NEWSLETTER

grupobeit.com

BLOG DEL CEO

En 2026, los modelos tradicionales de monitoreo han quedado atrás. El Security Operations Center (SOC) y el Network Operations Center (NOC) ya no son áreas aisladas que reaccionan a incidentes; hoy representan el núcleo de la resiliencia operativa y la continuidad del negocio...

EDICIÓN 54

Qué esperar de SOC y NOC en 2026

El 2026 estará marcado por tres grandes transformaciones en operaciones de seguridad y red...

WEBINAR 3/03

THALES

Desbloqueando la Ley de la Nube: Lo que todo líder debe saber sobre la privacidad, el riesgo y el cumplimiento de los datos...

EVENTOS BEIT

Evento exclusivo: Protección de los datos: Estrategia de Ciberseguridad

NOTICIA BEIT

Ciberataque masivo a entidades públicas en México pone en evidencia la necesidad de SOC y NOC

México enfrentó uno de los eventos de ciberseguridad más críticos de los últimos años. Recientes reportes técnicos de empresas especializadas...

Edición 54

SOC y NOC en 2026 — De centros operativos a plataformas estratégicas de resiliencia digital

Por: Elías Cedillo, Fundador y CEO GrupoBeIT

En 2026, los modelos tradicionales de monitoreo han quedado atrás. El Security Operations Center (SOC) y el Network Operations Center (NOC) ya no son áreas aisladas que reaccionan a incidentes; hoy representan el núcleo de la resiliencia operativa y la continuidad del negocio.

Los datos lo confirman. El IBM Cost of a Data Breach Report 2025 indica que el costo promedio global de una brecha supera los USD 4.5 millones, y que las organizaciones con capacidades avanzadas de detección y respuesta reducen el costo en promedio hasta en USD 1.76 millones frente a aquellas con capacidades inmaduras.

A esto se suma que, según el Verizon Data Breach Investigations Report 2025 (DBIR), más del 68 % de las brechas involucran el factor humano, pero la mayoría de los ataques exitosos permanecen sin ser detectados durante días o semanas cuando no existe monitoreo continuo efectivo.

Para 2026, una estrategia madura de SOC + NOC debe construirse sobre tres pilares fundamentales:

1. Monitoreo 24/7 con correlación avanzada

La superficie de ataque híbrida exige correlación en tiempo real. Gartner estima que para 2026, más del 60 % de las organizaciones consolidarán funciones de seguridad y operaciones de TI para mejorar visibilidad y reducir tiempos de respuesta.

Un SOC moderno debe integrar SIEM, SOAR, inteligencia de amenazas y telemetría extendida (XDR), mientras que el NOC garantiza disponibilidad, rendimiento y estabilidad de red bajo un enfoque proactivo.

2. Reducción del MTTD y MTTR

Según el reporte de IBM, el ciclo de vida promedio de una brecha es de 204 días para identificarla y 73 días para contenerla. Cada día sin detección incrementa el impacto financiero y reputacional.

Un SOC/NOC maduro debe enfocarse en:

- Reducción del MTTD (Mean Time to Detect)
- Reducción del MTTR (Mean Time to Respond)
- Automatización de playbooks de respuesta

Las organizaciones que integran automatización y respuesta orquestada reducen significativamente el tiempo de contención.

3. SOC como indicador de gobernanza y cumplimiento

Regulaciones como ISO 27001, NIST CSF y marcos regulatorios financieros en México exigen monitoreo continuo y capacidad de respuesta documentada.
Un SOC estratégico ya no reporta solo alertas técnicas; reporta:

- Riesgo residual
- Tendencias de ataque
- Exposición sectorial
- Nivel de madurez de controles

En 2026, los consejos directivos exigen métricas claras de resiliencia operativa, no solo reportes técnicos.

En definitiva, SOC y NOC evolucionan de centros reactivos a plataformas estratégicas que protegen reputación, ingresos y continuidad operativa.

Fuentes:

- IBM — Cost of a Data Breach Report 2025: Cost of a data breach 2025 | IBM
- Verizon — Data Breach Investigations Report 2025 (DBIR): 2025-dbir-data-breach-investigations-report.pdf
- Microsoft — Digital Defense Report 2025: Informe de Defensa Digital de Microsoft 2025 - Cibersecurity.io
- Gartner — Security Operations Forecast 2025: Security Operations Primer for 2025

Ciberataque masivo a entidades públicas en México pone en evidencia la necesidad de SOC y NOC

NOTICIA BeIT

México enfrentó uno de los eventos de ciberseguridad más críticos de los últimos años. Recientes reportes técnicos de empresas especializadas señalan que un grupo de amenazas conocido como Chronus habría comprometido sistemas de al menos 25 dependencias públicas y privadas en México, exponiendo información sensible de aproximadamente 36.5 millones de personas.

Entre las entidades afectadas se mencionan organismos como el Servicio de Administración Tributaria (SAT), instituciones de salud y educación, así como gobiernos estatales, lo que sugiere un ataque con impacto transversal en servicios clave del país.

Aunque algunas autoridades han negado compromisos en sus sistemas, el análisis independiente de firmas de seguridadindica que la sofisticación del ataque se basó en técnicas de escalamiento de privilegios y persistencia prolongada en la red antes de la exfiltración de datos.

Implicaciones para el monitoreo y las operaciones

Este tipo de brechas no se detectan de manera inmediata en ambientes con monitoreo fragmentado o reactivo, lo que pone de manifiesto varios desafíos operativos que las organizaciones deben contemplar:

- Visibilidad insuficiente: demasiadas dependencias no cuentan con un monitoreo centralizado de eventos de seguridad y rendimiento.
- Detección tardía: sin correlación entre eventos de red e indicadores de seguridad, los ataques pueden permanecer latentes por largos periodos.
- Respuesta descoordinada: ante eventos que afectan tanto a la seguridad de la información como a la disponibilidad de servicios, la falta de integración entre funciones de seguridad (SOC) y operaciones de red (NOC) dificulta la contención efectiva.

Integrar un SOC con capacidades avanzadas de correlación de eventos, detección de intrusiones y respuesta automatizada, junto con un NOC que garantice disponibilidad, resiliencia y monitoreo de red proactivo, es crítico para detectar tempranamente este tipo de amenaza y mitigar su impacto.

La protección de datos personales de millones de usuarios y la continuidad de servicios públicos esenciales exigen estructuras operativas integradas, procesos automatizados de respuesta y métricas en tiempo real que solo un enfoque SOC + NOC maduro puede ofrecer.

Agenda una asesoría.
Contacto:

+52 56 5100 8613 admmarketing@buromc.com

Qué esperar de SOC y NOC en 2026

El 2026 estará marcado por tres grandes transformaciones en operaciones de seguridad y red.

Primero, la automatización inteligente. Según Gartner, para 2026 más del 75 % de los SOC incorporarán automatización basada en IA para triage de alertas, priorización y respuesta inicial.

Segundo, monitoreo centrado en identidad. Microsoft confirma que el abuso de credenciales continúa siendo el vector dominante de ataque. El SOC moderno deberá priorizar visibilidad sobre identidades, privilegios y accesos.

Tercero, métricas orientadas a negocio. El directorio ya no pregunta cuántas alertas se atendieron; pregunta cuánto riesgo se redujo y cuánto tiempo puede operar la organización ante un incidente.

Para prepararse estratégicamente, las organizaciones deben:

- Adoptar monitoreo unificado SOC + NOC
- Automatizar procesos repetitivos
- Integrar inteligencia de amenazas contextual
- Medir MTTD, MTTR y resiliencia operativa
- Reportar métricas ejecutivas de riesgo

La conclusión es clara: en 2026, el SOC y el NOC dejarán de ser centros de costo para convertirse en habilitadores de continuidad, confianza y ventaja competitiva.

Para fortalecer tu estrategia de monitoreo y resiliencia digital, consulta nuestras soluciones NOC y SOC en: Buro MC | Liderazgo en Tecnología e Innovación

En un entorno donde las amenazas digitales evolucionan cada día y las regulaciones son cada vez más estrictas, proteger la información crítica de tu organización ya no es una opción, sino un pilar indispensable de continuidad, cumplimiento y confianza.

Te invitamos a un evento exclusivo:

Protección de los datos: Estrategia de Ciberseguridad

Un enfoque holístico para blindar tus datos, cumplir normativas y fortalecer tu operación.
Durante esta **sesión y desayuno**, presentaremos una solución diseñada para fomentar un nivel de ciberseguridad de la información robusto, alineado tanto con los requerimientos internos de cada organización como con las regulaciones establecidas por entidades gubernamentales.

Nuestra estrategia se basa en tres pilares fundamentales:

1. Compliance

Garantiza el cumplimiento normativo mediante políticas, controles y procesos que aseguran integridad, trazabilidad y apego a estándares.

2. Trazabilidad y visibilidad del Dato (Arexdata DSPM)

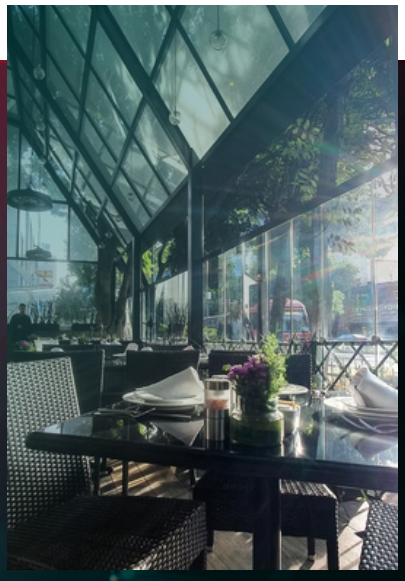
Ofrece una visibilidad profunda sobre el uso, movilidad y acceso a la información, permitiendo tomar decisiones informadas y prevenir riesgos asociados al manejo de datos.

3. Data Loss Prevention (DLP)

Previene fugas, filtraciones y uso indebido de información sensible mediante controles avanzados que protegen el ciclo de vida completo de los datos.

¿Por qué asistir?

- Comprender cómo adaptar una estrategia de ciberseguridad a las necesidades particulares de tu organización
- Integrar nuestros tres pilares para fortalecer la protección de tus activos de información
- Obtener recomendaciones prácticas para elevar tu postura de protección y cumplir normativas vigentes



Registro

Fecha y hora
Jueves 16 de abril de 8 a 11 a.m

Modalidad
Presencial Saks Barranca ubicado en: Av. Insurgentes Centro 1641, San José Insurgentes, Benito Juárez, 03900 Ciudad de México, CDMX y virtual.
Será un gusto contar con tu participación y acompañarte en la evolución de tu estrategia de ciberseguridad.

Contacto: ***+52 56 5100 8613*** ***admmarketing@buromc.com***

“Desbloqueando la Ley de la Nube: Lo que todo líder debe saber sobre privacidad, riesgo y cumplimiento de datos”

03 de marzo de 2026

La adopción acelerada de la nube impulsada por la madurez digital, la IA y el avance hacia tecnologías cuánticas ha incrementado de forma significativa las preocupaciones sobre seguridad, privacidad y soberanía del dato. En sectores regulados como finanzas, defensa e infraestructuras críticas, este riesgo se agrava debido al **U.S. Cloud Act**, que permite a autoridades estadounidenses solicitar acceso a datos gestionados por proveedores bajo su jurisdicción, incluso cuando la información se almacena fuera de EE. UU.

Expertos de **Thales, Kyndryl y KeyFactor** explicaron cómo la extraterritorialidad del **Cloud Act** afecta también a organizaciones sin presencia en EE. UU., generando riesgos como exposición a jurisdicciones extranjeras, complejidad regulatoria en entornos multinube y pérdida de control criptográfico sobre datos distribuidos.

Se analizó también la tensión entre el **Reglamento General de Protección de Datos** (GDPR sus siglas en inglés) y normas como el **Cloud Act y Foreign Intelligence Surveillance Act** (FISA 702) , consideradas incompatibles por el Tribunal de Justicia de la Unión Europea, lo que llevó a la invalidación del Privacy Shield y reforzó la relevancia estratégica de la soberanía digital.
El webinar destacó la necesidad de incrementar el control del cliente mediante modelos de gobernanza criptográfica como BYOK, HYOK y protección End-to-End, que permiten administrar claves fuera del proveedor y reducir riesgos regulatorios.

Asimismo, se subrayó el valor de la gestión criptográfica centralizada en entornos híbridos y multinube, facilitando coherencia operativa entre AWS, Microsoft 365, Google Cloud, Oracle, Salesforce, SAP y nubes privadas.

Finalmente, se abordó la amenaza emergente Harvest Now, Decrypt Later, donde actores maliciosos roban datos cifrados hoy para descifrarlos en el futuro con computación cuántica, un riesgo crítico para información de largo ciclo de vida.

Conclusión

Las organizaciones enfrentan un doble desafío: gestionar el riesgo regulatorio transfronterizo y prepararse para un futuro poscuántico donde el cifrado tradicional podría quedar obsoleto. La soberanía digital es ya un imperativo estratégico.