



# SERVICIOS DE CIBERSEGURIDAD

ASEGURAMOS SUS OPERACIONES ESENCIALES

# LOS CIBERATAQUES SON UNA REALIDAD. Y LOS RIESGOS SON ALTOS.

Para las organizaciones que tienen la tarea de gestionar operaciones esenciales, cualquier tiempo de inactividad de sus sistemas pone vidas en riesgo cuando fallar no es opción. Pero los ciberataques siguen aumentando en cantidad, frecuencia e impacto. De hecho, se espera que el costo anual de los daños del cibercrimen alcance los \$5 billones de dólares en 2020.<sup>1</sup>

El malware, ransomware, phishing, ataques de intermediarios, ataques distribuidos de negación de servicio, inyecciones de SQL y ataques con vulnerabilidades de día cero son algunas de las agresiones usuales que podrían interrumpir operaciones esenciales de manera imprevista. Muy a menudo, se crean estrategias de seguridad para “marcar la casilla” de cumplimiento de seguridad o como reacción a un ataque específico. Claramente, las estrategias usadas en el pasado para asegurar las operaciones esenciales son inadecuadas para protegerse contra las actuales amenazas cibernéticas, las cuales siguen avanzando.

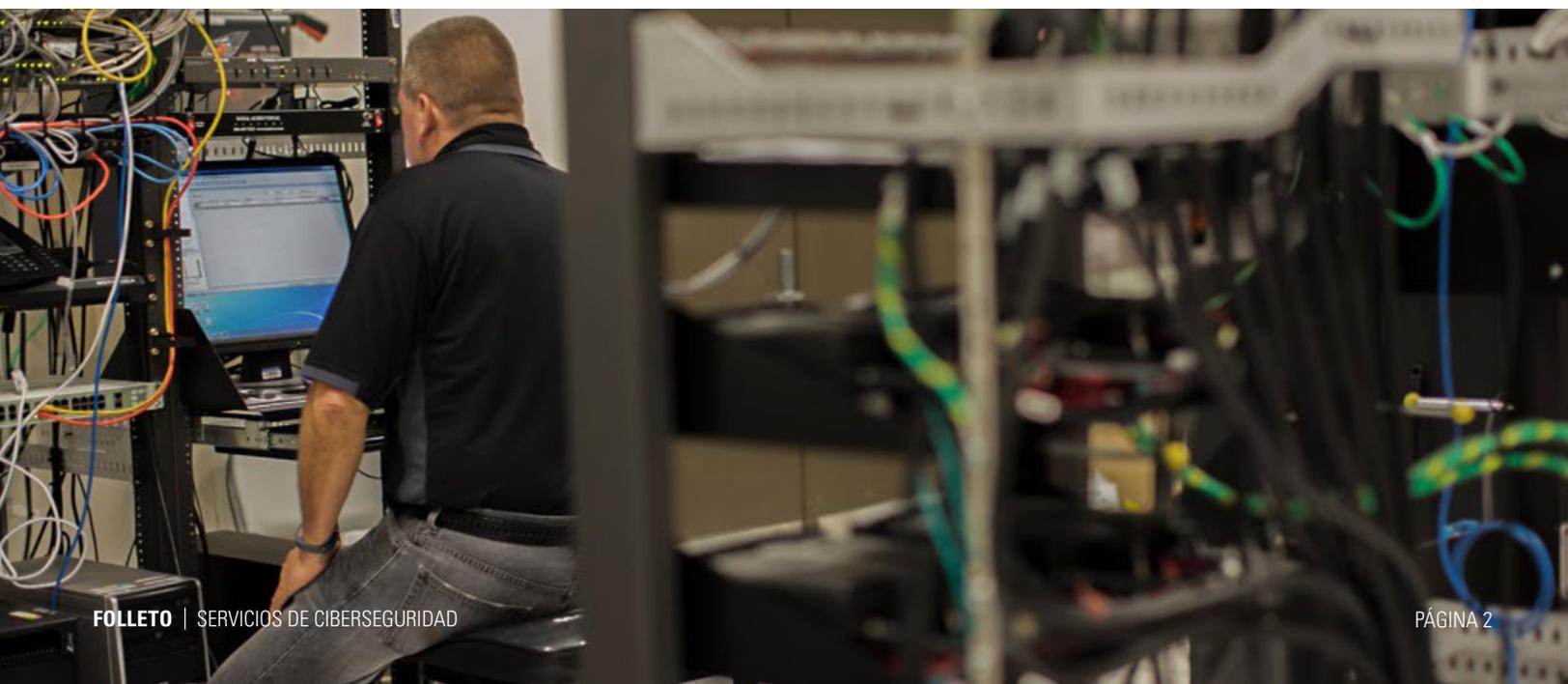
La incertidumbre y las implicaciones de los ciberataques han hecho que la ciberseguridad sea la preocupación principal de las organizaciones. Los avances en las técnicas de ciberataques y un sistema basado en IP que evoluciona constantemente están poniendo una presión incesante sobre los recursos internos. Existe una necesidad constante de actualizar las habilidades y pericia para poder administrar un ambiente complejo y reforzar la resiliencia cibernética. Adicionalmente, las inversiones en las herramientas de seguridad de última generación para

prevenir y combatir amenazas sofisticadas siguen representando un reto, ya que las organizaciones están enfrentando reducciones presupuestales.

¿Qué se necesita? Un enfoque holístico sobre ciberseguridad, con una mentalidad centrada en los riesgos y que se enfoque en opciones de mitigación, monitoreo continuo, diagnóstico y remediación. Podemos ayudarle.

Contamos con una línea de productos y servicios de seguridad que abarcan su ecosistema esencial: redes, software de centro de comando, video y radios. Evolucionamos nuestro portafolio continuamente para garantizar que cuente con la resiliencia cibernética para mantenerse un paso adelante a los sofisticados ataques que van en aumento.

Con la articulación continua de nuestros talentos altamente especializados, procesos de seguridad líderes en la industria y herramientas de vanguardia, le ayudamos a administrar la complejidad de la ciberseguridad para que pueda enfocarse en su misión principal.



# ASEGÚRESE CON MOTOROLA SOLUTIONS: SERVICIOS PARA LA RESILIENCIA CIBERNÉTICA

Nuestro enfoque de ciberseguridad incluye un conjunto de servicios holísticos que van desde la valoración de riesgos y consultoría hasta los parches y monitoreo de seguridad. Adicionalmente, estamos expandiendo el portafolio para incluir servicios de respuesta y recuperación, así como capacitación en ciberseguridad. Todas nuestras ofertas siguen de cerca al Marco de Trabajo de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos, el cual se enfoca en ayudar a que las organizaciones administren la concientización sobre riesgos cibernéticos, su detección, respuesta y recuperación.

## MARCO DE TRABAJO DE CIBERSEGURIDAD DEL NIST, LÍDER EN LA INDUSTRIA



### IDENTIFIQUE



### PROTÉJASE



### DETECTE



### RESPONDA



### RECUPÉRESE

IDENTIFIQUE	PROTÉJASE	DETECTE	RESPONDA	RECUPÉRESE
<p><b>Evalúe riesgos</b></p> <p>Activos y sistemas de inventario crítico</p> <p>Proporcione un análisis de riesgos exhaustivo</p>	<p><b>Desarrolle salvaguardas</b></p> <p>Desarrolle políticas, procedimientos; introduzca herramientas de protección</p> <p>Implemente controles de acceso y auditoría adecuados</p>	<p><b>Descubra oportunamente</b></p> <p>Monitoreo continuo 24/7/365</p> <p>Habilite las capacidades de auditoría</p>	<p><b>Tome acción</b></p> <p>Establezca un plan de respuesta robusto</p> <p>Cree, analice, clasifique y responda a los eventos detectados</p>	<p><b>Restablezca la funcionalidad</b></p> <p>Instituya un plan de recuperación</p> <p>Cree mejoras para prevenir ataques futuros</p>

## SERVICIOS DE CIBERSEGURIDAD



# CONSULTORÍA Y VALORACIÓN DE RIESGOS

Con base en nuestras décadas de experiencia trabajando de cerca con agencias de seguridad pública, gobiernos y clientes empresariales, hemos redefinido una valoración administrativa de riesgos reproducible y sistemática que le permite entender mejor su ambiente de seguridad específico. Esto abarca todo su ecosistema de tecnologías, incluyendo el centro de comando, redes LMR, radios y cámaras de video.

Comenzamos con una valoración previa para entender sus requisitos y necesidades específicas, aplicamos una mezcla de observación física, entrevistas presenciales y herramientas tanto comerciales como personalizadas. Posteriormente, realizamos la valoración en el sitio para garantizar el apego con el Marco de Trabajo del Seguridad del NIST, evaluamos los escenarios de riesgo potenciales y valoramos los riesgos potenciales a la confidencialidad,

integridad y disponibilidad del sistema de comunicación de sus organizaciones. Después de la valoración, entregamos un plan claro con pasos de mitigación tales como cambios en la arquitectura de seguridad, integración de productos específicos o instrumentación de nuevos controles procedimentales. Todos los riesgos se identifican, entienden claramente y priorizan.

Al finalizar la valoración, recibirá una tarjeta de puntuación de riesgos que prioriza cada hallazgo con base en severidades baja, moderada, alta y crítica. A cada hallazgo le sigue una remediación o recomendaciones de aceptación de riesgo. Finalmente, con base en las brechas identificadas, podemos presentarle tecnologías nuevas y proporcionar servicios que le ayudarán a continuamente sobrellevar amenazas de seguridad.

## PROCESOS REPETIBLES, EVALUACIÓN Y CONCIENTIZACIÓN CONTÍNUA



## PARCHES DE SEGURIDAD

Los parches de seguridad son una de las herramientas más importantes que a menudo se pasan por alto y que sirven para defenderse contra los ciberataques. Todo el software, sistemas y dispositivos necesitan parches continuos para mantenerse seguros. Trabajaremos con usted en tres fases: identificación, pruebas e instalación, para garantizar que sus procedimientos de parchado sean tan eficientes y seguros como sea posible.

Primero, nuestro laboratorio especializado de seguridad informática identifica y valida las actualizaciones de seguridad para ubicar cualquier brecha en los parches de su sistema. Todos los activos de hardware y software, flujos de comunicación y redes y dependencias se identifican, mapean, clasifican y administran de acuerdo con su criticidad. Si bien es importante aplicar parches tan pronto como sea posible y se lancen al mercado, para los sistemas esenciales es de total importancia probarlos

exhaustivamente antes de su despliegue. El servicio de actualizaciones de seguridad de Motorola Solutions prueba previamente las últimas definiciones antimalware y todos los parches de software aplicables en los laboratorios de pruebas especializados. Una vez que se validan como seguras, trabajamos de cerca con usted en la fase de instalación. Haremos actualizaciones para usted o las pondremos a su disposición en nuestra red externa segura para que las pueda implementar a fin de que su organización pueda desplegarlas fácilmente bajo sus propias condiciones.

Los sistemas viejos no se pueden parchar efectivamente. Las redes esenciales basadas en IP de hoy en día requieren mejoras frecuentes para mantenerse actualizadas. Motorola Solutions proporciona mejoras de sistema para habilitar las actualizaciones en tecnologías de hardware y software a lo largo de su infraestructura mientras garantiza la disponibilidad de sus sistemas.

# MONITOREO DE SEGURIDAD

El monitoreo de seguridad remoto le proporciona la forma más segura y económica de monitorear sus redes. Nuestras capacidades de monitoreo remoto permiten que tenga una protección 24/7/365, las entregan nuestros expertos técnicos y se respalda con automatización.



Utilizamos un proceso sistemático para detectar, analizar, investigar, resolver y reportar los incidentes para proteger su sistema.

**DETECTE AMENAZAS POTENCIALES** - Sus sistemas de Motorola Solutions están preconfigurados con sensores de detección de intrusiones, integración de servidores de registro y autenticación e integración con antivirus para detectar virus, gusanos y otras formas de software malintencionado. El sistema también se alimenta constantemente con la información sobre amenazas de los sitios de noticias globales y de redes sociales. Existen herramientas listas para capturar y examinar las bitácoras de sistema a lo largo de su infraestructura de red, dispositivos, sistemas operativos, software y aplicaciones. Si se detecta un efecto de intrusión o malware en su sistema, se generará una alerta y se tomarán las acciones pertinentes.

**ANALICE DATOS AUTOMÁTICAMENTE** - Con los algoritmos de aprendizaje automático, todos los eventos de su sistema se filtrarán automáticamente para mostrar los incidentes reales, omitiendo las amenazas falsas. Este sistema se programa y entrena para identificar los intentos de intrusión, infecciones de malware, escaneo basado en redes y actividad de autenticación.

**INCIDENTES DE INVESTIGACIÓN** - Los detalles de los incidentes se generan y envían automáticamente al analista de seguridad quien los investigará y analizará exhaustivamente, aprovechando la base de conocimiento para hacer una clasificación y solución competente de problemas.

**RESUELVA UN INCIDENTE** - Si se confirma un incidente en su sistema, nuestros especialistas en tecnología trabajarán rápidamente para identificar e implementar un arreglo. Estos monitorearán el evento hasta que se resuelva integralmente y que el incidente se cierre y usted se encuentre satisfecho con esto. Para cerrar el caso, proporcionarán asistencia en sitio para asegurarse de que la situación se remedió y que la operación de su sistema haya regresado a la normalidad.

**REPORTE PERSPECTIVAS** - Queremos mantenerlo informado de cualquier cambio a la salud de su sistema. Nuestros reportes posteriores al incidente se generan rápidamente y se utilizan para implementar medidas preventivas, las cuales se comparten con su equipo y se aprovechan en las operaciones de seguridad futuras para proteger sus redes de manera más efectiva.

## PORTAL DE MYVIEW

Entendemos que para usted es crítico tener una visibilidad total del rendimiento de todo su ecosistema tecnológico. Nuestro portal de administración basado en web proporciona perspectivas prácticas del estado y salud de su sistema, lo cual le permite mantener la vigilancia de la salud de su ecosistema esencial. Se le conoce como el Portal de MyView y le proporciona perspectivas rápidas y sencillas para sus incidentes de seguridad y estados de entrega de servicios desde una plataforma simple basada en la web.



# LA VENTAJA DE MOTOROLA SOLUTIONS: PERSONAS, PROCESOS Y HERRAMIENTAS

La ciberseguridad efectiva va más allá de la tecnología. Nuestro talento líder en la industria, procesos de seguridad y herramientas de vanguardia son parte de un enfoque integrado que optimiza la complejidad y facilita el manejo de riesgos en su organización.

## PERSONAS

Nuestro personal es la fuerza motora de nuestra cultura de seguridad, la cual se integra totalmente en todo lo que hacemos. Nuestros expertos guían todo el rango de nuestras soluciones de ciberseguridad y constantemente se esfuerzan por ser más predictivos y proactivos. Estos tienen las mejores certificaciones en ciberseguridad de la industria, tales como las de los Sistemas Informáticos de Justicia Criminal (CJIS), Estándares de Procesamiento de Información Federal (FIPS) y de la Ley de Administración de Seguridad Informática Federal (FISMA); y se mantienen actualizados con capacitaciones integrales y constantes. Creamos el Programa de Campeones de Soluciones Cibernéticas de Motorola, el cual inculca principios y conocimiento de ciberseguridad a nivel constitutivo a lo largo de cada faceta de la compañía.

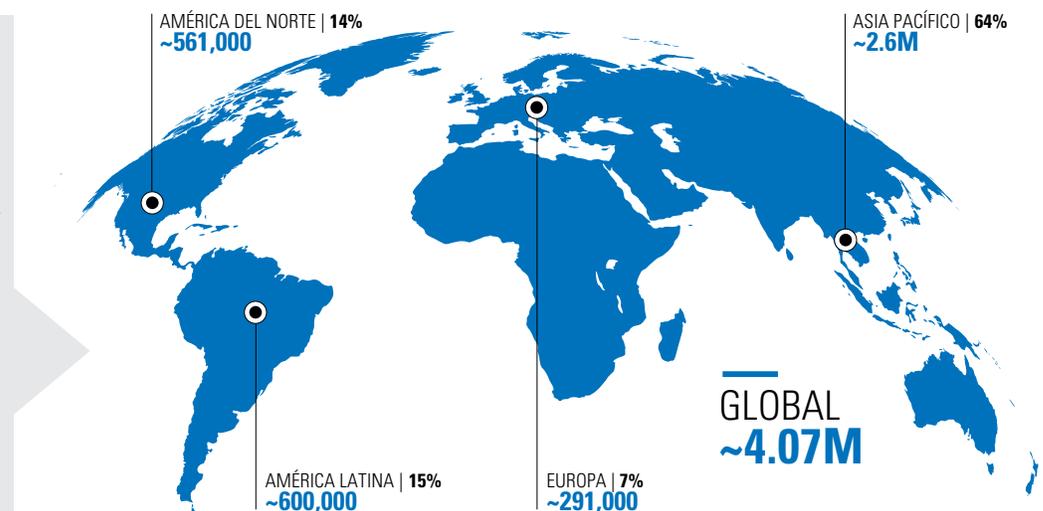
Invertimos constantemente en educación y capacitación cibernética, ya que, cuando nuestros expertos en

ciberseguridad están listos para el éxito, también lo estará usted. Utilizamos el Marco del Personal para la Ciberseguridad del NIST para guiar nuestros esfuerzos de educación y capacitación en esta materia.

Adicionalmente, el equipo de Inteligencia contra Amenazas de Motorola Solutions crea una vista holística del panorama de amenazas cibernéticas y de cómo esto impacta a las prioridades de negocios e infraestructura de nuestros clientes. El equipo analiza y comunica la capacidad, oportunidad e intención de una amenaza cibernética que apunta a los productos y clientes de Motorola Solutions. Este nivel de conciencia situacional proporciona a los principales interesados y responsables la información necesaria para priorizar los recursos y habilitar mejores decisiones de seguridad. Nuestros expertos están aquí para ayudarle a navegar este ambiente de tecnología compleja para que su personal pueda enfocarse en su misión y no en la tecnología.

## LA CRISIS DE PERSONAL EN CIBERSEGURIDAD

La escasez global de personal de ciberseguridad se estima en 4 millones de profesionales con más de 500,000 de estos puestos ubicados en América del Norte. Asia Pacífico, con sus economías en crecimiento y nuevas regulaciones de privacidad, está experimentando la escasez más grande, calculada en 2.6 millones de puestos.<sup>3</sup>





---

## PROCESOS

Nuestro proceso de ciberseguridad se guía por tres objetivos principales: confidencialidad, integridad y disponibilidad. Los datos e información deben confinarse a las personas autorizadas para acceder a este y no debe divulgarse a otros; los datos deben mantenerse intactos, completos y exactos, mientras tiene sus sistemas de TI operando y toda la información debe estar disponible para los usuarios autorizados cuando sea que se necesite. Si bien muchas organizaciones simplemente se enfocan en la prevención, bajo el entorno actual de amenazas, toda empresa debe estar plenamente preparada para el “peor” escenario en caso de un ataque cibernético.

---

## HERRAMIENTAS

Los criminales y entes estatales están en constante evolución en cuanto a la tecnología que utilizan para llevar a cabo ataques cibernéticos. Para estar siempre un paso adelante, constantemente buscamos ser más predictivos y proactivos, invirtiendo en herramientas sofisticadas tales como las de análisis y automatización. Cuando se aplican adecuadamente, la analítica y automatización pueden reducir los costos operativos, acelerar la respuesta de servicios y aumentar la toma de decisiones predictiva al

Con el Marco de Trabajo de Ciberseguridad del NIST, nuestro acercamiento a la ciberseguridad se enfoca en opciones de mitigación, monitoreo continuo, diagnóstico y remediación para asegurar y proteger los sistemas y redes. Adicionalmente, nos alineamos con las prácticas administrativas ITIL, reconocidas en la industria, con el diseño, transición y operaciones de servicios para la entrega de los mismos. Nuestro equipo de expertos marca un conocimiento global extensivo para desarrollar un modelo de entrega de servicios, arquitectura y políticas que se ajustan a sus necesidades.

eliminar muchos de los tardados procesos de tipo manual involucrados en el manejo de amenazas. Adicionalmente, el utilizar analítica avanzada para examinar las amenazas y patrones de falla a lo largo del sistema puede periódicamente prevenir incidentes de seguridad con mayor eficiencia al enfrentar las causas de raíz antes de que impacten al sistema. Con base en un “data lake” robusto, estas herramientas continuamente optimizan el rendimiento del sistema.

# LA RESILIENCIA CIBERNÉTICA CORRECTA

Los ataques cibernéticos pueden sucederle a cualquiera y en cualquier momento. ¿Está listo? Nuestros servicios de ciberseguridad ofrecen la experiencia, tecnología de vanguardia y capacidad de respuesta para ayudarle a estar preparado. El asociarse con Motorola Solutions para tener ciberseguridad le permite a su equipo enfocarse en su misión principal y no en el mantenimiento de los sistemas. Administramos la complejidad por usted, lo cual significa que siempre se mantendrá en ritmo con la innovación a un costo predecible. Nuestro equipo de especialistas se convertirá en parte del suyo, asegurando holísticamente sus

activos de comunicación más importantes, anticipando problemas antes de que surjan y mejorando continuamente los planes para prevenir ataques futuros.

Por algo Motorola Solutions es el líder en comunicaciones esenciales. En cada uno de nuestros servicios de ciberseguridad, le proporcionamos la misma confianza y compromiso en las cuales ha confiado por más de 90 años. Con procesos, herramientas y personal líder en la industria, estamos redefiniendo lo que significa garantizar la resiliencia de operaciones esenciales.

## EXPERIENCIA Y ESCALA GLOBAL

4M

USUARIOS BAJO  
NUESTRO SERVICIO  
ADMINISTRADO

20M

EVENTOS MONITOREADOS  
PROACTIVAMENTE  
CADA DÍA

13K

SISTEMAS  
INSTALADOS

100K

CLIENTES A LO LARGO  
DE 100 PAÍSES

90+

AÑOS DE  
EXPERIENCIA

### NOTAS

1 Revista de defensa cibernética

2 2018 encuesta de comparación de mercado para sistemas de administración LMR de Motorola Solutions

3 Estudio de Personal de Seguridad ISC2 2019, 2019

Conozca cómo Motorola Solutions puede ayudarle a mantener segura su organización. Visite [www.motorolasolutions.com](http://www.motorolasolutions.com) para obtener más información.



Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. 800-367-2346 [motorolasolutions.com](http://motorolasolutions.com)

MOTOROLA, MOTO, MOTOROLA SOLUTIONS y el logotipo de la M estilizada son marcas comerciales o marcas comerciales registradas de Motorola Trademark Holdings, LLC y son utilizadas bajo licencia. Todas las demás marcas comerciales pertenecen a sus respectivos propietarios. ©2020 Motorola Solutions, Inc. Todos los derechos reservados. 03-2020a