NEWSLETTER

grupobeit.com

BLOG DEL CEO

En el contexto actual, la continuidad operativa ya no depende únicamente de la disponibilidad de equipos o de una infraestructura robusta...

EDICIÓN 57

SOC y NOC: la ventaja operativa de las organizaciones que no pueden detenerse
Continuidad operativa: la nueva moneda de competitividad

En un entorno donde los modelos productivos, industriales y de servicios dependen de infraestructuras digitales cada vez más complejas,

EVENTOS

Webinar | SOC como servicio para gobierno
La presión sobre las instituciones públicas para anticipar, detectar y responder a amenazas de ciberseguridad nunca ha sido tan alta.

XX Aniversario GrupoBeIT
estamos muy emocionados de compartir y celebrar contigo un momento histórico: nuestro 20º aniversario.

Edición 57

SOC y NOC: el corazón de la continuidad operativa en la era digital

Por: Elías Cedillo, Fundador y CEO GrupoBeIT

En el contexto actual, la continuidad operativa ya no depende únicamente de la disponibilidad de equipos o de una infraestructura robusta. Depende, cada vez más, de la capacidad de prevenir, analizar y responder en tiempo real a eventos que impactan tanto la operación tecnológica como los procesos productivos.

Hoy, **SOC (Security Operations Center) y NOC (Network Operations Center)** han evolucionado de funciones reactivas a componentes estratégicos del negocio. No son centros de monitoreo aislados: son aquellos componentes que permiten mantener operaciones activas, seguras y controladas.

La nueva realidad operativa

La digitalización de procesos industriales, la adopción de OT (Operational Technology), IoT y sistemas interconectados ha incrementado exponencialmente la superficie de riesgo.

Un incidente de red, una alerta no atendida o una brecha de seguridad puede derivar en:

- Paros de producción no planeados
- Pérdida de inventario o materia prima
- Incumplimientos contractuales
- Afectaciones regulatorias
- Daño reputacional y financiero

Según reportes recientes de IBM y Ponemon Institute, el **promedio global para detectar y contener un incidente supera los 270 días**, y en entornos industriales cada hora de indisponibilidad puede representar pérdidas millonarias.

Aquí es donde SOC y NOC dejan de ser mero soporte y se convierten en importantes habilitadores de continuidad operativa.

NOC: estabilidad operativa antes de que el impacto escale

El **Network Operations Center (NOC)** es responsable de la **disponibilidad, desempeño y estabilidad** de la infraestructura tecnológica:

- Redes
- Enlaces
- Servidores
- Plataformas OT e industriales
- Sistemas críticos de producción

Un NOC maduro debe no solamente responder a fallas; sino anticiparse. Mediante monitoreo continuo, correlación de eventos y análisis de desempeño, permite:

- Detectar degradaciones antes de que se conviertan en fallas
- Evitar interrupciones de líneas productivas
- Garantizar niveles de servicio
- Reducir tiempos de inactividad no planeados

En entornos donde la producción es continua, la falta de visibilidad de red es uno de los mayores riesgos operativos.

SOC: seguridad como habilitador de la operación

Mientras el NOC protege la disponibilidad, el **Security Operations Center (SOC)** protege la **integridad y la confiabilidad** de la operación.

Hoy, más del 60% de los incidentes que generan paros productivos tienen un origen en incidentes de ciberseguridad: credenciales comprometidas, malware, accesos no autorizados o errores humanos.

Un SOC permite:

- Detectar amenazas en tiempo real
- Correlacionar eventos de seguridad y operación
- Responder de forma temprana antes de impactar producción
- Reduccir el tiempo de exposición y contención
- Proteger entornos IT y OT de forma integrada

Sin SOC, los incidentes suelen detectarse cuando el daño ya ocurrió.

Hoy, la pregunta no es si ocurrirá un incidente, sino qué tan preparada está la organización para prevenirlo, detectarlo y contenerlo antes de afectar la producción.

SOC y NOC no son centros de costo. Son mecanismos de resiliencia, continuidad operativa y protección del negocio. En un entorno donde el tiempo de inactividad no es opción, la visibilidad y la respuesta temprana son la diferencia entre continuidad y crisis.

Contacto:

+52 56 5100 8613 admmarketing@buromc.com

Edición 57

NEWSLETTER BeIT

SOC y NOC: la ventaja operativa de las organizaciones que no pueden detenerse Continuidad operativa: la nueva moneda de competitividad

En un entorno donde los modelos productivos, industriales y de servicios dependen de infraestructuras digitales cada vez más complejas, la continuidad operativa se ha convertido en un diferenciador estratégico. Hoy, detener operaciones por minutos u horas ya no es una opción, especialmente en industrias como manufactura, energía, retail, salud y servicios financieros.

Las organizaciones con mayor madurez digital comparten una característica clave: **operan con visibilidad en tiempo real.** No esperan a que un incidente impacte la producción; lo detectan, lo contienen y lo corrigen antes de que el negocio lo resienta.

En este contexto, el S**OC (Security Operations Center)** y el **NOC (Network Operations Center)** se consolidan como habilitadores directos de la continuidad del negocio.

El costo real de la interrupción operativa

Los datos son contundentes. Diversos estudios confirman que el impacto de una caída operativa va mucho más allá del área de TI:

- El costo promedio global del downtime por incidentes cibernéticos oscila entre USD 5,600 y USD 9,000 por minuto, dependiendo del sector. En manufactura, la cifra puede alcanzar hasta USD 17,000 por minuto, debido a paros de líneas de producción y disrupciones en la cadena de suministro.

- Investigaciones de Aberdeen Research señalan que el 82% de las empresas ha experimentado paros no planeados en los últimos tres años, con costos que alcanzan USD 260,000 por hora en operaciones críticas.

- En 2025, Kaspersky y VDC Research estimaron pérdidas potenciales por más de USD 18 mil millones en la industria manufacturera global solo por ransomware, considerando tiempos de inactividad y mano de obra improductiva.

NOC: disponibilidad, desempeño y prevención del fallo operativo

El Network Operations Center (NOC) es responsable del monitoreo continuo de redes, servidores, plataformas OT y sistemas críticos que sostienen la operación diaria.
Organizaciones que han adoptado NOC con monitoreo proactivo 24/7 obtienen ventajas medibles:

- Hasta 70 % menos downtime comparado con organizaciones sin monitoreo proactivo, según análisis citados por Gartner.
- 98 % de las empresas con monitoreo proactivo reportan menos interrupciones, de acuerdo con datos consolidados en estudios de gestión operativa
- Estudios de Cisco indican que 80 % de las caídas de red podrían evitarse mediante detección temprana y respuesta oportuna, capacidades propias de un NOC maduro.

SOC: reducir el impacto antes de que se convierta en crisis

Si el NOC protege la disponibilidad, el SOC protege la continuidad frente a amenazas de seguridad, hoy una de las principales causas de paros operativos.

- El tiempo promedio global para identificar y contener una brecha supera los 270 días en organizaciones sin capacidades avanzadas de detección, de acuerdo con el IBM Cost of a Data Breach Report.
- El SANS 2024 SOC Survey confirma que las organizaciones con SOC formal reducen significativamente los tiempos de detección y respuesta frente a incidentes que afectan sistemas productivos y de negocio.
- Análisis comparativos de Ponemon Institute muestran que un SOC efectivo reduce el impacto financiero de una brecha en millones de dólares, al acortar el ciclo de vida del incidente.

En entornos industriales y de producción, este diferencial de tiempo es crítico: horas pueden significar millones.

SOC + NOC: cuando la operación y la seguridad avanzan juntas
El verdadero diferencial competitivo aparece cuando SOC y NOC operan de forma integrada.

Reportes de Fortinet e ISG Research señalan que la convergencia SOC–NOC permite:

- Correlacionar eventos de red y seguridad para identificar ataques que simulan fallas técnicas.
- Priorizar incidentes según impacto al negocio y producción.
- Reducir significativamente el Mean Time to Detect (MTTD) y el Mean Time to Respond (MTTR).
- Acelerar la recuperación operativa y minimizar pérdidas económicas.

Organizaciones con esta integración avanzan más rápido en resiliencia digital y presentan mayor madurez operativa frente a auditorías, clientes y aseguradoras.

Asimismo, las organizaciones que implementan SOC y NOC no solo reaccionan mejor ante incidentes: operan con ventaja. Detectan antes, responden más rápido y continúan produciendo cuando otras se detienen.

En un entorno donde el tiempo muerto se traduce directamente en pérdidas financieras y reputacionales, la continuidad operativa ya no es una aspiración técnica; es una decisión estratégica.

Contacto:

+52 56 5100 8613 admmarketing@buromc.com

Fuentes:

- Gartner — Proactive IT Monitoring & Downtime Analytics: Proactive IT Management: 20 Industry Stats You Should Know
- Ponemon Institute / IBM — Cost of a Data Breach Reports: Cost of a data breach 2025 | IBM
- Kaspersky & VDC Research — Manufacturing Ransomware Impact 2025: Kaspersky and VDC Research reveal over $18B in potential losses from ransomware attacks on the global manufacturing industry in 2025
- Aberdeen Research — Cost of Unplanned Downtime: The cost of downtime: Manufacturing's worst nightmare and how to solve it | Smart Industry
- Fortinet — Bridging the NOC–SOC Divide: Bridging the NOC-SOC Divide
- ISG Research / NTT DATA — SOC & NOC Integration Briefing: NTTData-ISG Briefing Notes
- World Bank — Economic Costs of Cyber Incidents: **World Bank Document**

Ataque de ransomware a proveedor mexicano expone riesgos operativos en cadenas de suministro

NOTICIA BeIT

A inicios de 2026, autoridades mexicanas y analistas de ciberseguridad confirmaron un ataque de ransomware dirigido a PCM, un proveedor mexicano de servicios tecnológicos, el cual provocó interrupciones operativas parciales y expuso información estratégica vinculada a procesos críticos de negocio. El ataque fue atribuido a un grupo criminal con presencia activa en América Latina, el cual logró acceder a la infraestructura mediante movimientos laterales no detectados y escasa correlación de eventos de seguridad y red. Aunque el incidente se originó en un tercero, el impacto se propagó rápidamente hacia clientes corporativos que dependían de ese proveedor para operación diaria, soporte y procesamiento de información. Expertos advirtieron que este tipo de ataques muestran cómo la falta de monitoreo continuo, detección temprana y respuesta coordinada puede convertir un incidente de seguridad en un evento de interrupción operativa, incluso para organizaciones que no fueron el objetivo inicial.

Lecciones clave para la continuidad operativa

Análisis posteriores destacaron que el incidente evidenció brechas críticas en:

- Visibilidad en tiempo real de la infraestructura, típica de organizaciones sin un NOC maduro.
- Capacidad de detección temprana de amenazas, asociada a la ausencia de un SOC 24/7.
- Falta de correlación entre eventos de red, sistemas y seguridad.
- Respuesta reactiva, cuando la afectación operativa ya era evidente.

De acuerdo con los especialistas consultados, un SOC y un NOC integrados habrían permitido identificar señales tempranas del ataque, contener la amenaza y evitar la propagación del impacto hacia clientes y procesos productivos.

Por qué SOC y NOC son críticos en este contexto

SOC y NOC permiten:

- Detectar anomalías antes de que se transformen en paros operativos.
- Evaluar el impacto real de un incidente en tiempo real.
- Tomar decisiones informadas para mantener la operación activa.
- Reducir el tiempo de indisponibilidad y el daño financiero.

El incidente confirmó que los ataques modernos no solo buscan robar información, sino interrumpir operaciones. Para organizaciones en México, 2026 deja claro que operar sin SOC y NOC es asumir un riesgo innecesario frente a amenazas que avanzan en minutos, no en días. La resiliencia operativa comienza con visibilidad.

Contacto:

+52 56 5100 8613 admmarketing@buromc.com

Fuentes:

·Filtraciones e intrusiones en México abren 2026 y el punto débil vuelve a ser humano. (2026). El Economista. Recuperado de: https://www.eleconomista.com.mx/tecnologia/filtraciones-e-intrusiones-mexico-abren-2026-punto-debil-vuelve-humano-20260204-798336.html

Webinar | SOC como servicio para gobierno

La presión sobre las instituciones públicas para anticipar, detectar y responder a amenazas de ciberseguridad nunca ha sido tan alta.

Te invitamos al webinar “SOC como servicio para gobierno” impartido por Fortinet, en el cual se analizará cómo un Centro de Operaciones de Seguridad (SOC) gestionado permite fortalecer la postura de seguridad, ampliar capacidades críticas y responder a incidentes sin incrementar la carga operativa interna.

Durante la sesión se explorará:

- Tendencias clave
- Desafíos reales que enfrentan las instituciones gubernamentales
- Recomendaciones prácticas para mejorar la detección y respuesta ante amenazas

Fecha: Miércoles 13 de mayo

🕒 10:00 a.m. – Costa Rica, El Salvador, Guatemala, Honduras, México
🕒 11:00 a.m. – Colombia, Ecuador, Panamá, Perú
🕒 12:00 p.m. – Bolivia, Chile, Puerto Rico, República Dominicana
🕒 1:00 p.m. – Argentina, Paraguay, Uruguay

👉 **Regístrate y fortalece la seguridad de tu institución:**
Microsoft Virtual Events Powered by Teams

BURÖMC SEGURIDAD INFORMÁTICA

Grupo BeIT

ELIT INFRASTRUCTURE SERVICES

20 ANIVERSARIO

En **Grupo BeIT** estamos muy emocionados de compartir y celebrar contigo un momento histórico: nuestro **20° aniversario.**

Hoy, al acercarnos a dos décadas de trayectoria, queremos invitarte a reservar la fecha para una celebración muy especial en la que conmemoraremos nuestros logros y reconoceremos las alianzas que nos han fortalecido en compañía de un invitado especial.

Save the Date

03 • JULIO • 2026