Protección de Datos:
Estrategia Integral de Ciberseguridad

Miércoles, 26 de agosto de 2026

Ponentes

Elías Cedillo

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

Ponentes

Roberto Cano

Gerente de Operaciones

Ingeniero Industrial con más de 15 años de experiencia en tecnología, ciberseguridad y cumplimiento normativo. He dirigido proyectos que fortalecen la seguridad, eficiencia y transformación digital en sectores 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 InterpretacióndelanormaISO/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

Estructura de Soluciones

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

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
- Infraestructura
- Respaldos
- Cómputo

Partners:

ELIT INFRASTRUCTURE SERVICES, Schneider Electric, H3C The Leader in Digital Solutions, 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)

BUROMC SEGURIDAD INFORMÁTICA · Grupo BeIT · ELIT INFRASTRUCTURE SERVICES

Nuestros Clientes

Gobierno

Finanzas

Telecom

Servicios

Retail

Salud

Otros

Protección de datos: el costo real del incumplimiento

Cifras clave de cumplimiento regulatorio para salud y farmacéutica

$10.93M USD

Costo promedio de una brecha de datos en salud — más del doble del promedio global ($4.88M USD)

181 días

Tiempo promedio para detectar e identificar una brecha de datos, antes de poder contenerla

65–70%

De las brechas se originan por error humano o mal uso de credenciales internas

$30M+ MXN

Sanciones bajo la LFPDPPP, que se duplican cuando se trata de datos sensibles de salud

Fuentes: IBM Cost of a Data Breach Report 2026 · Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), vigente 2026

Caso de referencia: Novo Nordisk, junio 2026

Robo de datos de ensayos clínicos en una farmacéutica global — mismo riesgo, misma industria

Marzo 2026

Acceso inicial no detectado mediante credenciales robadas (infostealers): 211 credenciales de empleados y 2,932 cookies de sesión activas circulando en foros criminales.

1 de junio

El grupo de extorsión FulcrumSec contacta a Novo Nordisk y exige un rescate de $25M USD. La empresa se niega a pagar.

11 de junio

Novo Nordisk confirma públicamente el acceso no autorizado a un número limitado de sistemas internos.

15 de junio

FulcrumSec comienza a filtrar 1.3 TB de datos: ensayos clínicos, código fuente y modelos de IA propios.

Qué se expuso

- Datos seudonimizados de ~11,500 pacientes de ensayos clínicos: identificadores, biomarcadores y hábitos de salud
- Información de empleados y médicos vinculados a la compañía
- Código fuente y fórmulas de fármacos comercializados y en desarrollo
- Modelos internos de IA y datos de operaciones/manufactura

2+ meses de acceso silencioso antes de ser detectado

La lección, mapeada a nuestros 3 pilares

Gobernanza y visibilidad

Sin visibilidad continua, el acceso no autorizado circuló más de dos meses sin ser detectado.

DSPM

Miles de cookies de sesión activas sin monitoreo de postura permitieron sesiones autenticadas sin contraseña ni MFA.

DLP

1.3 TB de datos —clínicos, código fuente y de IA— salieron de la organización sin ser bloqueados.

Fuentes: comunicado de Novo Nordisk (11 jun 2026) · Reuters · reportes de FulcrumSec vía Ransomnews (jun 2026)

Estrategia de Protección del Dato (Modelo de 3 Pilares)

Objetivo

Proteger el dato a lo largo de todo su ciclo de vida (creación, uso, tránsito y almacenamiento), asegurando:

- Cumplimiento normativo
- Visibilidad y trazabilidad total del dato
- Prevención de fuga o mal uso

Pilar 1:
Clasificación y tratamiento del Dato (Gobierno + Cumplimiento + Uso)

Objetivo
Entender qué datos tienes, qué tan sensibles son y cómo deben tratarse.

Componentes clave
Modelo de clasificación

Pilar 2:
DSPM (Aquí está el corazón técnico de control real)

Objetivo
Tener visibilidad y la trazabilidad total del dato:

- Dónde está
- Quién lo usa
- Cómo se mueve

Basado en
Data Security Posture Management (DSPM)

Pilar 3:
DLP (Prevención de Fuga de Información)

Objetivo
Evitar que el dato salga, se comparta o se use indebidamente.

Basado en:
Data Loss Prevention

Data in Use (en uso)

Bloqueo de:

- Copiar/pegar datos sensibles
- Capturas de pantalla
- Uso en apps no autorizadas

Pilar 1: Cumplimiento Normativo basado en ISO/IEC 27001 + CIS Control

Objetivo: Establecer un marco de control sólido, auditable y alineado a mejores prácticas internacionales.

- Mapear controles de:
  - ISO 27001 (enfoque de gestión)
  - CIS Controls (enfoque técnico y operativo)
  - Definir niveles de madurez (Inicial → Optimizado)

3 Líneas de acción

1.-Gobierno y liderazgo

•Políticas y normativas formales

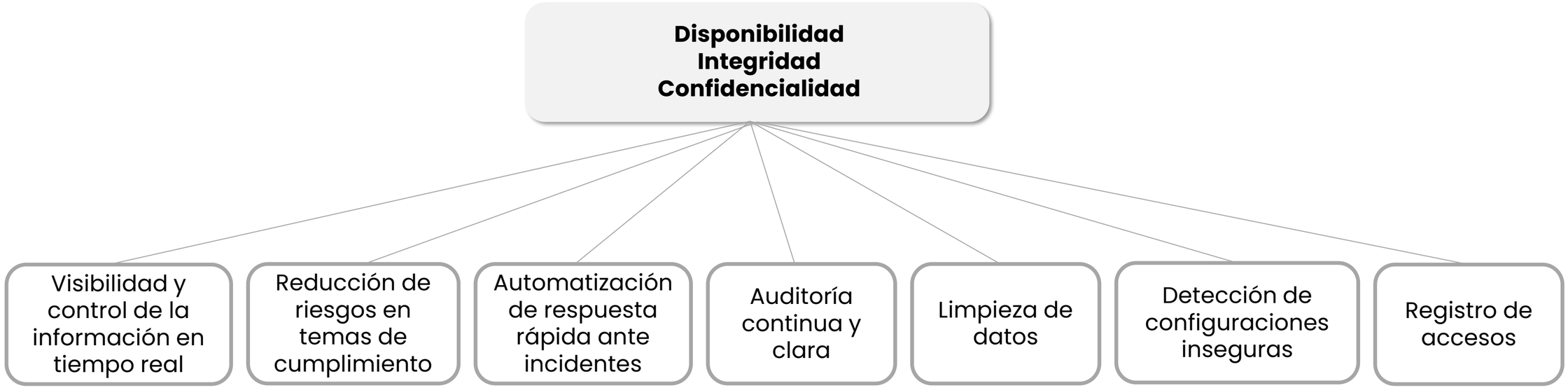
2.- Gestión de riesgos

• Identificación de activos críticos
•Evaluación de riesgos (impacto vs probabilidad)
•Plan de tratamiento

3.- Controles prioritarios (Quick Wins CIS)

•Inventario de activos (CIS 1)
•Gestión de vulnerabilidades (CIS 7)
•Control de accesos (CIS 6)
•Monitoreo continuo (CIS 8)

Beneficios obtenidos con una estrategia de ciberseguridad de datos



Transformar el cumplimiento normativo en un proceso dinámico, eficiente y demostrable

Fases de ciclo de vida: seguridad, integridad, disponibilidad y confidencialidad

Estados del dato y su tratamiento1. (RED, NUBE, ENDPOINT)

1 Creación / Captura (DSPM)

Qué es: Cuando el dato se genera

Tratamiento:

- Validación de datos (formato, tipo, obligatoriedad)
- Clasificación inicial (público, interno, confidencial, sensible)
- Control de origen (fuente confiable)
- Registro de trazabilidad (quién lo creó y cuándo)
- Minimización de datos (solo lo necesario)

2 Almacenamiento (DSPM) (DLP)

Qué es: Cuando el dato se guarda.

Tratamiento:

- Cifrado en reposo (AES-256, por ejemplo
- Control de accesos (RBAC, ABAC)
- Segmentación de datos
- Backups y redundancia
- Políticas de retención
- Hardening de infraestructura

3 Procesamiento / Uso / Eliminación (DSPM) (DLP)

Qué es: Cuando el dato se consulta, modifica, analiza o utiliza para operación o negocio.

Tratamiento:

- Control de acceso por roles
- Monitoreo y auditoría (logs)
- Integridad del dato (hash, validaciones)
- Prevención de fuga (DLP)
- Uso de entornos seguros (sandbox, entornos segregados)
- Enmascaramiento o anonimización (si aplica)

4 Transmisión / Compartiendo (DLP)

Qué es: Cuando el dato se mueve entre sistemas, redes o usuarios.

Tratamiento:

- Cifrado en tránsito (TLS 1.2/1.3, VPN)
- Autenticación mutua (certificados)
- Integridad (firmas digitales)
- Protección contra ataques (MITM, sniffing)
- Control de endpoints

Políticas de tratamiento

Define para cada nivel:

- Acceso (quién y cómo)
- Retención
- Cifrado requerido
- Compartición permitida

Integración con procesos

- Alta de sistemas → deben clasificar datos desde el diseño (privacy by design)
- Contratos → incluir manejo de datos
- Auditorías → validar cumplimiento

Integración entre los 3 pilares (CLAVE)

- Sin clasificación → DLP no sabe qué proteger
- Sin DSPM → no sabes dónde está el riesgo
- Sin DLP → no puedes detener fugas

¿Cómo una solución facilita el cumplimiento normativo en seguridad del dato?

Sin DSP estás ciego, y sin DSPM estás expuesto
Sin compliance no se tiene estrategia .

Diferencias entre DSPM y DLP

Aspecto	DSPM (Gestión de la Postura de la Seguridad de los Datos)	DLP (Prevención de Perdida de Datos)
Definición	Descubre, clasifica, mapea y evalúa el riesgo del dato.	Previene la fuga, exposición o uso indebido del dato.
Objetivo	Visibilidad y trazabilidad total del dato.	Protección en tiempo real.
Enfoque	Proactivo.	Preventivo y reactivo.
Pregunta clave	¿Dónde están?, ¿Quién tiene acceso?, ¿Cómo se utilizan? y ¿Cuál es la postura de seguridad?	¿Cómo evito que se filtren o se usen mal?
Cobertura	Activo donde radica el dato. (nube, servidor, equipos y aplicativos)	Datos en uso, en movimiento y en reposo.
Funciones	Automatización de actividades de detección y trazabilidad y protección de los datos.	Monitoreo, inspección, bloqueo, cifrado, alertas.
Visibilidad	Estructura del dato.	Operacional (eventos).
Acción	Visualizar (identificar).	Bloquea o restringe en tiempo real.
Dependencia	Correcta clasificación y análisis de riesgo.	Depende de clasificación.

Pilar 2: Trazabilidad y Visibilidad del Dato

Objetivo: : Tener visibilidad total del ciclo de vida del dato: origen, uso, transformación y destino

Estrategia

•Implementar data lineage + data tracking
•Clasificar la información (crítica, sensible, pública)
•Identificar riesgos asociados al movimiento del dato

1. Líneas de acción

- Identificación automática
- Descubrimiento de datos de repositorios
- Mapeo de flujos de información

2. Clasificación y etiquetado

- Datos personales
- Datos financieros
- Datos estratégicos

3. Monitoreo de uso

1. Quién accede
2. Desde dónde
3. Qué hace con el dato

4. Análisis de riesgo del dato

- Exposición
- Transferencias no autorizadas
- Shadow IT

Pilar 3: Data Loss Prevention (DLP)

Objetivo: Prevenir la fuga, filtración o uso indebido de información sensible.

Estrategia

Implementar Data Loss Prevention (DLP) integrado con clasificación y trazabilidad.

Cubrir los tres frentes:

- Endpoint
- Red
- Nube

Gracias.

Elías Cedillo

CEO y Fundador Grupo BeIT

Roberto Cano

Gerente de Operaciones y Cumplimiento

rcano@buromc.com

BURŌMC SEGURIDAD INFORMÁTICA

Grupo BeIT

ELIT INFRASTRUCTURE SERVICES