NEWSLETTER

Edición número 40

Blog CEO

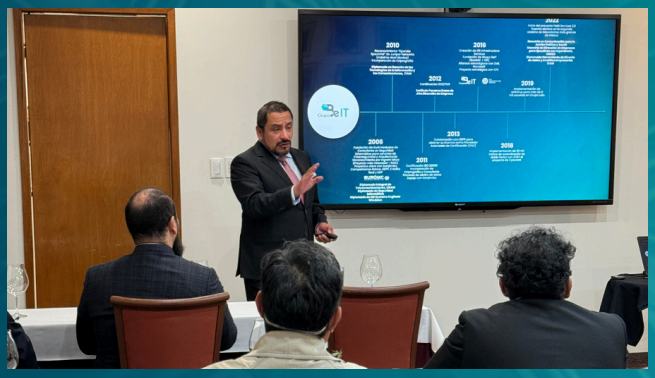
Redefiniendo el futuro empresarial con inteligencia, agilidad y precisión

Noticia BeIT

La nueva cara del cibercrimen a través de sitios wordpress

Edición 40°

En 2025 pasamos de un Sistema de Gestión de Seguridad de la Información a la construcción de un Sistema de Gestión de la Ciberseguridad Industrial



ELIT INFRASTRUCTURE SERVICES

BURÖMC SEGURIDAD INFORMÁTICA

www.grupobeit.com

Desde la Dirección Cuentas Estratégicas, celebramos el XIX aniversario de GrupoBeIT, consolidándose como un referente en innovación tecnológica, ciberseguridad y desarrollo empresarial en sectores industriales claves. Este aniversario refleja la evolución de una visión estratégica que ha sabido adaptarse con éxito a los desafíos del entorno y avanzar hacia un presente definido por la convergencia tecnológica.

Desde nuestro espacio, hemos tenido el privilegio de acompañar este crecimiento, aportando valor en proyectos estratégicos mediante el diseño y aplicación de estructuras contractuales sólidas —legales, administrativas y operativas— orientadas a prevenir riesgos, garantizar el cumplimiento normativo y fortalecer la seguridad de cada iniciativa. Esta labor ha sido esencial para asegurar operaciones eficientes, confiables y alineadas con los más altos estándares empresariales.

La implementación de estas estructuras contractuales desde el primer contacto con clientes y prospectos ha sido clave para comprender a fondo sus objetivos estratégicos y ofrecer soluciones precisas, adaptadas a sus necesidades. Esta disciplina ha permitido construir relaciones de confianza y sostenibles a lo largo de estos 19 años.

Nos enorgullece formar parte de esta historia junto a GrupoBeIT, BuróMC Seguridad Informática y Elit Infrastructure Services. Agradecemos profundamente la confianza depositada en nuestro equipo y renovamos nuestro compromiso de seguir siendo un aliado estratégico en la construcción de proyectos sólidos, sostenibles y de alto impacto.

Sergio Barranco
GrupoBeIT
Director Jurídico y
Cuentas Estratégicas

Redefiniendo el futuro empresarial con inteligencia, agilidad y precisión

Por: Elías Cedillo , Fundador y *CEO GrupoBeIT*

En un entorno donde la disrupción tecnológica se ha convertido en la norma, las organizaciones enfrentan el desafío junto a oportunidades de reinventarse. Este 2025 ha marcado un punto de inflexión: las empresas que logren integrar de forma estratégica la inteligencia artificial, los datos y la automatización no solo sobrevivirán, sino que liderarán la transformación de sus industrias.

La evolución tecnológica ya no se limita a la adopción de herramientas digitales. Hoy, las compañías deben rediseñar sus modelos operativos desde la raíz. La inteligencia artificial generativa (GenAI), por ejemplo, está revolucionando la forma en que se crean contenidos, se automatizan procesos complejos y se toman decisiones estratégicas. Esta tecnología no solo mejora la eficiencia, sino que también abre nuevas vías de generación de valor.

En paralelo, el Internet de las Cosas (IoT) se consolida como un pilar clave en la optimización de operaciones, tanto en entornos industriales como en aplicaciones domésticas. La capacidad de recopilar y analizar datos en tiempo
real permite una toma de decisiones más ágil y fundamentada, lo que se traduce en ventajas competitivas tangibles.

La infraestructura tecnológica que sustenta esta transformación (particularmente los semiconductores) cobra una relevancia estratégica sin precedentes. Estos componentes son esenciales para el funcionamiento de sistemas de IA, dispositivos conectados y plataformas digitales avanzadas. Su disponibilidad y evolución determinarán en gran medida la velocidad con la que las empresas puedan escalar sus innovaciones.

El panorama regulatorio y geopolítico añade una capa de complejidad que no puede ser ignorada. Las organizaciones deben navegar un entorno donde las normativas cambian rápidamente y los riesgos cibernéticos se intensifican. La anticipación y la resiliencia se convierten en competencias clave para mitigar amenazas y garantizar la continuidad operativa.

La reinvención del modelo de negocio no es una opción, sino una necesidad. Las empresas que logren integrar eficientemente la analítica de datos, la automatización de servicios y la optimización operativa estarán mejor posicionadas para capitalizar las oportunidades emergentes. Esto implica no solo reducir costos, sino también rediseñar la experiencia del cliente y acelerar la innovación.

El 2025 no es un año solo de ajustes, sino de transformaciones profundas. Las organizaciones que adopten una mentalidad de liderazgo proactivo, inviertan en capacidades tecnológicas clave y mantengan una visión clara, serán las que definan el rumbo del mercado. La tecnología, bien implementada, no es solo una herramienta: es el motor de una nueva era empresarial.

Referencia:

PwC

NOTICIA BeIT

Panorama Global

La nueva cara del cibercrimen a través de sitios wordpress

Una nueva campaña de ciberataques ha encendido las alarmas en la comunidad de seguridad informática. Investigadores han detectado una operación maliciosa que combina el uso del troyano de acceso remoto **NetSupport RAT** con una técnica de ingeniería social cada vez más popular: **ClickFix**. Esta combinación representa una amenaza sofisticada y altamente efectiva, especialmente porque se apoya en la manipulación psicológica del usuario más que en vulnerabilidades técnicas.

El ataque comienza con la explotación de sitios WordPress legítimos pero comprometidos. Estos portales, que aparentan ser seguros, contienen scripts maliciosos ocultos en sus metadatos. Cuando un usuario accede a uno de estos sitios, es redirigido a una página falsa que simula una verificación CAPTCHA o una solución técnica urgente.

Aquí entra en juego la técnica **ClickFix**, que ha ganado notoriedad desde su aparición en 2024. Esta táctica no requiere exploits ni malware inicial: simplemente convence al usuario de ejecutar manualmente un comando malicioso.

¿Qué es ClickFix y por qué es tan efectivo?

ClickFix es una forma de ataque basada exclusivamente en **ingeniería social.** El atacante presenta una interfaz convincente —como una alerta de error o una verificación de seguridad— que instruye al usuario a seguir una serie de pasos simples:

1. Hacer clic en un botón que supuestamente "soluciona" un problema.
2. Presionar Win + R para abrir la ventana de ejecución.
3. Pegar un comando previamente copiado al portapapeles.
4. Presionar Enter.

Este comando suele ser un script de PowerShell que descarga e instala NetSupport RAT, otorgando al atacante control remoto sobre el sistema.

Lo más alarmante es que, al ser el propio usuario quien ejecuta el código, muchas soluciones de seguridad no detectan la actividad como maliciosa. Además, los atacantes adaptan el mensaje según el contexto: desde problemas técnicos hasta verificaciones de identidad, todo con el objetivo de parecer legítimos.

NetSupport Manager es una herramienta legítima de administración remota, pero ha sido reutilizada por cibercriminales como **NetSupport RAT**. Una vez instalado, permite al atacante:

- Controlar el equipo de forma remota.
- Transferir archivos.
- Registrar pulsaciones de teclado.
- Realizar reconocimiento de red.
- Mantener persistencia en el sistema mediante modificaciones en el registro.

En esta campaña, los servidores de comando y control (C2) están alojados en Moldavia, y los atacantes utilizan técnicas para evitar ser detectados, como el fingerprinting del navegador y el almacenamiento local para no repetir el ataque en visitas futuras.

La combinación de ClickFix y NetSupport RAT representa una evolución preocupante en el panorama de amenazas. No se basa en vulnerabilidades técnicas, sino en la **confianza del usuario** y su disposición a seguir instrucciones aparentemente inofensivas.

Este tipo de ataques demuestra que la **educación en ciberseguridad** es tan importante como las herramientas de protección. Enseñar a los usuarios a desconfiar de instrucciones no solicitadas y a verificar la legitimidad de los sitios web puede marcar la diferencia entre un sistema seguro y uno comprometido.

Referencia:

Kaspersky
Cybersecuritynews

Edición 40

NEWSLETTER BeIT

En 2025 pasamos de un Sistema de Gestión de Seguridad de la Información a la construcción de un Sistema de Gestión de la Ciberseguridad Industrial

Una publicación conjunta de los departamentos de Infraestructura y Compliance de Elit Infrastructure Services – GrupoBeIT

En un contexto donde las tecnologías de la información (IT) y tecnologías operacionales (OT) es cada vez más común, las organizaciones enfrentan el reto de proteger infraestructuras críticas sin comprometer la continuidad operativa. Para abordar esta necesidad, la combinación de los estándares ISO/IEC 27001/2 e ISA/IEC 62443 ofrece un enfoque integral y complementario para la gestión de la ciberseguridad en entornos industriales.

ISO/IEC 27001 establece los requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI) aplicable a cualquier tipo de organización. Este estándar se centra en la protección de la infraestructura IT, proporcionando un marco estructurado para identificar riesgos, establecer controles y mejorar continuamente la postura de seguridad. ISO/IEC 27002, por su parte, ofrece directrices detalladas para la implementación de controles de seguridad, sirviendo como referencia para seleccionar medidas adecuadas en función del análisis de riesgos.

La serie ISA/IEC 62443 está diseñada específicamente para proteger los Sistemas de Automatización y Control Industrial (IACS), que forman parte esencial de las infraestructuras OT. Esta norma aborda los desafíos únicos de estos entornos, como la necesidad de alta disponibilidad, integridad y rendimiento, donde una interrupción puede tener consecuencias graves para la salud, la seguridad o el medio ambiente.

ISA/IEC 62443 se estructura en diferentes partes que cubren desde los requisitos para propietarios de activos (62443-2-1), hasta especificaciones para proveedores de servicios (62443-2-4) y fabricantes de productos (62443-4-1 y 62443-4-2). Además, introduce el concepto de niveles de seguridad (SL) para adaptar las medidas de protección al nivel de riesgo tolerable.

Aunque ISO/IEC 27001/2 y ISA/IEC 62443 tienen enfoques distintos, su integración permite una cobertura completa de la ciberseguridad organizacional. Mientras ISO/IEC 27001/2 proporciona la estructura de gestión y controles generales, ISA/IEC 62443 aporta los requisitos técnicos y operativos específicos del entorno OT.

Por ejemplo, controles como el bloqueo automático de pantallas o la aplicación de parches, comunes en IT, pueden generar riesgos en OT si no se adaptan adecuadamente. ISA/IEC 62443 contempla estas particularidades, permitiendo excluir o modificar controles para evitar impactos negativos en la operación.

Adaptación de un Sistema de Gestión de la Ciberseguridad Industrial (SGCI) en entornos OT

En un principio, las organizaciones industriales centraban sus esfuerzos de ciberseguridad principalmente en los entornos de tecnologías de la información (IT), dejando en segundo plano los sistemas de tecnología operativa (OT), que son esenciales para la automatización y el control de procesos industriales. Sin embargo, con el tiempo, se hizo evidente que los riesgos cibernéticos también afectaban gravemente a estos entornos OT, lo que llevó a la necesidad de ampliar el enfoque tradicional de seguridad.

Una de las soluciones más recomendadas fue extender el Sistema de Gestión de Seguridad de la Información (SGSI), basado en las normas ISO/IEC 27001 y 27002, para incluir también el entorno OT. Esta ampliación debía realizarse con cuidado, asegurando que la estructura del sistema fuera lo suficientemente flexible como para no comprometer su eficacia. Para lograrlo, se estableció la importancia de definir claramente las responsabilidades entre los equipos de IT y OT, planificar los recursos con habilidades técnicas específicas, y utilizar una terminología común que facilitara la colaboración entre ambas áreas.

En paralelo, la norma ISA/IEC 62443-2-1, aunque no define un SGSI como tal, introdujo un requisito clave: los programas de seguridad para los sistemas de automatización y control industrial (IACS) debían estar coordinados con cualquier SGSI existente. Esto impulsó la recomendación de alinear los elementos del SGSI con los Elementos del Programa de Seguridad (SPE) definidos en dicha norma, integrando los controles relevantes de ISO/IEC 27001/2 en cada uno de ellos.

Para facilitar la aplicación práctica de estas directrices, surgió la necesidad de formalizar este enfoque bajo un nuevo concepto: el Sistema de Gestión de la

Ciberseguridad Industrial (SGCI). Este sistema debía construirse sobre dos pilares fundamentales. El primero, la independencia e integración: el SGCI debía ser compatible con otros sistemas de gestión existentes, pero también debía contar con autonomía suficiente para ser implantado incluso en organizaciones con baja madurez en ciberseguridad industrial. El segundo pilar era la agilidad y operatividad: el sistema debía priorizar medidas básicas de ciberprotección desde el inicio, permitiendo una evolución progresiva hacia requisitos más avanzados.

Consciente de esta necesidad, el Centro de Ciberseguridad Industrial (CCI) tomó la iniciativa de elaborar una guía específica para apoyar a las empresas del sector. Así nació la "Guía para la construcción de un SGCI", que presenta un marco de referencia general y lo desarrolla, cada uno dedicado a los distintos dominios que conforman el sistema.

El objetivo final de esta guía es claro: proporcionar a los responsables de las organizaciones industriales —desde quienes gestionan los procesos productivos hasta los encargados de la operación, las áreas técnicas y de ciberseguridad— todos los recursos y elementos necesarios para llevar a cabo una gestión eficaz, eficiente y continua de los riesgos de ciberseguridad en los entornos de automatización y control industrial.

Ilustración 1. *Marco de referencia del SGCI (Centro de Ciberseguridad Industrial, 2016, p. 5).*

Referencias:

Fortinet
IBM
Palo Alto
Rosmiman
Gartner

Ejemplo práctico: acceso remoto seguro

Un caso ilustrativo es el subelemento NET 3 de 62443-2-1, que trata el acceso remoto seguro. Este requiere que solo se permitan aplicaciones autorizadas, que las conexiones estén documentadas y que se terminen tras un periodo de inactividad. ISO/IEC 27001/2 complementa este enfoque con controles sobre teletrabajo, protección de servicios en redes públicas y acuerdos de confidencialidad, lo que permite una protección más robusta y contextualizada.

Además de cubrir a los propietarios de activos, ISA/IEC 62443 extiende sus requisitos a proveedores de servicios y fabricantes de productos, promoviendo un enfoque de defensa en profundidad. Esto permite a las organizaciones exigir certificaciones a sus proveedores, garantizando que los productos y servicios cumplen con estándares de seguridad desde su diseño hasta su operación.

La integración de ISO/IEC 27001/2 e ISA/IEC 62443 permite a las organizaciones establecer programas de ciberseguridad sólidos, adaptados tanto a IT como a OT. Para facilitar esta integración, se recomienda desarrollar un mapeo de controles ISO/IEC 27001/2 bajo cada SPE de 62443-2-1, ajustándolo a las necesidades específicas de cada organización. Iniciativas como la de la Alianza Global de Ciberseguridad de ISA (ISAGCA) están considerando la creación de referencias comunes para apoyar este proceso.

Este enfoque combinado no solo mejora la protección de las instalaciones operativas, sino que también fortalece la resiliencia organizacional frente a amenazas cibernéticas cada vez más sofisticadas.

Referencias:

Centro de Ciberseguridad Industrial. (2016). Guía para la construcción de un Sistema de Gestión de la Ciberseguridad Industrial (Primera Parte).

ISA – Global Cybersecurity Alliance - Applying ISO/IEC 27001/2 and the ISA/IEC 62443 Series for Operational Technology Environments

vicarius netskope PARTNERS BeIT

FIELD SERVICES 2.0

Servicio técnico especializado en ciberseguridad los 365 días del año

Grupo BeIT junto a Vicarius y Netskope te invitan este **21 de agosto** a vivir la evolución de los servicios en campo en nuestro evento exclusivo **Field Services 2.0**, donde presentaremos cómo nuestro modelo transforma la operación tradicional mediante tecnología en la nube, soporte remoto, mantenimiento predictivo y un enfoque de ciberseguridad basado en Zero Trust; todo impulsado por ingenieros especializados y una **visión proactiva que optimiza costos, tiempos y seguridad**. Acompáñanos para descubrir cómo esta propuesta está revolucionando sectores como Food & Beverage, Salud, Banca y Finanzas, entre otras.

¡No te lo pierdas!

Escríbenos
y aparta tu lugar

ó

Da clic o escanea el QR
y aparta tu lugar

CONFERENCIA PRENSA

PRENSA BeIT

Rueda de prensa conmemorativa XIX aniversario

TECNOEMPRESA

Internet Dedicado De Alta Velocidad Con Cobertura De Fibra Óptica Abrir

Grupo BeIT cumple 19 años impulsando la transformación digital en México

Publicado por Redacción en ciberseguridad, NEGOCIOS, TECNOLOGÍA Publicado julio 18, 2025, 4:26 pm

SITIO

Eventos

Grupo BeIT fortalece su oferta en ciberseguridad, OT e inteligencia distribuida

Grupo BeIT lanza Smart BeIT y entra al sector industrial con nuevas soluciones de ciberseguridad

Everardo Martínez Jul 19, 2025 0

Infochannel

Channel Channel Home

Grupo BeIT refuerza su portafolio con ciberseguridad industrial, Field Services y arquitecturas como servicio

Por Diana Payan | 18 de julio de 2025

COMPARTIR

Elías Cedillo, director general de Grupo BeIT

BOLETÍN DE LA COMPUTACIÓN

Grupo BeIT, 19 años impulsando la ciberseguridad en México

Brenda Rodríguez Hace 2 días

Last Updated: 22 de julio de 2025 98

2 minutos de lectura

Anuncíate

Canales TI

México Casos de Éxito Seguridad

La ciberseguridad también requiere optimización tecnológica

EL ECONOMISTA

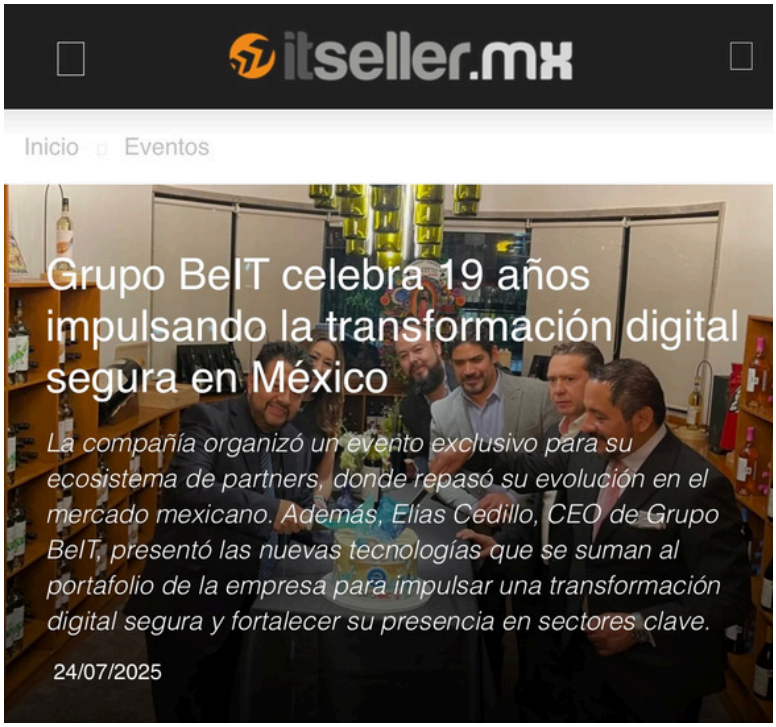
ÚLTIMAS NOTICIAS | **TENDENCIAS:** FINANZAS PERS

TECNOLOGÍA

Lectura **3:00 m**

Transformación tecnológica responde a los riesgos cibernéticos

México fue objetivo de más de 80,000 millones de intentos de ciberataques, siendo uno de los países más atacados en América Latina, según la Asociación Mexicana de Ciberseguridad.



itseller.mx

Inicio Eventos

Grupo BeIT celebra 19 años impulsando la transformación digital segura en México

La compañía organizó un evento exclusivo para su ecosistema de partners, donde repasó su evolución en el mercado mexicano. Además, Elías Cedillo, CEO de Grupo BeIT, presentó las nuevas tecnologías que se suman al portafolio de la empresa para impulsar una transformación digital segura y fortalecer su presencia en sectores clave.

24/07/2025