TLP:CLEAR

España | digital 2026

Defensa de endpoints en sistemas de control industrial

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

TLP:CLEAR

Mayo 2023

INCIBE-CERT_GUIA_DEFENSA_DE_ENDPOINTS_EN_SCI_2023_v1.0

Índice

ÍNDICE DE FIGURAS

1. Sobre esta guía

La presente guía pretende explicar en mayor medida todo sobre los *endpoints* y su seguridad a un nivel teórico.

La redacción tiene un carácter técnico, pero entendible para cualquier persona que quiera conocer tanto el concepto de *endpoint*, como las defensas de los mismos. Adicionalmente, se enumeran y explican diferentes defensas de perímetro posibles, es decir, se explican tanto las defensas a nivel de *endpoint* como a nivel externo.

El orden de los contenidos se encuentra distribuido de tal forma, que inicialmente se tenga un conocimiento introductorio a los *endpoint* en los sistemas de control industrial, junto con unos riesgos generales en los SCI y las defensas para estos dispositivos finales.

Por último, se realiza una conclusión en la que se valora este tipo de defensas sobre los dispositivos *endpoint*.

2. Organización del documento

La presente guía tiene una estructura enfocada al aprendizaje paulatino, empezando con una breve **3.- introducción** sobre los *endpoints* tanto a nivel IT como a nivel OT, centrándose sobre todo en esta última. Con esta introducción damos paso a una breve pero concisa explicación sobre **4.- que es un *endpoint*** y que tipo de medidas generales de seguridad requieren estos dispositivos.

Posteriormente, para poder dar un enfoque más cercano a las medidas de seguridad, se introducen diferentes **5.- riesgos a nivel industrial** que pueden afectar a este tipo de dispositivos. Esto se ve cumplimentado con el siguiente apartado sobre la protección de los *endpoints* en cuanto a la **6.- defensa en profundidad**.

Centrando ya la guía en las defensas, se hace un listado y una explicación de diferentes **7.- soluciones específicas de los endpoints**, así como sobre la seguridad física y en el sistema operativo. También se detallan ciertas limitaciones que pueden afectar a estos equipos industriales para incluirles diferentes métodos de seguridad. A su vez, y para contrarrestar las limitaciones de implementar agentes sobre los propios equipos, se detallan diferentes soluciones para **8. los endpoints a nivel de perímetro**.

Por último, para la finalización de la guía, se recogen unas **9.- Conclusiones** basadas en las diferentes soluciones **de** defensa para los *endpoints*.

3. Introducción

[1]Desde hace varios años se habla de la Industria 4.0 y la digitalización de los procesos industriales. Esta evolución ha hecho que los dispositivos encargados de controlar los procesos industriales hayan sido sustituidos paulatinamente por otros con mejores capacidades y mayor inteligencia, además de poder interconectarse entre ellos a través de una red, estos dispositivos se conocen como **dispositivos IoT** (*Internet of Things*[1]) o como **dispositivos IIoT** (*Industrial Internet of Things*[2]) en el caso de que se encuentren en un entorno industrial. Para concretar la magnitud del crecimiento, tanto en dispositivos, como de interconexiones entre ellos, en el artículo de INCIBE-CERT de Predicciones en Seguridad Industrial en 2023[3], se indica una previsión sobre el número de dispositivos inteligentes conectados en el año **2025, dicha previsión concluye en que se llegará a la cifra de 21,5** billones de dispositivos conectados.

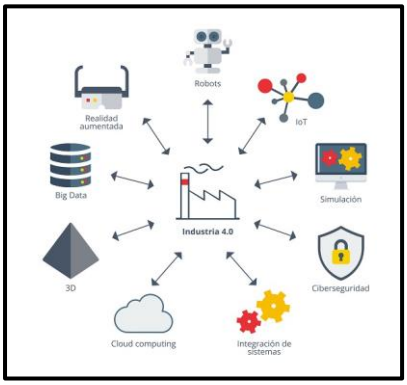


Ilustración 1: Industria 4.0 y sus conectividades[1]

Desde el momento en que un dispositivo se conecta a una red, debe ser debidamente protegido para evitar acciones maliciosas sobre él, esto no solo se aplica a dispositivos en cualquier red, sino que también es aplicable a los dispositivos industriales. Existen múltiples medidas de protección que se adaptan a las distintas necesidades que puede presentar un dispositivo de red, por lo que el **objetivo de la presente guía** es **presentar soluciones para la defensa de dispositivos finales o "*endpoints*".**

La protección de los dispositivos industriales, es uno de los mayores retos en cuanto a la seguridad en el ámbito industrial debido a su particularidad, ya que normalmente se tratan de dispositivos diseñados para desempeñar una tarea concreta, lo cual no permite mucho margen a la hora de configurarlos. Además, hasta hace unos años, la ciberseguridad no ha sido un factor que se haya tenido en cuenta en el proceso de diseño de los dispositivos industriales, lo que resulta en equipos con pocas capacidades en cuanto a ciberseguridad.

A esto se suma la **dificultad intrínseca de la tarea de actualización y aplicación de parches a los dispositivos industriales**, lo que radica en la persistencia de las vulnerabilidades detectadas en los equipos. Al igual que en ámbito de IT, el sector industrial también sufre ataques, y, muchas veces, con un impacto directo en las personas, ya que muchas de las actividades del sector industrial son dedicadas a satisfacer servicios básicos de la sociedad, como la luz, el agua, etc.

CrashOverride, el ataque a Colonial Pipeline[4] o a una estación de tratamiento de aguas residuales en Florida, son algunos ejemplos de los ataques a sistemas de control industrial

[1] https://www.incibe.es/incibe-cert/blog/iot-protocolos-comunicacion-ataques-y-recomendaciones

[2] https://www.incibe.es/incibe-cert/blog/mejora-del-iiot-entornos-industriales

[3] https://www.incibe.es/incibe-cert/blog/que-esperar-de-la-ciberseguridad-industrial-en-2023

[4] https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/interrupcion-el-suministro-del-oleoducto-colonial-pipeline

que ha habido en la última década, y todos ellos tuvieron un impacto directo en las personas.

4. ¿Qué es un *endpoint*?

Cuando se habla de un dispositivo ***endpoint***, se habla de un activo final presente a nivel de red. Entre estos dispositivos podemos encontrar desde, estaciones de ingeniería (*workstations*), hasta servidores, HMI, SCADA, PLC entre otros. Estos dispositivos son puntos clave desde el punto de vista de la seguridad, ya que sus vulnerabilidades podrían afectar a otros activos dentro de la red.

Con el **crecimiento exponencial de dispositivos IoT e IIoT,** la superficie de exposición en entornos industriales ha aumentado. Obligando a bastionar los equipos siguiendo el concepto de defensa en profundidad o desplegando soluciones para la defensa de los *endpoint*. El conjunto de dispositivos finales conforma la primera línea de defensa de toda red de comunicaciones a nivel lógico, ya sea industrial o no, ya que la mayor parte de los ataques intentan vulnerar estos dispositivos mal protegidos.

Las **soluciones de protección para los *endpoint* hacen referencia a las defensas para estos activos industriales base**. En la actualidad, ya no solo vale con la introducción de un cortafuego para la protección perimetral negando el acceso a posibles actores maliciosos, sino que es necesaria una capa de seguridad adicional, es ahí, donde entran las defensas de los *endpoints*.

Como ya se ha mencionado anteriormente, en términos generales los *endpoints* hacen referencia a cualquier dispositivo conectado a la red. Mirando esto desde la perspectiva IT y los niveles superiores del modelo Purdue[5], los *endpoints* podrían ser ordenadores sobremesa, portátiles, teléfonos móviles, impresoras y enrutadores. Pero en caso de hacer referencia a las capas inferiores del modelo Purdue y más a la parte operacional, los *endpoints* incluyen a los controladores lógicos programables (PLC), sistemas de control de supervisión y adquisición de datos (SCADA), sistemas instrumentados de seguridad (SIS), unidades terminales remotas (RTU), dispositivos electrónicos inteligentes (IED) e interfaces hombre-máquina (HMI).

Todos estos dispositivos de la parte industrial de cualquier empresa son un punto muy crítico en cuanto a su funcionalidad y seguridad, es por ello, que la defensa de los mismos, es crítica, y aunque muchos sean dispositivos propietarios (cuya configuración es difícil de modificar para mejorar la seguridad) y dispositivos heredados (diseñados e implementados antes de que existieran preocupaciones en cuanto a la ciberseguridad de estos sistemas), existen diferentes soluciones, mecanismos o herramientas para protegerlos.

A alto nivel, podemos definir diferentes acciones para realizar una mejora en cuanto a la seguridad de los *endpoints*:

- Utilización de un inventario de activos[6] bien actualizado, tanto a nivel de *hardware* como de *software*, para conocer que versiones y posibilidades existen para proteger al dispositivo.

[5] https://www.incibe.es/incibe-cert/blog/ciberseguridad-el-modelo-purdue-dispositivos-nivel-1

[6] https://www.incibe.es/incibe-cert/guias-y-estudios/guias/guia-para-la-gestion-de-un-inventario-de-activos-en-sistemas-de-control

- Control de las conexiones externas de la red industrial tanto a Internet como por acceso remoto. Minimizar la conectividad en mayor medida y controlar estrictamente las autorizaciones de seguridad.
- Configurar correctamente, y siempre y cuando sea posible, la seguridad de los dispositivos finales.
- Implementar soluciones para monitorizar de forma continua y en tiempo real todos los dispositivos *endpoint*.
- Desarrollar y mejorar políticas y procedimientos sobre la seguridad de los dispositivos finales.

5. Riesgos en los sistemas de control industriales

Dentro de la infraestructura de cualquier empresa industrial **coexisten dos entornos muy claros, el entorno IT** (*Information Technologies*) y el **entorno OT** (*Operation Technologies*), es por ello que existen una gran cantidad de dispositivos finales conectados, y aunque este avance de interconexión entre estos dos entornos tan diferentes[7] ha generado una mejora en la visibilidad, la eficiencia y la velocidad en las comunicaciones, también ha derivado en una **mayor exposición a diferentes amenazas para el entorno de los SCI**[8] (Sistemas de Control Industrial), ya que la dicha conectividad genera que las amenazas que se ciernen sobre el entorno IT puedan afectar a los sistemas industriales.

Esta unión entre entornos a la que se ha hecho referencia anteriormente implica una conexión entre los procesos de gestión, control y comercio, con los procesos físicos del entorno operacional. Derivando en el intercambio de datos, el control de diferentes operaciones y el seguimiento de los procesos industriales desde el entorno IT. Son los *endpoints* en los entornos industriales, los encargados del desarrollo, control y seguimiento.

Para tener un mayor conocimiento sobre los **dispositivos *endpoints* y los riesgos que pueden generar sobre los sistemas de control industrial**, en la Ilustración 2, se muestran resaltados en rojo diferentes *endpoints* industriales dentro del modelo Purdue.

[7] https://www.incibe.es/incibe-cert/blog/diferencias-ti-to

[8] https://www.incibe.es/incibe-cert/blog/amenazas-sci

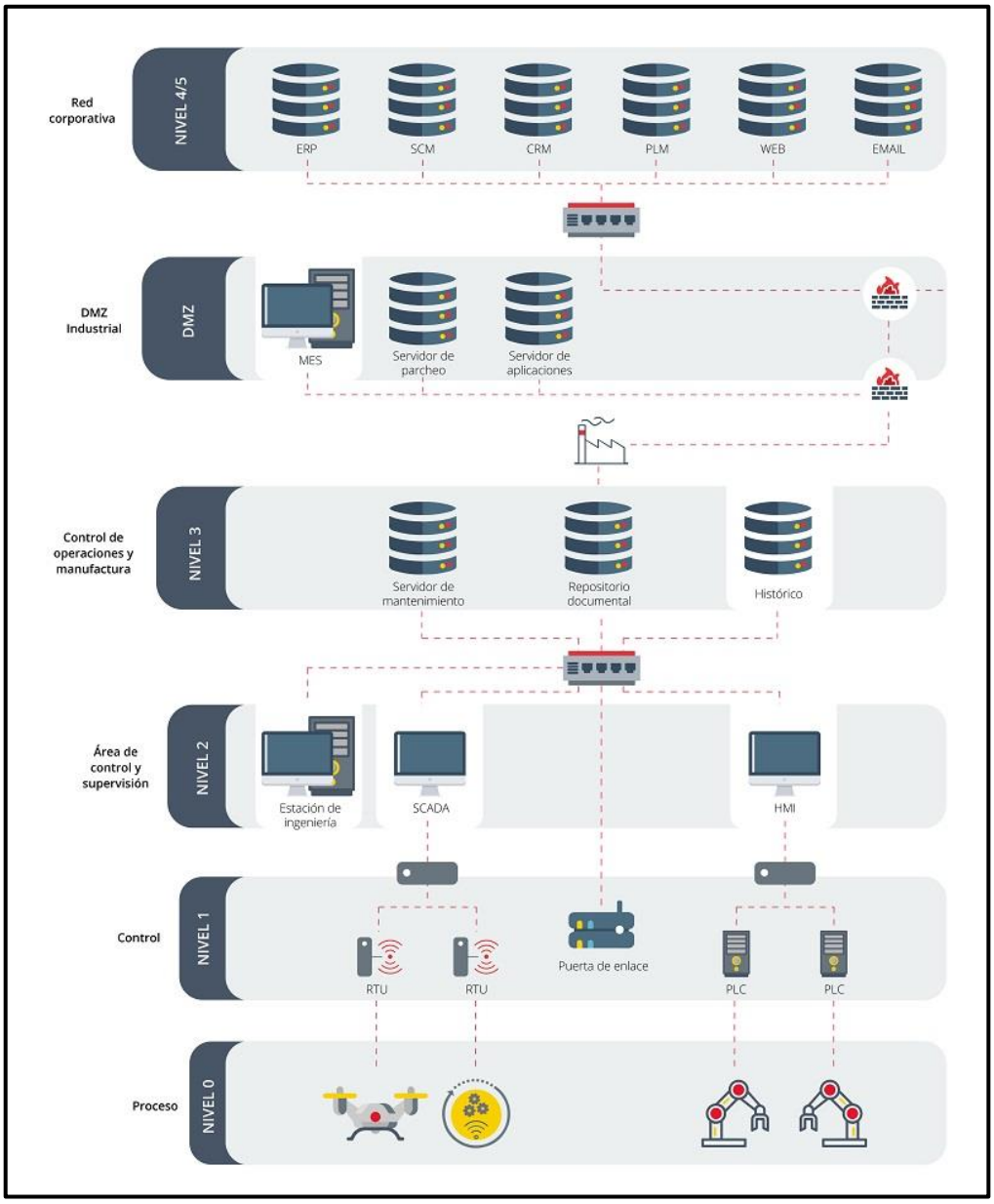


Ilustración 2: Dispositivos endpoint en un entorno IT/OT[9]

Poniendo el foco sobre los riesgos o vulnerabilidades que pueden afectar a los sistemas de control industrial, y el porqué de usar mecanismos o herramientas para la protección de sistemas industriales, a continuación, se presentan un conjunto de riesgos o vulnerabilidades que frecuentan en los entornos industriales:

- **Exposición a Internet:** originalmente, los entornos industriales eran entornos aislados y estaban limitados a las plantas. Como se puede observar en la Ilustración 2, y tal y como se ha mencionado anteriormente, la evolución industrial y la integración con una mayor cantidad de sistemas y plataformas (entre entornos IT y entornos OT) para facilitar el acceso, ha desembocado en que algunas empresas terminen conectando sus sistemas industriales o parte de ellos con Internet sin ninguna medida de seguridad.

[9] https://www.trendmicro.com/en_us/research/22/a/cybersecurity-industrial-control-systems-ics-part-1.html

La existencia de conexiones inseguras abre una puerta de acceso a entidades con intenciones maliciosas.

También es muy común proporcionar acceso externo a los proveedores para fines de mantenimiento, esto puede derivar en un punto de acceso para dichos atacantes con intenciones maliciosas. Los sistemas utilizados por los proveedores externos pueden amenazar la seguridad de la empresa cliente. Por otro lado, las malas configuraciones en las VPNs, en las que no se restringen los usuarios o las máquinas a las que se quiere dar acceso, también suponen un riesgo.

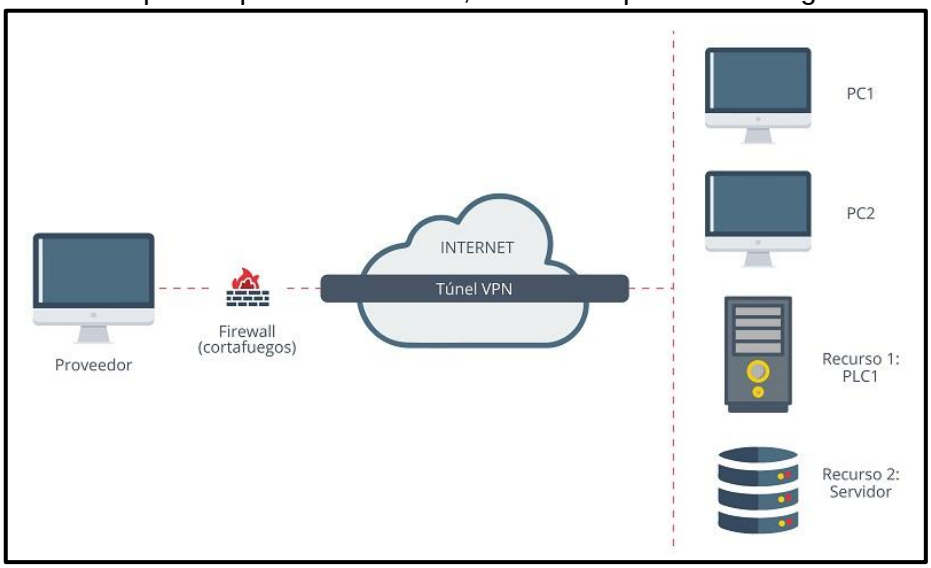


Ilustración 3: Túnel VPN entre un proveedor y los dispositivos en un entorno industrial[10]

- **Segregación débil:** la segregación débil entre los entornos IT y OT es uno de los factores más comunes que comprometen las redes industriales. Un control de acceso débil puede permitir que una máquina conectada a la red IT llegue a un dispositivo en la red ICS, y una infección de *malware* en el sistema IT puede permitir que se propague hasta OT.
- **Equipos desactualizados y con configuraciones por defecto:** no todas las empresas pueden permitirse el tiempo de inactividad para actualizar los equipos, ya que conduce a una disminución de la producción y a la pérdida de ingresos. Otras empresas sienten que sus sistemas industriales están aislados de forma segura, y no aplican parches que publican los fabricantes para corregir vulnerabilidades, o mantienen la configuración por defecto de los equipos.
- **Falta de integridad en los datos:** en el mundo industrial, una posible alteración de los datos puede significar graves problemas en diferentes procesos. Garantizar la integridad de los datos permite que la información almacenada o datos en curso entre dispositivos, sea completa, precisa y fiable; garantizando su protección ante ataques o acceso externos no autorizados. Es por ello que los dispositivos finales, o *endpoints* deben tener esa capacidad de garantizar la integridad de los datos.
- **Debilidad en los protocolos ICS:** los protocolos originales utilizados en ICS no se diseñaron teniendo en cuenta la seguridad. Han pasado los años, y se siguen utilizando los mismos protocolos que antes.

[10] https://www.antiun.com/vpn/

Ilustración 4: Protocolos industriales[11]

Por ejemplo, el protocolo MODBUS utiliza comunicación de texto sin cifrar, lo que puede permitir que un atacante espíe el tráfico, y tampoco presenta una autorización adecuada, lo que puede dar lugar a acciones no autorizadas, como actualizar el programa de lógica de escalera o apagar el PLC.

- **Debilidad en las aplicaciones de ICS:** las aplicaciones relacionadas con ICS a veces son vulnerables, como las interfaces web con la que cuentan algunos dispositivos para su gestión, las cuales pueden ser vulnerables a ataques dado que implementan protocolos no seguros como HTTP. Esto puede conducir a la divulgación de credenciales por la red o a secuestro de sesiones.
- **Falta de conciencia de seguridad:** debido a la falta de conciencia de seguridad, los empleados a menudo se convierten en víctimas de ataques de ingeniería social, *phishing* y *spear-phising*. A veces, un atacante sólo necesita un clic de una víctima para conseguir sus objetivos. Una vez comprometida una máquina, un atacante puede tratar de moverse en la red y vulnerar nuevos equipos.

[11] https://www.logicbus.com.mx/pdf/articulos/Protocolos-de-Comunicaci%C3%B3n-Industrial.pdf

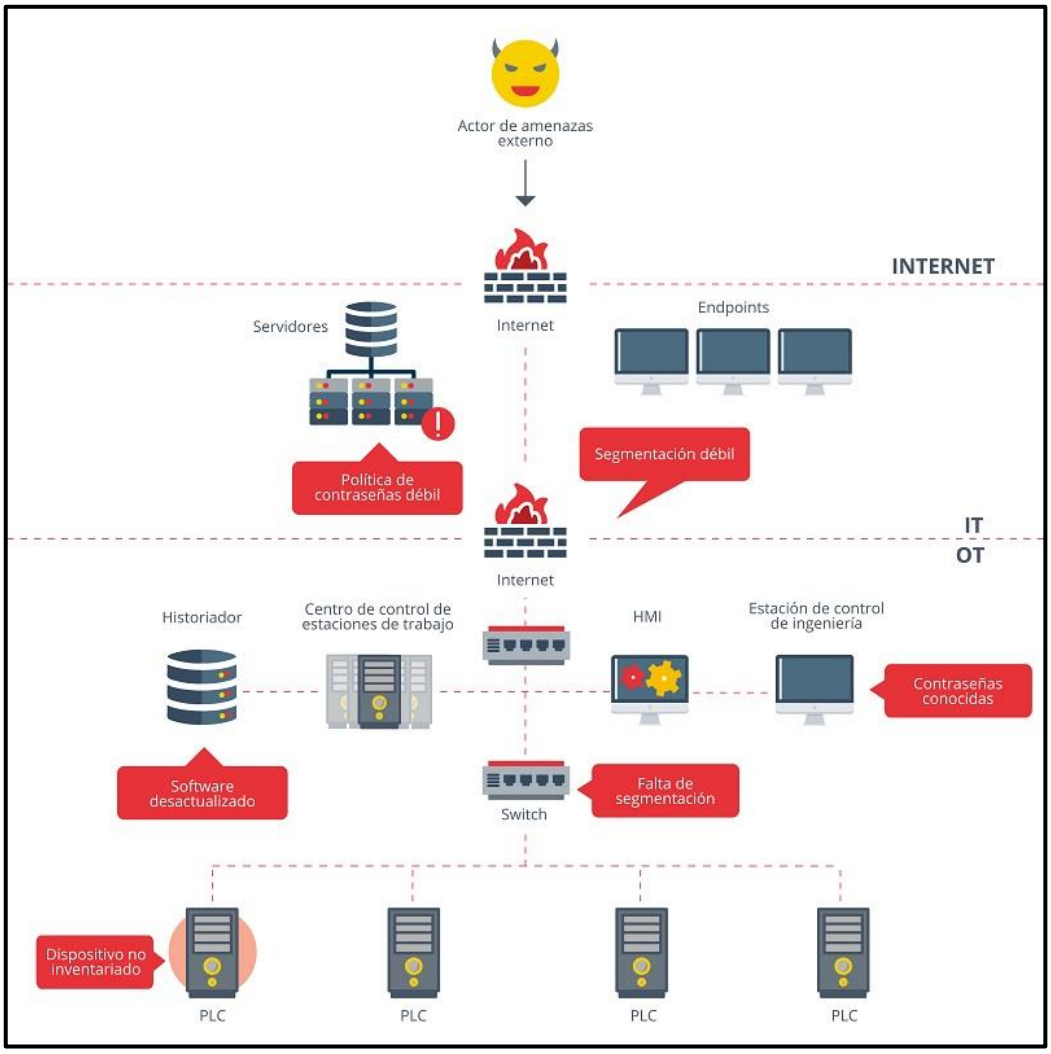


Ilustración 5: Diferentes riesgos de los entornos industriales[12]

[12] https://www.wizlynxgroup.com/mx/ciberseguridad-mexico/evaluacion-de-la-seguridad-de-los-sistemas-de-control-industrial

6. Protección de los *endpoint*: defensa en profundidad

Con el objetivo de dar una protección completa a los *endpoint*, se va a seguir una filosofía basada en el concepto de **defensa en profundidad**. Esto quiere decir que las protecciones se van a aplicar en múltiples capas, comenzando desde el nivel más bajo, desde el propio sistema operativo de los equipos y sus aplicaciones, hasta el nivel más alto, correspondiente con las defensas en el exterior del dispositivo, en su entorno.

La siguiente imagen muestra de forma esquemática las distintas capas de protección aplicables a un dispositivo, y cómo cada una de ellas forma un muro que protege a todas las anteriores.

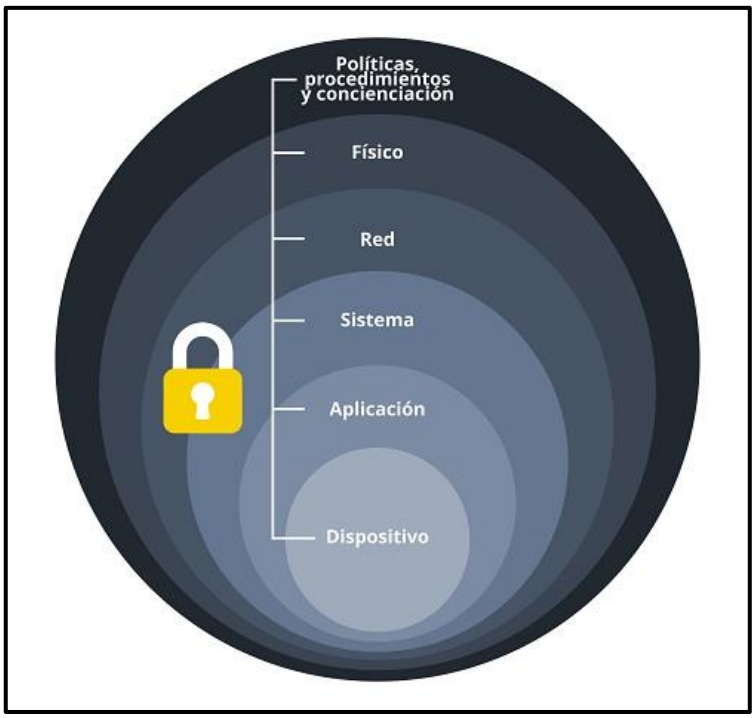


Ilustración 6: Capas para la defensa en profundidad[13]

A lo largo de la guía, se van a presentar varios tipos de defensas aplicables a dispositivos industriales. Estas defensas variarán dependiendo de la "capa" a la que pertenezcan y al propio activo que se quiera proteger, ya que no es lo mismo la protección que se aplicaría para la defensa de sistemas SCADA, que la protección que se aplicaría para un PLC. Por lo tanto, en los siguientes apartados se van a mostrar medidas de protección para los *endpoint* aplicables en los propios dispositivos, es decir a nivel de configuraciones o *software* de protección instalable, o protecciones desde el exterior y en su entorno.

[13] https://www.networkaccess.com/defense-in-depth/

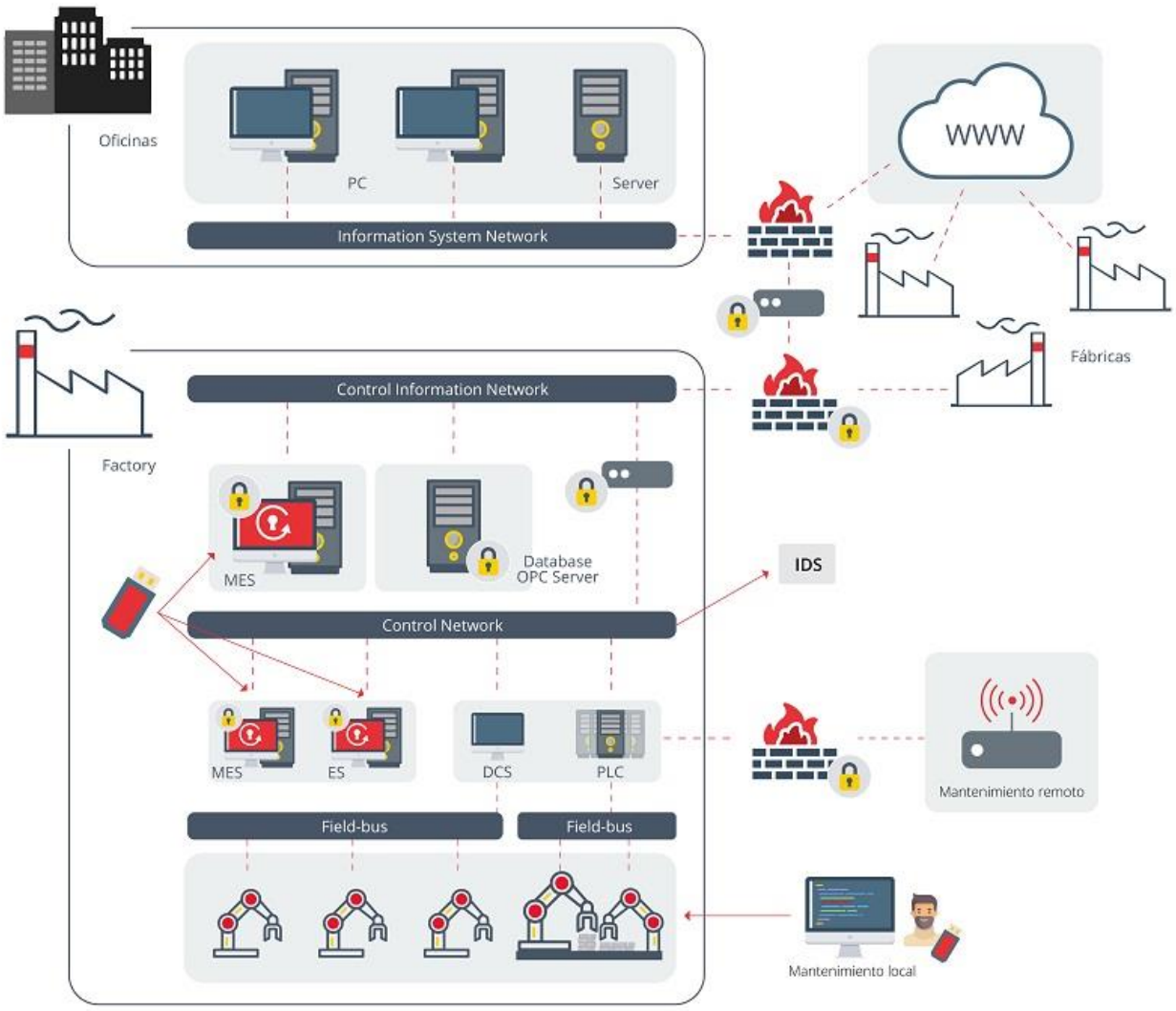


Ilustración 7: Protección de los endpoint en varias capas[14]

[14] TrendmicroSolution.pdf

7. Defensas en los *endpoint*

Este apartado se centra en las protecciones que se pueden aplicar a los propios *endpoint*. Se presentan formas de protección del propio sistema operativo o *firmware* de los equipos, y las aplicaciones que tengan instaladas, sin dejar de lado la instalación de *software* específico para la protección de los equipos, y teniendo en cuenta también la protección física de los activos.

7.1. Seguridad en aplicaciones y el sistema operativo: bastionado

El bastionado de los equipos o *hardening*, es el procedimiento mediante el cual se tratan de reducir las vulnerabilidades en un sistema. El desarrollo y manejo del bastionado de equipos industriales es necesario con el fin de controlar la seguridad de los distintos activos de manera individual y conjunta para mejorar la seguridad general de los sistemas industriales.

La aplicación de bastionado a equipos industriales reduce la exposición de los activos a posibles ataques, vulnerabilidades o configuraciones incorrectas que pueden ser aprovechadas para explotarlos. Esto se consigue aplicando configuraciones seguras en los equipos, las cuales deben tener en cuenta diferentes aspectos principales:

- Aplicaciones, servicios y protocolos de red.
- Acceso local.
- Acceso remoto.
- Autenticación AAA.
- Sistema operativo y *firmware*.
- El registro de eventos.

Para el desarrollo del bastionado de dispositivos, previamente debe realizarse un conjunto de **guías de bastionado**, en las cuales se especifican qué configuraciones se deben aplicar a cada equipo, porqué se están aplicando y que es lo que tratan de evitar con dicha protección. Dado que cada equipo es distinto y está orientado a una tarea diferente, las guías de bastionado deben ser personalizadas para cada uno, ya que en ellas se tiene en cuenta las particularidades y la situación de cada uno.

Para la elaboración de las guías de bastionado sería necesario disponer del dispositivo que se quiere proteger y su manual, con el fin de poder explorar todos los parámetros que dispone, configuraciones aplicadas, servicios, *software* etc. Gracias a esto, pueden identificarse todos los puntos posibles de protección para el equipo, y cuáles son las configuraciones que deberían aplicarse en cada uno de ellos. Todo esto quedará recogido en un documento personalizado para cada equipo en el que se indiquen todos los pasos a seguir para bastionar el equipo.

Para la elaboración de estas guías, es posible apoyarse en guías ya existentes como por ejemplo las **guías STIG de la DISA (*Defense Information System Agency*)**. Existen varias guías aplicables a distintos sistemas operativos o *software*, en las cuales se indica un listado con diferentes medidas de protección o configuraciones aplicables en los equipos. Estas configuraciones están catalogadas según su severidad permitiendo priorizar cuales de ellas quieran aplicarse.

Respecto a la aplicación de las guías de bastionado elaboradas, dado que los equipos a proteger son equipos industriales en los cuales la disponibilidad es su prioridad máxima, se recomienda que se prueben en un entorno de laboratorio seguro, y no en producción. Esto es debido a que algunas configuraciones aplicables a los equipos podrían limitar sus funcionalidades, afectando no sólo al propio equipo, si no a otros que puedan depender de él.

7.2. Endpoint Security (EDR)

Los **EDR** son un tipo de defensa muy completa para los activos industriales. Poseen varias capacidades o características que motivan su uso en entornos industriales. Algunas de ellas son las siguientes:

- Monitorizar áreas problemáticas y movimientos de tráfico.
- Detección de anomalías y capacidad de bloqueo.
- Protección de los datos almacenados en los equipos.
- Cortafuegos.
- *Sandboxing* de programas infectados o ambiguos.
- Integración con antivirus.
- Protección del equipo con mecanismos *software* que afecten en cierta medida a la parte física, como el bloqueo de dispositivos USB.
- Administración centralizada (no todos).

Ahora que ya se han mencionado las capacidades que poseen los EDR, se puede profundizar un poco más, enumerando algunas de las técnicas o las herramientas de las que disponen para desempeñar todas las tareas mencionadas anteriormente. Estas son algunas de ellas:

7.2.1. Whitelisting

Es **una de las protecciones más utilizadas a nivel industrial porque no tiene gran impacto sobre el sistema** donde se despliega. Consiste en una lista o registro de entidades que, por una razón u otra, pueden obtener algún privilegio o acceso particular. Es un mecanismo de seguridad que permite controlar los procesos ejecutados, *software* instalado, etc.

WHITELISTING	
VENTAJAS	Bloquea la mayoría del *malware*.
	Previene el uso de aplicaciones no autorizadas.
	No requiere actualizaciones diarias.
	El administrador del equipo es el encargado de autorizar las nuevas aplicaciones.
DESVENTAJAS	Añade carga al rendimiento del equipo.
	Requiere mantenimiento de forma regular.
	En ciertas ocasiones, puede resultar molesto para los usuarios.

	Las aplicaciones permitidas son susceptibles de ser comprometidas.

Tabla 1: Características del Whitelisting

7.2.2. Protección *antimalware*

Esta protección, como su propio nombre indica, se encarga de detectar, proteger y eliminar *software* malicioso. Lo hace mediante la detección y gestión de ficheros o acciones maliciosas que puedan afectar a un sistema.

Para ello, realiza escaneos de los ficheros de un equipo y los compara con su base de datos de firmas. Para que una pieza de *malware* pueda ser detectada, será necesario que esté incluida en las firmas del *software antimalware*, por lo que es de vital importancia su constante actualización.

Debido las capacidades que poseen algunos sistemas antiguos, puede que no sea posible el despliegue de agentes, por lo que se pueden utilizar herramientas externas como por ejemplo el uso de un dispositivo USB que contenga una herramienta *antimalware* en modo portable que permita un análisis exhaustivo del mismo y que no requiera de una instalación en el propio sistema. Algunos fabricantes ya proporcionan esta opción, la cual posee funcionalidades como el escaneo *antimalware*, obtención de información del sistema, integridad de ficheros, etc.

7.2.3. HIDS (Host-based Intrusion Detection System)

Un HIDS, también conocido como **Sistema de Detección de Intrusos en un Host**, busca detectar anomalías que indican un riesgo potencial, revisando las actividades en la máquina (host). Puede tomar medidas protectoras. En comparación con otras soluciones *endpoint*, este tipo de *software* es muy similar al de los IDS.

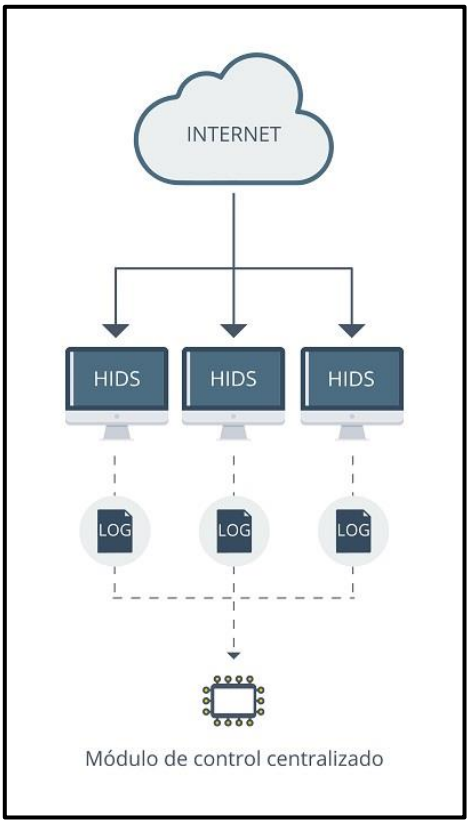


Ilustración 8: Arquitectura con las soluciones HIDS instaladas[15]

Los **HIDS** presentan las siguientes funciones:

- Gestión de virus.
- Análisis de *logs* locales.
- Comprobación de integridad de ficheros.
- Monitorización de políticas.
- Detección de *rootkits*.
- Monitorización de red, desde el punto de vista del host.
- Alertas en tiempo real.
- Respuesta activa.
- Inventariado del sistema.

7.2.4. IA y Machine Learning

Se pueden emplear técnicas avanzadas como la inteligencia artificial o el aprendizaje automático que permitan la detección temprana de forma proactiva de amenazas persistentes avanzadas (**APT**) a nivel industrial.

[15] https://www.comparitech.com/net-admin/network-intrusion-detection-tools/

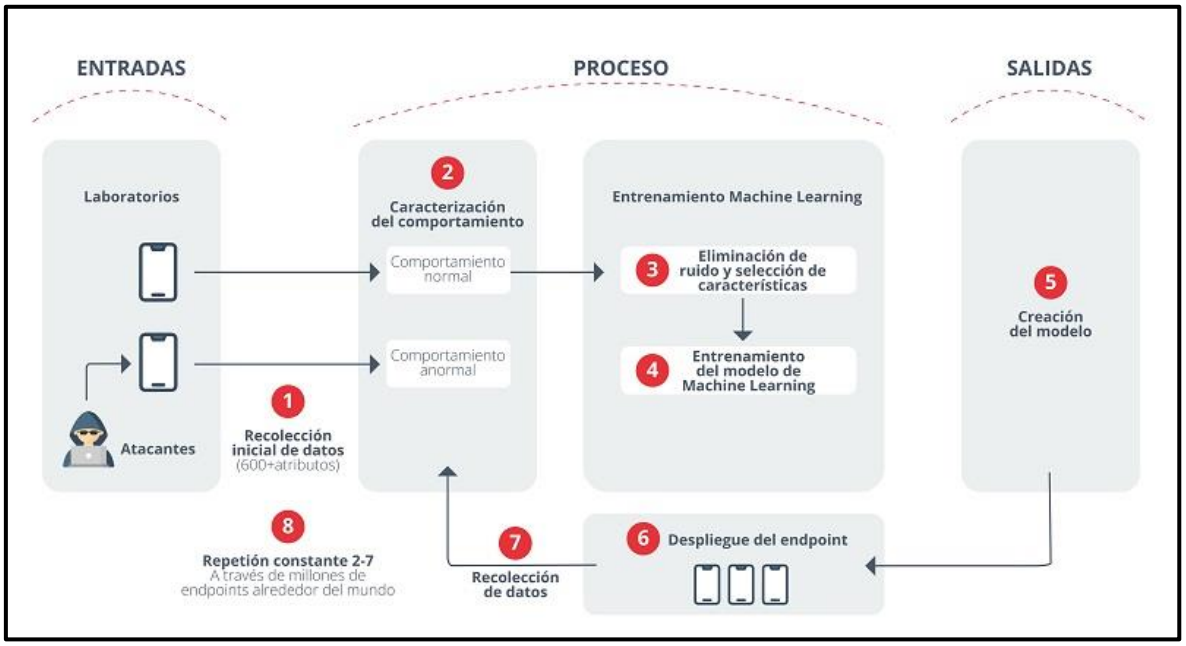


Ilustración 9: Proceso de entrenamiento de IA mediante diferentes comportamientos y su modelización

7.3. Seguridad física

La seguridad física recae sobre cualquier mecanismo para poder asegurar su integridad y preservación. Este tipo de seguridad ha de tratarse como un tipo de seguridad más en el ámbito de la ciberseguridad industrial.

El principal objetivo de la seguridad física es mantener a los diferentes operarios o trabajadores alejados de situaciones peligrosas, así como, proteger a los equipos de posibles agentes maliciosos que quieran acceder o interactuar físicamente con los equipos industriales.

Ilustración 10: Seguridad física.

La guía de buenas prácticas NIST 800-82 “Guide to Industrial Control Systems (ICS) Security”[16], recoge los atributos que han de considerarse a la hora de realizar una defensa en profundidad aplicada a la seguridad física. A continuación, se detallan dichos controles:

- Protección de las ubicaciones físicas.
- Control de acceso.
- Sistemas de monitorización de accesos.
- Sistemas de limitación de acceso.
- Sistemas que permitan el seguimiento de personas o activos.
- Sistemas de gestión de factores ambientales.
- Sistemas de control de condiciones ambientales.
- Sistemas de protección de corriente.
- Sistemas de protección adicionales para centro de control.
- Sistemas de control de los dispositivos de configuración portables.
- Sistemas de protección de cableado.

Como ha quedado evidente, la seguridad física de los equipos es un aspecto muy importante de la seguridad total de los dispositivos y por lo tanto, una buena defensa física[17] puede ser determinante tanto a la hora de proteger a los equipos ante posibles ataques tanto como a las personas que trabajan con ellos.

7.4. Limitaciones en los equipos industriales

Una vez identificados los mecanismos que utilizan las soluciones e*ndpoint* y sus capacidades, es necesario mencionar algunas particularidades que poseen los equipos de los sistemas industriales que los diferencian frente a equipos de entornos corporativos. Estas particularidades deben tomarse en consideración, ya que **pueden afectar directamente al modo de operación de las soluciones e*ndpoint*, limitando sus acciones o haciendo necesario el uso de otro tipo de soluciones para poder defender los equipos**.

- **Capacidad de procesamiento:** ciertos equipos industriales carecen de una elevada capacidad de procesamiento. Este aspecto es muy relevante y se debe tener en cuenta a la hora de instalar diferentes soluciones de seguridad en los *endpoint*, una sobrecarga del sistema o del dispositivo en sí, puede derivar en una falta de capacidad en la ejecución del proceso.
- **Equipos con tareas concretas:** los equipos industriales se consideran dispositivos fijos, es decir, la capacidad de modificar su configuración o la instalación de agentes externos se considera compleja y en muchos casos imposible. Esta problemática o limitación, se ve cumplimentada con la limitación de capacidad de procesamiento detallada anteriormente. Este caso es muy común en dispositivos PLC.
- **Despliegue en *hosts*.** algunas aplicaciones de fabricantes industriales pueden ser bastante sensibles al uso de ciertas versiones de sistemas operativos, parches instalados o instalaciones relacionadas con cambios en el sistema. Debido a esta problemática, modificar los sistemas operativos o versiones de algunos dispositivos sin el consentimiento expreso del fabricante puede derivar en un fallo del dispositivo y por

[16] https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

[17] https://www.incibe-cert.es/blog/el-punto-el-seguridad-y-ciberseguridad-convergen

lo tanto la consiguiente parada del proceso industrial o de la actividad que estuviese realizando. Además, en la mayor parte de los casos, la modificación de versión desautorizadas deriva en una pérdida de la garantía del dispositivo y por lo tanto el consiguiente coste económico en caso de un fallo accidental del dispositivo.

- **Incompatibilidades con fabricantes:** ciertos equipos industriales poseen un sistema operativo base como Windows o Linux, sobre el que va montado su aplicativo. La inclusión de una solución EDR que incluya la instalación de agentes puede suponer una limitación sobre el equipo. Esto puede suponer que las tareas de protección que desempeñe dicho EDR afecten directamente al funcionamiento del equipo. Entre estas funcionalidades afectadas se pueden encontrar las comunicaciones con puertos inseguros, servicios o puertos, etc.
- **Actualización de firmas:** muchas redes industriales están aisladas del exterior y no poseen salida a Internet. Esto genera dificultades para la actualización de las firmas de los antivirus.

8. Defensas en el exterior

Para una protección completa de los *endpoint* también será necesaria una defensa de estos desde el exterior, es decir, no delegar toda la protección a los equipos, sino securizar también su entorno.

8.1. Arquitectura segura

Los *endpoints* van a estar conectados entre ellos mediante una red, y su topología afecta directamente a la seguridad y la exposición de los equipos. Por ello, es importante que los equipos a proteger se encuentren conectados en una red cuya arquitectura siga unos principios de seguridad y haya sido estructurada debidamente. Para ello, el objetivo será segregar la red en distintas subredes para poder así con la ayuda de un *firewall* controlar todas las comunicaciones entre cada uno de los segmentos.

La aproximación que se aconseja seguir tratándose de equipos que se encuentran en sistemas industriales, es la marcada por la norma IEC 62443-3-2 "**Standard addresses security risk assessment and system design for IACS**", donde se introducen los conceptos de *zonas y conductos*[18] para una segmentación segura de las redes industriales aplicando la defensa en profundidad.

Una zona es una agrupación de activos físicos o lógicos que comparten requisitos comunes de seguridad, los cuales tienen la frontera física o lógica definida. Y los conductos son las conexiones entre las zonas, y deben contener medidas de seguridad que controlen el acceso a ellas, resistir ataques y proteger las comunicaciones.

8.2. Firewall industrial

Estos dispositivos son los encargados de aislar las diferentes zonas y permitir únicamente el tráfico autorizado entre los diferentes segmentos de la red, ya sea industrial o de carácter más corporativo, o incluso la frontera entre estos dos entornos. Poseen ciertas características que los diferencian de sus análogos de propósito general, tales como, su funcionamiento en modo transparente o la inspección profunda de paquetes, en la que analiza cada campo de los paquetes y realiza un filtrado en función de los valores específicos del protocolo.

[18] https://www.incibe.es/incibe-cert/blog/zonas-y-conductos-protegiendo-nuestra-red-industrial

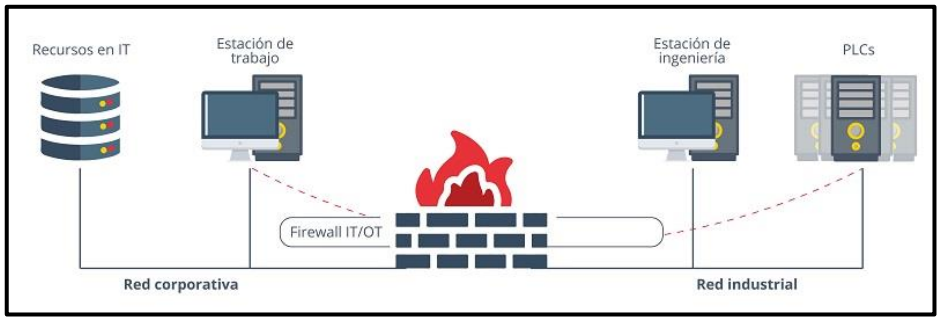


Ilustración 11: IT/OT firewall[19]

8.3. IDS e IPS

Los **IDS** (*Intrusion Detection System*), son sistemas que monitorizan el tráfico[20] en busca de anomalías o actividades sospechosas que puedan indicar el inicio de un ataque, con el fin de prevenirlo o, si no fuera posible, remediarlo cuanto antes. Este tipo de herramientas analizan el tráfico que circula por las redes en tiempo real sin necesidad de interrumpir el flujo de datos, actuando de forma pasiva, monitorizando el tráfico entrante, saliente y local.

Cuando detectan cualquier actividad sospechosa, emiten una alerta a los administradores del sistema, quienes deberán decidir qué medidas oportunas tendrán que llevarse a cabo. Estos accesos pueden ser ataques esporádicos realizados por usuarios malintencionados o repetidos cada cierto tiempo, gracias al uso de herramientas automáticas. Estos sistemas sólo detectan los accesos sospechosos[21] emitiendo alertas anticipadas de posibles intrusiones, pero no tratan de mitigar la intrusión.

También existen los **IPS** (*Intrusion Prevention System*), que además de las capacidades que poseen los IDS, pueden actuar sobre las comunicaciones descartando paquetes o cortando conexiones. Generalmente estos sistemas no son muy usados en entornos industriales, y se limitan al uso de IDS, que avisan, pero no actúan, para no interrumpir el proceso industrial.

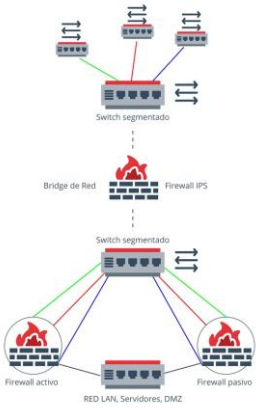


Ilustración 12: IPS[22]

[19] https://applied-risk.com/resources/4-ot-it-network-segmentation-techniques-selecting-a-cyber-resilient-configuration

[20] https://www.incibe.es/empresas/blog/son-y-sirven-los-siem-ids-e-ips

[21] https://www.incibe.es/incibe-cert/blog/diseno-y-configuracion-de-ips-ids-y-siem-en-sistemas-de-control-industrial

[22] https://tr0n3t.wordpress.com/2020/04/28/firewall-transparente-con-pfsense/

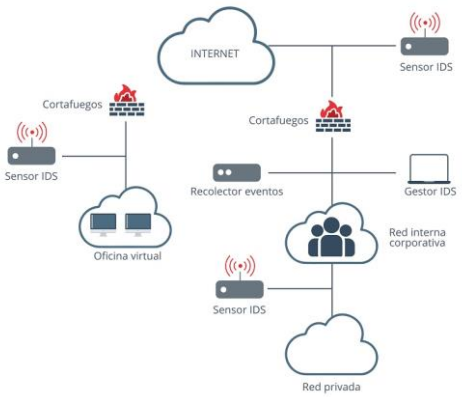


Ilustración 13: IDS

8.4. Accesos remotos seguros

Los accesos remotos seguros en sistemas industriales son uno de los aspectos clave en cuanto a la seguridad. Cada vez hay más proveedores que realizan comunicaciones de mantenimiento u operaciones a través de accesos remotos, para el cliente, este acceso es un punto de acceso a su red, por lo que debe buscar que sean lo más seguros posibles y que únicamente se utilicen cuando sean estrictamente necesarios.

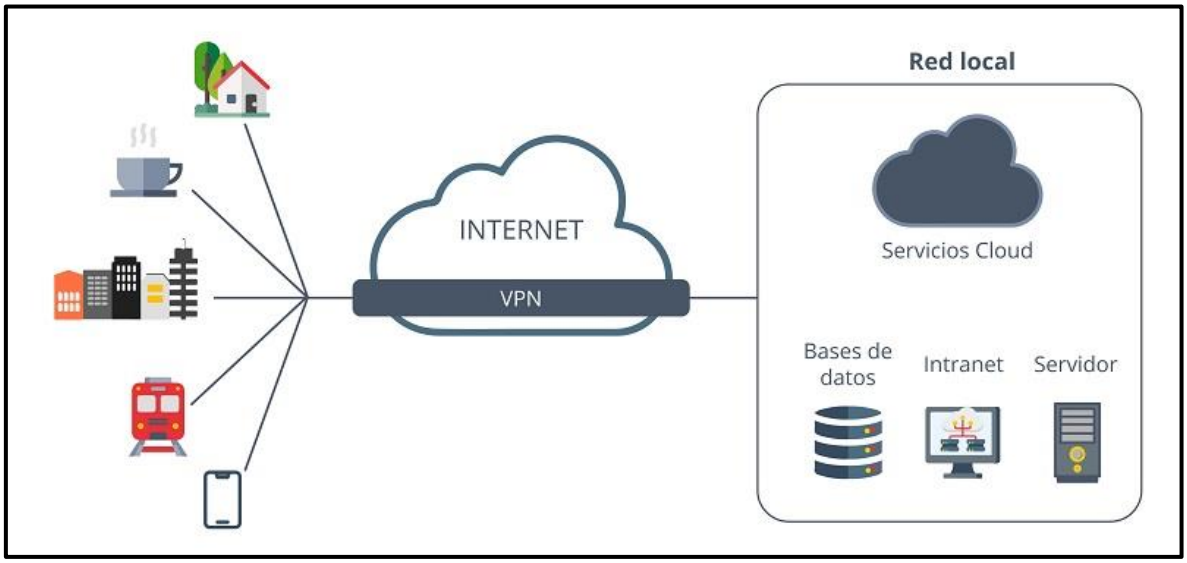


Ilustración 14: Uso de VPN para conexión remota[23].

Existen diferentes métodos de acceso remoto para sistemas ubicados en entornos industriales. A continuación, se enumeran algunos ejemplos:

- **Acceso directo a la red industrial:** es la más común pero también la más insegura, supone un acceso completo por parte del proveedor a la red industrial del cliente.

[23] https://blog.segu-info.com.ar/2020/03/teletrabajo-escritorio-remoto-vs-vpn-vs.html.

Para poder decir que la conexión es segura, se deberán implementar reglas punto a punto y el acceso externo deberá ser mediante VPN.

- **Uso de un equipo de salto:** mediante esta solución, si un usuario del entorno corporativo quiere acceder al entorno operacional, deberá acceder primero a un equipo de salto situado en la DMZ OT.
- **Solución específica de accesos remotos:** existen equipos y soluciones específicas que pueden proporcionar un acceso remoto seguro mediante el control de los puertos y aplicaciones que se van a utilizar de forma externa. El establecimiento de un túnel ya sea TLS o encapsulado mediante tráfico HTTPS son soluciones fiables para la conexión remota segura.

8.5. SIEM

Las soluciones SIEM son una solución híbrida entre SIM (*Security Information Management*) y SEM (*Security Event Manager*). Esta tecnología proporciona un análisis en tiempo real de alertas generadas, tanto por el *software*, como por el hardware de red.

El término SIEM recoge diferentes capacidades como pueden ser la recopilación de datos, el análisis y presentación de información de la red y de los diferentes dispositivos de seguridad que en ella se encuentran. Además, también es capaz de gestionar identidades y accesos, además de las vulnerabilidades.

A continuación, se resumen y completan las características de un SIEM descritas anteriormente:

- Identificar entre amenazas reales y falsos incidentes.
- Monitorizar de forma centralizada todas las amenazas potenciales.
- Redirigir la actuación a personal cualificado para su resolución.
- Aportar un mayor grado de conocimiento sobre los incidentes para facilitar su resolución.
- Documentar todo el proceso de detección, actuación y resolución.

Junto con los IDS, los SIEM pueden ayudar en el trabajo de monitorización de los equipos y de sus entornos exteriores, para poder detectar posibles amenazas incluso de forma temprana, y poder actuar en consecuencia.

9. Conclusiones

La **evolución de los sistemas industriales y su conexión con entornos corporativos e Internet ha dado paso a nuevos ciberataques**, que inicialmente no eran posibles o exigían una mayor dificultad debido a que se encontraban en entornos aislados. Esto, sumado a la antigüedad de muchos de los dispositivos, genera un riesgo en los sistemas industriales, que poseen vulnerabilidades explotables desde hace años.

Como medida de mitigación para evitar la explotación de estas vulnerabilidades será necesario el uso de soluciones para protección de los equipos, y entre ellos los equipos finales o e*ndpoints*.

Como resumen de las soluciones de protección para *endpoints* en sistemas industriales podemos decir:

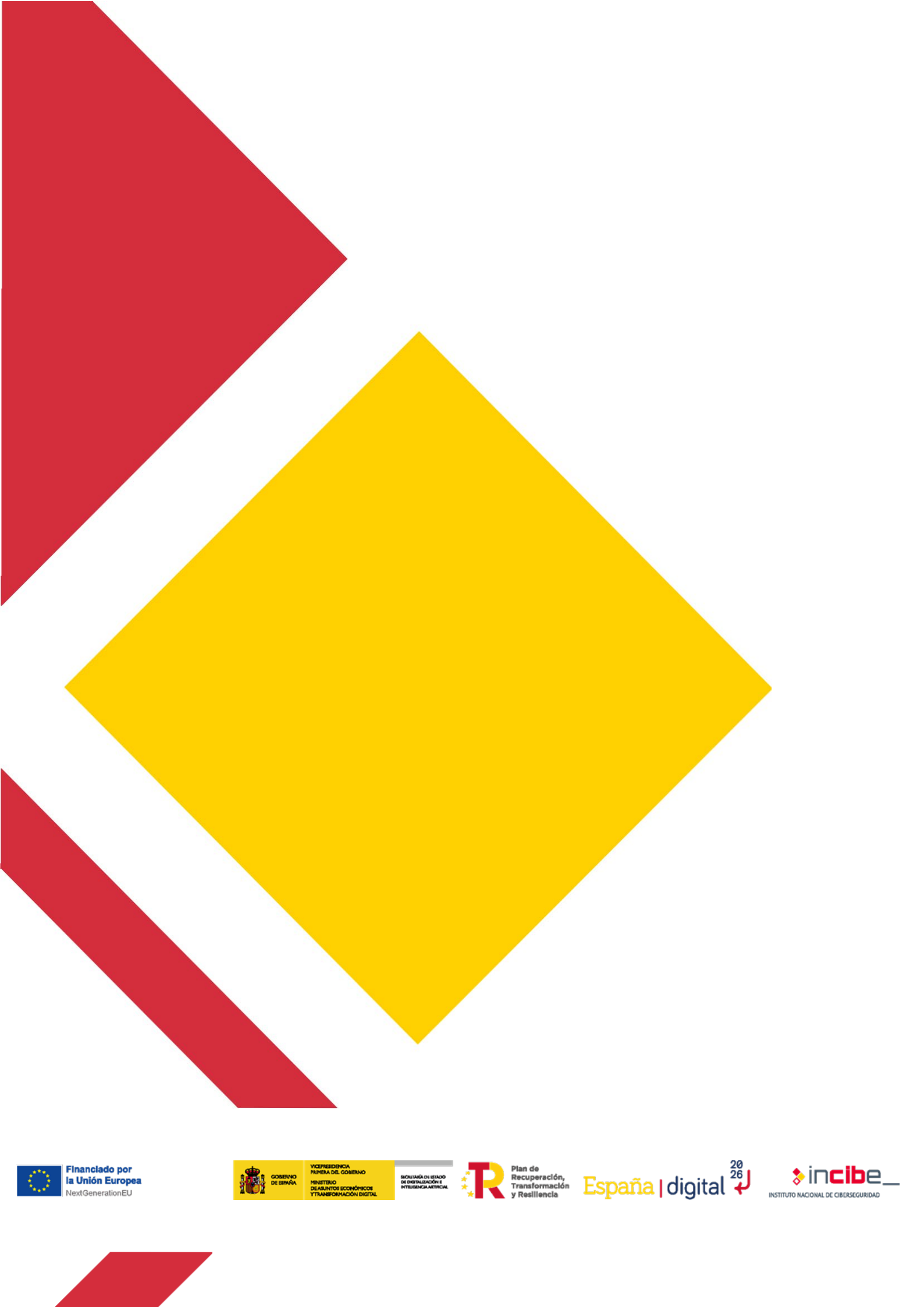
- Se puede realizar una aproximación del concepto de **defensa en profundidad** para securizar los *endpoint.*
- Los equipos pertenecientes a un sistema industrial poseen limitaciones que los hace particulares a la hora de protegerlos.
- El despliegue de **EDR** y la aplicación de **bastionado** en los equipos, permite añadir una **capa extra de seguridad** para evitar acciones maliciosas en los sistemas industriales.
- No debe dejarse de lado la **protección de los *endpoint* desde el exterior.**

10. Glosario de acrónimos

- **IoT**: Internet of Things
- **IIoT**: Industrial Internet of Things
- **IT**: Information Technologies
- **OT**: Operation Technologies
- **PLC**: Controlador Lógico Programable
- **SCADA**: Sistema de control de Supervisión y Adquisición de Datos
- **SIS**: Sistema Instrumentado de Seguridad
- **RTU**: Unidad Terminal Remota
- **IED**: Dispositivo Electrónico Inteligente
- **HMI**: Interfaz Hombre-Máquina
- **SCI**: Sistemas de Control Industrial
- **ISP**: Proveedor de Internet
- **VPN**: Virtual Private Network
- **XSS**: Cross Site Scripting
- **SQL**: Lenguaje de Consulta Estructurada
- **HIDS**: Host-based Intrusion Detection System.
- **IDS**: Intrusion Detection System
- **IPS**: Intrusion Prevention System
- **SIEM**: Security Information and Event Manager

11. Referencias

Referencia	Título, autor, fecha y enlace web
[Ref.- 1]	"Good Practices for Security of Internet of Things in the context of Smart Manufacturing" noviembre 2018 URL: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot
[Ref.- 2]	"Challenges and recommendations for the Industry Cyberdefense" URL: https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations
[Ref.- 3]	"Protége tu empresa: Que son y para qué sirven los IDS, IPS y los SIEM" URL: https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips
[Ref.- 4]	"Malware InfoTech Product Scorecard" URL: https://resources.malwarebytes.com/files/2020/04/Malwa-rebytes-InfoTech-Product-Scorecard-Report-March-2020.pdf



Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

España | digital 2026

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD