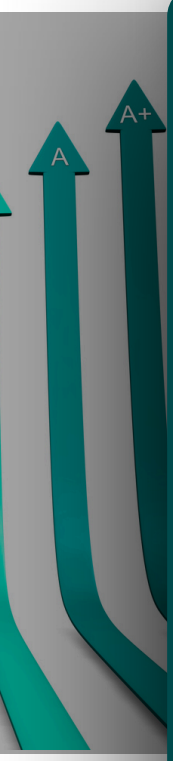
Abril 2025

NEWSLETTER BeIT

Edición Semanal #27



Protección de datos sensibles

En junio y agosto de 2024, **Gartner, Inc.** realizó una encuesta entre 318 líderes de seguridad sénior de organizaciones de diversas industrias y tamaños a nivel mundial. Un dato revelador de esta encuesta es que solo el 14% de los líderes de seguridad pueden proteger eficazmente los activos de datos de la organización y, al mismo tiempo, permitir el uso de los datos para alcanzar los objetivos del negocio.

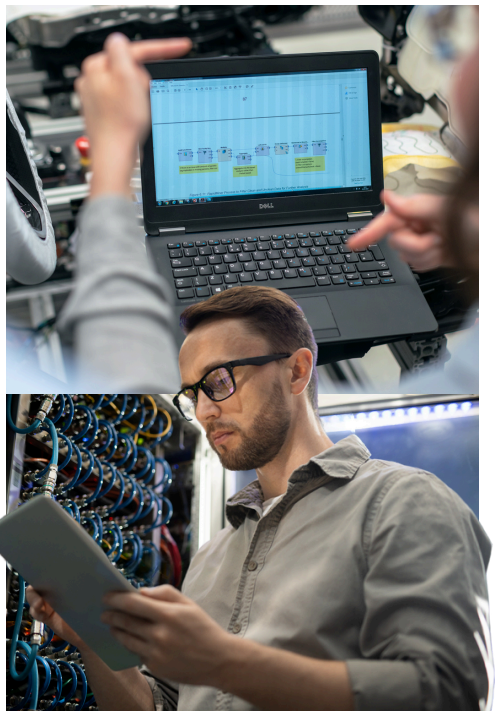
IBM destaca que los ciberataques tienen un impacto enorme y creciente en las empresas y la economía global. Según una estimación, la ciberdelincuencia costará a la economía mundial 10.5 billones de dólares anuales para 2025.

Leer ahora

Field Services 2.0 impulsa la eficiencia y la satisfacción del cliente

BLOG BeIT

Por: Elías Cedillo , *CEO Grupo BeIT*



La gestión de servicios de campo (Field Services Management, FSM) no solo es hablar de la gestión de activos, sino también de valor empresarial. Actualmente la eficiencia operativa, la optimización de recursos y la satisfacción del cliente son cruciales para el éxito. Aunque no es la única fórmula para lograrlo, se podría decir que es la más eficaz.

FSM se ha convertido en una herramienta esencial para las empresas que buscan optimizar y mejorar sus operaciones. Empresas como IBM, Mordor Intelligence e IDC proporcionan información valiosa que nos ayudará a entender mejor este campo y a sacar nuestras propias conclusiones.

Referirse al mercado de **FSM** es encontrarse con desafíos y oportunidades. Entre los desafíos se incluyen la complejidad de la integración, la escasez de talento y la intensa competencia en el mercado. Sin embargo, al adoptar la transformación digital, invertir en soluciones avanzadas como FSM y priorizar la entrega de servicios centrados en el cliente, las organizaciones pueden capitalizar estas oportunidades y superar los desafíos para tener éxito.

IDC menciona que el 47% de las organizaciones pueden reducir el tiempo de inactividad no planificada, aumentar la vida útil promedio de los activos en un 17% y mejorar la productividad de sus técnicos en un 26%.

El mercado de FSM está en expansión. Según **Mordor Intelligence**, el tamaño del mercado de FSM se estimó en 5.52 mil millones de dólares en 2025 y se espera que alcance 9.60 mil millones de dólares para 2030, con una tasa de crecimiento anual compuesta (CAGR) del 11.7%. Este crecimiento está impulsado por la adopción de soluciones basadas en la nube y la demanda de servicios más automatizados y eficientes.

IBM nos dice que conforme los activos se vuelven más complejos, las empresas deben adaptar sus métodos de gestión de servicios de campo. El futuro de esta gestión radica en fortalecer al técnico conectado, permitiéndole trabajar con cualquier activo, en cualquier momento, en cualquier lugar y utilizando cualquier nube.

Toda esa conceptualización la entendemos y aplicamos como Grupo BeIT, entendemos que la gestión de servicios de campo es más que una necesidad operativa; es una ventaja estratégica y competitiva. Al implementar soluciones avanzadas como Field Services 2.0, optimizamos nuestros recursos y mejoramos la eficiencia operativa, también de nuestros clientes. Al estar comprometidos, liderar con innovación y excelencia, asegurando cada vez más beneficios, como el cumplimiento de normativas de ciberseguridad.

Brindar un enfoque holístico es fundamental para proteger a la empresa desde sus usuarios. Esto incluye minimizar la superficie de ataque y prevenir compromisos mediante protección avanzada contra amenazas basadas en aprendizaje automático (ML). Además, se emplean técnicas de engaño y aislamiento para fortalecer aún más la seguridad. La protección de datos es crucial para prevenir la pérdida de información, tanto en línea como fuera de banda.

Abarcar la protección de infraestructuras como servicio (IaaS) y plataformas como servicio (PaaS) mediante soluciones CNAPP (plataforma de protección de aplicaciones nativas en la nube). También es vital ya que nos ayuda a resguardar los datos en plataformas SaaS, utilizando clasificación y controles avanzados de datos para asegurar su integridad y confidencialidad.

La conectividad "ZERO TRUST" se debe centrar en conectar aplicaciones en lugar de redes, para prevenir movimientos laterales no autorizados (ZTNA). Este enfoque incluye conectividad para sitios remotos y fábricas, así como conectividad multi nube. La segmentación de usuarios y aplicaciones, el perfilamiento y cumplimiento con los recursos de implementación son esenciales para mantener la seguridad sin romper políticas establecidas, asegurando una homologación adecuada para el uso de recursos e información.

Otro punto válido y necesario es la gestión de la experiencia digital, siendo clave para identificar y resolver problemas de rendimiento. El monitoreo punta a punta, que abarca desde el terminal hasta la red y las aplicaciones, es fundamental. Además, el monitoreo de servicios de comunicación unificada (UCaaS) como Zoom y Teams, permite asegurar una experiencia de usuario óptima y sin interrupciones.

En conclusión, la gestión de servicios de campo además de una herramienta operativa, ofrece la protección de datos y conectividad, basados en una gestión de experiencia digital más integral, permitiendo a las organizaciones prosperar en un entorno cada vez más vulnerable.

> *Las empresas con un gran equipo de campo tienen más razones que nunca para mejorar su eficacia y eficiencia. Las nuevas opciones tecnológicas pueden ayudar a superar las antiguas barreras para un mayor rendimiento.*

Guy Benjamin , Harrison Lung , y Murali de Raghu
McKinsey & Company

Fortinet en su informe global de investigación sobre concientización y formación en seguridad 2024 reveló que el 62% de las organizaciones espera que sus empleados sean víctimas de más ciberataques en el futuro, debido al uso malicioso de la inteligencia artificial (IA) por parte de los atacantes. Este dato subraya la necesidad urgente de fortalecer la formación y concientización en seguridad dentro de las empresas.

En otro de sus informes en el mismo año 2024, Cybersecurity Skills Gap, destacó las graves consecuencias que los ciberataques pueden tener para los altos directivos. Dentro de ese informe, mencionó que el 51% de las organizaciones afirmaron que sus altos directivos se han enfrentado multas (34%), penas de cárcel (16%) y pérdida de posición o empleo (33%) tras un ciberataque. Estas cifras reflejan la creciente responsabilidad y el riesgo personal que enfrentan los líderes empresariales en el ámbito de la ciberseguridad.

Sin duda alguna, el tamaño y la escala de las empresas atraer más ciberatacantes. Las organizaciones de cierto tamaño y de ciertas industrias tienden a experimentar múltiples ataques. El 36% de las empresas con 1,000-2,499 empleados informaron de cinco o más ataques en los últimos 12 meses, frente al 35% en 2022. De manera similar, el 34% de las empresas con 2,500-4,999 empleados reportaron cinco o más ataques, comparado con el 38% en 2022. Las empresas de petróleo y gas experimentaron la mayor incidencia de múltiples ataques de cualquier industria, con un 56% citando cinco o más, frente al 34% en 2022.

Los ciberataques son cada vez más sofisticados y ponen en riesgo infraestructuras esenciales como energía, transporte y telecomunicaciones. **Fortinet**, en su artículo "Cómo proteger la seguridad digital en las infraestructuras críticas" (2021), ya mencionaba que las infraestructuras críticas son vitales, y su seguridad puede ser un tema de seguridad nacional y económica, lo que las hace más visibles y objetivos para los ciberdelincuentes.

Los ataques actuales son rápidos y automatizados, realizados por grupos bien financiados que utilizan inteligencia artificial para encontrar y estructurar mejor las vulnerabilidades. La ciberseguridad debe incluir herramientas de automatización y redes que se auto protejan. Aislar las infraestructuras críticas no es suficiente, ya que las cadenas de suministro de software pueden ser comprometidas.

Las vulnerabilidades comunes incluyen sensores industriales, firewalls antiguos y sistemas de seguridad mal configurados. La superficie de ataque se amplía con la digitalización y el Internet de las Cosas (IoT), lo que requiere un cambio de mentalidad hacia una ciberseguridad de extremo a extremo.

Una **encuesta** reveló que la mayoría de las organizaciones han sufrido intrusiones en sus sistemas OT, afectando la eficiencia operativa y la seguridad física. La mejor manera de proteger las infraestructuras críticas es implementar una plataforma de ciberseguridad integral que ofrezca visibilidad centralizada y manejo simplificado. Esta debe ser una prioridad inmediata para organizaciones y gobiernos.

Hablar de vulnerabilidades, no solo es comunicar que existió un filtración, robo o encriptado de datos; también es hablar de daños financieros, reputacionales, insolvencias y hasta cierre de operaciones. A continuación te dejamos vario casos dentro de alguna de los sectores y/o industrias.

Sector Salud

Una **publicación** en un foro de hackers popular entre los ciberdelincuentes el 4 de Marzo del 2024, afirmó que UnitedHealth Group (UNH.N) pagó 22 millones de dólares en un intento por recuperar el acceso a los datos y sistemas cifrados por la banda de ransomware "Blackcat", según dos investigadores. Ni UnitedHealth ni los piratas informáticos involucrados han comentado sobre el supuesto pago de rescate, aunque una firma de rastreo de criptomonedas corroboró parcialmente la afirmación.

Sector Retail - Alimento y Bebidas

El ejemplo lo podemos tener en 2017 donde **Mondelez International** fue vulnerado por el ransomware NotPetya, creado en Ucrania en 2017. Este ciberataque afectó a más de 24,000 laptops y 1,700 servidores, generando un paro no planeado y un impacto financiero que se reflejó en pérdidas superiores a los 100 millones de dólares.

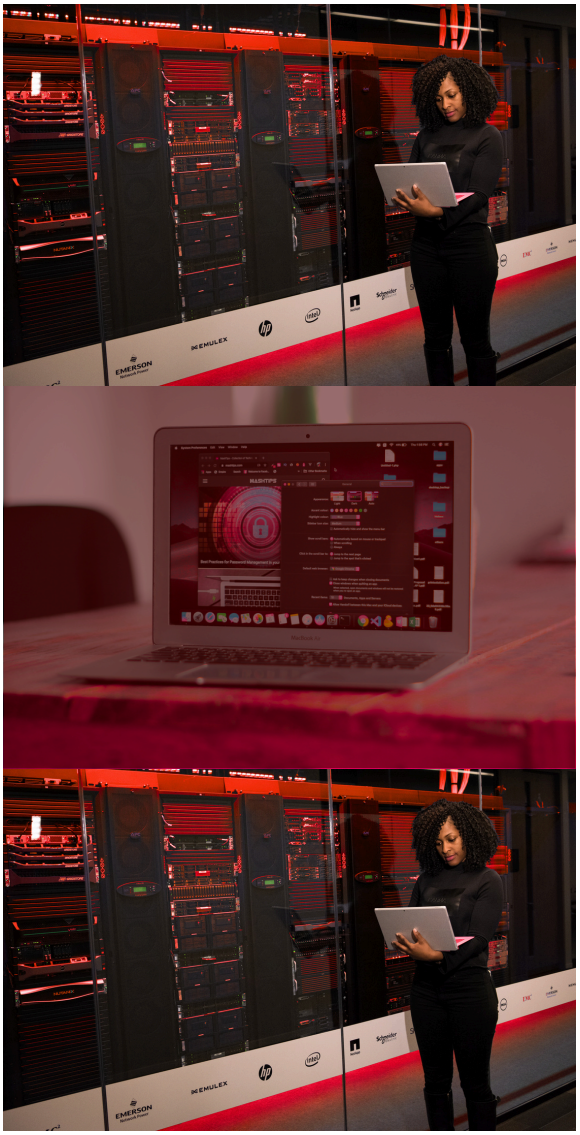
Sector Energía y Petróleo

En Latinoamérica, el 2 de septiembre de 2024 la empresa colombiana **Air-e** que distribuye y comercializa energía eléctrica en los departamentos de Atlántico, Magdalena y La Guajira sufrió un serio ataque de ransomware, el cual afectó sus sistemas y hasta dejó a los usuarios sin poder acceder a servicios como el pago de facturas a través de su sitio web. No solo la capacidad operativa de Air-e se vio afectada, sino que hubo retrasos en la atención de sus clientes, y hasta su gestión financiera y las operaciones logísticas quedaron paralizadas.

Como podemos observar, la afectación a las operaciones de los diversos sectores, y aún más a las infraestructuras críticas, se ha convertido en una prioridad tanto para las organizaciones privadas como gubernamentales. Estas infraestructuras se vuelven cada vez más atractivas para los ciberdelincuentes debido a su importancia estratégica.

Además, estas vulnerabilidades pueden llevar al cierre de operaciones o incluso a la declaración de insolvencia, como le sucedió a la empresa alemana de manipulación de materiales a granel **Kreisel GmbH & Co.**, que se declaró insolvente el 19 de noviembre de 2024. Este desenlace fue resultado de una combinación de factores, incluyendo un devastador ciberataque ocurrido en febrero de 2024.

La protección de infraestructuras críticas es esencial para la seguridad y la economía de las organizaciones. La implementación de un ecosistema o una plataforma de ciberseguridad integral debe ser una prioridad inmediata para organizaciones y gobiernos, garantizando visibilidad centralizada y manejo simplificado para enfrentar las amenazas cada vez más sofisticadas de los ciberdelincuentes.



La semana del 7 de Abril , nuestro equipo continuó con su compromiso. En esta ocasión, se embarcaron en una capacitación intensiva con nuestro socio en ciberseguridad, Fortinet. Esta colaboración nos permitió profundizar en conocimientos críticos y fortalecer nuestras habilidades en un área vital para la seguridad de las operaciones.

El enfoque principal de la capacitación fue la "Ciberseguridad de OT" (Tecnología Operacional). Siendo un tema de suma importancia, ya que la protección de los sistemas operativos industriales es crucial para prevenir posibles amenazas y garantizar la continuidad de las operaciones. Gracias a la experiencia y el apoyo de Fortinet, nuestro equipo pudo adquirir nuevas estrategias y técnicas avanzadas para enfrentar los desafíos actuales en este campo.

Estamos orgullosos de los logros alcanzados y confiamos en que esta formación contribuirá significativamente a brindar la mejor atención y soporte a nuestros clientes. La colaboración con Fortinet ha sido invaluable, y estamos entusiasmados por aplicar estos conocimientos en nuestras operaciones diarias, asegurando así un entorno más seguro y resiliente para todos.

Ciberseguridad en el Sector Industrial

Control de Accesos

En el año 2024, la ciberseguridad en el sector industrial ha cobrado una importancia sin precedentes debido al incremento de amenazas y vulnerabilidades. Proteger las infraestructuras industriales es vital para asegurar la continuidad de las operaciones y la integridad de los datos. En este escenario, el control de accesos se destaca como un componente esencial. Las nuevas tecnologías en control de accesos, incluyendo la integración del Internet de las Cosas (IoT) y la inteligencia artificial, están revolucionando la gestión de la seguridad en las empresas. Estas innovaciones permiten una vigilancia más eficiente y una respuesta rápida ante posibles intrusiones, garantizando que solo el personal autorizado pueda acceder a áreas críticas.