IBM Security

IBM

Compre e implemente seguridad en la nube – donde sea que estén sus datos

Ahora las organizaciones que se mueven a la nube o a modelos híbridos pueden alcanzar eficiencias en los informes de cumplimiento y en la detección avanzada de amenazas

Documento de IBM Seguridad

IBM QRadar brinda visibilidad en su red

Para las organizaciones de cualquier tamaño, asegurar datos y redes en la actualidad es una tarea abrumadora. Casi a diario se descubren nuevas vulnerabilidades; tan pronto como se escribe un nuevo script de detección para un tipo de malware se desarrollan nuevas variantes; y los criminales cibernéticos pueden comprar kits de explotación preempaquetados en la Darknet respaldados por equipos de soporte profesional. Como analista de seguridad, usted necesita más que un par de soluciones específicas diseñadas para defender la frontera de su red. Usted necesita visibilidad, perspectiva y un sentido innato para saber cuándo las cosas simplemente no se ven bien.

IBM QRadar es excelente en estas tareas. Ayuda a proteger los datos y las redes con un amplio rango de capacidades que le pueden mostrar quién está haciendo qué, dónde y cuándo. Usa paneles de control y visualizaciones avanzadas que resumen miles o millones de incidentes discretos en simples indicaciones de problemas sospechosos, y preserva registros detallados de cualquier actividad sospechosa para análisis futuro. A la vez, sus capacidades de registro avanzadas y las herramientas de generación de informes lo ayudan a cumplir rápidamente con los requisitos básicos tales como los mandatos de informes regulatorios.

Y ahora, con IBM QRadar on Cloud, puede evitar implementar y mantener el hardware y el software, y enfocarse, en su lugar, en usar la inteligencia que reúne QRadar. Seguirá teniendo el control porque su equipo monitorea lo que está sucediendo. Estudie el entorno, afine sus capacidades detección y colabore con colegas para profundizar todas sus habilidades de respuesta y detección de amenazas.

Las soluciones de nube de QRadar pueden procesar hasta

80.000

eventos por segundo.[1]

► Lea más en la web sobre IBM QRadar on Cloud.

1 "IBM Security Intelligence on Cloud onboarding", *IBM Knowledge Center.*

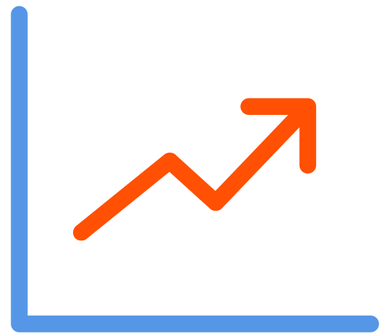
Cumpla con los requerimientos regulatorios de seguridad al mismo tiempo que las demandas

Lo más probable es que usted ya haya implementado medidas básicas de seguridad en el perímetro de su red para evitar ataques simples, pero la mayoría de los puntos terminales tienen fallas de seguridad y algunos usuarios simplemente no pueden resistirse a hacer clic en enlaces maliciosos. Los dispositivos y las credenciales quedan comprometidos con demasiada frecuencia, y esto abre la puerta a la pérdida de datos y a la potencial interrupción de los negocios.

Primero, considere los mandatos regulatorios. Estos requieren sistemas y datos adecuadamente bloqueados – y documentación para comprobar que todo está protegido –. Implementar un sistema de analítica de seguridad puede alivianar la carga de trabajo que los informes de cumplimiento pueden colocar sobre su equipo de seguridad. Eso es porque estos sistemas facilitan la preparación de informes comprensibles, con el formato correcto, y la recolección, curación y revisión de información de su red de manera amigable con las auditorías.

Ahora considere la complejidad de su entorno interno donde se crean, almacenan y transmiten datos críticos. Las redes modernas son cargadas con activos, cada uno de los cuales normalmente también lleva una falla de seguridad explotable. Esto incluye: la variedad de sistemas operativos de la red, su mezcla de hardware – desde servidores a ruteadores, desde conmutadores a firewalls – y software de aplicaciones, basados en la web o no. Cada elemento hace que sea más difícil de asegurar la red como una totalidad, y los criminales cibernéticos explotan los enlaces más débiles para obtener acceso.

Implementar un sistema de recolección de datos y de informes de cumplimiento es bastante fácil, pero dejar contentos a los auditores y proteger los datos críticos de su organización no lo es en absoluto. Cuanto más avanzado es el sistema – tal como QRadar, respaldado por IBM Sense Analytics Engine –, más concisamente lo prepara a usted para gestionar tanto las actividades de rutina como las violaciones de red inusuales que requieren investigación y respuesta ante incidentes.



En 2015, los incidentes de hackeos alcanzaron una alza de nueve años consecutivos, con un salto del

8,4 % *en comparación con 2014.*[1]

▶ Conozca más sobre las amenazas actuales a las empresas en IBM X-Force.

1 "Identity Theft Resource Center Breach Report Hits Near Record High in 2015", *Identity Theft Resource Center*, enero de 2016.

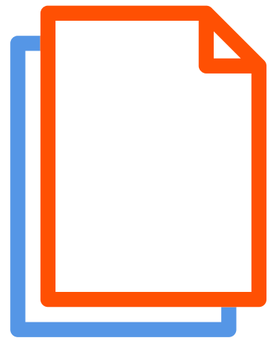
Adquirir un entendimiento profundo para respaldar el cumplimiento y la seguridad

La detección y la erradicación del malware, así como el establecimiento de reglas de firewall para proteger las subredes son importantes. Es por eso que probablemente usted invirtió en seguridad perimetral. Pero el software de analítica de seguridad se basa en el concepto fundamental de que ningún perímetro conectado a Internet es verdaderamente seguro y de que las organizaciones deben poder detectar cambios de comportamiento y anomalías.

Un modo de agregar analítica de seguridad es presupuestar para un gasto de capital grande, hacer espacio en el centro de datos y emplear semanas o meses implementando una solución local mientras su equipo programa un servicio de actualización automática, configura una fuente de inteligencia de amenazas, crea un programa de escaneado de red y define períodos de retención de datos – todo antes de producir mucho valor a partir de la inversión –.

Otro modo es implementar puertas de enlace de datos seguros y enviar sus datos de seguridad a un entorno de nube implementado y gestionado por expertos con tarifas predecibles por la operación mensual. El modelo de nube lo deja a usted en control – y le permite a su personal emplear la mayor parte de su tiempo monitoreando el entorno, afinando las reglas de detección y personalizando los informes regulatorios o de gestión más que aplicando parches de software y realizando copias de seguridad de datos –.

En días, su personal no será interrumpido por ningún evento de registro sencillo (Jackie Jones inició sesión a las 2:32 p. m. desde Chicago), pero recibirá una alerta por un cambio de comportamiento (Jackie Jones inició sesión más tarde esa semana a las 3:07 a. m. desde el sureste de Asia). Al eliminar distracciones innecesarias, tendrá el tiempo para descubrir si hay una explicación razonable para la diferencia (Jackie está viajando) o si está ocurriendo otra cosa.



QRadar puede crear más de

1500 *tipos de informes predefinidos, desde el cumplimiento de normas hasta la gestión de vulnerabilidades.*[1]

► Lea el documento de IBM para saber más sobre QRadar.

1 Lee Bell, “IBM builds QRadar Security Intelligence in the cloud”, *The Inquirer*, abril de 2015.

Ubique a su organización en el camino hacia el cumplimiento de normas

QRadar on Cloud cumple una importante función basada en el negocio. Al proteger los datos y preservar en un formato de auditoría un registro de las prácticas y eventos de seguridad que habilitan la protección, ayuda a las organizaciones a cumplir las normas gubernamentales e industriales. Si son ignorados, estos mandatos pueden hacer que una organización quede atrapada entre sanciones del mismo modo en que seguramente el malware puede generarle problemas con la pérdida de datos.

Una gran cantidad de requisitos y estándares de buenas prácticas diseñados para proteger la información financiera y personal del consumidor y aumentar la transparencia corporativa gobierna cómo se reúnen, almacenan y aseguran los datos organizacionales y del cliente. Sarbanes-Oxley (SOX), el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI DSS), la Ley de Transferencia y Responsabilidad de los Seguros Médicos (HIPAA), la Norma General de Protección de Datos de la Unión Europea (GDPR) y otras normas significan que las empresas podrían enfrentarse a sanciones penales o civiles, prohibiciones en el uso de tarjetas de pago y otros riesgos que pueden incluir devastadoras interrupciones del negocio por prácticas de incumplimiento.

Incluso sin la presión de las sanciones, el proceso de asegurar el cumplimiento de las normas sirve para fomentar las mejores prácticas en el almacenamiento de datos, el encriptado y la protección de nodos de red. Mientras que ningún software puede reemplazar el trabajo de diseñar y mantener una infraestructura que incorpora una arquitectura de almacenamiento y flujo de trabajo en cumplimiento con las normas, QRadar on Cloud lo ayuda a buscar prácticas en incumplimiento para garantizar un buen estado de salud para los datos y las aplicaciones.

Las violaciones de la ley HIPAA pueden incurrir en sanciones penales, así como en multas de hasta

USD 50.000

por violación, con un máximo anual de USD 1,5 millones.[1]

► Obtenga más información sobre lo permitido y lo no permitido del cumplimiento de normas en este documento.

1 "HIPAA Violations and Enforcement", *American Medical Association*. Consultado el 26 de julio de 2016.

Mire los datos de cerca para enfrentar amenazas nuevas y en evolución

Algunas amenazas de seguridad se pueden abordar tácticamente, usando herramientas especializadas que abordan aspectos individuales de la seguridad. Estas pueden ser útiles en el abordaje de amenazas definidas y problemas conocidos, y podrían generar respuestas tan simples como el bloqueo selectivo de puertos de red, la remoción de una instancia de malware o el emparchado de un activo vulnerable identificado.

Pero el software de QRadar puede ser mucho más valioso que las soluciones específicas porque este reúne una gama más amplia de datos de seguridad que se comparte en todos los módulos de inteligencia de seguridad. Una vez que observa y calcula umbrales para las normas de flujo de datos en su red, automáticamente detecta eventos que violan estos umbrales y lo advierte a su personal de seguridad. Las normas del umbral pueden ayudar a detectar transferencias de datos salientes inusualmente grandes, cambios en el uso de ancho de banda en aplicaciones o una cantidad sospechosamente elevada de intentos de inicio de sesión desde una dirección de IP inesperada.

QRadar también busca eventos conectados comparando identidades de usuarios, direcciones de IP de fuente y destino, y ubicaciones geográficas donde la actividad se originó. Examina estos eventos enlazados buscando contexto para distinguir mejor verdaderos ataques de las instancias aisladas de nuevos comportamientos. Incluso busca patrones de *no* uso, como cuando un servicio o activo particular desaparece inesperadamente. Esto podría significar que un activo está desconectado (quizás debido a malware) o que QRadar ha detectado una desviación del comportamiento base del usuario.

Los ataques criminales son la principal causa de violación de datos de registros

médicos

en el área de salud.[1]

► Obtenga más información sobre el profundo conocimiento de seguridad reunido por IBM X-Force.

1 "Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data", *Ponemon Institute*, mayo de 2016.

Adopte un nuevo modelo de gastos con software de seguridad basado en la nube

El software puede ser muy importante para habilitar operaciones de TI y empresariales, pero para la mayoría de las organizaciones, mantener el software de seguridad dentro de la empresa añade una carga de trabajo extra que realmente puede interponerse entre sus tareas de seguridad centrales. Reducir y simplificar la mezcla de roles que el personal de seguridad necesita desempeñar puede ser un motivo significante para la adopción de una alternativa basada en la nube.

Más aún, el ciclo de vida del hardware para hospedar en el sitio – desde la especificación inicial hasta la disposición eventual – puede acarrear una carga adicional. Con frecuencia significa tener suficientes piezas de repuesto a mano y seleccionar hardware con el mantenimiento en mente. Y normalmente todo se torna responsabilidad del personal local que ya está ocupado.

Lograr una mejor seguridad siempre requerirá de cierto nivel de recursos técnicos y humanos – pero con una solución hospedada, basada en la nube, el tiempo y los gastos asociados que el personal de seguridad emplea para deberes rutinarios se puede reasignar a análisis y planificación –. Las actualizaciones del sistema y las reparaciones de las aplicaciones pueden ser manejadas remotamente por especialistas y pueden ocurrir sin interrumpir su infraestructura de TI local. Con el acceso remoto que define a las aplicaciones de nube, los integrantes de su personal local no deben gastar tiempo instalando y aprovisionando físicamente servidores para obtener nuevas capacidades de software. Juntos, estos factores implican que las soluciones basadas en la nube se pueden adquirir y expandir en cualquier horario – normalmente en días o semanas – sin el sobreaprovisionamiento de recursos en el sitio.

La infraestructura de QRadar on Cloud es monitoreada

las 24 horas, los 7 días de la semana,

por profesionales de IBM de confianza.[1]

► Lea este documento de IBM para conocer más sobre cómo la adopción de software de nube puede ayudar a regular los gastos.

1 "IBM QRadar on Cloud", *IBM Corp.*, abril de 2015.

Prepárese para el cambio – y el crecimiento – con su inversión en seguridad

Como con casi cualquier otra tecnología, las herramientas de seguridad raramente son independientes. Las herramientas que trabajan juntas pueden abordar mejor un entorno de amenazas cambiante o añadir capacidades específicas – y eso incluye las herramientas de defensa perimetral en las cuales ya ha invertido.

QRadar on Cloud hereda más de 500 integraciones desarrolladas en la última década, respondiendo a solicitudes de clientes on-premise y asociándose con soluciones externas que complementan la plataforma de inteligencia de seguridad. Los profesionales experimentados que despliegan su implementación de nube raramente tendrán que desarrollar nuevos módulos de soporte para comenzar a aceptar datos de sus activos y aplicaciones. La mayoría de los clientes comenzarán a recibir valor en tan solo unos días después de que se firma un acuerdo.

Los datos de seguridad agrupados a través de IBM X-Force Threat Intelligence Research, por ejemplo, también se integran sin falla y de manera continua a su implementación de QRadar on Cloud, utilizando cientos de terabytes de información sobre vectores de amenaza en evolución y ataques observados así como también vulnerabilidades no reportadas previamente.

Usted puede descargar e instalar nuevas extensiones o aplicaciones desde el IBM Security App Exchange, que mejorarán sus capacidades de monitoreo de red, y su equipo de mantenimiento de nube de IBM le dará soporte a la extensión tecnológica. Ya hay decenas de estas extensiones con soporte incluidas nuevas visualizaciones, integraciones, parches, normas personalizadas y aplicaciones nuevas completas tales como la aplicación IBM QRadar User Behavior Analytics app. Todo el contenido del sitio es revisado por IBM Seguridad a través de su proceso de validación *Listo para IBM Inteligencia en Seguridad*.

QRadar puede reunir eventos de registros y flujos de red de
más de 500
aplicaciones o dispositivos.[1]

▶ Obtenga más información sobre los plug-ins y extensiones de QRadar a través del IBM Knowledge Center.

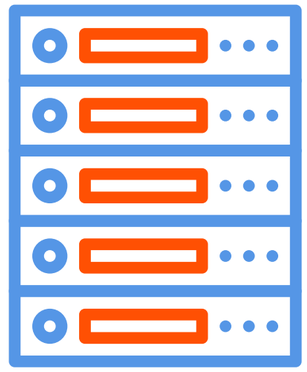
1 "Introducing the IBM Security App Exchange", *IBM Corp.*, diciembre de 2015.

Ponga a trabajar una infraestructura escalable y flexible cuando la necesite

Comprar software como servicio ofrece ventajas en escalabilidad y flexibilidad, porque implica que los cambios de capacidad no están asociados a infraestructura en el sitio, y estos son mucho menos dependientes de la disponibilidad del personal interno. Para comprender las ventajas del software Inteligencia en Seguriad y Analítica en la Nube, tiene sentido considerar dos clases diferentes de cambios de escala:

Estacionalidad: La mayoría de los negocios tienen altibajos en su carga de trabajo, algunos bastante predecibles en su alcance si no en sus tiempos exactos. Con las compras de software convencional, comprar en el peor de los escenarios (es decir, el momento más ocupado o demandante) puede ser la única opción, aún si eso implica gastos adicionales en hardware de lo que normalmente se requiere.

Crecimiento de la compañía: Del mismo modo, las compañías que planifican una unión, adquisición u otro crecimiento con frecuencia son obligadas a “comprar en grande” anticipada e innecesariamente para cubrir necesidades de mayor capacidad. Sin embargo, con las implementaciones basadas en la nube, una empresa puede comprar – o liberar – capacidad en pequeñas cantidades según sus necesidades. Debido a que la infraestructura habita en la nube y está diseñada para cambios de capacidad, no hay necesidad de cambiar el software localmente. La capacidad se puede aumentar o disminuir con poca anticipación y con una necesidad mínima de participación del cliente.



Muchas compañías han empleado hasta

5 veces

el espacio del centro de datos que necesitan para los ciclos de negocios de régimen estacionario.[1]

▶ Aprenda lo que los analistas tienen para decir sobre las ventajas financieras de mover los datos de su negocio a la nube.

1 David Linthicum, “Cloud Economics – Are You Getting the Bigger Picture?” *Cloud Technology Partners*, mayo de 2016.

Cuente con las capacidades del mundo real de IBM QRadar on Cloud

El software basado en la nube puede ayudarlo a evitar costos de infraestructura con frecuencia considerables – tales como el análisis, el aprovisionamiento y las pruebas del tiempo que el personal interno o consultores empleó – que requiere una implementación en las instalaciones. IBM QRadar on Cloud aplica la experiencia que ha ganado de miles de implementaciones QRadar en las instalaciones para satisfacer las necesidades de su ambiente. Es un impulso – en la nube –.

Al implementar QRadar on Cloud, puede mantener o expandir las capacidades de monitoreo que ya ha desarrollado, pero permitir que los analistas empleen más tiempo en comprender datos de inteligencia de amenaza o a aplicar sus habilidades para proteger activos existentes. No hay necesidad de mantener o retocar software de seguridad en las instalaciones. Con las actualizaciones automáticas de software y la escalabilidad según demanda, QRadar on Cloud hace la vida más simple para el personal de seguridad de TI al aportar gastos operacionales mensuales predecibles para la organización.

Una implementación de QRadar on Cloud significa que usted obtendrá la experiencia, el poder y la extensibilidad que necesita. El sistema puede hacer análisis de nivel empresarial, con capacidades que incluyen:

- Accesibilidad al explorador web
- Recolección de datos, capacidades de correlación y de generación de informes para alcanzar el cumplimiento de normas
- Grandes máximos de Evento Por Segundo (EPS) que satisfacen las necesidades de los clientes con cientos de ubicaciones globales
- Configuración del sistema altamente disponible para una disponibilidad prácticamente continua
- Aplicaciones, complementos y extensiones a través de IBM Security App Exchange
- Fuente de X-Force Threat Intelligence en situaciones en desarrollo

Y para organizaciones que necesitan ayuda más allá de las capacidades que su personal de seguridad tiene el tiempo o la experiencia para proporcionar, también hay disponibles servicios opcionales de gestión adicional.

Las compañías con una estrategia de nube gastaron el

22 % *menos en seguridad que quienes no la tenían.*[1]

▶ Mire este video para aprender más sobre QRadar on Cloud.

1 "Buying Intentions Survey: Security", *Nucleus Research*, febrero de 2016.

¿Por qué IBM?

Las soluciones de IBM Seguridad ayudan a las empresas a evitar, detectar y responder a las amenaza de seguridad y vulnerabilidades en una oferta integrada de hardware, software y servicios. Potencializado por una analítica profunda y la experiencia confiable de IBM Seguridad, el portafolio de IBM que cuenta con herramientas escalables y líderes en la industria ofrece inteligencia de seguridad de amplio rango.

QRadar on Cloud usa la misma tecnología subyacente para proporcionar gestión de registros, análisis de flujo de red, analítica histórica y en tiempo real y gestión de vulnerabilidades a cualquier tamaño de organización buscando externalizar la adquisición, implementación y gestión de la infraestructura de inteligencia de seguridad de QRadar. La solución es hospedada dentro de los centros de datos de nube de IBM y está disponible en todo el mundo. Para las regiones con requisitos específicos de almacenamiento de datos dentro del país, QRadar on Cloud está actualmente habilitado en las siguientes ubicaciones: EE. UU. – Dallas, Texas; Canadá – Toronto, Ontario; Unión Europea – Frankfurt, Alemania; América Latina – San Pablo, Brasil. Hay más ubicaciones planificadas.

Además, QRadar On Cloud tiene un marco abierto que habilita una integración sencilla con soluciones publicadas en el IBM Security App Exchange. IBM Security App Exchange permite a los asociados de negocio compartir aplicaciones, extensiones de aplicaciones de seguridad y mejoras a los productos de IBM Seguridad. Los equipos de seguridad que usan QRadar on Cloud pueden descargar e instalar las soluciones según su propia conveniencia usando un modelo de autoservicio sin modificaciones en los acuerdos de hosting existentes (salvo que se sobrepasen los términos básicos de licencias).

Para obtener más información

Para saber más sobre IBM QRadar Security Intelligence Platform en la nube, comuníquese con su representante de IBM o el Asociado de Negocios de IBM, o visite: **ibm.com**/software/products/en/qradar-on-cloud

Acerca de la Seguridad de IBM

IBM Seguridad ofrece uno de los portafolios empresariales de seguridad más avanzados e integrados de productos y servicios. El portafolio, con soporte del mundialmente conocido X-Force Research, proporciona inteligencia de seguridad para ayudar a las organizaciones a proteger integralmente sus infraestructuras, datos y aplicaciones, ofreciendo soluciones para la gestión de acceso e identidad, seguridad de base de datos, desarrollo de aplicaciones, gestión de riesgos, gestión de puntos terminales, seguridad de red y más.

Estas soluciones permiten a las organizaciones gestionar efectivamente el riesgo e implementar una seguridad integrada para los dispositivos móviles, la nube, las redes sociales y otras arquitecturas de negocios empresariales. IBM opera una de las organizaciones más amplias de investigación, desarrollo y entrega de seguridad del mundo, monitorea 15.000 millones de eventos de seguridad por día en más de 130 países, y tiene más de 3000 patentes de seguridad.

Además, IBM Global Financing proporciona numerosas opciones de pago para ayudarlo a adquirir la tecnología que necesita para que su negocio crezca. Proporcionamos gestión del ciclo de vida completo de los productos y servicios de TI, desde la adquisición hasta la disposición. Para obtener más información, visite: **ibm.com**/financing

IBM

IBM de México S.A.
Alfonso Nápoles Gandara 3111
Col. Parque corporativo de Peña Blanca
C.P. 01210
México D.F

Puede encontrar la página de inicio de IBM en:
ibm.com

IBM, el logotipo de IBM, ibm.com, QRadar, Sense Analytics Engine, y X-Force son marcas registradas de International Business Machines Corp., registradas en muchas jurisdicciones en todo el mundo. Otros nombres de productos y servicios pueden ser marcas registradas de IBM u otras compañías. Hay una lista actualizada de las marcas registradas de IBM en la web en “Información de copyright y marcas registradas” en **ibm.com**/legal/copytrade.shtml

Este documento está actualizado conforme a la fecha inicial de la publicación y puede ser modificado por IBM en cualquier momento. No todas las ofertas están disponibles en todos los países en los que opera IBM.

Los ejemplos de clientes citados se presentan solo para fines ilustrativos. Los resultados del rendimiento real pueden variar según las configuraciones y condiciones de funcionamiento específicas.

LA INFORMACIÓN PRESENTADA EN ESTE DOCUMENTO SE PROVEE “TAL CUAL” SIN GARANTÍA DE NINGÚN TIPO, NI EXPRESA NI IMPLÍCITA, INCLUYENDO, PERO NO LIMITADO A, LAS GARANTÍAS IMPLÍCITAS DE COMERCIO, CONVENIENCIA PARA UN PROPÓSITO PARTICULAR, O NO INFRACCIÓN. Los productos de IBM están garantizados de acuerdo a los términos y las condiciones de los acuerdos bajo los cuales se proporcionaron.

El cliente es responsable de garantizar el cumplimiento de las leyes y regulaciones correspondientes. IBM no brinda asesoría legal o representa o garantiza que sus servicios o productos garantizarán que el cliente esté en conformidad con cualquier ley o regulación.

Declaración de buenas prácticas de seguridad: la seguridad del sistema de TI incluye la protección de sistemas e información a través de la prevención, detección y respuesta de acceso indebido desde el interior y exterior de su empresa. El acceso inadecuado puede tener como resultado la alteración, destrucción, malversación o mal uso de la información, o puede tener como resultado el daño o uso indebido de sus sistemas, incluido el uso en ataques a otros. Ningún sistema de TI o producto debe considerarse completamente seguro y ningún producto, servicio o medida de seguridad puede ser completamente efectiva en la prevención del uso o acceso indebido. Los sistemas, productos y servicios de IBM están diseñados para ser parte de un enfoque de seguridad comprensivo y legítimo, que necesariamente implicará procedimientos operacionales adicionales, y puede requerir que otros sistemas, productos o servicios sean efectivos al máximo. IBM NO GARANTIZA QUE NINGÚN SISTEMA, PRODUCTO O SERVICIO SEA INMUNE A LA CONDUCTA MALICIOSA O ILEGAL DE ALGUNA PARTE, NI VOLVERÁ A SU EMPRESA INMUNE DE DICHA CONDUCTA.

© Copyright IBM Corporation 2017

WGW03245-MXES-01