NEWSLETTER

grupobeit.com

BLOG DEL CEO

Durante décadas, los servicios en campo fueron concebidos como una función esencial; no obstante, reactiva dentro de las organizaciones...

PARTNERS

CybrHawk

En BeIT, creemos en construir alianzas que eleven la calidad y profundidad de las soluciones que ofrecemos a nuestros clientes. Por ello, nos enorgullece presentar a CybrHawk, uno de los proveedores líderes en tecnologías de seguridad...

EVENTOS BEIT

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...

NOTICIA BEIT

Ciberataque a entidades Federales

A finales de enero de 2026 ocurrió un ciberataque masivo que derivó en la filtración de 2.3 terabytes de información, exponiendo datos personales de más de 36 millones de mexicanos...

Edición 53

Field Services 2.0: La evolución operativa que transforma el servicio en campo y virtual en una ventaja competitiva

Por: Elías Cedillo, Fundador y CEO GrupoBeIT

Introducción: del soporte reactivo a la operación inteligente

Durante décadas, los servicios en campo fueron concebidos como una función esencial; no obstante, reactiva dentro de las organizaciones. El modelo tradicional se basaba en responder a fallas: un equipo se detenía, un cliente levantaba un ticket y un técnico era enviado para resolver el problema. Aunque funcional, este esquema generaba altos costos, tiempos de inactividad prolongados y experiencias inconsistentes para el cliente. Hoy ese enfoque resulta insuficiente. La digitalización, la integración de Inteligencia Artificial (IA), la presión por mayor eficiencia operativa y las expectativas de inmediatez del mercado han impulsado un cambio profundo. En este contexto surge Field Services 2.0, un modelo que combina movilidad, analítica de datos, inteligencia artificial e IoT para convertir el servicio en campo en un proceso predictivo, automatizado y estratégico.

La evolución no es únicamente tecnológica. Representa una nueva forma de entender el servicio: no como un gasto necesario, sino como un diferenciador competitivo capaz de impactar directamente en ingresos, fidelización y continuidad del negocio.

La digitalización como base del nuevo modelo

Field Services 2.0 parte de un principio claro: no se puede optimizar lo que no se mide ni se conecta. Por ello, el primer paso ha sido la digitalización integral de las operaciones.

La adopción tecnológica en la industria ya es significativa. Estudios del sector muestran que alrededor del 70 % de las organizaciones de servicios en campo utilizan plataformas SaaS para gestionar órdenes de trabajo, inventarios y programación, mientras que cerca del 90 % opera sobre infraestructuras en la nube. Esta transición ha permitido visibilidad en tiempo real, colaboración entre equipos y escalabilidad operativa.

En paralelo, el trabajo móvil se ha convertido un estándar. Aproximadamente el 85 % de los técnicos utiliza aplicaciones móviles para recibir asignaciones, registrar evidencias, capturar firmas digitales y actualizar estatus desde el sitio. Esta conectividad elimina procesos manuales, reduce errores administrativos y brinda datos para acelerar la toma de decisiones.

La consecuencia directa es una operación más coordinada, donde cada intervención se registra, analiza y mejora de forma continua.

Inteligencia artificial y automatización: eficiencia a escala

Una vez digitalizada la operación, el siguiente paso natural es automatizarla. Aquí es donde la inteligencia artificial adquiere un papel protagónico.

Los sistemas actuales de Field Service Management pueden asignar órdenes de trabajo automáticamente según habilidades, ubicación, disponibilidad y prioridad del incidente. También son capaces de predecir tiempos de llegada, optimizar rutas y recomendar acciones basadas en históricos de desempeño.

La percepción de los propios técnicos respalda esta evolución. Investigaciones del sector indican que el 81 % considera que los agentes de IA pueden hacer su trabajo más eficiente. Las organizaciones que ya han integrado estas capacidades reportan mejoras medibles: hasta un 88 % de incremento en la utilización de técnicos y un 85 % de mejora en la productividad de los despachadores.

Más allá de los porcentajes, el impacto real se traduce en menos tiempos muertos, menos traslados innecesarios y más intervenciones exitosas por jornada. En otras palabras, mayor valor con los mismos recursos.

Experiencia del cliente y resultados operativos

Uno de los errores más comunes es pensar que la modernización del servicio en campo solo beneficia a la operación interna. En realidad, el mayor impacto se refleja en el cliente.

Las soluciones modernas de Field Service Management han demostrado incrementos de hasta 31 % en la resolución durante la primera visita. Este indicador es clave, ya que reduce segundas intervenciones, costos adicionales y frustración del usuario. Al mismo tiempo, se ha observado un aumento cercano al 32 % en la productividad de trabajadores móviles y una reducción de aproximadamente 26 % en desplazamientos, lo que impacta tanto en eficiencia financiera como en sostenibilidad ambiental.

Cuando el servicio es más rápido, preciso y predecible, la percepción de calidad mejora de manera inmediata. En sectores como telecomunicaciones, energía, manufactura o servicios industriales, esta experiencia puede ser el principal factor de retención de clientes.

Del mantenimiento correctivo al predictivo

Quizá el cambio más relevante que introduce Field Services 2.0 es el paso de la reacción a la anticipación.

La integración de sensores IoT y analítica avanzada permite monitorear activos críticos de forma continua. En lugar de esperar a que ocurra una falla, los algoritmos detectan patrones anómalos y generan alertas tempranas para intervenir antes de que el problema escale.

Este enfoque predictivo reduce interrupciones no planificadas, optimiza inventarios de refacciones y extiende la vida útil de los equipos. Además, transforma la relación con el cliente: la organización deja de "arreglar fallas" para "prevenir incidentes". Operativamente, esto significa menos emergencias, mejor planificación y costos más controlados. Estratégicamente, implica mayor confiabilidad y reputación de marca.

Aunado a esto, la integración de **SOC y NOC** impulsa directamente la continuidad operativa porque unifica la visibilidad sobre seguridad y desempeño de la red, reduciendo tiempos de detección y respuesta ante incidentes. Splunk proyecta que la fusión SOC–NOC, habilitada por IA y gestión federada de datos, permite correlacionar anomalías de rendimiento con señales de ataques, revelando patrones que antes pasaban desapercibidos y evitando interrupciones mayores en la operación. Cisco coincide en que compartir telemetría, herramientas y flujos ITSM entre ambos centros mejora la triage inicial, agiliza la escalación y fortalece la capacidad de contener incidentes antes de que impacten al negocio, especialmente en infraestructuras distribuidas y servicios críticos de TI.

Implicaciones estratégicas para las organizaciones

Adoptar este modelo implica más que implementar software. Requiere integrar datos, procesos y personas bajo una misma estrategia. Las organizaciones más exitosas alinean sus áreas de servicio, operaciones, tecnología y experiencia del cliente para generar visibilidad completa del ciclo de atención.

El valor real surge cuando la información del servicio híbrido (en campo y virtual) alimenta decisiones ejecutivas: planificación de capacidad, inversión en activos, diseño de contratos de servicio y nuevas oportunidades comerciales. En este punto, el servicio deja de ser reactivo y se convierte en una fuente constante de inteligencia de negocio.

Conclusión: el servicio en híbrido como motor de competitividad

Field Services 2.0 representa la madurez del servicio en campo e integración del virtual. Combina conectividad, automatización, datos y anticipación para ofrecer operaciones más eficientes y experiencias superiores para el usuario. Los resultados muestran mejoras claras en productividad, reducción de costos y calidad de servicio, mientras que la analítica predictiva abre la puerta a modelos completamente proactivos.

En un mercado donde la rapidez y la confiabilidad determinan la lealtad, mantener procesos manuales o desconectados ya no es sostenible. Las organizaciones que adopten esta evolución no solo resolverán incidentes con mayor eficacia, sino que posicionarán el servicio como un verdadero diferenciador estratégico.

El futuro del campo no es reaccionar mejor, sino anticiparse con inteligencia. Consulta más de nuestra solución Field Services 2.0 en: Field services – GrupoBelT | Liderazgo en Tecnología e Innovación

Contacto:

+52 56 5100 8613 admmarketing@buromc.com

Fuentes:

- Salesforce – Field Service Trends & Industry Insights: https://www.salesforce.com/service/field-service-management/trends/
- Salesforce – Field Service Management Impact Metrics: https://www.salesforce.com/service/field-service-management/
- Zipdo Research – Field Services Industry Statistics: https://zipdo.co/field-services-industry-statistics/
- Fieldwork – Field Service Management Trends & Automation: https://fieldworkhq.com/

Ciberataque a entidades Federales

NOTICIA BeIT

A finales de enero de 2026 ocurrió un ciberataque masivo que derivó en la filtración de 2.3 terabytes de información, exponiendo datos personales de más de 36 millones de mexicanos. El ataque fue atribuido al grupo de ciberdelincuentes Chronus o Cronus, que publicó la información robada en la deep web. Entre las instituciones afectadas se encuentran el SAT, IMSS, IMSS Bienestar, SEP, Secretaría de Salud, gobiernos estatales y municipales, además del partido Morena, cuyo padrón de afiliados también fue filtrado.

Los datos expuestos incluyen nombres completos, domicilios, CURP, RFC, números de seguridad social, teléfonos y correos institucionales, lo que representa un riesgo significativo de robo de identidad y otros delitos cibernéticos. Incluso la Comisión Nacional de Seguros y Fianzas (CNSF) confirmó una vulneración adicional en sus sistemas, aunque en su caso se trató de información mayormente pública.

Expertos consultados por Salles Sainz Grant Thornton señalaron que el incidente revela fallas estructurales en la estrategia nacional de ciberseguridad, destacando problemas como baja inversión tecnológica, legislación insuficiente y una alta rotación de proyectos dentro de las administraciones públicas. Estas debilidades institucionales amplificaron el alcance del ataque y la exposición de datos sensibles.

Además, especialistas advirtieron que el ataque ocurrió en un momento especialmente vulnerable, coincidiendo con el inicio del Mundial, periodo en el que aumenta el tráfico digital y proliferan sitios y aplicaciones falsas. Esto incrementa las

probabilidades de engaños, suplantación de identidad y fraudes dirigidos tanto a ciudadanos como a instituciones.

Hasta el momento, no existe un informe técnico oficial que detalle cómo ocurrió la intrusión. Sin embargo, los análisis disponibles indican que el ataque explotó debilidades en infraestructura digital y protocolos de seguridad que no han sido actualizados en años. La dimensión del hackeo, que compromete información de alrededor de una cuarta parte de la población mexicana, lo convierte en uno de los incidentes más graves en la historia reciente del país.

👉 Si tu organización necesita fortalecer su seguridad digital, implementar controles modernos o prevenir brechas como ésta, nosotros podemos ayudarte.

📩 Contáctanos hoy mismo para comenzar a blindar tu infraestructura tecnológica antes de que ocurra un incidente:

Contacto:

+52 56 5100 8613 admmarketing@buromc.com

Fuentes:

Ciberataque a SAT, IMSS y Morena exhibe fallas en ciberseguridad y expone datos de 36 millones

En BeIT, creemos en construir alianzas que eleven la calidad y profundidad de las soluciones que ofrecemos a nuestros clientes. Por ello, nos enorgullece presentar a CybrHawk, uno de los proveedores líderes en tecnologías de seguridad, especializado en SIEM y XDR, con capacidades avanzadas para ofrecer visibilidad completa, detección proactiva y respuesta rápida ante amenazas. La plataforma CybrHawk SIEM/XDR destaca por su capacidad de analizar datos provenientes de múltiples fuentes para detectar y prevenir ataques sofisticados, proporcionando visibilidad integral del entorno digital y reduciendo tiempos de respuesta mediante analítica avanzada y automatización. Su portafolio abarca capacidades de protección, detección, threat intelligence, respuesta a incidentes y monitoreo continuo, elementos esenciales en una postura de seguridad moderna.

Nuestra alianza con CybrHawk nos permite integrar estas capacidades dentro de nuestras soluciones, fortaleciendo tanto operaciones de seguridad como estrategias de gobernanza y protección de activos críticos. Gracias a su tecnología, podemos ofrecer a nuestros clientes ecosistemas más resilientes y una postura de seguridad que evoluciona al ritmo de las amenazas actuales. Juntos, combinamos experiencia, capacidad técnica y tecnología avanzada para entregar soluciones que garantizan protección, continuidad y confianza en cada etapa del negocio.
Si quieres fortalecer tu infraestructura con tecnología SIEM/XDR una implementación experta, contáctanos:

Contacto:

+52 56 5100 8613 admmarketing@buromc.com

Hola es un gusto saludarte,

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.

Por ello, queremos invitarte a nuestro evento:

Protección de la Información: Estrategia de Seguridad

Un enfoque integral para blindar tus datos, cumplir normativas y fortalecer tu operación.
Durante esta sesión, presentaremos una solución diseñada para fomentar un nivel de seguridad de la información robusto, alineado tanto con las necesidades internas 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. Arexdata

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?

✓ Comprenderás cómo adaptar una estrategia de seguridad a las necesidades particulares de tu organización.

✓ Verás cómo integrar nuestros tres pilares para fortalecer la protección de tus activos de información.

✓ Obtendrás recomendaciones prácticas para elevar tu postura de seguridad y cumplir normativas vigentes.

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

Modalidad
Presencial (en Saks Polanco) y virtual.
Será un gusto contar con tu participación y acompañarte en la evolución de tu estrategia de ciberseguridad.

Contáctanos para saber que contaremos con tu participación:
WhatsApp +52 56 5100 8613, e-mail: admmarketing@buromc.com