Grupo BeIT

NEWSLETTER

Blog CEO

Tecnologías de la operación deben ir alineadas a marcos internacionales de ciberseguridad

Noticia BeIT

El Gran Premio de Bélgica 2025 estuvo bajo amenaza digital, cibercriminales apuntaron a fanáticos y equipos de Fórmula 1

Edición 43

Respuestas a incidentes de Ciberseguridad

Edición 43

ELIT INFRASTRUCTURE SERVICES

BURÖMC SEGURIDAD INFORMÁTICA

En un entorno empresarial cada vez más competitivo y tecnológicamente exigente, GrupoBeIT, junto a BuróMC Seguridad Informática y Elit Infrastructure Services, se ha consolidado como un aliado estratégico para las organizaciones que buscan transformar sus operaciones, fortalecer su infraestructura y avanzar con seguridad hacia la digitalización.

Nuestro enfoque como área comercial está centrado en entender los desafíos, metas y objetivos que tienen nuestros clientes dentro de cada una de las industrias en las que se desenvuelve, y así brindar servicios y soluciones tecnológicas que no solo resuelven necesidades inmediatas, sino que también impulsan el crecimiento sostenible de nuestros clientes. A través de una oferta integral que combina innovación, especialización y cercanía operativa, acompañamos a las empresas mexicanas en su evolución digital sin comprometer su continuidad ni su eficiencia.

La clave de nuestro éxito radica en la capacidad de integrar tecnologías de vanguardia con una visión estratégica clara. Gracias a nuestras alianzas con fabricantes y partners líderes en ciberseguridad IT y OT, infraestructura crítica, energía y enfriamiento, ofrecemos un portafolio robusto, flexible y alineado con los objetivos de negocio de cada cliente. Esta sinergia nos ha permitido diseñar soluciones que se adaptan naturalmente a los procesos existentes, optimizando recursos y maximizando el retorno de inversión, como lo son SmartBits y Field Services 2.0.

Más allá de la tecnología, como GrupoBeIT entendemos que cada decisión es un compromiso adquirido, entregando valor desde la atención del primer contacto hasta la ejecución del proyecto.

GrupoBeIT no solo provee soluciones y servicios; sino que también construye relaciones de largo plazo basadas en confianza, resultados y visión compartida.

GrupoBeIT
Gerente Comercial

Tecnologías de la operación deben ir alineadas a marcos internacionales de ciberseguridad

Por: Elías Cedillo , Fundador y *CEO GrupoBeIT*

Hablar de tecnologías de la operación actualmente, es hablar de mayor interconectividad y exposición a riesgos cibernéticos, la ciberseguridad ha dejado de ser una función técnica para convertirse en una responsabilidad estratégica de los directivos. Alineando las organizaciones con marcos internacionales como ISO/IEC 27001, ISA/IEC 62443, y construir un Sistema de Gestión de la Ciberseguridad Industrial (SGCI) es una decisión que impacta directamente en la continuidad del negocio, la resiliencia operativa y la reputación corporativa.

Según Gartner, las organizaciones que integran la ciberseguridad en sus decisiones de negocio logran acelerar el valor empresarial. PwC México destaca que más del 80% de las empresas planean aumentar su presupuesto en ciberseguridad, reconociendo su impacto financiero directo. El Banco Interamericano de Desarrollo advierte que los entornos OT (tecnologías de la operación) requieren una gestión de riesgos diferenciada, debido a su criticidad para la infraestructura física y la seguridad pública.

La complementariedad para entornos IT/OT con estándares ISO/IEC 27001 establece los requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI), aplicable a cualquier organización. Por su parte, la serie ISA/IEC 62443 aborda los desafíos específicos de los entornos OT, como plantas industriales, sistemas SCADA, y redes de control. Ambos marcos son complementarios: ISO/IEC 27001 proporciona la estructura de gestión, controles y mejora continua; mientras que ISA/IEC 62443 adapta esos controles al entorno OT, considerando restricciones de disponibilidad, seguridad física, y compatibilidad tecnológica. Integrar ambos permite una protección holística de la infraestructura digital y física, alineando la seguridad con los objetivos del negocio.

El modelo de gestión para la ciberseguridad industrial está bajo la Guía para la construcción de un SGCI, desarrollada por el Centro de Ciberseguridad Industrial (CCI), propone un modelo estructurado en seis dominios: estrategia, gestión de riesgos, cultura organizacional, normativas técnicas, resiliencia y mejora continua. Este enfoque permite a las organizaciones industriales anticiparse a los riesgos, reducir el impacto de incidentes y garantizar la sostenibilidad operativa.

El modelo de gestión para la ciberseguridad industrial está bajo la Guía para la construcción de un SGCI, desarrollada por el Centro de Ciberseguridad Industrial (CCI), propone un modelo estructurado en seis dominios: estrategia, gestión de riesgos, cultura organizacional, normativas técnicas, resiliencia y mejora continua. Este enfoque permite a las organizaciones industriales anticiparse a los riesgos, reducir el impacto de incidentes y garantizar la sostenibilidad operativa.

Alinear la empresa con marcos internacionales de ciberseguridad y adoptar un SGCI ofrece beneficios tangibles que trascienden el ámbito técnico. En primer lugar, permite reducir significativamente los riesgos operativos y financieros, al prevenir incidentes que podrían paralizar procesos críticos o generar sanciones regulatorias. Además, fortalece el cumplimiento normativo y contractual, lo que es clave en sectores regulados como energía, salud o transporte.

Otro beneficio relevante es la mejora de la reputación corporativa. Las organizaciones que demuestran una postura proactiva en ciberseguridad generan mayor confianza entre inversores, clientes y socios estratégicos. Asimismo, la implementación de un SGCI optimiza recursos al integrar procesos de seguridad con otros sistemas de gestión, como calidad, medio ambiente o seguridad laboral, generando sinergias operativas. Finalmente, este enfoque permite capacitar al talento interno en ciberseguridad industrial, desarrollando competencias clave para enfrentar los desafíos del entorno digital.

Para que estos beneficios se materialicen, el CEO debe asumir un rol activo y estratégico en la transformación digital segura. En primer lugar, es fundamental impulsar desde la alta dirección la adopción de marcos como ISO/IEC 27001 e ISA/IEC 62443, asegurando que la ciberseguridad esté integrada en la estrategia corporativa. En segundo lugar, se recomienda establecer un SGCI como sistema transversal, autónomo y compatible con otros sistemas de gestión, permitiendo una visión integral de los riesgos.

También es clave asignar roles y responsabilidades claras, incluyendo la creación de un Comité de Ciberseguridad y la designación de un Responsable del SGCI con autoridad y recursos. Promover una cultura de seguridad es otro pilar esencial: la formación continua, la concienciación del personal y la definición de normativas específicas son acciones que fortalecen la postura defensiva de la organización. Finalmente, el CEO debe asegurar la existencia de indicadores clave de desempeño, auditorías periódicas y mecanismos de mejora continua que permitan evaluar la eficacia del SGCI y adaptarlo a los cambios del entorno.

En conclusión, la ciberseguridad ya no es solo un asunto técnico. Es una decisión de liderazgo. Alinear la organización con marcos internacionales y construir un SGCI es una inversión estratégica que protege el presente y asegura el futuro. El CEO debe ser el impulsor de esta transformación, liderando con visión, compromiso y responsabilidad.

Referencia:

El Economista: Ciberseguridad como inversión clave para la continuidad del negocio
PwC México: La ciberseguridad desde la perspectiva del CFO
Banco Interamericano de Desarrollo: Gestión de riesgos cibernéticos en entornos OT
Normas y estándares de ciberseguridad: qué son y cómo elegir el adecuado
Guía para la construcción de un Sistema de Gestión de la Ciberseguridad Industrial – Centro de Ciberseguridad Industrial. [PDF]
LATAM CISO Report 2024: Lecciones de la primera línea. [PDF]
Applying ISO_IEC 27001-2 and the ISA_IEC 62443 Series.pdf [PDF]
Informe 2024 sobre el estado de la tecnología operativa y ciberseguridad. [PDF]

BURŌMC SEGURIDAD INFORMÁTICA

ELIT INFRASTRUCTURE SERVICES

Panorama Global

NOTICIA BeIT

El Gran Premio de Bélgica 2025 estuvo bajo amenaza digital, cibercriminales apuntaron a fanáticos y equipos de Fórmula 1

Durante el pasado Gran Premio de Bélgica, celebrado el 27 de julio en el circuito de Spa-Francorchamps, mientras se preparaban a que los motores sonaran, se registró una serie de ciberataques dirigidos tanto a fanáticos como a equipos participantes. Lo que debía ser una celebración del automovilismo se convirtió en una oportunidad para actores maliciosos que aprovecharon la atención global del evento para ejecutar campañas fraudulentas y ataques digitales.

Los primeros indicios del ataque se remontaron a marzo de 2024, cuando los ciberdelincuentes lograron comprometer el correo electrónico oficial del evento. Desde esa plataforma, enviaron mensajes falsos que simulaban comunicaciones legítimas, ofreciendo entradas con descuentos y accesos exclusivos. El objetivo principal fue obtener datos personales y financieros de los aficionados.

Los investigadores identificaron al menos 16 dominios sospechosos registrados entre 2024 y 2025. Estos sitios imitaban páginas oficiales de la Fórmula 1 y del circuito Spa-Francorchamps, y fueron utilizados para:

- Distribuir malware disfrazado de entradas digitales o aplicaciones de streaming.
- Capturar credenciales mediante formularios fraudulentos.
- Comercializar productos falsificados de escuderías como McLaren y Ferrari.

Además de los fanáticos, varios equipos de Fórmula 1 reportaron intentos de intrusión en sus redes internas. Escuderías como Red Bull, Ferrari y Mercedes detectaron actividades maliciosas orientadas al robo de datos técnicos, estrategias de carrera y diseños de vehículos. En algunos casos, se identificaron campañas de ransomware que amenazaban con divulgar información confidencial si no se pagaba un rescate.

Las plataformas sociales también jugaron un papel en la campaña maliciosa. Cuentas falsas ofrecieron sorteos de entradas VIP, mercancía oficial y experiencias en el paddock, solicitando a los usuarios compartir publicaciones o entregar información personal. Uno de los casos más notorios involucró una cuenta falsa en Instagram que simulaba ser del equipo McLaren.

Tras los incidentes, expertos en ciberseguridad recomendaron:

- Comprar entradas únicamente en sitios oficiales como formula1.com.
- Activar la autenticación en dos pasos en servicios relacionados.
- Evitar enlaces sospechosos en correos y redes sociales.
- Utilizar software antivirus actualizado y conexiones seguras para ver las carreras en línea.

Los equipos, por su parte, reforzaron la capacitación de sus empleados, segmentaron sus redes críticas y establecieron alianzas con firmas especializadas en respuesta a incidentes.

Referencia:
Cybersecuritynews

BURÓMC SEGURIDAD INFORMÁTICA
ELIT INFRASTRUCTURE SERVICES

Edición 43

NEWSLETTER BeIT

Respuestas a incidentes de Ciberseguridad

La creciente sofisticación de los ciberataques ha convertido la respuesta a incidentes de ciberseguridad en una prioridad estratégica para organizaciones de todos los tamaños. Desde ataques de ransomware hasta vulnerabilidades de día cero, las empresas deben estar preparadas para detectar, contener, erradicar y recuperarse de estos eventos con rapidez y eficacia. Los incidentes de ciberseguridad pueden adoptar múltiples formas, pero destacan especialmente el ransomware, que cifra los datos y exige un rescate para su liberación, los exploits de día cero que aprovechan vulnerabilidades desconocidas, y los ataques basados en identidad como el robo de credenciales, que permiten a los atacantes moverse lateralmente dentro de la red.

Una respuesta efectiva a incidentes de ciberseguridad se estructura en varias fases. La preparación implica establecer políticas, formar equipos, definir roles y realizar simulacros. La detección temprana es clave, utilizando herramientas como firewalls, sistemas de detección de intrusos y análisis de comportamiento para identificar anomalías. En el caso de exploits de día cero, se recomienda el uso de aislamiento de navegador y firewalls avanzados para minimizar el riesgo. Una vez identificado el incidente, se deben aislar los sistemas afectados para evitar la propagación, lo que incluye desconectar redes, bloquear accesos y activar protocolos de emergencia. La erradicación consiste en eliminar el malware, cerrar brechas de seguridad y aplicar parches, evitando la reintroducción de infecciones. La recuperación implica restaurar sistemas y datos desde copias de seguridad limpias, preferiblemente almacenadas de forma inmutable. Finalmente, se realiza un análisis para mejorar procesos, actualizar políticas y reforzar la formación.

La respuesta a incidentes requiere una colaboración multidisciplinaria. Los roles más relevantes incluyen al CEO, quien lidera la estrategia global y garantiza recursos para la ciberseguridad; al CISO, que diseña y ejecuta la estrategia de seguridad de la información, coordina el equipo de respuesta y promueve la concienciación; al CSO, responsable de la seguridad física y tecnológica; al CIO o CTO, que supervisan la infraestructura tecnológica y su alineación con la estrategia de seguridad; al DPD/DPO (Europa), que asegura el cumplimiento normativo en protección de datos; al equipo de respuesta a incidentes, que detecta, analiza y responde a los eventos de seguridad; y a los usuarios finales, quienes deben estar capacitados para identificar amenazas como el phishing y actuar conforme a las políticas.

Un CISO debe tener formación en sistemas, telecomunicaciones o matemáticas, complementada con una Maestría en Ciberseguridad y certificaciones como CISSP, Aunque la respuesta es vital, la prevención sigue siendo la mejor defensa. Para evitar el ransomware, se recomienda la actualización constante del software para cerrar vulnerabilidades conocidas, la implementación de autenticación multifactor para reducir el riesgo de accesos no autorizados, la seguridad del correo electrónico para filtrar correos maliciosos y educar a los usuarios, la protección de puntos finales con antimalware y control de aplicaciones, el uso de copias de seguridad aisladas para garantizar la recuperación sin depender del rescate, y la adopción del modelo Zero Trust, que asume que ninguna entidad es confiable por defecto y limita el movimiento lateral de los atacantes.

La respuesta a incidentes de ciberseguridad no es solo una cuestión técnica, sino estratégica. Requiere liderazgo, coordinación, tecnología y cultura organizacional. Las empresas que invierten en prevención, formación y simulacros están mejor posicionadas para enfrentar los desafíos del entorno digital actual, donde los ataques son constantes y sin una protección, son casi inevitable.

Referencia:

Veeam: Ransomware trends
Cloudflare: How to prevent ransomware
Cloudflare: Zero day exploit
Cloudflare: What is a supply chain attack
CrowdStrike

BURÓMC SEGURIDAD INFORMÁTICA

ELIT INFRASTRUCTURE SERVICES

CybrHawk Transforming Cybersecurity · netskope · vicarius · PARTNERS BeIT

FIELD SERVICES 2.0

Tenemos el gusto de invitarte a un evento exclusivo de **Field Services 2.0,** centrado en sus desafíos y oportunidades junto con ponentes de primer nivel de nuestros aliados estratégicos.

FS 2.0 es una transformación estratégica que redefine la eficiencia operativa, la experiencia del cliente y la gestión del riesgo. Invertir en soluciones avanzadas y priorizar la entrega de servicios centrados en el cliente, contribuye a que las organizaciones pueden capitalizar estas oportunidades y superar los desafíos para tener éxito.

Fecha: Jueves, 28 de agosto
Horario: 2 – 6 pm
Sede: *La Hacienda de los Morales* ubicada en Juan Vázquez de Mella 525, Polanco, Polanco I Secc, Miguel Hidalgo, 11510 Ciudad de México, CDMX

Esperamos contar con tu valiosa presencia.

Atentamente,

Elías Cedillo
CEO y Fundador de GrupoBeIT

Registro para asistencia presencial

Registro para asistencia vía Zoom

+52 56 5100 8613
admmarketing@buromc.com