BURÓMC SEGURIDAD INFORMÁTICA

Grupo BeIT

ELIT INFRASTRUCTURE SERVICES

Sesión Plenaria
Comunidad de Seguridad

Protección de la operación industrial, no solamente la infraestructura tecnológica.

Elías Cedillo

CEO y Fundador de Grupo BeIT

CEO y socio fundador de las empresas Buró Mexicano de Consultores en Seguridad Informática S.A. de C.V. y Elit Infrastructure Services S.A. de C.V., la primera con más de 19 años de experiencia y especializada en tecnologías de la información, comunicaciones y protección de datos (seguridad informática y ciberseguridad), y la segunda con más de 5 años en el mercado de infraestructura y unificación de soluciones en TIC´s. Además, socio fundador de Grupo BeIT el cual aglomera a 5 empresas especializadas en Tecnologías de la Información (incluyendo las dos antes mencionadas).

Certificaciones:

- Maestría en Profesional de Ciberseguridad Industrial. Centro de Ciberseguridad Industrial (2025)
- Maestría en Comunicación para la Acción Política y Social 2021-2023
- Maestría en Dirección de Empresas para Ejecutivos con Experiencia (MEDEX)
- Instituto Panamericano de Alta Dirección de Empresa. 2012- A la fecha
- Licenciatura en Ciencias de Informática
- Unidad Profesional Interdisciplinaria de Ingeniería y Ciencias Sociales y Administrativas. Instituto Politécnico Nacional. 1997 – 2001
- Diplomado en Transformación Digital. MIT 2024-2025
- Diplomado Herramienta de Minería de Datos y Analítica Empresarial. ITAM 2019-2020
- Diplomado en Derecho de las Tecnologías de la Información y las Comunicaciones. ITAM 2010
  Diplomado Integral de Telecomunicaciones. UNAM 2008
- Diplomado de Seguridad Informática. 2003-2004
- Diplomado de MS Systems Engineer Windows 2001
- Doctorado honoris causa por parte de la Universidad Anáhuac 2019

Grupo BeIT BURÓMC SEGURIDAD INFORMÁTICA ELIT INFRASTRUCTURE SERVICES

Roberto Cano

Gerente de Operaciones ELIT

Ingeniero Industrial con más de 15 años de experiencia en tecnología, ciberseguridad y cumplimiento normativo. Ha dirigido proyectos que fortalecen la seguridad, eficiencia y transformación digital en sectores como financiero, gubernamental, asegurador e inmobiliario.

Certificaciones:

- Business Analysis
- Scrum Product Owner
- Interpretación de la norma ISO/IEC 9001:2015 Auditor Interno bajo la norma ISO 9001
- Interpretación de la norma ISO/IEC 20000-1:2011 Modelo CANVAS (Plan de Negocios)
- PCI compliance
- PCI- PRIVACY AND INFORMATION SECURITY
- Incident- handler
- Information Systems Auditor
- Seminario de Certificación PMP
- ISO/IEC 20000-1:2018
- ISO/IEC 27032 CYBERSECURITY PROFESSIONAL
- Auditor Líder ISO/IEC 27001:2022
- Seguridad en la nube 27018

Grupo BeIT BURÓMC SEGURIDAD INFORMÁTICA ELIT INFRASTRUCTURE SERVICES

Mario Carranza

Especialista OT

Ingeniero en Control y Robótica, certificado como programador de PLCs y Robots Industriales, con experiencia en el diseño, implementación, mantenimiento y optimización de sistemas automatizados. Especialista en la integración de PLCs, HMI, DCS, SCADA y robots industriales en diversos sectores, así como en el desarrollo e implementación de estrategias de ciberseguridad industrial orientadas a la protección de tecnologías operativas (OT).

Certificaciones:

- Maestría en Control Automático, con enfoque en procesos químicos y eficiencia de procesos industriales
- Formación y capacitación técnica, impartiendo cursos especializados en Automatización Industrial
- Programación de PLCs, HMI, SCADA
- Robótica Industrial

Rolando Rodríguez

Ingeniero en Ciberseguridad

Ingeniero Administrador en Tecnologías de la Información especializado en Ciberseguridad, con una sólida experiencia en pruebas de penetración y análisis de vulnerabilidades.

Actualmente se desempeña como Pentester en BuróMC, donde realiza intrusiones físicas, pruebas de seguridad en aplicaciones web y móviles, evaluación de infraestructuras y análisis de entornos Active Directory, aplicando metodologías OWASP y herramientas avanzadas como Bloodhound, Fryda y MobSF.

Certificaciones:

- CEH (Certified Ethical Hacker)
- eWPT (eLearnSecurity Web Application Penetration Tester)
- CompTIA Pentest+

Grupo BeIT

BURÓMC SEGURIDAD INFORMÁTICA

ELIT INFRASTRUCTURE SERVICES

Acerca de Grupo BeIT

En **Grupo BeIT** con nuestras marcas **BuróMC Seguridad Informática y Elit Infrastructure Services**, brindamos una protección completa , continuidad de negocio y rentabilidad eficiente mediante profesionales expertos, procesos con estándares internacionales y tecnología avanzada.

Integramos la **metodología NIST Cybersecurity Framework (CSF)**, así como los más altos estándares internacionales de seguridad de la información, como **ISO 27001:2022**, para ofrecer soluciones de vanguardia.

ISO/ IEC 20000-1:2018

ISO/IEC 27001:2022

Nuestros clientes

Gobierno

Finanzas

Telecom

Servicios

Retail

Salud

Otros

Portafolio de Soluciones 2026

Field Services 2.0

La evolución del servicio técnico híbrido virtual y en campo para activos y entornos de TI con ciberseguridad

- Integración con SOC y NOC.

Portafolio

- Activos (servidores, aplicaciones, información, monitoreo)
- Infraestructura de Data Center
- Energía y Enfriamiento
- Networking entre soluciones

SmartBits

Ofrecemos 3 bundles diseñados para diferentes desafíos en ciberseguridad:

Esencial (Protección Básica)	Bundle Avanzado (Protección Integral)	Bundle Premium (Máxima Protección)
Protección esencial para empresas que buscan seguridad sin grandes inversiones.	Protección integral para información sensible y mayor exposición a amenazas.	Máxima protección y cumplimiento normativo para organizaciones con altos requerimientos.

Ecosistemas de Ciberseguridad

Innovadores, especializados y a la medida que fortalecen la seguridad de la información y los activos de la empresa, protegiéndolos de amenazas cibernéticas en constante crecimiento, gestionando riesgos.

- Web Application Firewall (WAF)
- Disaster Recovery Plan (DRP)
- Identity and Access Management (IAM)
- Filtrado
- Zero Trust Network Access (ZTNA)
- Cloud Access Security Assessment (CASA)

Partners:

SOPHOS, FORTINET, netskope, THALES, vicarius, proofpoint, kartos, qondar, CybrHawk, OT Latam, elastic, Bitdefender, Hillstone Networks, AREXDATA

Cybersecurity as a Services

Cyber Security
- -Ethical Hacking (EH)
- -Security Operations Center (SOC)
- -Network Operation Center (NOC)

7 x 24

Mesa de Servicio.

Cumplimiento Normativo
-Estándares Internacionales

ISO/ IEC 20000-1:2018

ISO/IEC 27001:2022

IQNET

Seguridad Industrial
Operational Technology (OT)

Infraestructura | Data Center

Modernización para impulsar la transformación digital de la infraestructura TI centrándonos en el compliance, eficiencia operativa, estándares internacionales y mejores prácticas.

- Cableado / CCTV
- Energía y Enfriamiento
- Infraestructura
- Respaldos
- Cómputo

Partners:

ELIT INFRASTRUCTURE SERVICES, Schneider Electric, H3C, HUAWEI, veeAM, NUTANIX, HOKOWITS, DELL

Operational Technology (OT)

Consultoría y Gobierno Operational Technology (OT)
- Identificación de procesos críticos y líneas de producción
- Diseño del modelo de gobernanza OT
- Definición de roles y responsabilidades
- Desarrollo de políticas OT alineadas a normas del sector

Visibilidad y Gestión de Activos
- Levantamiento de activos OT críticos
- Clasificación y análisis de riesgos
- Priorización basada en impacto operacional

Protección de Infraestructura Industrial
- Segmentación de red OT por líneas de producción
- Definición de niveles de seguridad
- Implementación de firewalls industriales
- Control de accesos y protección antimalware

Cumplimiento y Mejora Continua
- Evaluaciones de cumplimiento normativo
- Auditorías y simulacros de incidentes
- Planes de mejora continua en ciberseguridad OT

Energía y Cooling

Power continuity
UPS, respaldo, mantenimiento

- Mantenimiento preventivo anual UPS mediano (50–200 kVA)
- Contrato full coverage 24x7 (UPS grande)
- Intervención correctiva sin contrato

Precisión cooling
Enfriamiento, optimización térmica

- Mantenimiento anual por unidad CRAC/InRow
- Optimización térmica de sala DC pequeña
- Proyecto de mejora térmica (DC mediano)

Data Center Infrastructure Management (DCIM)
Clientes que buscan visibilidad y eficiencia
Software, monitoreo, operación

- Diseño de DC
- Ingeniería eléctrica y mecánica
- Integración de energía, racks y cooling
- Puesta en marcha (commissioning)

Portafolio de Soluciones 2026

Operational Technology (OT)

Consultoría y Gobierno Operational Technology (OT)

- Identificación de procesos críticos y líneas de producción
- Diseño del modelo de gobernanza OT
- Definición de roles y responsabilidades
- Desarrollo de políticas OT alineadas a normas del sector

Visibilidad y Gestión de Activos

- Levantamiento de activos OT críticos
- Clasificación y análisis de riesgos
- Priorización basada en impacto operacional

Protección de Infraestructura Industrial

- Segmentación de red OT por líneas de producción
- Definición de niveles de seguridad
- Implementación de firewalls industriales
- Control de accesos y protección antimalware

Cumplimiento y Mejora Continua

- Evaluaciones de cumplimiento normativo
- Auditorías y simulacros de incidentes
- Planes de mejora continua en ciberseguridad OT

Grupo BeIT BURÓMC SEGURIDAD INFORMÁTICA ELIT INFRASTRUCTURE SERVICES

EL RIESGO

¿Qué sucede cuando un incidente de ciberseguridad afecta?

El impacto puede trascender la información y llegar directamente a la operación.

CONTINUIDAD

Una amenaza puede provocar interrupciones, pérdida de disponibilidad o degradación del proceso.

ELEMENTOS

Eventos sobre PLC, SCADA o HMI puede tener consecuencias sobre procesos y seguridad física pueden ser alcanzados por una afectación en una segmentación deficiente de una red, accesos a redes publicas, abiertas la falta de Firewalls o la mala configuración de estos.

VISIBILIDAD

Sin contexto OT, el equipo puede recibir alertas sin saber cuáles representan riesgo real.

La seguridad OT debe entender primero la operación.

Grupo BeIT

BURÓMC SEGURIDAD INFORMÁTICA

ELIT INFRASTRUCTURE SERVICES

RESPALDO

Marcos de referencia

Los marcos fortalecen el enfoque de seguridad; no sustituyen el contexto operacional de la solución.

IEC 62443

Referencia internacional para la ciberseguridad de sistemas de automatización y control industrial.

NIST SP 800-82

Guía específica para proteger sistemas de control industrial y gestionar riesgos en entornos ICS.

ISO/IEC 27001

Marco de gestión de seguridad de la información aplicable para fortalecer el gobierno de seguridad.

Siguientes pasos

Estado Actual

Con base en análisis de riesgo y madurez se identifica el nivel de ciberseguridad actual.

Estado Deseado

Atendiendo a las buenas practicas de los marcos de referencia se identifica el nivel de seguridad necesario.

El camino a seguir

Se plantean los procesos y tecnologías que permiten transitar de un nivel de ciberseguridad actual al deseado

Grupo BeIT

BURÓMC SEGURIDAD INFORMÁTICA

ELIT INFRASTRUCTURE SERVICES

Servicios Especializados

Administración de Activos

- Levantamiento de activos OT críticos
- Clasificación y análisis de riesgos
- Priorización basada en impacto operacional
- Análisis de vulnerabilidades
- Pentest

Resiliencia de Infraestructura

- Segmentación de red OT por líneas de producción
- Definición de niveles de seguridad
- Implementación de firewalls industriales
- Control de accesos y protección antimalware
- EDR OT
- SOC OT

Consultoría, Gobierno OT y Cumplimiento

- Identificación de procesos críticos y líneas de producción
- Diseño del modelo de gobernanza OT
- Definición de roles y responsabilidades
- Desarrollo de políticas OT alineadas a normas del sector

Mejora Continua

- Evaluaciones de cumplimiento normativo
- Auditorías y simulacros de incidentes
- Planes de mejora continua en ciberseguridad OT

Grupo BeIT BUROMC SEGURIDAD INFORMÁTICA ELIT INFRASTRUCTURE SERVICES

Los SOC tradicionales no entienden el contexto operacional

Las herramientas IT genéricas pueden detectar actividad, pero no necesariamente interpretar su significado dentro de una operación industrial.

LO QUE FALLA

- Exceso de falsos positivos en OT
- Falta de visibilidad de protocolos industriales
- Escaso contexto sobre procesos y activos
- Dificultad para priorizar por impacto operacional
- Superficie de ataque ampliada por la convergencia IT/OT

LO QUE SE NECESITA

- Monitoreo OT 24/7 con especialistas
- Detección protocolos
- Contexto industrial para interpretar eventos
- Correlación IT ↔ OT
- Priorización basada en riesgo operacional

Grupo BeIT BUROMC SEGURIDAD INFORMÁTICA ELIT INFRASTRUCTURE SERVICES

CÓMO FUNCIONA

Ver → Entender → Detectar → Priorizar → Responder

El servicio convierte datos de la operación en decisiones de seguridad accionables.

01

VER

Recolección pasiva de tráfico y telemetría de PLCs, SCADA, HMIs, estaciones de ingeniería y red OT.

02

ENTENDER

Construcción de registros de comportamiento operacional y análisis de comunicaciones industriales.

03

DETECTAR

Correlación de anomalías, firmas, inteligencia y contexto industrial.

04

PRIORIZAR

Analistas OT validan y priorizan según impacto operacional y riesgo real.

05

RESPONDER

Investigación estructurada, escalamiento y apoyo a contención/remediación.

Grupo BeIT

BURÓMC SEGURIDAD INFORMÁTICA

ELIT INFRASTRUCTURE SERVICES

QUÉ DETECTAMOS

Amenazas y anomalías que pueden afectar la operación

La detección combina comportamiento, protocolos industriales, inteligencia y contexto.

EQUIPOS DE CONTROL Y MONITOREO

Cambios de configuración o comandos no autorizados

RED OT

Comunicaciones inesperadas y patrones de tráficoanormales

COMANDOS

Secuencias o interacciones fuera del comportamiento esperado

ACCESOS

Sesiones remotas y accesos no autorizados

AMENAZAS

Indicadores de ransomware, APT y campañas dirigidas a OT

EMERGENTES

Amenazas desconocidas detectadas mediante anomalías

Grupo BeIT

BURÓMC SEGURIDAD INFORMÁTICA

ELIT INFRASTRUCTURE SERVICES

LA SOLUCIÓN

Una capacidad continua de seguridad OT

Los componentes de la solución.

Monitoreo 24/7

Vigilancia continua del entorno OT.

Visibilidad ICS

Consolidación de activos, comunicaciones y actividad.

Alertas priorizadas

Eventos clasificados por severidad e impacto.

Investigación

Validación y análisis estructurado de incidentes.

Escalamiento

Coordinación con el cliente para atención y respuesta.

Elementos de configuración

- Redes OT
- Equipos de Control y Monitoreo
- Firewalls
- Accesos remotos seguros

DIFERENCIACIÓN

¿Por qué un SOC especializado en OT?

La propuesta debe diferenciarse por conocimiento operacional, no solamente por tecnología.

ESPECIALIZACIÓN OT

No es un SOC IT adaptado: está orientado a ambientes industriales.

CONTEXTO OPERACIONAL

Las alertas se interpretan considerando proceso, activos e impacto.

PROTOCOLOS INDUSTRIALES

Visibilidad y detección sobre comunicaciones propias de ICS/OT.

24/7

Monitoreo continuo con especialistas dedicados a entornos industriales.

PUENTE IT–OT

Correlación de eventos para identificar posibles movimientos laterales.

ENFOQUE EN RIESGO

Se prioriza lo que puede afectar la continuidad, seguridad o integridad.

Grupo BeIT

BURÓMC SEGURIDAD INFORMÁTICA

ELIT INFRASTRUCTURE SERVICES

Gracias

Elías Cedillo,
CEO y Fundador
de Grupo BeIT

ecedillo@buromc.com

Roberto Cano
Gerente de Operaciones ELIT

rcano@buromc.com

Visita nuestro sitio web

Sesión Plenaria
Comunidad de Seguridad

¡Gracias por acompañarnos!