BURÓMC SEGURIDAD INFORMÁTICA

ELIT INFRASTRUCTURE SERVICES

Marzo 2025

NEWSLETTER BeIT

Edición Semanal #25

Protección de Infraestructuras

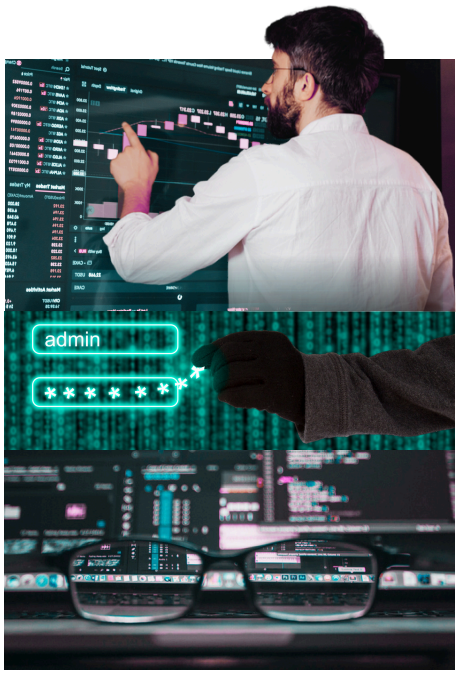
La protección de infraestructuras críticas es esencial para garantizar la estabilidad y seguridad de servicios vitales como la energía, el agua, las telecomunicaciones y el transporte. En la actualidad donde la digitalización se torna imprescindible, estas infraestructuras están cada vez más expuestas a ciberataques que pueden tener consecuencias devastadoras. La implementación de medidas de seguridad robustas y la colaboración entre sectores públicos y privados son fundamentales para mejorar la ciberresiliencia.

Leer ahora

Impacto de las filtraciones y la importancia de la Ciberseguridad

BLOG BeIT

Por: Elías Cedillo , *CEO Grupo BeIT y BuróMC*



En 2023, **Harvard Business Review** informó que las empresas que cotizan en bolsa sufrieron una caída promedio del 7,5 % en el valor de sus acciones tras una filtración de datos, junto con una pérdida promedio de capitalización bursátil de 5400 millones de dólares. Y las empresas tardaron un promedio de 46 días en recuperar el valor de sus acciones al nivel previo a la filtración.

Sin exagerar y siendo realistas ante las filtraciones, **IBM** en su reporte ¨Informe Cost of a Data Breach 2024¨ detallo que en 2023 el costo de una vulnerabilidad estuvo en 4.45 millones de dólares.

En 2024, este costo aumentó a 4.88 millones de dólares a nivel global, y para 2025 se proyecta que el costo incremente debido al uso de nueva tecnología como inteligencia artificial. Esto demuestra que las acciones hacia la protección deben ser más que preventivas; la implementación de soluciones de protección de ciberseguridad e infraestructura robustas es inminente.

Ser víctima de un ciberataque no solo causa un daño financiero significativo, sino que también afecta la reputación corporativa y genera desconfianza entre los clientes tras el robo o acceso no autorizado a la información. Esta combinación puede perjudicar gravemente a una empresa, incluso hasta el punto de llevarla al cierre de sus operaciones.

Si llevamos esto al interior de la empresa, específicamente en las líneas de producción con integración de inteligencia artificial, movimiento de cargas automatizadas, Centros de Distribución y almacenamiento (CEDIS), y robotización en las líneas de producción, ¿qué impacto puede tener?

El ejemplo más claro es el ransomware NotPetya, creado en Ucrania en 2017, que atacó a uno de los gigantes de alimentos y bebidas, Mondeléz International. Este ataque afectó a más de 24,000 laptops y 1,700 servidores, generando un paro no planeado debido a la imposibilidad de emitir órdenes de producción a la línea. El impacto financiero se reflejó en pérdidas superiores a los 100 millones de dólares

Siemens, en su informe "*The True Cost of Downtime 2024*" hace referencia que el tiempo de inactividad no planificado les cuesta a las 500 empresas más grandes del mundo el 11% de sus ingresos..

Pero no todo es motivo de pánico; también existen casos de éxito con la implementación de servicios como Field Services 2.0. Este modelo incluye la implementación de software de control, la consolidación de la línea base de TI, la homologación de políticas de seguridad, el control de accesos a la red mediante Zero Trust Network (ZTN) y respuestas automáticas a incidentes. Este ecosistema o modelo de servicio va más allá de lo tradicional, superando la simple utilización de un antivirus o contraseñas.

La importancia de un enfoque basado en compliance

Se ha escrito mucho sobre los impactos, riegos e implicaciones asociadas a temas de Ciberseguridad, pero pocas veces se establecen o definen las directrices relevantes que se refieren al cumplimiento normativo, regulatorio, sectorial, legal entre otras y solo por mencionar algunas, y sobre todo cuando se habla de sectores con infraestructuras críticas.

Compliance en BuroMC es un conjunto de procedimientos y buenas prácticas adoptados para identificar y clasificar los riesgos normativos, operativos, legales y regulatorios a los que se enfrentan y establecer mecanismos internos de prevención, gestión, control y reacción frente a los mismos

Dentro del marco normativo no han de considerarse únicamente las normas legales, como leyes y reglamentos, sino que también deberían incluirse en el mismo las políticas internas, los compromisos con clientes, proveedores o terceros y, especialmente, los códigos éticos que la empresa se haya comprometido a respetar, pues existen multitud de casos en los que una actuación puede ser legal pero no ética.

> *Ya la protección tradicional esta siendo sobrepasada por las nuevas tecnologías, los intereses maliciosos y financieros de los ciberdelincuentes.*

Las redes industriales son fundamentales para sectores críticos como el petróleo, gas, energía, manufactura, transporte, agua entre otros. Sin embargo, estas redes están expuestas a amenazas cibernéticas que requieren atención urgente. Esto debido a la amenazas que pueden comprometer de manera grave la seguridad informática industrial, interrumpiendo operaciones y provocando pérdidas económicas significativas.

La seguridad en las industrias de los diversos sectores no es solo un requisito regulatorio, es un compromiso ético y una responsabilidad requerida. Las herramientas tecnológicas han demostrado ser aliados indispensables para prevenir incidentes, ya que permiten una supervisión constante de las operaciones y una respuesta proactiva ante cualquier riesgo.

La ciberseguridad ha sido durante mucho tiempo un tema central en distintos sectores, ahora se considera la principal preocupación de las empresas. Ahora mantener una infraestructura de TI segura es una tarea difícil y cada vez es más compleja y muchas veces con costos elevados. Pero las filtraciones de datos y ciberataques son noticia casi a diario y, por lo general, la responsabilidad recae en el CIO.

Schneider, 'Minimizar el riesgo cibernético' (2025)
Schneider, 'La Seguridad Industrial: Más Allá del Cumplimiento' (2025)

Gartner define la seguridad de OT como "las prácticas y tecnologías utilizadas para proteger a las personas, activos e información; monitorear o controlar dispositivos físicos, procesos y eventos; e iniciar cambios de estado en los sistemas de OT empresariales". Las soluciones de seguridad de OT abarcan una amplia gama de tecnologías, desde firewalls de próxima generación (NGFW) hasta sistemas de gestión de eventos e información de seguridad (SIEM), así como herramientas de acceso y administración de identidad, entre otras.

Una infraestructura con tecnologías operativas (OT) incluye varios componentes esenciales que permiten la supervisión y control de procesos industriales, así como la asignación de mantenimientos preventivos y la monitorización en tiempo real de los equipos. Entre sus componentes se encuentran los sistemas de control industrial, dispositivos de campo (sensores, actuadores y PLC), redes de comunicación y software de gestión.

En Julio 2024, **Kaspersky LATAM** reportó que los ciberataques fueron dirigidos a infraestructuras críticas, siendo 27% (petróleo, gas y energía), 18% (logística y transporte), 15% (manufactura).

Otro dato interesante que nos brinda **Kaspersky LATAM** ahora en 2025, es , que el 18% de los altos directivos en América Latina admite no entender los términos que usan sus propios equipos de seguridad informática. ¿Las consecuencias? Un 55% ha sufrido ciberincidentes, incluyendo filtraciones de datos, debido a esta brecha de comprensión y comunicación.

Esta información da cabida a la falta de resiliencia a la ciberseguridad, donde el eslabón más débil siempre ha sido el humano.

Ahora que entendemos, que es la seguridad OT, cuales son las estadísticas en los sectores ante ciberataques y cómo la poca resiliencia a la ciberseguridad pueden ser los ingredientes perfectos para crear un efecto de caos e incertidumbre ante una vulnerabilidad.

Pero no todo es datos que ayuden a generar conciencia, sino también poder mostrar a nuestros clientes y lectores, cómo junto a nuestro partners, podemos brindamos soluciones que ayuden a prevenir y mitigar estas vulnerabilidades. Y así estar un paso adelante ante los ciberdelincuente, que en 2024 generaron perdidas de **4.88 millones de dólares** a nivel mundial y en México superaronn los **8.000 millones de dolares.**

Empresas, cómo Schneider Electric, buscan brindar una seguridad industrial más allá del mero cumplimiento de normativas, adoptando un enfoque proactivo, utilizando tecnologías y soluciones avanzadas.

Schneider Electric en su artículo ¨*Minimizar el riesgo cibernético y hacerlo de forma simplificada, 2025* ¨ indica que al menos el 60 % de los dispositivos en las empresas se encuentran desactualizados y el 78 % de ellos presentan vulnerabilidades conocidas que los hackers maliciosos podrían explotar.

Ahora, imaginen esto en una línea de producción, una estación de extracción de petróleo, gas, en una empresa de suministro de energía. Donde el uso de tecnologías de sistemas de control y automatización industrial son implementadas como *PLC, PC industrial , RTUs, HMI, DCS y SCADA* que pueden verse afectadas.

Schneider Electric se destaca en la protección de infraestructuras críticas mediante una serie de soluciones avanzadas que abarcan desde PLCs hasta sistemas SCADA. Los PLCs Modicon, por ejemplo, están diseñados con características de seguridad avanzadas que pueden incluir la detección de anomalías y la protección contra accesos no autorizados, asegurando la integridad y disponibilidad de los procesos industriales. Los PC industriales de Schneider Electric, equipados con sistemas operativos seguros y herramientas de monitoreo, permiten una rápida detección y respuesta a amenazas cibernéticas, manteniendo los sistemas críticos operativos y protegidos.

Además, las RTUs SCADAPack combinan capacidades de monitoreo y comunicación con la potencia de procesamiento de un PLC, ofreciendo una solución robusta para la supervisión y control remoto de infraestructuras críticas. Las soluciones HMI, como EcoStruxure Operator Terminal Expert, proporcionan una visualización segura y eficiente de los datos operativos, con funciones de autenticación y autorización que protegen el acceso a información sensible. Los sistemas DCS, como EcoStruxure Foxboro DCS, integran medidas de seguridad avanzadas como la segmentación de redes y la encriptación de datos, mientras que el software SCADA, como EcoStruxure Geo SCADA Expert, ofreciendo una plataforma segura y escalable para la gestión de activos remotos, permitiendo una gestión proactiva de la seguridad y el rendimiento de las infraestructuras críticas. Con estas tecnologías, Schneider Electric ayuda a las organizaciones a enfrentar los desafíos de seguridad cibernética y garantizando continuidad de sus operaciones.

EVENTOS BeIT

ELIT
INFRASTRUCTURE
SERVICES

Durante el mes de marzo, nuestro equipo de Elit Infrastructure Services tuvo la gran oportunidad de recibir capacitaciones por parte de Schneider Electric México. Estas sesiones fueron fundamentales para profundizar en las Soluciones para Centros de Datos, donde expandieron sus conocimientos sobre las últimas innovaciones en infraestructura y gestión de energía. La capacitación les permitió entender cómo optimizar de mejor manera el rendimiento y la eficiencia de los centros de datos, asegurando una operación continua y segura.

Schneider Electric

Además, exploramos el software y los servicios para Edge Computing, una tecnología clave para mejorar la conectividad y el procesamiento de datos en tiempo real. Estas capacitaciones no solo ampliaron el conocimiento de nuestro equipo de Elite Infrastructure Services de manera técnica, sino que también nos equiparon con las habilidades necesarias para implementar soluciones de vanguardia en nuestros proyectos futuros.

ELIT
INFRASTRUCTURE
SERVICES

Durante el mes de marzo, nuestro equipo de Elit Infrastructure Services tuvo la gran oportunidad de recibir capacitaciones por parte de Schneider Electric México. Estas sesiones fueron fundamentales para profundizar en las Soluciones para Centros de Datos, donde expandieron sus conocimientos sobre las últimas innovaciones en infraestructura y gestión de energía. La capacitación les permitió entender cómo optimizar de mejor manera el rendimiento y la eficiencia de los centros de datos, asegurando una operación continua y segura.

Schneider Electric

Además, exploramos el software y los servicios para Edge Computing, una tecnología clave para mejorar la conectividad y el procesamiento de datos en tiempo real. Estas capacitaciones no solo ampliaron el conocimiento de nuestro equipo de Elite Infrastructure Services de manera técnica, sino que también nos equiparon con las habilidades necesarias para implementar soluciones de vanguardia en nuestros proyectos futuros.

Infraestructuras de Energía

Cableado Estructurado

Panduit es una empresa líder en soluciones de infraestructura de red y cableado eléctrico industrial. Se especializa en el desarrollo de productos y soluciones que facilitan la transformación digital y mejoran la eficiencia operativa. Entre sus ofertas destacan los sistemas de mapeo de redes, que automatizan la documentación de cables, y los sistemas de cableado de fibra Base-8 y Base-16, que preparan los centros de datos para el futuro.

Panduit también se enfoca en la sostenibilidad y la seguridad, con productos como el Sistema de energía gestionada por fallos (FMPS), que cumple con los nuevos estándares UL para una entrega de energía más segura y confiable. Además, colabora con empresas como Cisco para impulsar la sostenibilidad en los centros de datos mediante la integración de unidades de distribución de energía inteligentes (iPDUs).