativas a la ciberseguridad en todos los niveles de la organización:

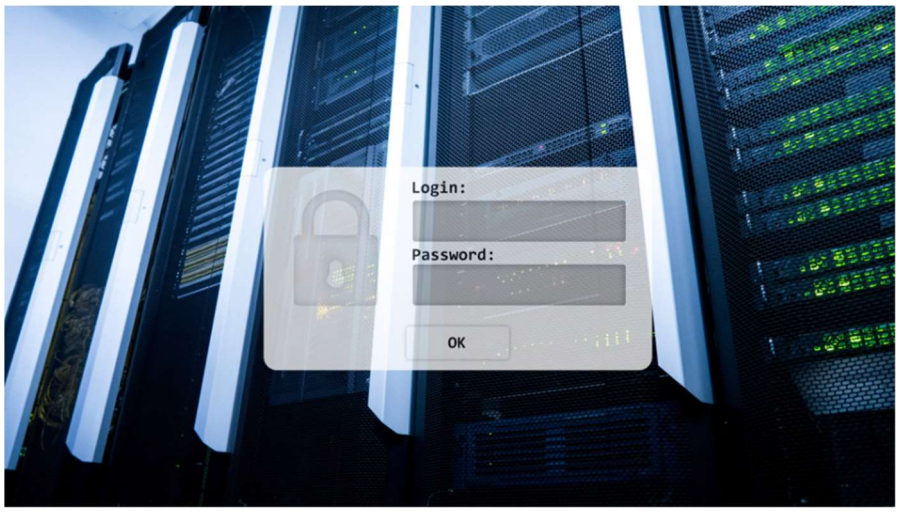
- Alta dirección
- Gerentes
- Gestores
- Técnicos
- Personal de base

Es imprescindible que todo el personal sea consciente de su rol en la ciberseguridad de la organización, ya que los usuarios finales y los empleados de todos los niveles de responsabilidad son la primera línea de defensa contra las ciberamenazas. Si disponen de la formación y concienciación adecuada, tienen la capacidad de identificar y evitar amenazas como correos electrónicos fraudulentos, enlaces sospechosos y descargas no seguras. Por tanto, la concienciación y la formación permanente son claves para construir una cultura de ciberseguridad dentro de las organizaciones.

Una de las medidas más efectivas a la hora de mejorar la ciberseguridad es la formación y concienciación. Una persona sin la formación adecuada es una de las mayores amenazas que existen para el correcto funcionamiento de una organización. Por ello, se debe proporcionar a todo el personal la formación necesaria para que conozca los procedimientos operativos y de ciberseguridad para el correcto desarrollo de las actividades inherentes a su puesto de trabajo. Esta formación debe ser planificada teniendo en cuenta las necesidades presentes y futuras.

La ciberseguridad es cosa de todos

La formación y concienciación en ciberseguridad no sólo se debe proporcionar en el momento de su incorporación a la organización, sino que debe actualizarse periódicamente respecto a las nuevas amenazas que surgen diariamente y los cambios en la legislación aplicable. Conocer las amenazas más comunes y cómo protegerse de ellas es el primer paso para crear un entorno digital más seguro.



Todos los miembros de una organización, cada uno a su nivel, deben tener perfectamente claro qué "se debe hacer" y qué "no se debe hacer" para no poner en riesgo a la organización. Por ejemplo:

Qué no se debe hacer

- X Utilizar los recursos informáticos para fines no autorizados.
- X Dejar el ordenador desatendido y sin bloquear durante períodos prolongados.
- X Compartir usuarios y contraseñas.
- X Revelar datos confidenciales a personas no autorizadas.
- X Instalar software no autorizado.
- X Desactivar o desinstalar el antivirus, antispyware u otro software de seguridad.
- X No informar de los incidentes de ciberseguridad.
- X Conectar equipos no autorizados a la red de la organización.
- X .....

Qué se debe hacer

- ✓ Conocer y entender su responsabilidad respecto a la ciberseguridad.
- ✓ Mantenerse informado sobre las políticas y procedimientos de ciberseguridad.
- ✓ Conocer los principales tipos de ciberamenazas y la manera de actuar ante ellas.
- ✓ Informar de los incidentes de ciberseguridad y eventos extraños.
- ✓ Actualizar las contraseñas de acuerdo con la política en vigor.
- ✓ Conocer y aplicar los procedimientos de uso del correo electrónico.
- ✓ ….

La ciberseguridad es una responsabilidad compartida que requiere la implicación de todos los miembros de la organización, desde la alta dirección hasta el último empleado de base.

Los técnicos de ciberseguridad no pueden proteger a la organización por sí solos, aunque dispongan de los mejores recursos técnicos. Siempre van a necesitar el apoyo y la colaboración de todos los miembros de la organización.

Del mismo modo, por muy comprometida que esté la alta dirección con la ciberseguridad, promulgue una política robusta, implante un buen modelo organizativo y dote al personal de los recursos necesarios, si no consigue crear una conciencia y compromiso colectivo de todo el personal, esta inversión no servirá de nada.

La ciberseguridad no debe ser vista como una tarea exclusiva de técnicos, sino como una responsabilidad colectiva que requiere la participación de todo el personal de la organización.

“La ciberseguridad es cosa de todos”

Ricardo Cañizares Sales

El desafío de la seguridad en los dispositivos de almacenamiento

En la era digital, la protección de la información es una prioridad para individuos y organizaciones. Los dispositivos de almacenamiento, discos duros, memorias USB y la nube, son esenciales para el resguardo de datos, pero también representan una de las principales vulnerabilidades en materia de seguridad de estos. ¿Estamos realmente preparados para garantizar su seguridad?

Uno de los principales riesgos es el acceso no autorizado a la información. Dispositivos de almacenamiento sin cifrado pueden ser fácilmente sustraídos o comprometidos, exponiendo datos sensibles. La solución más evidente es la implementación de cifrado robusto, pero sorprendentemente, muchas empresas aún no lo adoptan de manera generalizada.

Otro problema clave es la proliferación de dispositivos extraíbles. Si bien son prácticos, estos dispositivos pueden ser una puerta de entrada para malware y robo de información. Las organizaciones deben establecer controles estrictos sobre su uso, incluyendo restricciones de acceso y monitoreo continuo.

El almacenamiento en la nube también plantea interrogantes. A pesar de que los proveedores ofrecen medidas de seguridad avanzadas, los riesgos persisten, especialmente si los usuarios no adoptan buenas prácticas como la autenticación multifactor y la gestión adecuada de permisos.

La eliminación segura de los datos es un aspecto muchas veces ignorado. Recuperar información de un disco duro formateado es más fácil de lo que se cree, lo que hace indispensable la aplicación de técnicas de borrado seguro o destrucción física en casos críticos.

La seguridad de los dispositivos de almacenamiento no es solo una cuestión técnica, sino también de cultura organizacional y personal. Es imperativo que individuos y empresas adopten estrategias efectivas para proteger la información, entendiendo que la prevención siempre será la mejor defensa en el mundo digital.

El desafío de la seguridad en los dispositivos de almacenamiento

Desde el punto de vista del Esquema Nacional de Seguridad (ENS), la mejor manera de gestionar los dispositivos de almacenamiento es adoptando un enfoque integral que combine medidas técnicas, organizativas y procedimentales. Este enfoque debe estar alineado con los niveles de seguridad establecidos (Básico, Medio y Alto) y contemplar los siguientes aspectos clave:

1. Clasificación y Evaluación de la Información

- **Identificación y Clasificación:** Antes de gestionar cualquier dispositivo, es esencial clasificar la información almacenada en función de su sensibilidad. Esto permite definir el nivel de protección requerido y aplicar las medidas correspondientes.

2. Control de Acceso y Autenticación

- **Acceso Restringido:** Solo el personal autorizado debe tener acceso a los dispositivos de almacenamiento. Se deben implementar mecanismos de autenticación robustos que eviten accesos no autorizados tanto en el ámbito físico como en el lógico.

3. Cifrado de Datos

- **Protección en Reposo y en Tránsito:** Es imprescindible cifrar los datos almacenados utilizando algoritmos aprobados por el Centro Criptológico Nacional (CCN). El cifrado protege la confidencialidad de la información, incluso en caso de pérdida o robo del dispositivo.

4. Protección Física y Lógica

- **Medidas Físicas:** Los dispositivos deben ubicarse en entornos controlados y seguros, con acceso restringido a personal autorizado.
- **Medidas Lógicas:** Además del cifrado, es recomendable implementar firewalls, sistemas de detección de intrusiones y otras medidas de seguridad que dificulten el acceso no autorizado desde el ámbito digital.

5. Registro, Auditoría y Monitorización

- **Seguimiento de Accesos:** Se deben establecer registros de auditoría que documenten quién accede a los dispositivos y qué operaciones se realizan. Esta monitorización continua es clave para detectar y responder a posibles incidentes de seguridad.

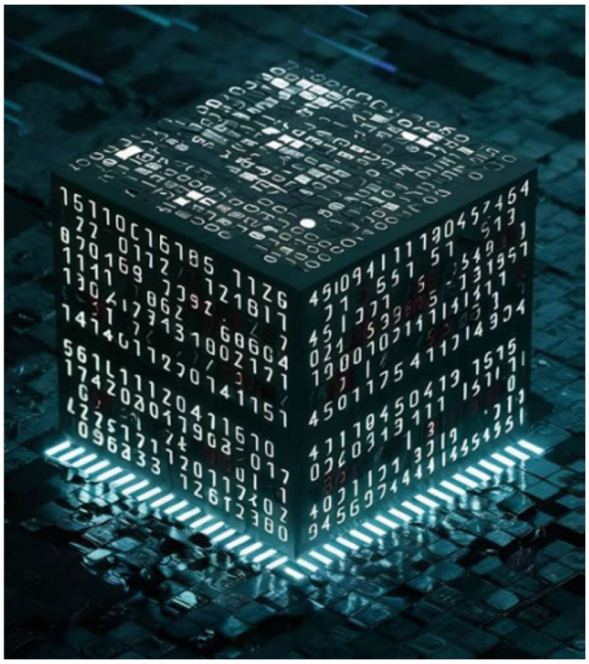
6. Gestión de Dispositivos Extraíbles

- **Control Estricto:** Dado que los dispositivos extraíbles (como USB o discos duros portátiles) pueden representar una vulnerabilidad, es fundamental restringir su uso a través de políticas claras y herramientas de control que impidan la conexión de dispositivos no autorizados.

7. Procedimientos de Eliminación Segura

- **Borrado Irreversible:** Cuando un dispositivo de almacenamiento se retira de servicio o se desecha, deben aplicarse métodos de eliminación segura (como la destrucción física) para garantizar que la información no pueda ser recuperada.

En función de la categorización de los datos, y siguiendo con lo que dictamina el ENS, así como el tipo de organización tendremos las siguientes medidas técnicas y organizativas:



Medidas Técnicas

Cifrado de la Información

- **Nivel Básico:**
  Utilizar cifrado para datos sensibles en dispositivos externos, aunque de forma no obligatoria para toda la información.
- **Nivel Medio:**
  Implementar cifrado obligatorio en reposo y, cuando sea posible, también en tránsito. Se deben utilizar algoritmos aprobados por el Centro Criptológico Nacional (CCN).
- **Nivel Alto:**
  Requerir el cifrado de todos los datos almacenados en dispositivos externos con algoritmos robustos y certificados. Además, se puede exigir el uso de módulos criptográficos hardware (HSM) para operaciones críticas.

Monitorización y Auditoría

- **Registro de Actividades:**
  Configurar sistemas de logging y auditoría para registrar la conexión, el uso y la desconexión de dispositivos externos, permitiendo rastrear accesos no autorizados o comportamientos anómalos.
- **Alertas y Detección:**
  En niveles medios y altos, implementar soluciones de monitorización en tiempo real que generen alertas ante actividades sospechosas o intentos de conexión de dispositivos no autorizados.

Protección Física y Lógica

- **Protección Física:**
  Asegurar que los dispositivos externos se utilicen en entornos controlados. Por ejemplo, mantener áreas restringidas y controladas donde se conecten estos dispositivos, especialmente en casos de alta sensibilidad.
- **Actualización y Parcheo:**
  Garantizar que tanto los dispositivos como los sistemas a los que se conectan cuenten con las últimas actualizaciones y parches de seguridad.

Control de Acceso y Gestión de Dispositivos

- **Inventario y Registro:**
  Mantener un inventario actualizado de todos los dispositivos de almacenamiento externos que se conectan a la red, con registros de asignación y uso.
- **Autenticación y Autorización:**
  Establecer mecanismos de autenticación (por ejemplo, contraseñas robustas, autenticación multifactor) para el acceso a los datos almacenados en dispositivos externos, especialmente en entornos de nivel medio y alto.
- **Control de Puertos y Conexiones:**
  Implementar soluciones de gestión de dispositivos (MDM o software de control de puertos USB) que permitan autorizar únicamente dispositivos previamente registrados.

El desafío de la seguridad en los dispositivos de almacenamiento

Actualmente encontramos distintas organizaciones con los puertos “mapeados”, deshabilitados, impidiendo así infecciones maliciosas, fuga de información, control sobre los datos…, veamos algunas de las ventajas y desventajas sobre está práctica tan extendida:

Ventajas de Deshabilitar Puertos

Reducción de Riesgos de Malware y Exfiltración: Al limitar el uso de dispositivos externos, se disminuye la posibilidad de que se conecten medios infectados o se extraiga información sensible de forma no autorizada.

Control de Dispositivos No Autorizados: Restringir el uso de dispositivos extraíbles ayuda a garantizar que solo se usen aquellos autorizados y configurados conforme a las políticas de seguridad.

Consideraciones y Desafíos

Impacto en la Productividad: Muchos empleados dependen de la conectividad a través de puertos USB o similares para actividades laborales legítimas (por ejemplo, transferencia de datos o conexión de periféricos autorizados). Deshabilitar estos puertos podría entorpecer el flujo de trabajo, por lo que es importante equilibrar la seguridad con la operatividad.

Flexibilidad y Excepciones**:** En algunos casos, puede ser preferible implementar soluciones de control de dispositivos, que permitan registrar y autorizar conexiones específicas, en lugar de una desactivación total. Esto se alinea con la necesidad del ENS de aplicar medidas adaptadas al nivel de riesgo y a las necesidades del entorno.

Estrategia Multicapa:
El ENS promueve un enfoque integral, por lo que la protección del perímetro no debe depender únicamente de la desactivación de puertos. Se recomienda combinarla con otras medidas, como el cifrado de datos, la gestión centralizada de dispositivos (MDM), monitorización de accesos y políticas de uso, para crear una defensa en profundidad.

Medidas Organizativas

Políticas y Procedimientos

- **Política de Uso de Dispositivos Externos:**
  Definir y comunicar claramente las políticas de uso, estableciendo qué dispositivos pueden conectarse, en qué situaciones y bajo qué condiciones se permite el acceso a la información.
- **Procedimientos de Autorización:**
  Establecer un proceso formal para la solicitud, revisión y autorización de dispositivos externos, asegurando que solo se utilicen aquellos que cumplan con los estándares de seguridad exigidos.

Formación y Concienciación

- **Capacitación Regular:**
  Impartir programas de formación y concienciación sobre los riesgos asociados al uso de dispositivos externos, el correcto manejo de la información y las buenas prácticas de seguridad.
- **Simulacros y Evaluaciones:**
  Realizar simulacros y evaluaciones periódicas para comprobar el cumplimiento de las políticas de seguridad y la correcta respuesta ante incidentes relacionados con dispositivos externos.

Gestión de Incidentes y Respuesta

- **Protocolos de Respuesta:**
  Diseñar y documentar procedimientos específicos para la detección, análisis y respuesta ante incidentes que involucren dispositivos externos, incluyendo el borrado seguro de datos y la revocación de accesos.
- **Auditorías y Revisión Periódica:**
  Realizar auditorías internas y externas de forma regular para verificar el cumplimiento de las medidas implementadas y detectar posibles áreas de mejora.

Control de Proveedores y Equipos

- **Evaluación de Proveedores:**
  Asegurar que los proveedores de soluciones (como sistemas de cifrado o de gestión de dispositivos) cumplan con los estándares y directrices del ENS.
- **Actualización de Equipos:**
  Garantizar que los equipos y dispositivos externos se sometan a revisiones periódicas para asegurar su integridad y la correcta aplicación de las medidas de seguridad.

Para trabajar de forma segura con dispositivos de almacenamiento externos, el **ENS recomienda** adoptar un *enfoque en capas* que combine medidas técnicas –como el cifrado, el control de acceso, la monitorización y la protección física– con medidas organizativas, tales como políticas claras, formación, procedimientos de autorización y protocolos de respuesta ante incidentes. La implementación de estas medidas debe adaptarse a los diferentes niveles de seguridad (Básico, Medio y Alto), asegurando que en cada caso se minimicen los riesgos asociados a la utilización de dispositivos externos sin afectar la operatividad de la organización.

Jorge Noguerales Bautista

IT y OT en la era del ciberpeligro:
¿Quién protege a los guardianes del mundo digital e industrial?

Introducción: Un mundo conectado, un riesgo aumentado

Imagina una fábrica automatizada, donde brazos robóticos ensamblan productos con precisión milimétrica. Al otro lado del espectro, una empresa multinacional mueve millones de datos en la nube cada segundo. Ahora, imagina que un ataque cibernético paraliza ambos mundos al mismo tiempo: las máquinas se detienen, los datos son secuestrados y el caos se apodera de la organización.

Esto no es un guion de ciencia ficción. IT (Tecnologías de la Información) y OT (Tecnologías de Operación) están cada vez más interconectadas, y con ello, la superficie de ataque crece exponencialmente. La pregunta ya no es si sucederá un ciberataque, sino cuándo y cómo de preparados estamos para enfrentarlo.

Bienvenido al campo de batalla de la ciberseguridad en IT y OT.

La seguridad y ciberseguridad son aspectos esenciales en los entornos de IT (Tecnologías de la Información) y OT (Tecnologías de Operación). A medida que la digitalización y la interconexión de sistemas avanzan, la protección de infraestructuras críticas y sistemas industriales se vuelve fundamental. Este artículo explora las diferencias y similitudes entre IT y OT, la importancia de la ciberseguridad en ambos entornos y el marco normativo en Europa y España, incluyendo normativas de obligado cumplimiento y voluntarias, con especial énfasis en IEC 62443, ENS, NIS2, CRA y el reglamento delegado RED.

1. **IT vs. OT: Dos Mundos en Colisión**

   Durante años, IT y OT han sido universos paralelos con objetivos distintos:

   ¿Qué es IT?

   Las Tecnologías de la Información (IT) engloban los sistemas utilizados para la gestión de datos, comunicaciones y procesamiento de información en organizaciones. Se centran en la integridad, confidencialidad y disponibilidad de la información. Algunos ejemplos de IT incluyen:

   - ✅ Redes corporativas
   - ✅ Servidores y bases de datos
   - ✅ Aplicaciones empresariales
   - ✅ Sistemas de correo electrónico

Protege la información. Su foco está en la confidencialidad, la integridad y la disponibilidad de los datos.

¿Qué es OT?

Las Tecnologías de Operación (OT) incluyen los sistemas de control industrial (ICS) que supervisan y gestionan procesos físicos en sectores como la energía, manufactura, transporte y agua. OT se enfoca en la seguridad y disponibilidad de los sistemas. Algunos ejemplos incluyen:

- Sistemas SCADA (Supervisory Control and Data Acquisition)
- Controladores Lógicos Programables (PLC)
- Redes industriales
- Sensores y actuadores

Asegura la operación. Su prioridad es la disponibilidad, seguida de la integridad y, en último lugar, la confidencialidad.

Pero en un mundo hiperconectado, estos mundos ya no pueden mantenerse separados. La Industria 4.0, la digitalización y el IoT industrial (IIoT) han abierto puertas que antes no existían.

¿En qué se parecen y en qué chocan?

Lo que antes eran barreras infranqueables entre IT y OT ahora son puertas de entrada para ciberdelincuentes.

A medida que IT y OT convergen en la Industria 4.0, la ciberseguridad en OT se vuelve un desafío crucial, ya que estos sistemas fueron diseñados originalmente sin considerar amenazas cibernéticas avanzadas.

Si no reforzamos la seguridad de ambos, la convergencia puede convertirse en una vulnerabilidad masiva.

2. El auge del cibercrimen en la industria

Los ataques ya están aquí. Casos como el ransomware que paraliza empresas esenciales, como los ciberataques a redes eléctricas en Ucrania son solo la punta del iceberg. Los delincuentes han entendido que atacar OT no solo genera pérdidas económicas, sino que puede desatar el caos en sectores clave como energía, transporte y salud.

IT y OT en la era del ciberpeligro:
¿Quién protege a los guardianes del mundo digital e industrial?

La importante digitalización de infraestructuras críticas hace que un ciberataque pueda generar apagones, interrupciones en la cadena de suministro o incluso poner en riesgo vidas humanas.

Ambos entornos están expuestos a amenazas como:

- ✅ Ataques de ransomware que pueden paralizar operaciones
- ✅ Vulnerabilidades en software y hardware
- ✅ Acceso no autorizado a sistemas críticos
- ✅ Amenazas internas (empleados con acceso privilegiado)
- ✅ Ransomware: Cifrado de datos y equipos industriales, paralizando la producción.
- ✅ Ataques de phishing: Accesos indebidos que terminan en intrusiones en redes críticas.
- ✅ Exploits en software heredado: Muchos sistemas OT operan con software obsoleto y sin actualizaciones.
- ✅ Manipulación de procesos: Alteraciones en sensores y PLCs que pueden causar fallos catastróficos.

El reto es que muchas organizaciones aún operan bajo el mito de que "OT está aislado", cuando en realidad, cada vez más dispositivos industriales están conectados a redes IT y a Internet.

3. La Ciberseguridad en IT y OT no es una opción, es una necesidad

Las empresas ya no pueden depender de la seguridad por oscuridad. Es momento de adoptar una ciberseguridad proactiva y regulada.

Europa y España han tomado cartas en el asunto con normativas clave que definen qué organizaciones deben cumplir con requisitos de seguridad mínimos.

Normativas obligatorias en ciberseguridad

- NIS2 (Directiva de Seguridad de Redes y Sistemas de Información 2)
  - ↳ Afecta a sectores esenciales como energía, transporte y salud.
  - ↳ Exige una gestión de riesgos y respuesta ante incidentes más estricta.
- ENS (Esquema Nacional de Seguridad - España)
  - ↳ Aplica a administraciones públicas y empresas que trabajan con ellas.
  - ↳ Exige controles de seguridad para proteger datos y servicios digitales.
- CRA (Cyber Resilience Act)
  - ↳ Impacta a fabricantes de hardware y software.
  - ↳ Obliga a diseñar productos con seguridad integrada desde el inicio.
- Reglamento delegado RED
  - ↳ Garantiza que dispositivos inalámbricos sean seguros antes de venderse.
  - ↳ Impide que equipos inseguros sean comercializados en la UE.

Normativas voluntarias y buenas prácticas

- IEC 62443:

  ↳ El estándar de referencia para proteger sistemas OT e industriales. Framework de referencia para proteger sistemas industriales.

  ↳ Aplicable a fabricantes, integradores y operadores de OT

- ISO 27001:

  ↳ La biblia de la gestión de seguridad en IT. Estándar internacional para establecer un Sistema de Gestión de Seguridad de la Información (SGSI).

Cumplir con estas normativas no es solo evitar sanciones; es construir un escudo de defensa robusto frente a los ciberataques.

4. Claves para blindar IT y OT: De la teoría a la acción

No basta con conocer las normativas, hay que aplicarlas de manera efectiva. Aquí algunas recomendaciones para cada marco regulador:

- IEC 62443 (Ciberseguridad en Sistemas Industriales)

  ✅ Segregación de redes: Separar IT y OT con firewalls industriales.

  ✅ Control de accesos: Aplicar el principio de “mínimos privilegios”.

  ✅ Monitorización en tiempo real: Detectar anomalías antes de que se conviertan en incidentes.

- ENS (Esquema Nacional de Seguridad)

  ✅ Auditorías periódicas: No esperar a ser atacado para detectar vulnerabilidades.

  ✅ Autenticación robusta: Prohibido el uso de credenciales débiles o compartidas.

  ✅ Planes de contingencia: Simular ataques y preparar respuestas eficientes.

- NIS2 (Resiliencia en Infraestructuras Críticas)

  ✅ Registro y análisis de incidentes: Notificar ataques en un plazo de 24 a 72 horas.

  ✅ Gestión de proveedores: Asegurar que terceros cumplen con estándares de ciberseguridad.

- CRA y RED (Seguridad en Productos Digitales e Inalámbricos)

  ✅ Security by Design: Diseñar software y hardware con ciberseguridad integrada.

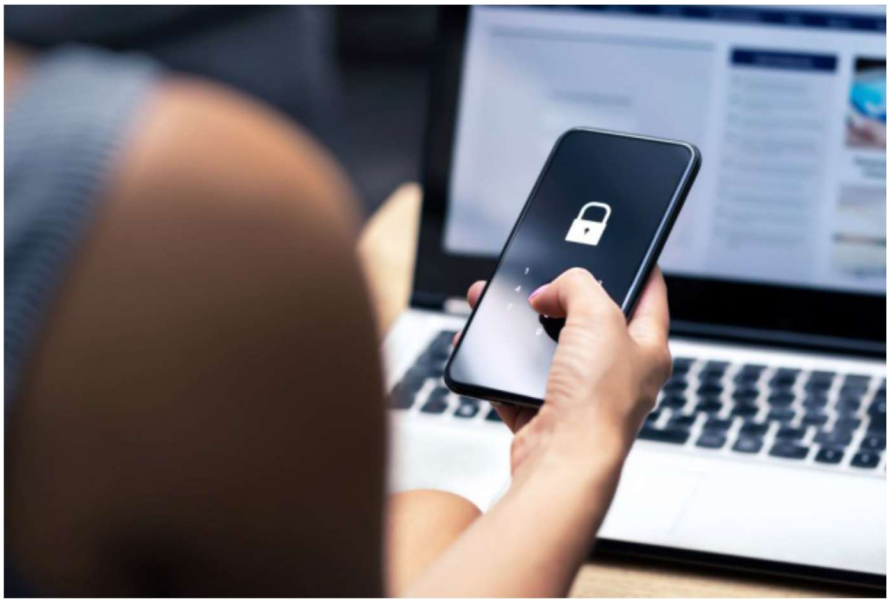
  ✅ Asegurar que el software de productos digitales se actualice regularmente.

  ✅ Implementar requisitos de seguridad desde la fase de diseño (Security by Design).

  ✅ Actualización continua: No dejar productos vulnerables en el mercado.

  ✅ Verificar que los dispositivos cumplen con los requisitos de ciberseguridad antes de su comercialización.

  ✅ Evaluar el impacto de posibles vulnerabilidades en redes conectadas.



Conclusión: El futuro es seguro o no será

La convergencia entre IT y OT está cada vez más presente, pero también lo son los riesgos. Cada dispositivo conectado es una posible puerta o vector para atacantes. Cada brecha de seguridad puede costar millones y poner en peligro infraestructuras críticas e incluso a las personas.

La convergencia entre IT y OT requiere estrategias de ciberseguridad robustas para proteger tanto la información como la infraestructura crítica. Cumplir con normativas como NIS2, ENS, CRA y el reglamento RED es fundamental para garantizar la seguridad en ambos entornos. Además, adoptar estándares como IEC 62443 fortalece la resiliencia de los sistemas industriales frente a ciberataques.

Las organizaciones deben pasar de la ciberseguridad reactiva a la ciberseguridad preventiva. Implementar regulaciones, fortalecer controles y fomentar la conciencia en seguridad es la única forma de proteger el futuro digital e industrial.

La ciberseguridad en IT y OT dependerá de la integración de buenas prácticas, normativas y tecnologías avanzadas para mitigar riesgos en un mundo cada vez más interconectado.

Porque al final, la pregunta no es si te van a atacar, sino si estarás preparado cuando ocurra.

César de la Serna

¿Qué Formación en Ciberseguridad necesitamos en Seguridad Privada?

En un escenario donde los sistemas de seguridad que protegen domicilios, empresas, administraciones públicas e infraestructuras críticas son digitales y por tanto potenciales objetivos de ciberataques, la Formación en Ciberseguridad es una necesidad estratégica para la Seguridad Privada. Instalar una cámara o configurar una central de alarmas requiere entender los riesgos digitales en cada uno de los procesos y en todas nuestras actividades. Es indispensable saber cómo proteger los dispositivos conectados y cómo reaccionar ante un incidente de ciberseguridad.

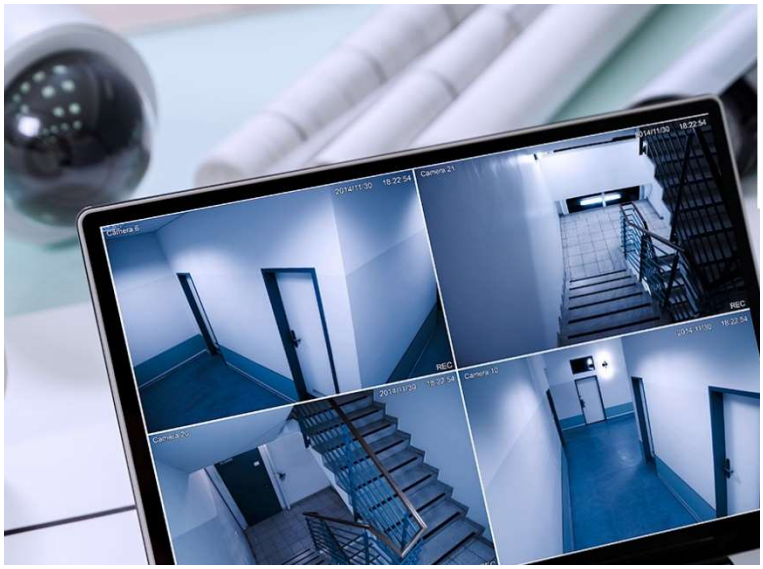
Las Administraciones y las Fuerzas de Seguridad alertan de que el crecimiento de los ciberataques es exponencial y las ciberamenazas se incrementan en varios frentes, desde la ciberdelincuencia común, los grupos y amenazas avanzadas, hasta el ciberterrorismo o ciberactivismo derivado de un escenario geopolítico muy inestable.

La Ciberseguridad debe formar parte de la formación esencial del personal de las empresas de seguridad, así como de los usuarios que gestionen sus sistemas, pero no existe una fórmula única, sino que debemos planificar el tipo de formación que resulta más adecuada para cada perfil y organización.

¿Qué Formación en Ciberseguridad necesitamos en Seguridad Privada?

La Convergencia de la Seguridad Física y la Ciberseguridad

Tradicionalmente, la Seguridad Física y la Ciberseguridad han sido mundos separados. Una se ocupaba de proteger lo tangible —personas, edificios, bienes— y otra exclusivamente de lo digital —datos, redes, software—. Si el bien a proteger es digital se dejaba al cuidado del departamento de IT. Ahora sabemos que plantearlo así es un error, ya que las tecnologías, como el Internet de las Cosas (IoT), los sistemas de videovigilancia IP o las centrales de alarmas inteligentes, han eliminado esa separación.



Un ataque a un sistema de seguridad ya no requiere necesariamente estar en el lugar para forzar una puerta o desactivar una alarma. Basta con vulnerar un router mal configurado, acceder remotamente a una cámara IP con una contraseña débil o explotar un fallo en el software de una central receptora de alarmas (CRA). Los ciberdelincuentes pueden atacar desde cualquier parte del mundo.

Debemos ser conscientes de los riesgos que para nuestras organizaciones supondría dejar cámaras de videovigilancia sin la suficiente protección, o sistemas de control de acceso que puedan ser indebidamente manipulados a distancia, o instalaciones de seguridad integral comprometidas por técnicas de ransomware, spoofing o denegación de servicio. Todo esto nos lleva a pensar que, sin una capa sólida de Ciberseguridad, incluso el sistema de seguridad más sofisticado es vulnerable.

Las Brechas de Formación en el Sector de la Seguridad Privada

A pesar de esta realidad, la mayoría de los profesionales del sector de la seguridad privada no cuenta con una formación sólida en ciberseguridad. Instaladores, vigilantes, operadores de CRAs, técnicos comerciales y directores de seguridad siguen recibiendo, en muchos casos, una capacitación centrada exclusivamente en la seguridad física o en la tecnología desde un punto de vista funcional, pero no desde una perspectiva del riesgo digital.

¿Qué Formación en Ciberseguridad necesitamos en Seguridad Privada?

La normativa actual en Seguridad Privada no exige conocimientos específicos de ciberseguridad a los profesionales del sector, lo que genera una peligrosa brecha. Como bien sabemos en el sector, los mínimos exigidos por la normativa suelen ir por detrás de las capacidades (y vulnerabilidades) tecnológicas, los riesgos y las amenazas reales.

Incluso cuando se trabaja con sistemas tecnológicamente avanzados, el conocimiento sobre configuraciones seguras, gestión de contraseñas robustas, detección de accesos no autorizados o actualizaciones de firmware suele ser demasiado superficial o inexistente.

Este vacío formativo y falta de concienciación expone a clientes (pensemos en industrias, servicios esenciales, o infraestructuras críticas), y puede provocar incidentes que impacten en la reputación y responsabilidad de las propias empresas de seguridad. Un fallo de ciberseguridad en un sistema instalado por una empresa puede derivar en consecuencias legales, económicas y de imagen.

¿Qué Formación en Ciberseguridad necesita el Sector?

En primer lugar, como toda formación, la de ciberseguridad debe estar adaptada a los distintos perfiles profesionales del sector de la seguridad privada.

No todo el personal puede ni debe profundizar en los aspectos más técnicos del hacking ético o el pentesting. Se trata de ofrecer conocimientos adecuados adaptados al puesto, y para ello, debemos analizar los objetivos y temarios contemplados en la formación para asegurarnos que es la más conveniente.

Competencias de Ciberseguridad según Perfil Profesional

Perfil Profesional	Competencias Clave de Ciberseguridad
Instaladores / Técnicos de Sistemas	• Configuración segura de equipos y dispositivos. • Gestión de contraseñas y credenciales de acceso. • Segmentación de redes y uso de VPN. • Actualización de firmware.
Operadores de CRA	• Conocimiento básico de ciberamenazas: phishing, spoofing, denegación de servicio. • Reconocimiento de señales sospechosas y anomalías digitales. • Protocolos de respuesta ante incidentes digitales.
Vigilantes de Seguridad / Supervisores	• Concienciación sobre amenazas digitales (ingeniería social, dispositivos USB maliciosos). • Identificación de posibles intentos de sabotaje tecnológico. • Coordinación con equipos técnicos ante anomalías digitales.
Directores de Seguridad, responsables y mandos intermedios	• Gestión del riesgo. • Cumplimiento (RGPD, ENS, ISO 27001, NIS, etc.). • Desarrollo de políticas internas. • Planes de Continuidad y Resiliencia. • Protección de Infraestructuras Críticas (PIC)
Gestión, Comerciales / Preventa	• Conocimiento de normativas y exigencias legales aplicables. • Concienciación frente a ciberamenazas actuales • Argumentario de ciberseguridad para clientes. • Evaluación de riesgos tecnológicos en instalaciones.

Dificultades al escoger los recursos formativos adecuados

Dependiendo del nivel de profundidad requerido, existen recursos que pueden ayudar a los profesionales de la seguridad privada a adquirir las competencias en Ciberseguridad que necesitan.

El problema principal es distinguir la formación adecuada ante la ausencia actual de una **Formación reglada claramente identificada.** Muchos centros ofrecen módulos de Ciberseguridad, pero los ciclos reglados, de grado medio o superior de sistemas de telecomunicación pueden ser muy extensos, costosos y resultar poco operativos.

También existen cursos básicos de concienciación gratuitos o de bajo coste disponibles a través de plataformas y Administraciones Públicas como INCIBE, pero su objetivo es la concienciación a nivel de entrada y pueden no ser suficientes al nivel necesitado en cada caso por las empresas.

Dado que existen múltiples centros generalistas que ofrezcan formación en ciberseguridad, ante la falta de regulación actual es recomendable consultar con formadores que entiendan las particularidades de la Seguridad Física y la Seguridad Privada, el funcionamiento de las empresas y como adaptar las necesidades a aspectos concretos, como los Centros de Control y las CRA, las tecnologías utilizadas en videovigilancia, el control de accesos o los sistemas de alarmas, así como la normativa específica.

Además, al estar familiarizados con los perfiles profesionales concretos del sector —vigilantes, instaladores, operadores, directores— pueden adaptar los contenidos a su contexto operativo real. Esta orientación práctica y sectorial maximiza la eficacia de la formación y permite una integración más rápida y natural de los conceptos de ciberseguridad en el día a día de los equipos.

Debemos reclamar a nuestros centros de formación, que propongan programas sobre Ciberseguridad lo más adaptados posible a nuestro sector y a sus perfiles profesionales.

La formación en Ciberseguridad no es única, debe estar adaptada a los conocimientos previos y objetivos específicos del personal, y aprovechar metodologías online que permitan realizar itinerarios personalizados y que sean compatibles con la actividad profesional.

Para los casos en los que se requieran certificaciones técnicas, debemos tener un conocimiento previo para distinguir las más relevantes o reconocidas, como ISO 27001, CompTIA, C-Council, CISM o CISA.

Por último, debemos tener en cuenta la formación específica proporcionada por los fabricantes de seguridad electrónica, que ofrecen módulos sobre la Ciberseguridad, aplicada a sus productos.

En todos los casos, será esencial que las empresas de seguridad fomenten la formación continua de su personal, asignen presupuestos específicos y evalúen periódicamente el nivel de Ciberseguridad de sus equipos.

La Formación en Ciberseguridad como mejora competitiva

Además, los clientes están cada vez más informados y preocupados por la ciberseguridad. Incluir esta dimensión en la propuesta de valor de una empresa de seguridad privada ya no es un extra, sino una necesidad.

Invertir en formación no es solo una cuestión de prevención y protección, también representa una oportunidad competitiva para las empresas de seguridad que puede traer beneficios directos para las empresas y los profesionales, como:

- **Mejora de la calidad del servicio:** ofrecer soluciones seguras, robustas y con garantías digitales.
- **Diferenciación comercial**: destacar frente a competidores que no cubren la dimensión cibernética.
- **Reducción de incidentes:** menor riesgo de brechas, reclamaciones o sanciones.
- **Adaptación a futuras normativas:** estar preparados ante posibles exigencias regulatorias.
- **Confianza del clien**te: transmitir una imagen de profesionalidad y responsabilidad digital.

Conclusiones y recomendaciones para las empresas de seguridad

La frontera entre la Seguridad Física y la Ciberseguridad ya no existe. En la práctica, todo sistema de seguridad es hoy también un sistema informático, y por tanto, susceptible de ser atacado digitalmente. Profesionales y empresas del sector de la seguridad privada deben tomar conciencia de esta realidad y prepararse en consecuencia.

La formación en ciberseguridad no es una opción, sino una responsabilidad y también una oportunidad de mejora competitiva. No solo para proteger los activos de los clientes, sino también para garantizar la integridad de las empresas proveedoras y la continuidad de negocio. Mejorar la Formación en Ciberseguridad con determinación nos prepara mejor para ofrecer un servicio más completo y

seguro, contribuyendo al objetivo de la Seguridad Privada que es elevar el nivel general de protección (y también ciberprotección) en nuestra sociedad.

Para una ello, las empresas de seguridad privada deben tener planes de formación para adoptar una cultura de ciberseguridad, para todos los empleados y realizar algunas estrategias concretas.

Las empresas deberían empezar por evaluar el nivel actual de ciberpreparación de sus equipos de profesionales y Diseñar planes de formación escalables, comenzando por los perfiles técnicos y directivos.

De esta forma estarán preparados para establecer políticas de ciberseguridad internas, con protocolos claros y permanentemente actualizados. Si es necesario, las empresas pueden contar con expertos externos en ciberseguridad para auditorías, simulacros o formaciones específicas.

Las empresas pueden contar actualmente con la ayuda de las Asociaciones y las Administraciones Públicas, conocer como impulsan programas de formación, y generan marcos normativos que incluyen la ciberseguridad a la vez que fomentan promover buenas prácticas entre los profesionales.

Fernando Sánchez Raya

Borrado seguro qué es, métodos y por qué aplicarlo

Desde que existe registro de datos, hace miles de años, borrar lo que estaba grabado ha sido sencillo. Con la digitalización de los datos, la eliminación de estos de manera definitiva se hace cada vez más complicada. Un archivo eliminado no desaparece completamente. Su contenido podría ser recuperado con las herramientas adecuadas. Para proceder a la eliminación segura y permanente de datos, ya sean escritos, esquemas, o imágenes, debemos contemplar dos aspectos: métodos y normativa.

Cuando la información deja de ser necesaria para una organización llega a la última fase de su ciclo de vida y es necesario destruirla de forma segura.

Eliminar o "formatear" un archivo desde un sistema operativo común no borra la información, solo "vacía" el espacio que ocupaba para volver a ser utilizado. En la práctica, los datos siguen allí y pueden ser recuperados con software especializado.

Para borrar de manera efectiva un archivo existen diferentes métodos, algunos de ellos son:

- desmagnetización del soporte
- borrado mediante firmware incorporado al soporte físico
- sobreescritura de la información con protocolos que hagan imposible su reconstrucción
- cifrado de la información con criptografía fuerte y ofuscación de la clave de cifrado

La normativa que regula en España la destrucción certificada es la ISO 15713:2010. También se puede consultar la extensa información sobre este tema en el INCIBE.

La obligación del borrado seguro de imágenes en videovigilancia

La videovigilancia está afectada por las normas de protección de datos personales y la grabación de imágenes y metadatos se pueden considerar datos personales. Uno de los aspectos más importantes en el tratamiento de estos datos es el borrado obligatorio.

El creciente uso de los sistemas de videovigilancia en los ámbitos privado y público, plantea dudas sobre el impacto de estas tecnologías en la privacidad de las personas. En España, la captación y el tratamiento de imágenes por cámaras de seguridad están regulados por el Reglamento General de Protección de Datos (RGPD), en vigor desde 2018, y la Ley Orgánica de Protección de Datos y Garantía de los Derechos

Digitales (LOPDGDD). Ambas normativas exigen que los datos personales, incluidas las imágenes captadas por videovigilancia, sean tratados de forma lícita, leal y transparente, y que solo se conserven durante el tiempo necesario para cumplir con su finalidad.

Según la Agencia Española de Protección de Datos (AEPD), las grabaciones obtenidas mediante cámaras de seguridad deben eliminarse en un plazo máximo de 30 días, salvo excepciones.

El cumplimiento de la obligación de borrado no solo es un requisito legal, además debe formar parte del tratamiento de los datos de videovigilancia en las organizaciones. Además, los ciberataques o brechas de seguridad en los sistemas de almacenamiento pueden exponer estas grabaciones, aumentando el riesgo de uso inapropiado.

Para garantizar el cumplimiento de la obligación de borrado, es necesario contar con sistemas de videovigilancia que incluyan funcionalidades automatizadas para la eliminación de grabaciones. Habitualmente las imágenes de videovigilancia se encuentran almacenadas en discos duros. Veamos a continuación cómo borrarlos.

Cómo borrar de forma segura un disco duro para que los datos no puedan recuperarse

Lo primero que nos viene a la mente es formatear el disco. El formateo de una unidad de almacenamiento ya sea disco duro, SSD, USB, tarjeta SD, etc. es el proceso de preparar la unidad para que pueda guardar y organizar los datos.

¿Qué significa esto y qué tiene que ver con la recuperación de datos? Cuando se elimina un archivo o formatea un disco, esta información no se borra instantáneamente. En lugar de eso, como hemos mencionado al principio del artículo, el sistema operativo simplemente marca el espacio que ocupaban esos datos como "disponible" para ser sobrescrito por nueva información. Mientras no se

escriban nuevos datos en ese espacio, la información original sigue allí. Es como si borramos la tapa de un libro, eliminamos el título, pero la información sigue ahí.

¿Qué factores afectan la recuperación? La probabilidad de éxito de la recuperación depende de varios factores clave:

- **Tiempo transcurrido desde la eliminación:** Cuanto antes se intente la recuperación, mayores serán las posibilidades. Cada vez que se usa el disco después de la eliminación, aumenta el riesgo de que los datos originales sean sobrescritos.
- **Uso del disco después de la eliminación:** Si se ha continuado usando el disco después de borrar los datos, es probable que se haya escrito nueva información sobre los archivos borrados, lo que los hace irrecuperables.

Cómo borrar de forma segura un disco duro para que los datos no puedan recuperarse

Hay muchas formas de eliminar la información confidencial almacenada en los discos duros, quizás la primera es destruir el disco físicamente, pero además del trabajo y el gasto, si esto no se hace de forma adecuada puede incluso en algunos casos ser ineficaz; en cualquier caso, hay otras formas de asegurarnos de que los datos no puedan ser recuperados ni siquiera con técnicas forenses avanzadas. Estas formas nos serán de utilidad si se va a desechar o reutilizar los equipos y por supuesto, para

proteger la información personal o confidencial de la organización y en definitiva, la reputación.

1. **Destrucción física (como último recurso), destruir físicamente el disco:**
   - Perforar los platos con un taladro.
   - Romper la placa de circuito.
   - Triturar o llevar a una empresa especializada en destrucción de hardware.

   Incluso en este caso, se podrían recuperar datos parcialmente.

2. **Borrado mediante sobreescritura múltiple**

Una de las técnicas más seguras es sobrescribir todo el contenido del disco con datos aleatorios varias veces. Como ejemplo podemos hablar del “formateo a bajo nivel” o el "zeroing"; son métodos utilizados para borrar datos de un disco duro. Consiste en sobrescribir todos los sectores del disco con ceros (0). Este proceso elimina la información existente y hace que sea más difícil recuperar los datos originales. Aunque es una forma de borrado seguro no es tan robusto como otros métodos que sobrescriben los datos múltiples veces con patrones aleatorios.

Existen herramientas especializadas que permiten hacerlo:

- Windows: usando programas como Eraser o CCleaner (en su modo de borrado seguro).
- Mac: utiliza la opción “Borrar de forma segura” desde la Utilidad de Discos (aunque en versiones recientes, esta opción se limita si el disco es SSD).
- Linux: El comando shred o dd permite sobrescribir datos múltiples veces

Lo recomendable son al menos 3 pasadas, aunque estándares como el DoD 5220.22-M (del Departamento de Defensa de EE.UU.) sugieren hasta 7 pasadas

3. **Uso de herramientas de borrado especializado**

Herramientas diseñadas específicamente para borrar discos completos de forma segura:

- DBAN (Darik's Boot and Nuke): Muy eficaz para discos mecánicos (HDD). Borra todo el contenido al arrancar desde un USB o CD.
- Blancco Drive Eraser: Más avanzada y con certificación profesional, ideal si necesitas una garantía de borrado para auditorías o cumplimiento legal.

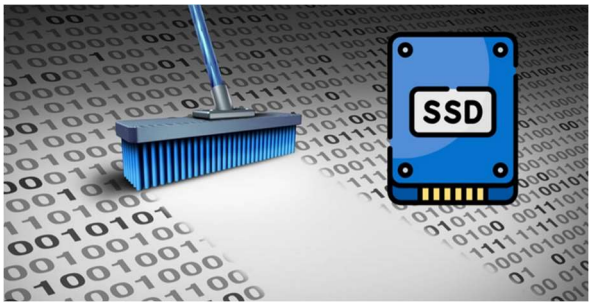
El lado oscuro es que muchos de estos programas ofrecen una versión gratuita que te permite escanear y ver qué archivos son recuperables.

4. **Criptoborrado (especial para discos SSD)**

El cifrado de discos duros es un proceso de seguridad que transforma los datos almacenados en un disco en un formato ilegible, utilizando algoritmos matemáticos y una clave de cifrado. Esto significa que, si alguien no autorizado intenta acceder a los datos, solo verá una secuencia de caracteres sin sentido, a menos que tenga la clave correcta para descifrarlos.

Los discos SSD funcionan diferente y no siempre es posible sobrescribir cada sector. En estos casos, lo más eficaz es:

Encriptar el disco completo previamente y luego borrar la clave de cifrado. Sin la clave, los datos permanecen inaccesibles. O bien,



Usar herramientas del fabricante del SSD (como SanDisk Dashboard, etc.) que ofrecen funciones de borrado seguro a nivel de firmware.

En cualquier caso, y como final, aquí van algunas recomendaciones clave sobre el proceso de borrado:

- Integrar las normativas y sus procesos en el reglamento interno de TI de la compañía
- Incluir los procesos como requisito en licitaciones con proveedores de reciclaje y almacenamiento de equipos de grabación de videovigilancia
- Establecer responsables del proceso dentro del equipo de cumplimiento o seguridad.
- Vincularlo con la estrategia de borrado seguro en la nube si se utiliza la grabación en cloud. Esto daría para otro artículo…

Laura Alcázar

Criterios de selección de elementos de un Sistema de Seguridad

Como casi siempre, la selección de los componentes de un sistema de seguridad es un ejercicio de ponderación entre los beneficios y los costes de cada opción. Tanto unos como otros no son tan fáciles de enumerar ni su evaluación es evidente.

No cabe duda de que quien debe efectuar la selección tiene unos criterios sobre los requerimientos y exigencias que deseará equilibrar con los recursos presupuestarios. Los requerimientos se ajustan a los servicios y funcionalidades que como mínimo debe prestar cada elemento y aquellos que adicionalmente y sin ser imprescindibles serían también de valor. En este análisis entra ya el grado de confianza en que ese rendimiento sea como se ofrece, y eso se relaciona con la reputación del fabricante, de quien ofrece la solución y de las referencias en las que puedan apoyarse las promesas de estos, en ocasiones respaldadas por certificaciones o acreditaciones por parte de terceras entidades.

A continuación, procede ponderar "los costes". Aquí los criterios pueden conducir a considerar más unos factores en detrimento de otros. La fiabilidad, la facilidad de instalación, la capacidad de integración, la sencillez en el uso o la versatilidad para cumplir las funciones pueden ser algunos de estos factores. El uso del ancho de banda en las comunicaciones, el almacenamiento de datos, e incluso el consumo eléctrico se han sumado a la lista de factores a considerar, resultando en ocasiones determinantes para realizar la selección.

No obstante, existen algunos requisitos que se presentan como de obligado cumplimiento. Estos son los relacionados con la habilitación técnica de los elementos para ser utilizados en el sistema de seguridad. Nos referimos a ellos como certificaciones u homologaciones y en muchos casos son ajenos a la propia iniciativa de quien especifica el sistema y vienen impuestas por regulaciones técnicas o administrativas aplicables. En otras ocasiones sí son una elección voluntaria del especificador y corresponden a su intención de establecer unos mínimos de capacidad técnica y prestaciones avalados por la evaluación independiente del organismo certificador.

Entre estas últimas se encuentran las certificaciones de ciberseguridad. Si bien no existe hoy una certificación de obligado cumplimiento en la UE, la creciente preocupación por la protección ante ciber ataques se refleja en un número creciente de normativas y marcos de cumplimiento que reclaman una atención especial.

En ese contexto, encontramos los requerimientos derivados del CRA (Cyber Resilience Act), que incorpora un conjunto de medidas básicas de protección de ciber seguridad que se aplican a todos los dispositivos electrónicos con comunicaciones que se comercialicen en la UE. No obstante, aunque en vigor desde su aprobación en abril de 2024 (no precisa trasposición), sus exigencias van siendo efectivas de manera progresiva y serán totalmente ejecutivas después de un plazo de 36 mese, es decir, en abril de 2027. Además, esta normativa aplica a los dispositivos, y se incorporará a la auto certificación de la marca CE lo que supone que por defecto todos los productos que formen parte de los sistemas deberán cumplir con la norma.

Más controvertida es la aplicación derivada de la directiva NIS 2, cuya trasposición en ley está aún pendiente en España (anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad). Esta directiva , que pretende elevar el nivel de protección en ciberseguridad de las principales entidades de la UE, no establece en sí misma una certificación obligatoria para los elementos de los sistemas (salvo que así lo acabase indicando el desarrollo de la ley o su reglamento), pero establece la exigencia de ciertas medidas técnicas y organizativas que pueden implicar que los dispositivos y elementos de software cuenten con características y servicios necesarios para facilitar o garantizar el cumplimiento normativo.

Algo similar sucede con el Esquema Nacional de Seguridad (ENS) cuya certificación es aplicable a entidades y sistemas, aunque para alcanzar la certificación exigida (especialmente de nivel medio o alto) puede ser necesario contar con elementos que exhiban certificaciones de ciberseguridad reconocidas por el organismo técnico de control (CCN).

Observamos, por lo tanto, que hemos de incorporar un nuevo y relevante criterio a la hora de seleccionar los elementos de un sistema de seguridad, y no es otro que el del cumplimiento normativo en ciberseguridad y en cualquier caso las medidas necesarias o convenientes para una protección eficiente. Cabe destacar, que no siempre hablamos de certificaciones o funcionalidades estrictamente relativas al elemento del sistema, sino que bien puede tratarse de medidas y funcionalidades que permitan y colaboren a la certificación y/o cumplimiento del sistema. En esa línea, se convierten en importantes las herramientas que se habiliten y encuentren disponibles para la gestión de ciberseguridad de los diferentes dispositivos, lo que forzosamente tendrá un alto impacto en la capacidad de cumplimiento y en los costes asociados que se deriven de ese cumplimiento.

En definitiva, a todos los criterios de ponderación que intervenían en la selección de elementos de un sistema debemos añadir (y posiblemente priorizar) el criterio de la ciberseguridad, tanto en su aspecto de protección como en el del cumplimiento normativo.

A la espera de que se incorpore (si no lo ha hecho ya) el enfoque de la sostenibilidad, el factor ciberseguridad ha venido a trastocar y mucho los criterios de selección de elementos de los Sistemas de Seguridad.

Alberto Alonso

¿Cumplió España con la NIS2 y el CER?

Nueve meses después del plazo límite para la trasposición de la Directiva NIS2 (17 de octubre de 2024), España ha logrado aprobar finalmente su legislación nacional para adaptarse a esta normativa europea. Sin embargo, el proceso ha sido más lento de lo deseado y ha generado tensiones tanto dentro del país como con las instituciones europeas. Aunque el Gobierno salvó in extremis las posibles sanciones con la aprobación del marco legal en el primer trimestre de 2025, la implementación práctica aún enfrenta desafíos.

La Directiva NIS2 y el Reglamento CER ya no son promesas en papel: están en fase de despliegue y control activo por parte de las autoridades nacionales y europeas. Mientras tanto, Bruselas continúa auditando el grado de cumplimiento de los Estados miembros, en un contexto geopolítico cada vez más tenso y tecnológicamente competitivo.

¿Legislar o innovar? El dilema europeo persiste

Europa ha seguido apostando por la regulación como herramienta principal: NIS2, CER, DORA, la Ley de Cibersolidaridad, el Reglamento de Ciberresiliencia... El marco legal se ha consolidado, pero aún queda la gran incógnita: ¿es suficiente regular sin reforzar significativamente la inversión en I+D y tecnología estratégica?

Mientras tanto, China continúa su avance en inteligencia artificial aplicada a ciberdefensa, y Estados Unidos —incluso bajo el impacto político de las elecciones de 2024— ha mantenido una posición dominante en innovación y capacidades digitales. Europa, en cambio, sigue con una inversión fragmentada, lo que limita su autonomía tecnológica.

Derechos fundamentales y economía: el equilibrio sigue siendo frágil

La Declaración Europea sobre Derechos y Principios Digitales sigue vigente como guía ética. No obstante, el reto de armonizarla con las demandas de competitividad tecnológica es mayor que nunca. Las preocupaciones sobre protección de datos, transparencia algorítmica y ética digital siguen siendo prioritarias, pero requieren un enfoque que no entorpezca el desarrollo de soluciones tecnológicas propias.

La clave continúa siendo el equilibrio: proteger sin paralizar, regular sin asfixiar. Porque si Europa no desarrolla sus propias tecnologías, acabará dependiendo de terceros, lo cual compromete precisamente esos derechos que busca defender.

Balance de la implementación de NIS2

Hoy, julio de 2025, las críticas iniciales a la NIS2 siguen presentes: falta de claridad sobre las entidades esenciales, excesiva carga para las pymes y dificultades técnicas para los Estados miembros. En el caso de España, aunque ya existe un marco legal vigente, muchas organizaciones aún están adaptando sus sistemas de gestión de riesgos y notificación de incidentes, lo que plantea dudas sobre la efectividad real del cumplimiento.

Lecciones de otros países

Alemania y Francia, que lideraron la trasposición desde 2023, han demostrado una mayor madurez en la aplicación práctica de NIS2. Países Bajos y Dinamarca han reforzado sus ecosistemas con alianzas público-privadas que hoy permiten respuestas más ágiles frente a incidentes cibernéticos. España, por su parte, aún necesita consolidar su coordinación institucional y su cultura de ciberseguridad, especialmente en sectores esenciales y digitales.

España evitó por poco las sanciones económicas por su retraso, pero la advertencia de la Comisión Europea sigue siendo clara: el acceso a fondos europeos para digitalización y ciberseguridad está condicionado al cumplimiento riguroso. Hoy en

día, las oportunidades siguen abiertas, pero con mayores exigencias de rendición de cuentas.

Trump reelegido. Contexto Geopolítico

La reelección de Donald Trump en las elecciones de noviembre de 2024 ha reconfigurado la relación transatlántica en materia de ciberseguridad. EE. UU. ha dado prioridad a su agenda nacional y ha reducido parcialmente la cooperación tecnológica con la UE. Esto obliga a Europa a redoblar su apuesta por la autonomía digital, aunque también ha generado incertidumbre sobre la orientación de futuras inversiones conjuntas.

¿Dónde debe enfocarse Europa y, en particular, España?

Ya no se trata solo de legislar o invertir, sino de ejecutar con visión estratégica. España necesita consolidar sus capacidades institucionales, formar talento especializado y fomentar la innovación tecnológica nacional. La ciberseguridad no es un mero cumplimiento normativo: es un activo clave para la soberanía digital y para la competitividad futura.

Jorge Noguerales Bautista

PC-Herramienta

En este articulo vamos a intentar poner encima de la mesa los riesgos asociados al uso, por parte de los técnicos de Sistemas Electrónicos de Seguridad, de los PC-Herramienta.

Lo primero es dejar claro qué entendemos por un PC-Herramienta en el campo que nos atañe. Un PC-Herramienta es un ordenador portátil u otro dispositivo informático que los técnicos de sistemas utilizan para realizar tareas técnicas y operativas en el ámbito de la configuración, mantenimiento, verificación y asistencia de Sistemas Electrónicos de Seguridad, entre los que se incluyen sistemas de detección de intrusión (IDS), circuitos cerrados de televisión (CCTV), sistemas de control de accesos, alarmas técnicas, así como otros componentes críticos de infraestructuras de seguridad física y electrónica.

Un PC-Herramienta es un elemento imprescindible de la “caja de herramientas” de un técnico de sistemas, igual que lo son un destornillador o un alicate. Hoy en día, hay múltiples tareas que un técnico de sistemas no puede realizar sin un PC-Herramienta.

PC-Herramienta

El uso de un PC-Herramienta implica la existencia de una serie de ciberriesgos que deben ser identificados, evaluados y gestionados adecuadamente. Estos riesgos se incrementan cuando dicho equipo se conecta a múltiples redes corporativas de clientes y cuando el usuario, el técnico de sistemas, dispone de privilegios de administrador, lo que lo convierte en un activo de alto riesgo desde el punto de vista de la ciberseguridad.

Al conectarse a redes de distintos clientes, el equipo actúa como un nodo itinerante que puede convertirse en vector de propagación de amenazas entre entornos que, en principio, deberían estar aislados. Además, el acceso a los Sistemas de Seguridad Electrónica y las infraestructuras de comunicaciones del cliente implica que una brecha en el PC-Herramienta pueda traducirse en una vulnerabilidad directa en los sistemas e infraestructuras del cliente.

Entre los principales ciberriesgos asociados al uso de estos dispositivos citaremos:

- Malware

  El PC-Herramienta puede ser infectado por malware en cualquiera de las redes a las que se conecta y convertirse en un vector de difusión. El malware puede actuar como puerta trasera para acceder a redes de clientes, capturar credenciales o manipular configuraciones de sistemas críticos.

- Riesgo de explotación de privilegios

  El hecho de que el usuario disponga de privilegios de administrador amplifica el impacto de cualquier ataque. Un atacante que comprometa el equipo podría ejecutar comandos con privilegios elevados, instalar software malicioso, desactivar protecciones o modificar configuraciones de seguridad.

- Fuga de información sensible

  Durante las tareas de asistencia técnica, el PC-Herramienta puede almacenar planos de instalaciones, contraseñas de sistemas, configuraciones de dispositivos o grabaciones de vídeo. Si el equipo no está cifrado o protegido adecuadamente, la confidencialidad de esta información puede verse comprometida.

- Ataques “Man-in-the-Middle”

  Al conectarse a redes Wi-Fi públicas o mal configuradas, el equipo puede ser víctima de ataques “Man-in-the-Middle”.

- Uso de software no autorizado o desactualizado

  La instalación de herramientas de diagnóstico, firmware o software de terceros sin validación previa puede introducir vulnerabilidades. Asimismo, el uso de versiones obsoletas de software de configuración puede exponer el equipo a exploits conocidos.

- Riesgo de suplantación de identidad

  En caso de robo o extravío, si el equipo no cuenta con mecanismos de autenticación robustos (como cifrado de disco, autenticación multifactor o gestión centralizada), un tercero podría utilizarlo para acceder a sistemas de clientes haciéndose pasar por el técnico autorizado.

- Conexiones inseguras entre redes

  El uso de túneles VPN mal configurados, conexiones directas entre el PC-Herramienta y dispositivos del cliente en redes sin segmentación o sin securizar puede facilitar la difusión de amenazas entre redes y el movimiento lateral de las mismas.

Para minimizar los ciberriesgos asociados al uso de los PC-Herramienta es necesario aplicar de forma rigurosa una serie de medidas de seguridad tanto técnicas como procedimentales, enmarcadas en una política de ciberseguridad específica para su naturaleza y función que facilite el cumplimiento de la legislación vigente como las directas NIS2 y CRE, el RGPD, el ENS y estándares como ISO/IEC 27001.

Por todo ello, al diseñar un modelo de uso de los PC-Herramienta se deben contemplar como mínimo las siguientes medidas:

Medidas Técnicas

- Protección del Sistema Operativo
  - Actualizaciones automáticas: el sistema debe estar configurado para instalar automáticamente parches de seguridad, especialmente aquellos que corrigen vulnerabilidades críticas.
  - Securización del sistema: deshabilitar servicios innecesarios, restringir el uso de scripts y macros, y aplicar configuraciones seguras en el registro del sistema.

  - Control de integridad: implementar herramientas que verifiquen la integridad de archivos del sistema y alerten ante modificaciones no autorizadas.
- Compatibilidad y Seguridad de Herramientas de Configuración
  - Utilizar únicamente el software oficial y actualizado de fabricantes de sistemas de seguridad.
  - Verificar que las herramientas de configuración no introducen vulnerabilidades (por ejemplo, puertos abiertos, contraseñas por defecto).
- Antivirus y Antimalware
  - Solución avanzada: utilizar software de seguridad con capacidades de detección proactiva, análisis de comportamiento y protección contra amenazas persistentes.
  - Protección en tiempo real: activar la supervisión constante de procesos, archivos y tráfico de red.
  - Escaneos programados: realizar análisis completos del sistema semanalmente y análisis rápidos diarios.

- Cifrado de Datos
  - Cifrado de disco completo: aplicar cifrado con algoritmos robustos (AES-256) para proteger la información almacenada en el disco duro.
  - Cifrado de medios extraíbles: obligar al cifrado de cualquier dispositivo USB o disco externo que se conecte al portátil.
  - Cifrado de comunicaciones: asegurar que todas las conexiones remotas (por ejemplo, a DVRs/NVRs o paneles de intrusión) se realicen mediante protocolos cifrados (HTTPS, SSH, VPN).
- Gestión de Contraseñas y Autenticación
  - Contraseñas seguras: requerir contraseñas complejas, únicas y renovadas periódicamente.
  - Autenticación multifactor (MFA): activar MFA para el acceso al sistema operativo y a herramientas de configuración remota.
  - Gestor de contraseñas: utilizar un gestor cifrado para almacenar credenciales de acceso a sistemas de clientes.
- Control de Acceso y Privilegios
  - Principio de mínimo privilegio: aunque el usuario tenga privilegios de administrador, se recomienda operar con una cuenta estándar para tareas rutinarias.
  - Separación de entornos: crear cuentas o entornos virtuales separados para cada cliente o tipo de sistema (CCTV, intrusión, etc.).
  - Bloqueo automático: configurar el bloqueo de sesión tras un periodo de inactividad.
- Seguridad de Red
  - Firewall personal: activar y configurar el firewall para bloquear conexiones no autorizadas.
  - VPN corporativa: utilizar una VPN para acceder a redes de clientes, evitando conexiones directas sin cifrado.
  - Segmentación de red: cuando sea posible, conectar el portátil a redes de configuración separadas de las redes corporativas del cliente.

- Protección contra amenazas avanzadas
    - EDR (Endpoint Detection and Response): implementar soluciones EDR para detectar y responder a amenazas sofisticadas.
    - Monitorización de logs: registrar eventos del sistema, accesos y cambios en configuraciones de seguridad.
- Backup y Recuperación
    - Copias de seguridad cifradas: realizar backups de configuraciones de sistemas (cámaras IP, paneles de intrusión) y almacenarlos de forma segura.
    - Pruebas de restauración: verificar que los backups pueden restaurarse correctamente en caso de fallo.
- Seguridad Física del Dispositivo
    - Protección contra robo: utilizar sistemas de bloqueo físico (candados, fundas de seguridad) y mantener el dispositivo bajo supervisión.
    - Geolocalización y borrado remoto: activar funciones de rastreo y borrado remoto en caso de pérdida o robo.

Medidas Procedimentales

- Política de uso
    - Uso exclusivo profesional: el PC-Herramienta debe utilizarse únicamente para tareas relacionadas con la asistencia técnica de sistemas de seguridad.
    - Prohibición de software no autorizado: no se debe instalar software sin la validación del área de seguridad.
    - Registro de intervenciones: documentar cada intervención técnica incluyendo fecha, cliente, sistema intervenido y acciones realizadas.

- Gestión de Conexiones a Sistemas de Clientes
  - Evaluación previa: antes de conectar el PC-Herramienta a un sistema del cliente, verificar que se cumplen los requisitos mínimos de seguridad.
  - Entornos aislados: utilizar máquinas virtuales o contenedores para cada cliente o tipo de sistema, evitando la contaminación cruzada.
  - Desconexión segura: finalizar sesiones y eliminar credenciales temporales tras cada intervención.
- Manejo de Información Sensible
  - Clasificación de datos: etiquetar la información según su nivel de sensibilidad (planos de instalación, credenciales de acceso, configuraciones de cámaras).
  - Almacenamiento seguro: guardar datos sensibles en ubicaciones cifradas y protegidas por contraseña.
  - Eliminación segura: utilizar herramientas de borrado seguro para eliminar archivos que ya no se necesiten.
- Formación y Concienciación
  - Capacitación continua: el técnico debe recibir formación periódica en ciberseguridad, incluyendo buenas prácticas en la configuración de sistemas electrónicos de seguridad.
  - Simulacros de seguridad: realizar simulacros de incidentes para mejorar la capacidad de respuesta.
  - Boletines de seguridad: mantener a los técnicos informados sobre vulnerabilidades en sistemas de videovigilancia, paneles de intrusión, etc.
- Gestión de Incidentes
  - Protocolo de respuesta: definir un procedimiento claro para la gestión de incidentes, incluyendo el protocolo de contacto con el cliente y con el equipo de seguridad.
  - Notificación inmediata: informar sin demora ante cualquier sospecha de compromiso del dispositivo o de los sistemas del cliente.
  - Registro de incidentes: documentar todos los incidentes, acciones tomadas y medidas preventivas adoptadas.

- Auditorías y Revisiones
    - Revisión periódica: auditar la configuración del sistema y las políticas de seguridad al menos una vez al trimestre.
    - Pruebas de seguridad: realizar pruebas de penetración y análisis de vulnerabilidades en entornos de prueba.
    - Evaluación de cumplimiento: verificar el cumplimiento de normativas aplicables como NIS2, CER, RGPD, ENS y estándares de seguridad electrónica.

El uso de los PC-Herramienta en la asistencia técnica de sistemas electrónicos de seguridad requiere de una estrategia de ciberseguridad integral adaptada a los riesgos específicos del sector. La combinación de medidas técnicas y procedimentales permite proteger tanto el dispositivo como los sistemas de los clientes, garantizando la continuidad del servicio y el cumplimiento normativo.

La seguridad debe ser un proceso continuo basado en la mejora constante, la formación y la colaboración entre técnicos, clientes y responsables de seguridad.

Ricardo Cañizares Sales

La banalización de la seguridad en las comunicaciones

1. Introducción

Definición de banalización de la seguridad en las comunicaciones

La banalización de la seguridad en las comunicaciones hace referencia a la tendencia a restar importancia a las medidas y prácticas que garantizan la protección de la información personal, profesional o institucional. En un entorno donde la inmediatez, la comodidad y la hiperconectividad son prioridades, las precauciones de seguridad suelen percibirse como obstáculos innecesarios. Esto provoca que se adopten hábitos inseguros que, aunque puedan parecer inofensivos, exponen a individuos y organizaciones a riesgos significativos.

Importancia de la seguridad en las comunicaciones en la actualidad

En la actualidad, la seguridad en las comunicaciones es un aspecto crítico debido al volumen de datos que se transmite constantemente a través de plataformas digitales. La información personal, financiera y corporativa circula a diario en redes sociales, correos electrónicos, aplicaciones de mensajería y sistemas en la nube. La falta de protección adecuada no solo expone a los usuarios a fraudes o pérdidas económicas, sino que también pone en riesgo la reputación y la confianza en las organizaciones. La seguridad, por tanto, es un elemento esencial para garantizar la estabilidad y la integridad en el ecosistema digital.

Objetivo de la publicación

El objetivo de este documento es analizar de forma estructurada el fenómeno de la banalización de la seguridad en las comunicaciones, identificando sus causas, consecuencias y ejemplos prácticos. Asimismo, se plantean estrategias para contrarrestar este fenómeno, con el fin de fomentar una cultura de responsabilidad individual y colectiva en torno a la protección de la información.

2. 2. El contexto actual de las comunicaciones

La evolución de las comunicaciones: de lo analógico a lo digital

La transformación de lo analógico a lo digital ha supuesto un cambio radical en la forma en que nos comunicamos. Antes, los canales de comunicación eran limitados y más controlables, como el correo postal, el teléfono fijo o los medios impresos. Hoy en día, internet y las aplicaciones digitales han multiplicado las vías de interacción, ofreciendo rapidez y alcance global. Sin embargo, esta transición también ha ampliado la superficie de exposición a riesgos de seguridad.

Dependencia de la tecnología en la vida diaria y en las empresas

La dependencia tecnológica es evidente tanto en la vida cotidiana como en el ámbito empresarial. Desde las transacciones bancarias hasta la gestión de procesos corporativos, gran parte de nuestras actividades requieren conexión a internet y dispositivos electrónicos. Esta dependencia, aunque aporta eficiencia y comodidad, también implica que cualquier fallo de seguridad pueda tener consecuencias graves a nivel económico, social o personal.

La ubicuidad de internet y las redes sociales

La ubicuidad de internet y la omnipresencia de las redes sociales han generado un entorno en el que compartir información se percibe como algo natural e inmediato. Publicar datos personales, imágenes o ubicaciones en tiempo real se ha convertido en una práctica común, pero pocas veces se reflexiona sobre el impacto que puede tener. El exceso de confianza en estas plataformas refuerza la banalización de la seguridad.

3. Factores que contribuyen a la banalización

La comodidad y la inmediatez frente a la seguridad

La búsqueda de comodidad y rapidez en las interacciones digitales provoca que muchos usuarios omitan medidas de seguridad básicas. Por ejemplo, elegir contraseñas fáciles de recordar en lugar de claves seguras, o compartir archivos sensibles sin cifrado para agilizar procesos. Esta preferencia por la inmediatez fomenta la percepción de que la seguridad es un obstáculo más que una necesidad.

Falta de concienciación y educación sobre los riesgos

Una de las principales causas de la banalización de la seguridad es la falta de educación digital. Muchas personas desconocen cómo funcionan los ciberataques, qué riesgos implica la exposición de datos o cuáles son las buenas prácticas de protección. Esta carencia de conocimiento genera un terreno fértil para hábitos inseguros.

Confianza excesiva en las herramientas y plataformas digitales

La confianza desmedida en que aplicaciones, sistemas operativos y plataformas sociales ofrecen toda la seguridad necesaria conduce a una falsa sensación de protección. Los usuarios asumen que estas herramientas son infalibles, cuando

en realidad son vulnerables a errores de diseño, fallos de actualización y ataques externos.

Normalización de las filtraciones de datos y ciberataques

La frecuencia con que se difunden noticias sobre filtraciones masivas de datos o ataques cibernéticos ha generado cierta indiferencia social. Muchas personas han llegado a ver estos incidentes como inevitables, lo que contribuye a la normalización del problema y a la falta de reacción preventiva.

Presión por compartir información rápidamente y sin filtros

El ritmo acelerado de la sociedad digital impulsa a compartir información de manera inmediata, sin verificar la veracidad de los datos ni valorar las consecuencias de su difusión. Este comportamiento, reforzado por la cultura de la inmediatez en redes sociales, debilita los mecanismos de protección y eleva la vulnerabilidad.

4. Consecuencias de la banalización de la seguridad

Pérdida de privacidad y datos personales

La primera consecuencia de la banalización es la pérdida de privacidad. Información como direcciones, hábitos de consumo o datos familiares pueden quedar expuestos a terceros sin consentimiento. Esto erosiona la capacidad de control sobre la propia identidad digital.

Robo de identidad y fraude financiero

La falta de precaución facilita el robo de identidad, que puede derivar en fraudes financieros. Los ciberdelincuentes aprovechan datos aparentemente inofensivos para acceder a cuentas bancarias, solicitar créditos o realizar compras fraudulentas en nombre de la víctima.

Daño a la reputación personal y profesional

Las imprudencias en la gestión de la seguridad digital también afectan a la reputación. Una publicación descuidada, un comentario sin filtro o la filtración de correos privados pueden tener consecuencias duraderas en la vida personal y en la trayectoria profesional.

Vulnerabilidad ante ciberataques y malware

Ignorar medidas básicas de seguridad deja abiertas puertas de entrada a ciberataques y malware. Esto afecta tanto a usuarios individuales como a empresas, que pueden ver comprometidos sus sistemas internos y su información sensible.

Implicaciones legales y sanciones

La falta de medidas de protección también puede tener consecuencias legales. Legislaciones como el Reglamento General de Protección de Datos (RGPD) en Europa establecen obligaciones claras sobre la protección de la información. No cumplirlas puede dar lugar a multas, sanciones y pérdida de confianza de clientes o socios.

5. Ejemplos prácticos de banalización

Uso de contraseñas débiles y repetidas

Un ejemplo común es la utilización de contraseñas simples como '123456' o 'password', o repetir la misma clave en múltiples servicios. Esta práctica reduce significativamente la seguridad y facilita ataques de fuerza bruta o acceso indebido.

Compartir información sensible en redes sociales

Publicar datos personales como ubicaciones, números de teléfono o información laboral en redes sociales puede convertirse en una fuente de información para delincuentes. Muchas veces estos detalles se comparten sin reflexionar en las posibles consecuencias.

Descarga de software de fuentes no confiables

La descarga de programas desde páginas no oficiales expone a los dispositivos a virus, troyanos y otros tipos de malware. Sin una verificación de la procedencia, los usuarios ponen en riesgo su información y la integridad de sus sistemas.

Ignorar las actualizaciones de seguridad

Otro ejemplo habitual es desatender las actualizaciones de software y sistemas operativos. Estas actualizaciones suelen incluir parches de seguridad diseñados para cerrar vulnerabilidades, pero al ignorarlas, los usuarios dejan abiertas puertas que los atacantes pueden explotar.

Conexión a redes Wi-Fi públicas sin precauciones

El uso de redes Wi-Fi abiertas en aeropuertos, cafeterías o centros comerciales sin el respaldo de medidas adicionales, como el uso de una VPN, facilita la interceptación de datos por parte de terceros. Este descuido puede comprometer información sensible como contraseñas o datos bancarios.

6. Estrategias para combatir la banalización

Educación y concienciación sobre seguridad digital

La educación digital es la herramienta más efectiva para contrarrestar la banalización de la seguridad. Programas de formación, campañas de sensibilización y talleres prácticos permiten a los usuarios comprender los riesgos reales y adoptar hábitos más seguros en su vida digital.

Implementación de buenas prácticas de seguridad

El uso de contraseñas fuertes y únicas, junto con la implementación de la autenticación en dos factores, son prácticas fundamentales. Además, es recomendable evitar compartir información sensible en entornos inseguros y mantener hábitos de verificación constante de las fuentes de información.

Uso de herramientas de seguridad

Antivirus actualizados, redes privadas virtuales (VPN) y gestores de contraseñas son recursos que fortalecen la protección digital. Aunque no son soluciones infalibles, su utilización reduce significativamente el nivel de exposición frente a amenazas.

Revisión y actualización constante de políticas de seguridad

Las organizaciones deben revisar y actualizar periódicamente sus políticas de seguridad. Esto incluye la adaptación a nuevas normativas, la implementación de protocolos de respuesta ante incidentes y la auditoría constante de los sistemas para detectar vulnerabilidades.

Fomento de una cultura de seguridad en organizaciones y hogares

Más allá de las herramientas, es imprescindible consolidar una cultura de seguridad que abarque tanto el entorno laboral como el familiar. Fomentar la responsabilidad compartida en torno a la protección de la información genera una mayor resiliencia frente a los riesgos digitales.

7. El Papel de la responsabilidad individual y colectiva

La importancia de la responsabilidad personal en la protección de la información

Cada individuo es el primer guardián de su información personal. Adoptar medidas simples como desconfiar de enlaces sospechosos, configurar correctamente la privacidad en redes sociales y no compartir datos innecesarios puede marcar una diferencia significativa en la seguridad global.

El rol de las empresas y organizaciones en la promoción de la seguridad

Las empresas tienen la responsabilidad de proteger los datos de clientes, empleados y socios. Para ello, deben invertir en infraestructuras seguras, formar a su personal y establecer protocolos claros para la gestión de incidentes. La transparencia en la comunicación sobre medidas de seguridad refuerza la confianza de los usuarios.

La necesidad de colaboración y cooperación entre individuos, empresas y gobiernos

La seguridad digital es un desafío que trasciende fronteras y sectores. La cooperación entre usuarios, compañías y gobiernos resulta clave para enfrentar ciberamenazas globales. Iniciativas conjuntas, marcos legales adecuados y campañas públicas coordinadas son esenciales para construir un entorno digital más seguro.

8. Conclusiones

La banalización de la seguridad en las comunicaciones es un fenómeno creciente que se origina en la búsqueda de inmediatez, la falta de educación digital y la confianza excesiva en las plataformas tecnológicas. Sus consecuencias van desde la pérdida de privacidad hasta graves implicaciones legales.

La seguridad no debe considerarse un obstáculo, sino un pilar esencial de la vida digital. Solo a través de la concienciación y el compromiso será posible reducir la vulnerabilidad de las personas y organizaciones frente a los riesgos.

Es necesario que cada usuario asuma un rol activo en la protección de sus datos, que las empresas fortalezcan sus políticas de seguridad e inviertan en concienciación y formación, y que los gobiernos continúen generando marcos regulatorios sólidos. La colaboración y la responsabilidad compartida son el camino para frenar la banalización de la seguridad en las comunicaciones.

Pablo Carmona

La Ciberseguridad de los Sistemas Electrónicos de Seguridad es un asunto demasiado importante para dejarlo en manos de los técnicos

Parafraseando a Georges Clemenceau al que se le atribuye la frase "*La guerra es un asunto demasiado serio para dejarla en manos de los militares*", hoy podríamos decir que "*La Ciberseguridad los Sistemas Electrónicos de Seguridad es un asunto demasiado importante para dejarlo en manos de los técnicos*".

Es un reto tan trascendental para cualquier organización, que dejarlo solo en las manos expertas de los técnicos sería un error que podría tener consecuencias impredecibles. Con esta analogía queremos resaltar que para hacer frente a desafíos muy complejos es necesario aunar pensamiento estratégico, visión de conjunto y liderazgo decidido.

No podemos olvidar que, dentro de la ciberseguridad, destaca la de los Sistemas Electrónicos de Seguridad (SES) que, como la de cualquier otro sistema de nuestra organización, debe ser una de las prioridades de la alta dirección que debe asumirla como un elemento clave de negocio y no solo como un reto tecnológico.

Hace tiempo ya que los Sistemas Electrónicos de Seguridad abandonaron el mundo analógico para pasar al mundo digital por lo que hoy en día, podemos considerarlos como sistemas OT y muchos de sus componentes son elementos IoT e incluso AIoT, formando parte del ciberespacio.

Esto los convierte en parte de la frontera entre el ciberespacio y el mundo físico, lo que convierte a la ciberseguridad de los SES en un elemento clave no solo para la protección de ellos mismos, sino para la protección del resto de sistemas de la organización, de los activos físicos y de las personas.

Tal como establece el Esquema Nacional de Seguridad y las directivas europeas NIS2 y CER, la protección efectiva de estos sistemas trasciende de la mera implementación de soluciones técnicas; exige una visión estratégica y un compromiso decidido de la alta dirección, lo que supone su implicación directa en la toma de decisiones sobre ciberseguridad, su responsabilidad en la gestión de riesgos, la asignación de recursos y la gobernanza de la seguridad.

La Ciberseguridad de los Sistemas Electrónicos de Seguridad es un asunto demasiado importante para dejarlo en manos de los técnicos

Las empresas de seguridad que se dedican a instalar y mantener Sistemas Electrónicos de Seguridad no solo son responsables de instalar y mantener dichos sistemas correctamente con eficacia y eficiencia, sino que deben realizar dichas tareas aplicando criterios y medidas de ciberseguridad. Además, tienen la obligación de transmitir a sus clientes la necesidad de contemplar la ciberseguridad como un elemento central en los proyectos de instalación de los SES.

Hoy en día nos encontramos en un entorno complejo de seguridad en el que la superficie expuesta a un ciberataque crece con cada nueva conexión, ya no basta con securizar los sistemas, también es imprescindible que las empresas de seguridad que diseñan, los SES informen y sensibilicen a los clientes de que, a la hora de tomar decisiones de inversión, tengan en cuenta la importancia de integrar las medidas y los servicios de ciberseguridad desde la definición de necesidades del proyecto.

De esta manera, las empresas instaladoras y mantenedoras se convierten en agentes clave para impulsar la transformación cultural y garantizar que la seguridad digital no sea una idea abstracta, sino una práctica concreta desde la concepción del proyecto hasta su operación continua. Esta obligación va más allá del cumplimiento normativo y debe responder a la visión estratégica de defender tanto los intereses del cliente como la reputación del propio sector.

Uno de los principales problemas a los que nos enfrentamos a la hora de proteger adecuadamente nuestros Sistemas Electrónicos de Seguridad, es la percepción errónea de la ciberseguridad como un gasto prescindible cuando la realidad es que se trata de una inversión estratégica. Es imprescindible entender que cada euro invertido en la ciberseguridad de nuestros sistemas tiene repercusión directa en la protección de los activos y las personas a las que protegen esos sistemas, lo que al final se traduce en un aumento de la resiliencia del negocio, la reputación de la compañía y la confianza de los clientes y el resto

de las partes interesadas. Las directivas NIS2 y CER refuerzan este enfoque exigiendo pruebas fehacientes de la asignación de recursos suficientes, de la implicación de la alta dirección en la supervisión de las inversiones y de la implantación de medidas de protección, tanto técnicas como organizativas.

Y es que, aunque la máxima responsabilidad recae sobre la alta dirección "*la ciberseguridad es tarea de todos*", y es fundamental reconocer que debe involucrar a todas las personas que forman parte de la organización lo que incluye tanto al personal que utiliza y opera los SES como a las personas a las que ofrece protección.

Esta corresponsabilidad implica que la formación, la sensibilización y la vigilancia en el cumplimiento de las políticas y procedimientos de ciberseguridad deben estar presentes en todos los niveles. La cultura de ciberseguridad debe ser impulsada desde la alta dirección, pero debe permear cada proceso, cada decisión y cada acción cotidiana. Solo así se crea un entorno verdaderamente resiliente, donde el error humano, a menudo el eslabón más débil, se minimiza gracias a la concienciación y la implicación colectiva.

La visión y la percepción de la necesidad de ciberseguridad por parte de los equipos técnicos son esenciales a la hora de diseñar, instalar y mantener los Sistemas de Seguridad Electrónica, pero su perspectiva suele estar limitada al ámbito tecnológico. La ciberseguridad, como subrayan el ENS, NIS2 y CER, requiere una visión interdisciplinar, integrando la gestión de riesgos, el cumplimiento normativo, la formación, la respuesta a incidentes y la alineación con los objetivos estratégicos de la organización. Los técnicos, por sí solos, carecen de la autoridad para coordinar la estrategia global que debe emanar desde la dirección y ser respaldada por políticas y recursos adecuados.

Abordar el problema de la ciberseguridad únicamente desde un punto de vista técnico puede llevar a soluciones tecnológicamente avanzadas pero desalineadas con las necesidades reales de los Sistemas Electrónicos de Seguridad a los que

tienen que proteger. Esta protección debe realizarse aplicando las políticas y procedimientos promulgadas por la dirección de la organización, que debe crear estructuras de gobernanza que integren la seguridad en todos los niveles bajo la supervisión directa de los órganos de gobierno.

Debido a todo lo anterior, un temor habitual es que la ciberseguridad pueda restar agilidad u obstaculizar la eficacia y eficiencia de los Sistemas Electrónicos de Seguridad, sin embargo, tanto la experiencia como la regulación internacional demuestran que una estrategia bien diseñada debe (y puede) garantizar la ciberseguridad sin sacrificar la operatividad. Los principios de "*seguridad por diseño*" y "*seguridad por defecto*", recogidos en las directivas europeas y en el Esquema Nacional de Seguridad, promueven la integración de la protección desde el diseño de los sistemas, logrando que la ciberseguridad sea un facilitador y no un obstáculo para que los SES cumplan con su objetivo de proteger a personas y bienes. El reto se encuentra en proteger sin paralizar, adaptándose a los cambios tecnológicos y a las nuevas amenazas manteniendo siempre un rumbo firme que persiga la mejora continua.

Garantizar la ciberseguridad de los SES es uno de los mayores retos para cualquier organización ya que si alguno se viera comprometido por un ciberataque supondría un riesgo sobre el objeto de protección, las personas y los bienes que ninguna organización puede obviar.

En resumen, las empresas deben tener claro que dejar la ciberseguridad en manos exclusivas de los técnicos es insuficiente y que esta responsabilidad recae en la alta dirección. Ahora bien, garantizar un adecuado nivel de ciberseguridad solo es posible si todos los miembros de la organización comprenden que "la ciberseguridad es cosa de todos".

Además, una de las piezas fundamentales para abordar la protección de los SES son las empresas de seguridad, que juegan un papel esencial a la hora de garantizar la ciberseguridad de estos y deben informar y asesorar a sus clientes sobre la importancia de tener en cuenta las necesidades de ciberseguridad durante todo el ciclo de vida del sistema, desde la definición de necesidades, hasta pasando por el diseño y, la instalación, hasta y el mantenimiento.

Ricardo Cañizares Sales

Cyber RED: El cambio normativo que pone en riesgo miles de productos conectados

El nuevo marco normativo derivado de la Directiva RED 2014/53/UE, *relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos radioeléctricos*, y el Reglamento Delegado (UE) 2022/30, *que completa la Directiva 2014/53/UE del Parlamento Europeo y del Consejo en lo que respecta a la aplicación de los requisitos esenciales contemplados en el artículo 3, apartado 3, letras d), e) y f),* supone un punto esencial para el mercado europeo de equipos radioeléctricos. A partir del 1 de agosto de 2025, todo dispositivo que se conecte a redes, procese datos personales o permita transacciones electrónicas estará sujeto a un escrutinio más estricto: solo quienes demuestren cumplimiento de los nuevos y exigentes requisitos de ciberseguridad podrán obtener el marcado CE. Las empresas que no se adapten a tiempo podrían enfrentarse a retrasos críticos, incertidumbre regulatoria y riesgos para su continuidad en el mercado.

Este cambio es significativo: muchos productos quedarán fuera de cumplimiento si los fabricantes no actúan a tiempo. La mayoría de las empresas aún desconoce el alcance real de estas obligaciones, y se arriesgan a ver detenida su comercialización, rediseños urgentes o incluso la retirada de productos del mercado.

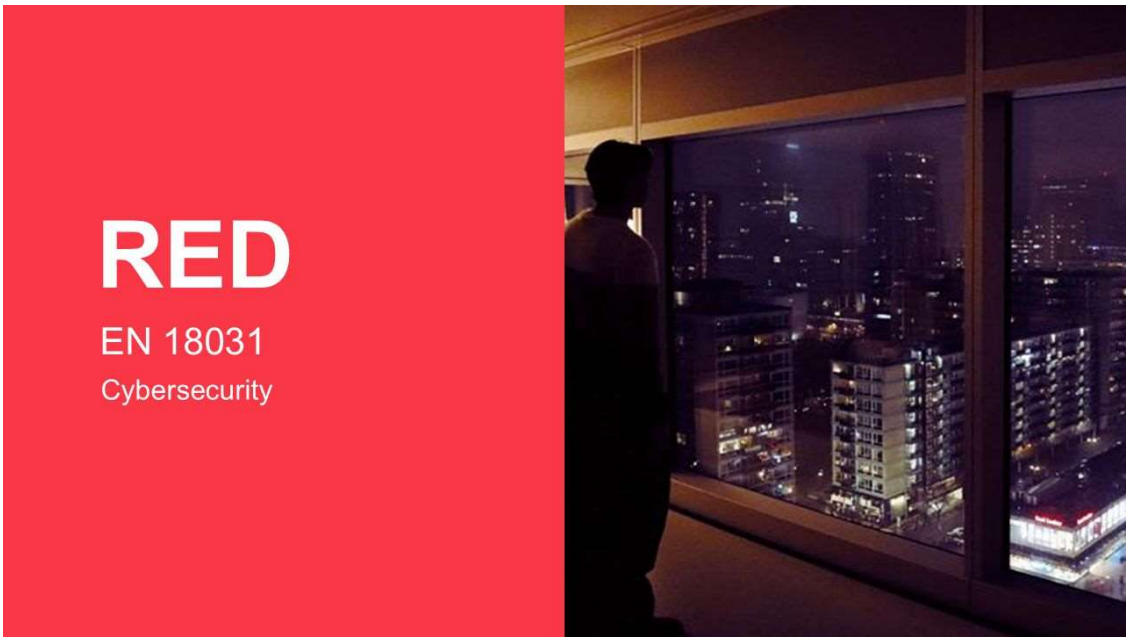
Este documento ofrece una visión clara y necesaria de lo que ya está en vigor. Explicamos los nuevos requisitos técnicos, las normas armonizadas, los desafíos en la presunción de conformidad y cómo el proceso de certificación puede convertirse en un retraso crítico para quienes no se hayan preparado. En un entorno regulatorio que evoluciona rápidamente, comprender y anticipar estos requisitos no es una opción, es una condición indispensable para seguir operando.

Introducción a la Directiva RED

La Directiva RED (2014/53/UE) regula la comercialización de equipos radioeléctricos en la Unión Europea, garantizando que sean seguros, eficientes y compatibles con el entorno electromagnético. Desde su entrada en vigor en 2016, es el marco legal de referencia para dispositivos *eléctricos o electrónicos que emite o recibe intencionadamente ondas radioeléctricas para radiocomunicación o radiodeterminación, así como para productos que requieren accesorios para dichas funciones* como móviles, routers, wearables y otros productos que utilizan tecnologías inalámbricas como puedan ser los productos

de intrusión y control de accesos para sistemas de seguridad, o para sistemas de incendios.

Con la publicación del Reglamento Delegado (UE) 2022/30, la Directiva se amplía para incluir requisitos nuevos y fundamentales. Estos requisitos van dirigidos a fortalecer la ciberseguridad, la protección de datos y la resistencia de los dispositivos conectados. Tales modificaciones pretenden asegurar que los equipos radioeléctricos conserven un grado suficiente de defensa ante amenazas digitales que van apareciendo.



Nuevos Requisitos de Ciberseguridad

El Reglamento Delegado (UE) 2022/30, incorpora tres requisitos esenciales de ciberseguridad al artículo 3.3 de la Directiva RED. Estos requisitos son obligatorios a partir del 1 de agosto de 2025 para todos los equipos radioeléctricos conectados a redes públicas o que traten datos personales o transacciones electrónicas.

Requisitos clave:

- Artículo 3.3 (d): Protección de redes
- Artículo 3.3 (e): Protección de datos personales
- Artículo 3.3 (f): Prevención del fraude

Estos requisitos refuerzan la seguridad digital en el mercado europeo, alinean los productos con las expectativas de protección frente a ciber amenazas, y aumentan la confianza del consumidor**.**

Aplicabilidad a Equipos de Radio

La aplicabilidad de los nuevos requisitos depende de las funcionalidades del equipo radioeléctrico.

No todos los dispositivos están sujetos a ellos, pero es imprescindible realizar un análisis de riesgos para determinar si aplican.

Presunción de Conformidad y Normas Técnicas

Para facilitar el cumplimiento de los requisitos de ciberseguridad, la Comisión Europea ha armonizado la serie de normas EN 18031, que permiten la presunción de conformidad bajo la Directiva RED.

Normas armonizadas:

- EN 18031-1: Protección de redes
- EN 18031-2: Protección de datos personales
- EN 18031-3: Prevención del fraude

Otras normas relevantes:

- ISO/IEC 62443: – Enfocada en la ciberseguridad en sistemas de automatización y control industrial (ICS)
- ETSI EN 303 645: Este es el referente en ciberseguridad para dispositivos IoT de consumo.

Restricciones y consecuencias

A partir de la fecha en que el Reglamento Delegado (UE) 2022/30 es de obligado cumplimiento, los equipos radioeléctricos que no muestren que cumplen con los nuevos requisitos de ciberseguridad no se podrán comercializar ni usar en el mercado europeo. La falta de cumplimiento podría conllevar la retirada o prohibición de venta de los productos afectados, y también a sanciones administrativas o económicas impuestas por las autoridades que correspondan.

Estructura y Evaluación de las Normas EN 18031

La serie de normas EN 18031 ha sido publicada en el Diario Oficial de la Unión Europea y se convierte en referencia para demostrar el cumplimiento de los requisitos de ciberseguridad de la Directiva RED. Cada norma aborda un apartado específico del artículo 3.3 y define mecanismos técnicos como autenticación, cifrado, control de acceso, actualizaciones seguras, etc.

Documento	Cubre el requisito esencial	Aborda los activos y riesgos de seguridad	Aborda los activos y riesgos de la red	Aborda los activos y riesgos de privacidad	Aborda los activos y riesgos financieros
EN 18031-1	3.3.(d)	✓	✓	X	X
EN 18031-2	3.3.(e)	✓	X	✓	X
EN 18031-3	3.3.(f)	✓	X	X	✓

Para cumplir con cada uno de los requisitos, la norma establece un conjunto de mecanismos, que son:

Requirements	3.3.(d)	3.3.(e)	3.3.(f)
[ACM] Access Control Mechanism	✓	✓	✓
[AUM] Authentication Mechanism	✓	✓	✓
[SUM] Secure Update Mechanism	✓	✓	✓
[SSM] Secure Storage Mechanism	✓	✓	✓
[SCM] Secure Communication Mechanism	✓	✓	✓
[LGM] Logging Mechanism	-	✓	✓
[DLM] Deletion Mechanism	-	✓	-
[UNM]User Notification Mechanism	-	✓	-
[RLM] Resilience Mechanism	✓	-	-
[NMM] Network Monitoring Mechanism	✓	-	-
[TCM] Traffic Control Mechanism	✓	-	-
[CCK] Confidential Cryptographic Keys	✓	✓	✓
[GEC] General Equipment Capabilities	✓	✓	✓
[CRY] Cryptography	✓	✓	✓

Evaluaciones requeridas:

1. Evaluación conceptual

   Verifica que el diseño del equipo o del sistema integre de manera consistente los principios de ciberseguridad que se requieren. De esta forma, la arquitectura que se propone maneja de forma apropiada los riesgos que se esperan.

2. Evaluación de integridad funcional

   Revisa que las funciones de seguridad que se han puesto en marcha, como el cifrado, la autenticación o el control de acceso, funcionen bien y no interfieran con el resto de las operaciones del sistema.

3. Evaluación de suficiencia funcional

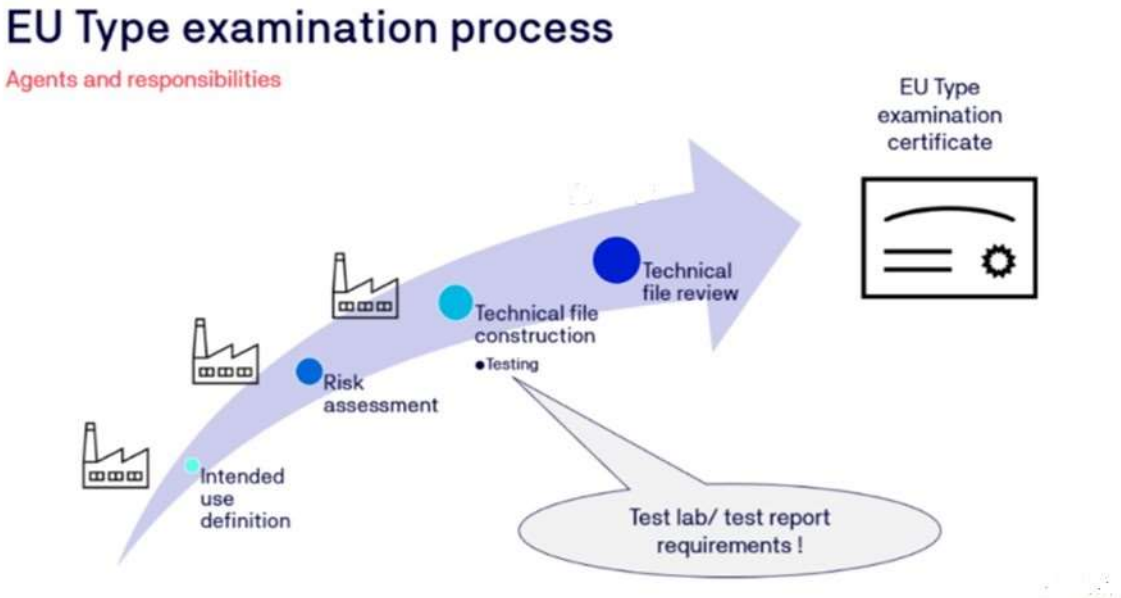
   Evalúa si el grado de protección que ofrecen las medidas de seguridad resulta suficiente ante el tipo de amenaza que se prevé. Toma en cuenta la clase de dispositivo y el ambiente en el que opera.

Proceso de Certificación de Examen UE de Tipo

Este proceso para equipos radioeléctricos bajo la Directiva RED y el Reglamento Delegado 2022/30 sigue una secuencia estructurada que permite validar la seguridad del producto y obtener el marcado CE.

Fases del proceso:

1. Solicitud
2. Workshop
3. Definición de activos y alcance
4. Entrega de muestras y documentación
5. Evaluaciones funcionales
6. Certificación



Restricciones en la Armonización

Aunque las normas EN 18031 permiten la presunción de conformidad, existen restricciones técnicas que pueden limitar su aplicación directa. Si el producto no cumple con estas restricciones, será necesario recurrir a un Organismo Notificado para validar el cumplimiento. Principales restricciones:

- Fortaleza de contraseñas
- Control parental
- Actualizaciones seguras

Estrategia de Cumplimiento para Empresas

La adaptación a los nuevos requisitos de ciberseguridad exige una estrategia clara, proactiva y alineada con el ciclo de vida del producto. Recomendaciones clave:

- Seguridad desde el diseño
- Análisis de riesgos
- Selección de normas aplicables
- Documentación técnica
- Roadmap de certificación

Conclusiones y Recomendaciones Finales

La incorporación de requisitos de ciberseguridad en la Directiva RED representa un cambio significativo en la regulación de equipos radioeléctricos en Europa. Las empresas deben prepararse para este nuevo escenario normativo mediante:

- Integración de la seguridad como parte del diseño del producto
- Adopción de normas armonizadas o equivalentes
- Planificación de procesos de evaluación y certificación
- Formación interna sobre requisitos técnicos y regulatorios

Rafael Rodríguez Muñoz

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