POSITION PAPER

¿QUÉ ES LA **CIBERSEGURIDAD INDUSTRIAL**?

MAYO DE 2023

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

aniversario 50 1973 - 2023

¿Qué es la ciberseguridad industrial?

La ciberseguridad industrial ha adquirido gran relevancia en los últimos años debido a la creciente dependencia de la tecnología dentro del concepto de Industria 4.0 o cuarta revolución industrial. Si bien son innegables los beneficios de esta transformación digital, como la mejora de la eficiencia y la productividad, también aumenta la exposición a posibles ciberataques y compromisos de la seguridad de la información. Por lo tanto, es crucial que las empresas adopten medidas de ciberseguridad adecuadas para proteger sus sistemas y datos sensibles.

En este contexto, se define la ciberseguridad industrial como la protección de la información, la infraestructura y los procesos industriales que pueden ser susceptibles de ciberataques. Se trata de prevenir las interferencias (intencionales o no) con la operación correcta de los sistemas de automatización y control industriales, que gestionan servicios esenciales como la electricidad, el agua, el transporte o las comunicaciones.

La ciberseguridad industrial es esencial para garantizar la protección de las redes de control operacional, y se basa en principios básicos de gestión de la seguridad de sistemas de información. Para asegurar la seguridad de un sistema, es necesario considerar tres aspectos clave:

- ✓ Confidencialidad: protección del acceso a los datos, de modo que sólo aquellas personas o entidades autorizadas deben tener acceso a la información y que se debe evitar que terceros no autorizados accedan o conozcan la información.
- ✓ Integridad: protección de los datos y sistemas contra cualquier tipo de alteración o modificación no autorizada.
- ✓ Disponibilidad: capacidad de los usuarios autorizados para acceder a los datos y sistemas de manera adecuada y consistente. Esto incluye la interrupción intencional o accidental del funcionamiento de los sistemas.

En general, la disponibilidad es el principio particularmente relevante en lo que respecta a la ciberseguridad industrial. Por ejemplo, la interrupción de la producción en una fábrica puede tener graves consecuencias económicas para la organización y también para todas las empresas del ecosistema al que pertenece.

Ataques más conocidos en el sector industrial

En los últimos años, se han producido numerosos ciberataques de gran importancia que han afectado a sistemas industriales. Uno de los primeros casos fue el malware Stuxnet en el año 2010, diseñado específicamente para atacar a sistemas de control industrial (ICS), incluyendo instalaciones nucleares y otras infraestructuras críticas. Stuxnet se propagaba a través de dispositivos extraíbles, como USB, y explotaba vulnerabilidades en el sistema operativo Microsoft Windows y en el software Siemens Step7. Una vez infectado un sistema, identificaba sistemas de control industrial específicos y los reprogramaba para realizar ciertas acciones, como acelerar o ralentizar la rotación de las centrifugadoras en una instalación nuclear con el objetivo de dañarlas.

Adicionalmente, se detectó el malware Triton en el año 2017, dirigido específicamente a sistemas de control industrial (ICS) utilizados en la industria del petróleo y el gas, con la

capacidad de interrumpir el funcionamiento de los sistemas de protección, lo que podría conllevar a daños físicos o incluso a la pérdida de vidas humanas.

Estos ataques fueron diseñados para afectar específicamente a sistemas de control industrial, aunque ataques más genéricos dirigidos a infraestructuras IT pueden también perjudicar instalaciones industriales de forma colateral. Uno de los casos más relevantes es un ataque de ransomware a Colonial Pipeline en mayo de 2021, que tuvo un impacto significativo en el suministro de gasolina y diésel en la costa este de Estados Unidos. Finalmente, Colonial se vio obligado a pagar el rescate por un total de 4,4 millones de dólares en Bitcoin.

Gestión de la seguridad y riesgos

La gestión de la seguridad de la información se basa en su mayor parte en la adecuada gestión de los riesgos, y se realiza mediante un proceso de mejora continua con una identificación inicial de activos y su importancia, y un análisis de vulnerabilidades y amenazas a las que están expuestos. Con esta información, se realiza un análisis de riesgo para una priorización basada en su impacto y probabilidad de ocurrencia. Aquellos riesgos que la organización considera no asumibles se deben tratar para reducir su impacto o probabilidad de ocurrencia. Para tratar dichos riesgos, se deberán incluir nuevos mecanismos o controles de seguridad y mejorar los existentes, de forma que el riesgo baje a un nivel aceptable.

La ciberseguridad industrial presenta unos riesgos característicos, que se presentan a continuación.

❑ Convivencia entre dispositivos modernos y antiguos

Como ya se ha mencionado anteriormente, la disponibilidad es un aspecto muy relevante, por lo que se intenta evitar cualquier parada de los dispositivos, incluidas las paradas por actualizaciones. Generalmente, se realiza una parada general de forma semestral o anual para realizar el mantenimiento de todos los dispositivos y la instalación de actualizaciones, por lo que se pueden llegar a acumular distintas vulnerabilidades.

Adicionalmente, dada la larga vida de los dispositivos industriales, habrá casos en los que no se realizarán actualizaciones para corregir las vulnerabilidades existentes. Por ello, aparecen también riesgos debidos a la convivencia de dispositivos antiguos y modernos. Dado que será necesaria una comunicación entre ambos y en algunos casos los dispositivos más antiguos no tendrán los protocolos de comunicación más actualizados, los dispositivos modernos tendrán que usar protocolos de comunicación antiguos, que pueden incrementar la falta de seguridad.

❑ Conexiones remotas

Otra de las malas prácticas habituales es la de facilitar conexiones remotas sin control. Cuando surge un problema en un dispositivo, la prioridad máxima es recuperar el sistema. El tiempo de desplazamiento y arreglo de un experto puede suponer un periodo de tiempo en el que no se garantiza la disponibilidad. Por ello, se suele incorporar un equipo con algún tipo de conexión remota para que el experto pueda acceder rápidamente cuando ocurre un problema. Aunque la recuperación del incidente es mucho más rápida, la seguridad de las conexiones remotas no está siempre garantizada, ya que no existe un control correcto de la misma.

- Ecosistema

Este riesgo está relacionado con un ciberataque o una brecha de seguridad a través de un proveedor directo o cualquier otra empresa del ecosistema industrial. En los últimos años se ha visto un incremento en este tipo de ataques, siendo el caso de la herramienta de gestión de red Solarwinds en 2020 uno de los más representativos, cuando un grupo ruso fue capaz de infiltrar *malware* en la herramienta y utilizarlo para acceder a los sistemas de las empresas y gobiernos afectados.

- Intervención de las personas

Mientras que los servidores y otros dispositivos críticos permanecen aislados en un Centro de Procesado de Datos (CPD) o habitaciones especiales en un entorno IT, los dispositivos en la industria están en el lugar de trabajo. Aunque están diseñados para soportar distintas temperaturas y humedades, son propensos a posibles accidentes como roturas de algún cable o golpes.

Guías para la gestión de la ciberseguridad industrial

La utilización de guías y normas basadas en las mejores prácticas permitirá mejorar la gestión de la ciberseguridad industrial y mitigar los riesgos presentados anteriormente. Algunas de ellas utilizadas ampliamente en el sector TIC, como la ISO/IEC 27000[1] o el NIST Cybersecurity Framework[2], pueden ser de gran utilidad, aunque se recomienda utilizar aquellas diseñadas específicamente para proteger sistemas de control industrial, principalmente la norma ISA/IEC 62443[3] y la guía NIST SP 800-82[4].

Guía NIST SP-800-82

La Guía *NIST SP 800-82 Guía de diseño y configuración de redes industriales* es un documento de orientación publicado por el Instituto Nacional de Normas y Tecnología (NIST) de los Estados Unidos. La guía proporciona recomendaciones y directrices para la implementación de redes industriales seguras, incluyendo la protección de sistemas de control de procesos y sistemas de automatización de la producción.

La guía cubre temas como la selección de componentes de red seguros, la configuración de *firewalls* y sistemas de detección de intrusiones, y la implementación de políticas y procedimientos de gestión de la seguridad.

Norma ISA/IEC 62443

La norma ISA/IEC 62443 es una norma internacional que establece los requisitos de seguridad para sistemas de control industrial (ICS). Esta norma se divide en cuatro partes (Figura *1*):

- ✓ Parte 1: Marco general para la gestión de seguridad cibernética de los sistemas de control industrial.
- ✓ Parte 2: Requisitos de seguridad para los componentes de los sistemas de control industrial, incluyendo hardware, software y firmware.

[1] https://www.iso.org/standard/73906.html

[2] https://www.nist.gov/cyberframework

[3] https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

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

- ✓ Parte 3: Requisitos de seguridad para la integración y configuración de los sistemas de control industrial.
- ✓ Parte 4: Requisitos de seguridad para la operación y mantenimiento de los sistemas de control industrial.

Figura 1 Estructura ISA/IEC 62443[5].

Este estándar contempla dos principios básicos que deben ser considerados en todas las actividades: defensa en profundidad y zonas y conductos.

❑ Defensa en profundidad

La defensa en profundidad se basa en la implementación de varias capas de protección para evitar la infiltración de amenazas en un sistema (Figura *2*). En el contexto de la ciberseguridad industrial, se utiliza para proteger los sistemas industriales y de control de procesos de ataques más críticos frente a intrusiones.

Incluye tanto medidas preventivas como medidas de respuesta ante posibles ataques. Mientras que las primeras incluyen la implementación de políticas de seguridad sólidas, la formación del personal en ciberseguridad, la implementación de *firewalls* y sistemas de detección de intrusiones, y la aplicación de parches de seguridad de forma preventiva, las segundas incluyen la creación de planes de respuesta a incidentes de ciberseguridad y la implementación de medidas de recuperación de desastres para minimizar los daños causados por un ataque.

[5] https://www.microchip.com/en-us/about/media-center/blog/2021/understanding-the-isa-iec-62443-standard-and-secure-elements-0

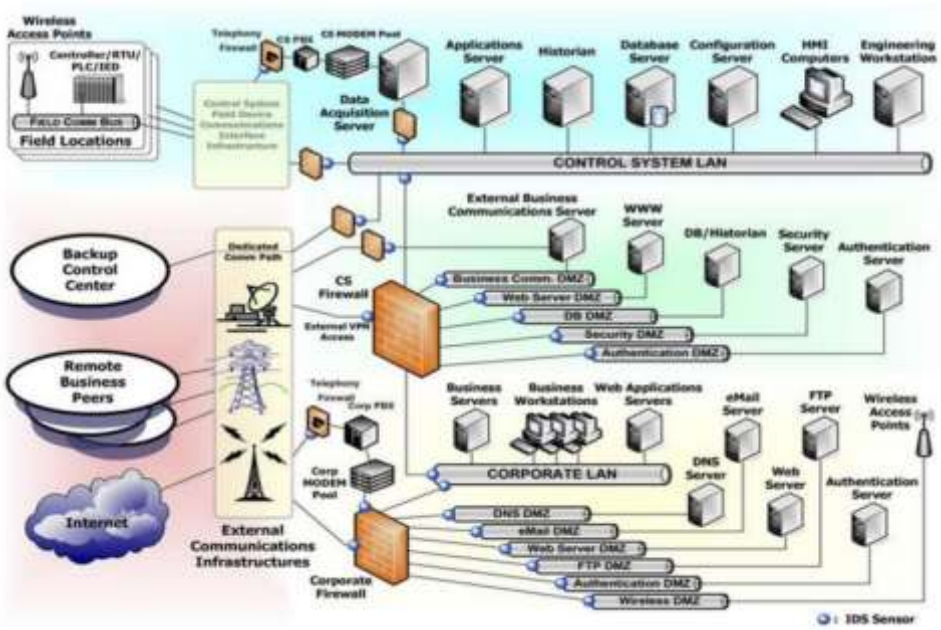

Figura 2 Defensa en profundidad[6].

❑ Zonas y conductos

El principio de zonas y conductos se basa en la segmentación de una red en diferentes áreas o "zonas" con diferentes niveles de acceso y protección. Cada zona está diseñada para proteger un conjunto específico de activos, y se utilizan "conductos" seguros para conectar las diferentes zonas entre sí de manera controlada.

El principio de zonas y conductos se utiliza para limitar el acceso a los activos críticos y reducir el riesgo de que una brecha de seguridad en una zona menos crítica se propague a otras zonas más críticas. Por ejemplo, se puede establecer una zona de alto nivel de protección para los sistemas de control de procesos críticos y una zona de bajo nivel de protección para los sistemas de oficina.

Igualmente, los componentes industriales con un ciclo de vida largo y con vulnerabilidades que no se puedan corregir, se podrán incluir en zonas aisladas, únicamente accesibles mediante determinados conductos controlados para mitigar el riesgo de que se exploten dichas vulnerabilidades.

Retos tecnológicos

Esta sección plantea algunos retos tecnológicos y sociales asociados a la implementación de la ciberseguridad en los entornos industriales. Ahora bien, no se puede olvidar que la mayoría de los ataques que consiguen su objetivo aprovechando errores humanos, la concienciación y formación de los trabajadores será fundamental para mejorar el nivel de prevención de las empresas.

❑ Adaptación de soluciones existentes

En la actualidad, la mayoría de las herramientas de monitorización de activos y redes existentes no explotan todo su potencial o incluso son incompatibles en los entornos industriales dado que

[6] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

se trata de entornos complejos, en los que se utiliza un mayor número de protocolos si se compara con las Tecnologías de la Información (IT). Adicionalmente, las empresas industriales pueden tener múltiples ubicaciones físicas y albergan activos críticos frecuentemente, por lo que las herramientas de detección de amenazas tradicionales no sean eficientes, e incluso que su uso sea contraproducente.

Aunque no es necesario inventar nuevas soluciones, las soluciones IT disponibles se deberán adaptar a los requerimientos únicos de las redes OT como sus largos periodo de mantenimiento o los recursos limitados en términos de CPU, memoria y espacio disponible. De esta forma, las nuevas soluciones permitirán gestionar los sistemas de control industriales como cualquier otro dispositivo IT desde el punto de vista de la ciberseguridad industrial.

- Prevalencia de sistemas heredados

Un reto fundamental para la ciberseguridad industrial es la prevalencia de los sistemas, ya que se espera que muchos sistemas industriales operen sin cambios significativos durante más de 15 años, en oposición a una media entre 3 y 5 años de los sistemas IT. En este caso, se deberá abordar la capacidad de analizar automáticamente el comportamiento y respuesta de esos sistemas para mejorar la efectividad de las medidas de protección y limitar el impacto de los ataques.

- Desarrollo de nuevos estándares

Para abordar la gran diversidad de protocolos industriales específicos, es necesario abordar la estandarización de diversos componentes entre diferentes sectores industriales para conseguir un conjunto común de requerimientos de ciberseguridad. A medida que se incorporan los requerimientos del estándar ANSI/ISA 62443-4-2 para eventos auditables, cada vez son más los productos industriales que incorporan estos formatos estándares.

- Falta de especialización industrial

La mayoría de los profesionales que trabajan en Centros de Operaciones de Seguridad (SOC) carecen de las herramientas y los conocimientos específicos del dominio industrial, más allá de las características propias de un entorno de Tecnologías de la Información.

Situación en España

Según el informe IBM Security X-Force[7], el sector industrial y manufacturero fue el sector que registró el mayor número de ciberataques en 2021 a nivel global. En España, también se han producido ataques de ransomware a empresas industriales que les han obligado a detener su operativa habitual. Uno de los casos más sonados fue el de la empresa Damm en noviembre de 2021, ya que tuvo que parar la producción de cerveza en su fábrica del Prat del Llobregat durante varias horas.

El inventariado de activos, la gestión de parches, la gestión de vulnerabilidades, las listas blancas de aplicaciones, el proceso de reducción de vulnerabilidades del sistema, la segmentación de las redes, el control de usuarios, el control de accesos remotos, etc., son herramientas muy valiosas y disponibles para cualquier empresa. Ahora bien, el principal reto de la ciberseguridad industrial no es la falta de tecnología disponible, sino la falta de capacidad por parte de la

[7] https://www.ibm.com/reports/threat-intelligence

mayoría de las empresas, PYMES principalmente, para gestionar esa tecnología y desplegar correctamente y mecanismos de protección en poco tiempo.