it

Formación y una estrategia definida, claves del éxito de la Ciberseguridad Industrial

gmv
INNOVATING SOLUTIONS

Formación y una estrategia definida, claves del éxito de la Ciberseguridad Industrial

Nos encontramos en un momento de transformación de una fabricación avanzada hacia procesos industriales inteligentes que se adaptan a los nuevos entornos digitales y plataformas conectadas. Las nuevas tecnologías asociadas a lo que se ha venido a denominar Industria 4.0 serán claves en el cambio del modelo productivo a un sistema que promueva el ahorro y la eficiencia energética, dos elementos de preocupación comunes a nivel global. En España, todavía hay mucho camino que recorrer para pasar de un modelo basado en un alto consumo y dependencia de los recursos, a otro que permita reducir la cantidad de energía necesaria para producir bienes y servicios. En este contexto, el mercado ya no solo demanda máquinas o componentes, sino soluciones innovadoras que incorporen más flexibilidad

y precisión, mayor eficiencia en la utilización de recursos a través de la economía circular y digitalización para prestar nuevos servicios avanzados y personalizados.

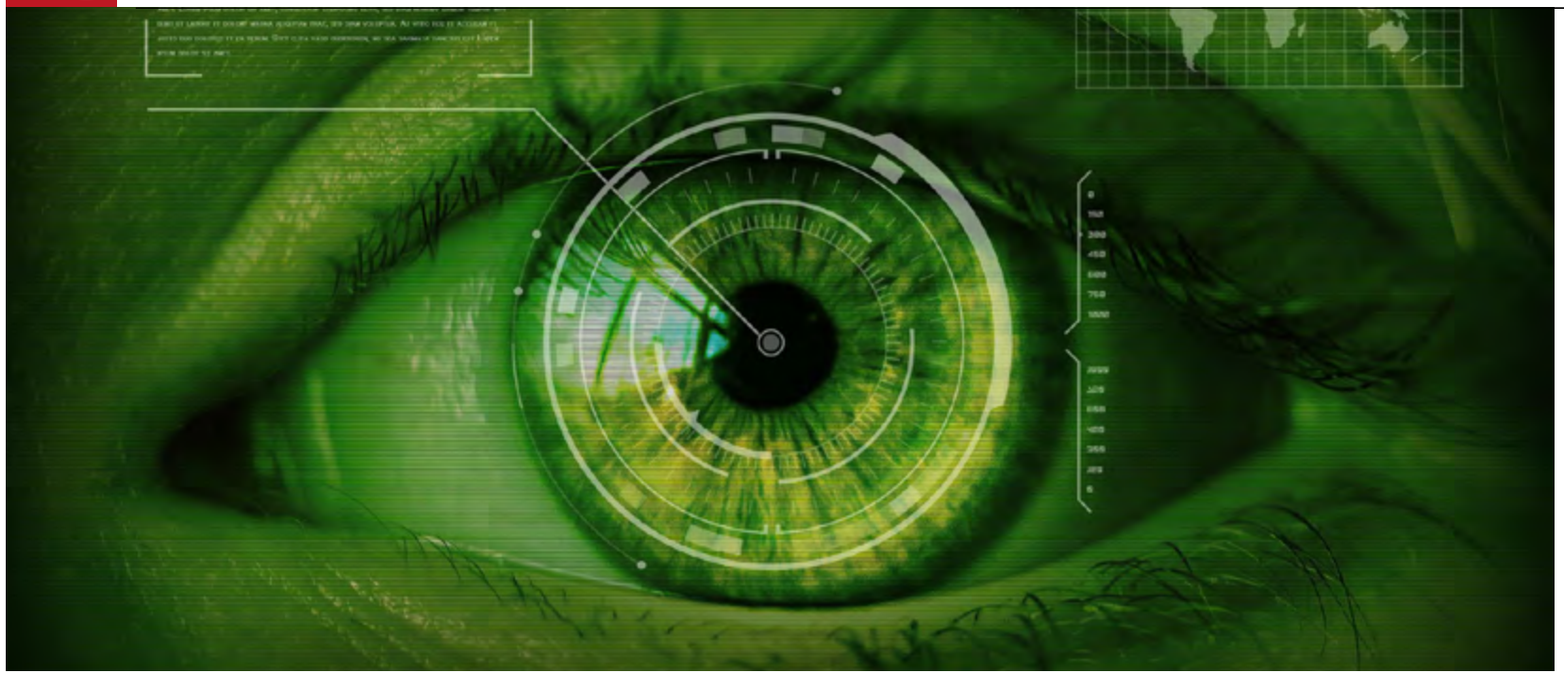
En definitiva, un entorno con un número creciente de procesos e instalaciones automatizadas y conectadas con el exterior que obliga a que nos replanteemos todo lo establecido en materia de seguridad. Así, la Ciberseguridad ha pasado a ocupar un lugar clave en el orden del día de estas empresas, con el objetivo de proteger los procesos tecnológicos de producción y los llamados sistemas ciber-físicos. Pero para poder avanzar en esta línea, se necesitan los conocimientos, las capacidades y las herramientas precisas, de ahí que sea fundamental contar con un aliado experto que les permita tener visibilidad de sus entornos convergentes y les ayude a definir la mejor arquitectura de Ciberseguridad para enfrentar estos retos.

RECOMENDACIONES DEL CENTRO DE CIBERSEGURIDAD INDUSTRIAL Y GMV PARA MEJORAR LA PROTECCIÓN DEL SECTOR INDUSTRIAL

EN QUÉ PUNTO ESTAMOS

En España falta mucho camino por recorrer, pero eso no quiere decir que no estemos progresando. Así, hay que partir de la base de que, como recuerdan desde el Centro de Ciberseguridad Industrial, también conocido por sus siglas CCI, algunos de los retos identificados en el mapa de ruta de la ciberseguridad industrial en España publicado en 2013 se han superados o están en un nivel de madurez avanzado, como, por ejemplo, elevar la concienciación general y proporcionar formación especializada según el nivel o tipo de usuario; el aumento de la investigación en Ciberseguridad Industrial; la creación de estrategias de Ciberseguridad para la industria; la creación de guías de buenas prácticas y estándares de referencia; la creación de laboratorios de prueba; la creación de concienciación dentro de los pilares de la seguridad industrial tradicional; o la difusión de productos y soluciones en materia de ciberseguridad industrial entre todos los actores implicados.

Tal y como explican desde este organismo, España es uno de los países del mundo con más sistemas que controlan todo tipo de instalaciones y procesos industriales, y todavía demasiados están conectados a Internet. Por ello, en el último lustro se ha invertido mucho trabajo y recursos en reducir las deficiencias de infraestructuras críticas en materia de ciberseguridad, y mejorarlas de forma continuada. Pero otras



> “Hay que incorporar a los nuevos proyectos de Industria 4.0 profesionales de ciberseguridad que puedan identificar los riesgos tecnológicos y establecer requisitos de ciberseguridad acordes con la regulación, los estándares y las necesidades del proyecto”
>
> JOSÉ VALIENTE, DIRECTOR Y RESPONSABLE DE COORDINACIÓN Y COMUNICACIÓN DEL CENTRO DE CIBERSEGURIDAD INDUSTRIAL (CCI)

infraestructuras industriales, que no están tan reguladas, de sectores como el químico, farmacéutico, alimentación o fabricación deben tener más en cuenta aspectos como el establecimiento de responsabilidades de Ciberseguridad en los diferentes niveles de la organización y en la cadena de suministro. Integrar la Ciberseguridad con la calidad o la seguridad operacional, pero sobre todo en materia de preparación para la gestión de incidentes y en la incorporación de requisitos de Ciberseguridad en los nuevos proyectos de automatización industrial.

¿CÓMO HACER FRENTE A ESTA REALIDAD?

Señalábamos la importancia de contar con un aliado con el conocimiento, las capacidades, la estrategia y las soluciones adecuadas para avanzar en este camino. Una figura con una posición única en este terreno es GMV, que cuenta con más de 30 años de experiencia ofreciendo soluciones y servicios de Ciberseguridad.

Según nos explica Javier Zubieta, Director de Marketing y Comunicación de Secure e-Solutions de GMV, “solemos ser prácticos en las recomendaciones a nuestros clientes industriales, porque muchos de ellos nos preguntan cómo pueden solucionar el problema de la Ciberseguridad cuando realmente lo que necesitan son respuestas con algo tangible”.

Asimismo, continúa, “siguiendo el sentido común, solemos hacer un diagnóstico de Ciberseguridad en el entorno industrial, que consiste primero en analizar la situación actual de Ciberseguridad desde el punto de vista de los riesgos, segundo en barajar distintas alternativas de solución y tercero exponer una hoja de ruta para poder mejorar la Ciberseguridad desde el punto de vista tanto técnico como de negocio. Y esto lo hacemos totalmente adaptados al mundo industrial, conociendo sus implicaciones propias y tratando por todos los medios que las recomendaciones calen en las personas y que puedan desarrollar su actividad de una forma natural y cibersegura. En muchos casos también acuden a GMV porque han sufrido un incidente. No es lo ideal, pero es la realidad. En ese sentido, GMV ofrece un

análisis forense del incidente y desarrolla un plan para que no se vuelva a producir".

FALTA DE PERSONAL CON LOS CONOCIMIENTOS Y CAPACIDADES ADECUADAS

Uno de los problemas a los que se enfrentan las empresas en este terreno es que no hay suficientes profesionales en Ciberseguridad, porque al ser un recurso valioso es escaso por definición. En este sentido, Javier Zubieta señala que "en GMV estamos convencidos de que todos los actores implicados en Ciberseguridad tenemos que hacer divulgación y capacitación, dado que cuantas más personas estén interesadas en este tema, más probabilidades habrá de que se dediquen a esto profesionalmente. En ese sentido, colaboramos con el CCI en sus actividades de divulgación y capacitación, que considero únicas en España y pioneras a nivel internacional".

FORMACIÓN EN CIBERSEGURIDAD

Para conocer más en detalle estas iniciativas del CCI, quisimos contar con las valoraciones de José Valiente, director y responsable de coordinación y comunicación del Centro de Ciberseguridad Industrial, que explica que "el año pasado el CCI creó una escuela profesional de Ciberseguridad Industrial para intentar capacitar a los profesionales del mundo TI y a profesionales que vienen del mundo industrial. Estamos mejorando la competencia técnica de todos los profesionales

¿Qué nos aporta un socio tecnológico como GMV?

La propuesta de GMV en lo referido a la Ciberseguridad Industrial se basa en servicios tales como:

❖ **Diagnósticos de ciberseguridad y de cumplimiento.** Elevación del nivel de ciberseguridad de los procesos, sistemas e instalaciones industriales e infraestructuras críticas, con la base en el ciclo de vida de los niveles de seguridad ISA-62443 (ISA-99). Los diagnósticos permiten tener una visión clara y tomar conciencia de la situación actual de ciberseguridad en los activos industriales. Estos diagnósticos se basan en estándares y buenas prácticas definidos por ISA, NIST, NERC, INCIBE, CCI… y su adaptación al sector industrial objeto del diagnóstico. Como resultado, se realizan análisis de intrusión, gestión de vulnerabilidades, Análisis GAP, definición de planes de mejora, bastionado de equipos…

❖ **Ciber-protección de redes IT/OT.** Dotar a las redes IT/OT de las capacidades necesarias para la identificación, protección, detección, respuesta y recuperación ante un ciber-incidente, minimizando así el impacto de las ciber-amenazas. Estos servicios incluyen el rediseño de redes, la implementación de soluciones de ciberseguridad en red, como diodos de datos o firewalls industriales, o la seguridad en la transferencia de datos entre dispositivos IIoT y la nube.

❖ **Protección específica de Centros de Control.** Se trata de un paquete de medidas de ciberseguridad orientadas a proteger el punto de conexión más crítico entre la red IT y la red OT: los Centros de Control. Implementación de FW/IDS en fronteras, aplicación de white-listing y bastionados de sistemas operativos de propósito general, creación de puestos duales seguros, monitorización y registro de actividad…

de la industria a través de publicaciones, capacitación, credenciales, guías basadas en estándares y conferencias. De hecho, las diversas publicaciones y herramientas que forman parte del material de la escuela han sido elaborados con las aportaciones y colaboración de profesionales y expertos del ecosistema".

"En 2019", continúa, "desde CCI estamos trabajando en dos plataformas muy relacionadas, una de ellas contendrá escenarios de incidentes de ciberseguridad industrial de alto impacto, así como recomendaciones para su gestión, lo que permitirá a las organizaciones estar mejor preparadas. Por otra parte, la segunda plataforma permitirá a las áreas de ingeniería disponer de un catálogo de requisitos de ciberseguridad adecuados para nuevos proyectos de automatización industrial facilitando la incorporación de estos requisitos en las peticiones de ofertas".

PASOS A DAR PARA UNA INDUSTRIA 4.0 SEGURA

Tal y como nos resumen nuestros dos interlocutores, "recomendaríamos incorporar a los nuevos proyectos de industria 4.0 profesionales de ciberseguridad que puedan identificar los riesgos tecnológicos y establecer requisitos de ciberseguridad acordes con la regulación, los estándares y las necesidades de disponibilidad, integridad y confidencialidad de cada uno de los componentes tecnológicos de estos proyectos".

De hecho, "no hay que transmitir un mensaje de miedo e incertidumbre, las empresas deben tener conciencia y adoptar una estrategia de Ciberseguridad. Es importante tener en cuenta que las amenazas están ahí, como en cualquier faceta de la vida, y no por ello debemos ni paralizar las iniciativas del negocio ni dejar la solución para más adelante, porque ya será demasiado tarde y caro. Por lo tanto, abordemos la Ciberseguridad desde el diseño y por defecto en todos los casos en los que sea posible".

Considerando que sistemas de control y sistemas instrumentados de seguridad han sido pirateados, plantas de producción de energía e instalaciones de proceso han sido paradas y las instalaciones dañadas físicamente, la amenaza es obviamente real pero existen medidas y profesionales para protegernos.

RETOS DE LA CIBERSEGURIDAD EN LA CONVERGENCIA ENTRE IT Y OT

La convergencia entre IT y OT, entre tecnología y operaciones, plantea una serie de retos. Los profesionales de Ciberseguridad deben acompañar y asesorar para la adopción de manera natural de tecnologías y plataformas dentro de las redes OT, que permitan asegurar estos procesos industriales, sin provocar pérdidas en la operación y sin afectar los flujos de la información. Esto, junto con permitir reducir el impacto y eliminar las barreras que se puedan generar por parte de las distintas áreas de la operación. Es necesario avanzar hacia la adopción de tecnologías que posibiliten aminorar la superficie de impacto frente a un ataque.

Por otro lado, es conveniente recordar que los beneficios de la coordinación, colaboración y comunicación entre IT y OT son múltiples, desde el incremento de la automatización y la visibilidad, pasando por un mayor rendimiento y una fuerza de trabajo más efectiva, hasta la mejora de la toma de decisiones estratégicas basadas en información más precisa y actual.

MÁS INFORMACIÓN

- Primer estudio de incidentes de Ciberseguridad Industrial en Servicios Esenciales de España
- Guía para la Construcción de un Centro de Operaciones y Respuesta de Ciberseguridad Industrial
- Ciberseguridad en Infraestructuras Críticas e Industria 4.0
- Requisitos del SGCI (Sistema de Gestión de la Ciberseguridad Industrial)
- Guía SGCI para la Construcción de un Sistema de Gestión de la Ciberseguridad Industrial

Prepara a tu organización industrial para incidentes de ciberseguridad de alto impacto

Un incidente es un evento imprevisto que causa daño interrumpiendo o alterando su servicio o función, en nuestro caso, sobre tecnologías de operación en el ámbito industrial.

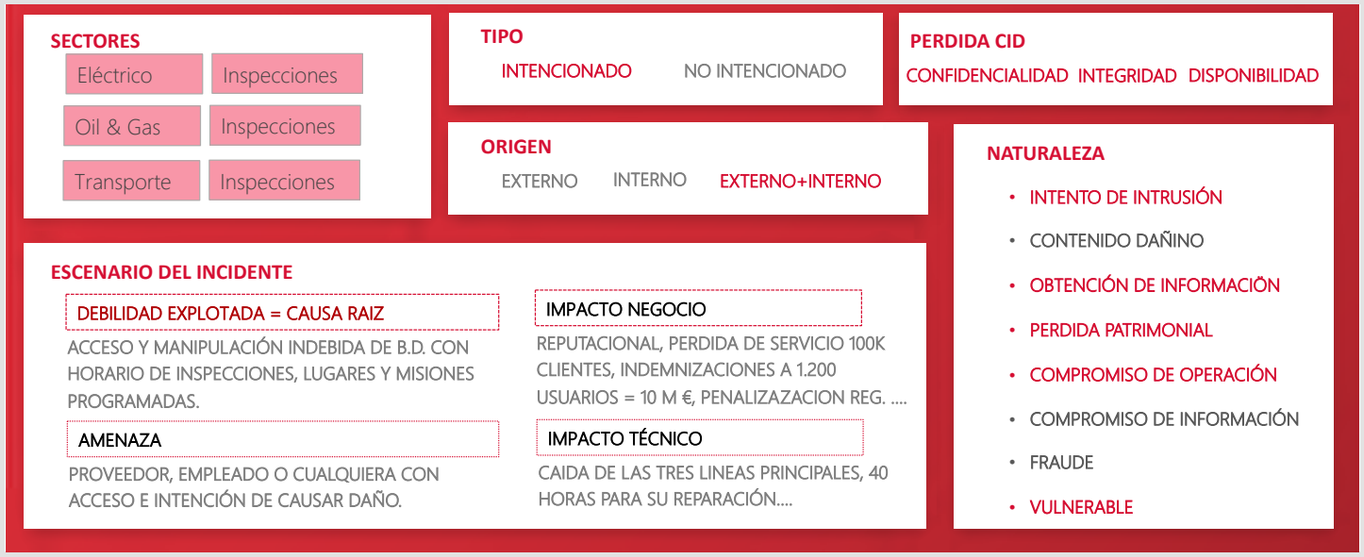
A modo de ilustración, imaginemos una organización que posee una fábrica en una ciudad del interior. El sistema de producción está centralizado y la provisión de materias primas se realiza por vía terrestre. Supongamos que, un día determinado, las materias primas no llegan a la planta, lo que conduce a la paralización de la producción. Este es un incidente que debe gestionarse con la máxima urgencia. Inmediatamente se descubre que, debido a un accidente de tráfico en la vía de uso habitual, no es posible el paso de vehículos que transportan las materias primas.

Conocido el problema y la causa raíz que ha originado el incidente, la solución puntual que se adoptó fue que los vehículos detenidos regresaran hasta el punto más próximo que les permitiera conmutar por una vía alternativa, aunque esta resultase más larga.

Esta solución al incidente no asegura que no suceda de nuevo, por ello una posible acción correctiva del problema sería ampliar la capacidad de almacenaje de la planta. De esta manera se podría seguir trabajando varios días ante la falta de suministro eventual. Pero si la causa raíz del incidente hubiera sido la alteración del sistema que realiza la petición de materias primas sustituyendo 1.000 unidades por solo 1, estaríamos ante un incidente tecnológico que hubiera tenido las mismas consecuencias sobre la producción, pero la acción correctiva en este caso consistiría en aplicar medidas de ciberseguridad, como fortalecer el control de acceso al sistema de pedidos, incorporar mecanismos de validación de las ordenes de pedidos...

Cuando se produce un incidente de ciberseguridad industrial son varias las cuestiones que debemos plantearnos. ¿Qué ha ocurrido? Parada de un proceso de producción, sobrecarga de una máquina o perdida de rendimiento, entre otras. ¿Dónde? En la planta de Albacete, en todas las plantas europeas. ¿Cómo? Se investigan alertas en sistemas, registros o información de actividad hasta encontrar la(s) causa(s).

Las organizaciones industriales están sufriendo incidentes tecnológicos a los que van poniendo remedio para no verse de nuevo afectadas, pero esto no es



Plataforma de escenarios de incidentes (CCI)

suficiente, las consecuencias de algunos incidentes tecnológicos, especialmente los intencionados, pueden ser de muy alto impacto, paralizando una o varias plantas durante días o semanas, comprometiendo sistemas de seguridad de las personas (safety) o provocando alteraciones que afecten gravemente a la calidad de la producción. Por ello, es fundamental que estas organizaciones se preparen frente a escenarios de incidentes de alto impacto.

Para facilitar la preparación de las organizaciones y sus proveedores industriales, el Centro de Ciberseguridad Industrial está construyendo una plataforma de escenarios de incidentes que permitirá conocer los incidentes de alto impacto que pueden afectar a un determinado sector y sus procesos automatizados.

Se describirá el escenario del incidente indicando su naturaleza y la causa raíz, así como el impacto técnico y el impacto para el negocio como puede observarse en la imagen.

Esta plataforma permitirá que las organizaciones puedan realizar ciberejercicios o revisar sus controles de ciberseguridad y anticiparse a incidentes de alto impacto sin tener que sufrir sus efectos. También proporcionará el ciclo de vida del incidente simplificado en cuatro fases, como puede observarse en la imagen.

Por último, facilitará las acciones de preparación, identificación, contención y recuperación necesarias para gestionar cada uno de estos incidentes. Prepararse adecuadamente ante los incidentes de ciberseguridad de alto impacto es hoy en día imprescindible para las organizaciones cuyo negocio depende de la salud de la automatización de sus procesos. ■

JOSÉ VALIENTE,
Director del Centro de Ciberseguridad Industrial

FASES DEL INCIDENTE

02 FEBRERO 2019 — **Paciente Cero**
Sabotaje desde el proveedor de mantenimiento sin restricciones en el acceso y sin registro de su actividad
Descarga de BD Misiones

Acceso Inicial
Acceso desde un equipo de ingeniería infectado que se ha conectado a la red de la B.D y a la app.
Acceso indebido desde proveedor de mantenimiento.

Persistencia
Se inhibio un control de seguridad para evitar ser detectados por sistemas de monitorización. Se utilizaron cuentas y tráficos poco sospechosos.

Efectos 05 MAYO 2019
Alteración BD Misiones
Modificación de las misiones de 5 lineas críticas que están programadas mismos días en una hora de intervalo para causar daño.

Ciclo de vida del incidente (CCI)

Prepararse adecuadamente ante los incidentes de ciberseguridad de alto impacto es hoy en día imprescindible para las organizaciones cuyo negocio dependen de la salud de la automatización de sus procesos