GBM as a Service

Proteja su organización mediante una visión estratégica

El panorama tan cambiante y evolucionado de las amenazas de seguridad, hacen que los líderes redefinan su estrategia para adaptarse a estos cambios. El reducir la complejidad, la aplicación de inteligencia artificial, la ejecución de controles cercanos a los datos, el establecimiento de las identidades de usuario como un nuevo perímetro de seguridad y la capacidad de respuesta a los incidentes, son temas centrales que estos líderes deben considerar, todo desde una estrategia integral.

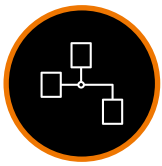
GBM está consciente de los retos que enfrentan las organizaciones en materia de seguridad y es por eso que ha definido un portafolio de soluciones y servicios que le permite a sus clientes apalancar sus esfuerzos en seguridad con tecnología de punta. Este catálogo se divide en dos verticales:

Security Operations & Response
Evolucione sus operaciones de seguridad para detener las amenazas avanzadas

Information Risk & Protection
Gestión de riesgos y protección de datos en un mundo interconectado

Security Operations & Response

Las amenazas de seguridad evolucionan muy rápidamente y cada día son más letales. Las organizaciones deben tener la capacidad de prevenir, detectar y responder a ellas proactivamente. Para ello hay que tomar en cuenta las siguientes temáticas:



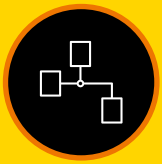
Network Security

Endpoint Management & Security

Security Intelligence & Sense Analytics

Incident Response

Network Security



Mientras lee este documento, los atacantes están trabajando constantemente para penetrar su red y están usando métodos cada vez más sofisticados para encontrar la manera de ingresar ¿Tiene la visibilidad para detenerlos? ¿Y los que ya ingresaron?

GBM cuenta con soluciones de seguridad de red de última generación que reconocen de manera inteligente incluso las amenazas desconocidas, y se adaptan para prevenirlas en tiempo real.

- Proteja su red con análisis de comportamiento y la última inteligencia de amenazas.
- Reduzca la exposición al *malware* avanzado al aumentar el control sobre la aplicación y el comportamiento del usuario.
- Investigue las últimas amenazas de seguridad global, y agregue inteligencia procesable.

Productos de Seguridad en la Red:

- **IBM QRadar Network Insights**

  Los atacantes no pueden ocultarse en su red con IBM QRadar Network Insights. Los equipos de seguridad están inundados de actividad de registro de seguridad todos los días, pero la inspección de esos registros no siempre genera el nivel de profundidad necesario para detectar amenazas modernas.

  QRadar Network Insights analiza datos de red en tiempo real para descubrir las huellas de un atacante y exponer amenazas de seguridad ocultas en muchos escenarios, antes de que puedan dañar su organización, incluidos correos electrónicos de *phishing*, *malware*, filtración de datos, movimiento lateral, DNS y otras aplicaciones abusivas y brechas de cumplimiento.

- **IBM QRadar Incident Forensics**

  IBM QRadar Incident Forensics le permite realizar un seguimiento de las acciones paso a paso de un posible atacante y, realizar de forma rápida y sencilla una investigación forense exhaustiva de presuntos incidentes de seguridad de red malintencionados. Reduce el tiempo que les lleva a los equipos de seguridad investigar los registros de incidentes, en muchos casos de días a horas, o incluso minutos. También ayuda a remediar una infracción de seguridad de la red y evitar que vuelva a suceder.

Endpoint Management & Security

Con los ataques cibernéticos cada vez más sofisticados, es solo cuestión de tiempo antes de que su organización sea un objetivo. Una vez que se han vulnerado sus puntos finales, cada minuto cuenta.

GBM puede ayudarlo a evaluar vulnerabilidades, acelerar la priorización de riesgos y responder rápidamente a la amenaza de seguridad en todos los puntos finales, dentro y fuera de la red corporativa.

- Controle y asegure cada punto final antes, durante y después de un ataque.
- Obtenga visibilidad y control en tiempo real en todos los puntos finales.
- Obtenga protección avanzada contra *malware* desde la identificación de amenazas hasta que los parches estén en su lugar.

Productos de Seguridad de Endpoints:

- **IBM BigFix**

  El entorno de los endpoints cambia constantemente. Los especialistas en seguridad e infraestructura de TI luchan para acceder a la información actual sobre sistemas operativos, versiones de software, uso de aplicaciones y de cumplimiento en cada PC, servidor, cajero automático o sistema de punto de venta en toda la empresa. Sin un adecuado descubrimiento, implementación y cumplimiento efectivos, la probabilidad de un ataque exitoso de punto final crece exponencialmente. Si no puedes verlo, no puedes corregirlo.

  Con IBM BigFix, las organizaciones de TI pueden reducir los costos operativos, comprimir los ciclos de administración de los puntos finales y aplicar el cumplimiento en tiempo real.

Security Intelligence & Sense Analytics

Mientras lee esto, los atacantes intentan violar las defensas de su compañía, utilizando métodos cada vez más sofisticados para encontrar la manera de ingresar ¿Tiene la visibilidad para detenerlos?

GBM puede ayudarlo a identificar y administrar las amenazas que representan el mayor riesgo para su negocio y requieren atención inmediata. El enfoque inteligente de IBM para el análisis

de seguridad lo ayuda a encontrar amenazas más rápidamente, acelerar dramáticamente los tiempos de investigación, automatizar el cumplimiento y responder a los incidentes.

- Identifique amenazas de alto riesgo con correlación casi en tiempo real y detección de anomalías de comportamiento.
- Detecte vulnerabilidades, gestione riesgos e identifique incidentes de alta prioridad entre miles de millones de puntos de datos.
- Obtenga una visibilidad completa de la red, la aplicación y la actividad del usuario.

Productos de Inteligencia de Seguridad:

- **IBM QRadar Platform**

  Aproveche la flexibilidad y la eficiencia de la plataforma moderna. En el núcleo del desafío de un analista de seguridad, hay demasiados datos repartidos en muchas herramientas. Una plataforma analítica integrada ofrece más que un SIEM (Security Information Event Management) básico para optimizar las capacidades críticas en un flujo de trabajo común y, ayudar al analista de seguridad a ser más eficiente. El ecosistema IBM Security App Exchange amplía las capacidades de la plataforma bajo demanda, agregando seguridad cognitiva con Watson, análisis de comportamiento del usuario y más, para agilizar la detección y respuesta de ataques.

- **IBM QRadar Advisor with Watson for Cybersecurity**

  El volumen de incidentes de seguridad y los datos de amenazas disponibles superan con creces la capacidad de incluso el profesional de seguridad más capacitado. Watson para ciberseguridad aumenta la capacidad del analista para identificar y comprender amenazas sofisticadas, al aprovechar datos no estructurados (por ejemplo, blogs, sitios web, documentos de investigación) y correlacionarlo con delitos de seguridad locales. IBM QRadar Advisor con Watson combina las capacidades cognitivas de Watson y la plataforma de análisis de seguridad QRadar, líder en la industria, para descubrir amenazas ocultas y automatizar ideas, revolucionando la forma en que se trabaja.

Incident Response

Una de las premisas que deben tener los líderes de seguridad en las empresas, es que los controles de seguridad implementados, por más robustos que sean, no serán infalibles siempre. Dada esta premisa, las capacidades de visualización de incidentes a través de toda la organización y, la orquestación y automatización de la respuesta a incidentes, se hace vital para minimizar el impacto de algún incidente de seguridad que suceda en la organización.

Productos de Respuesta a Incidentes:

- **IBM Resilient Incident Response Platform**

  La respuesta al incidente está en el ADN de IBM Resilient. La plataforma de respuesta a incidentes fue pionera en el mercado de software "IR". IBM Resilient aporta a la plataforma más de 100 años de experiencia de seguridad combinada.

  La Plataforma de respuesta a Incidentes Resiliente (IRP) es líder en orquestar y automatizar los procesos de respuesta a incidentes. El IRP se integra rápida y fácilmente con las inversiones de TI y seguridad existentes en su organización. Hace que las alertas de seguridad sean accionables instantáneamente, proporciona inteligencia valiosa y contexto de incidentes, y permite una respuesta que se adapta a amenazas cibernéticas complejas.

  La última innovación del IRP resistente, "Dynamic Playbooks", proporcionan la agilidad, la inteligencia y la sofisticación necesarias para lidiar con ataques complejos. Los "Dynamic Playbooks" se adaptan automáticamente a las condiciones de incidentes en tiempo real y aseguran que los pasos iniciales de selección repetitivos estén completos antes de que un analista abra el incidente.

Information Risk & Protection

A medida que las transacciones comerciales se desplazan fuera de los límites de la compañía, el perímetro de seguridad tradicional alrededor del Centro de Datos se está disolviendo. La gestión de riesgos de seguridad en una nube o entorno móvil es hoy una preocupación principal de los CISO (Chief Information Security Officer).

GBM puede ayudarlo a lograr la administración de amenazas de seguridad con inteligencia basada en riesgos, integración y la cartera de SaaS más grande de la industria. Para ello se deben tomar en cuenta las siguientes temáticas:

Data Security | **Identity & Access Management** | **Mobile Security** | **Application Security** | **Advanced Fraud Protection**

Data Security

Los datos de la empresa representan su capital intelectual, diferenciador competitivo y el alma de la organización. IBM ofrece seguridad y protección de datos que permite a los equipos de seguridad analizar automáticamente lo que sucede en el entorno de datos.

- Analice su riesgo de datos.
- Proteja los datos confidenciales de los actores externos e internos.
- Adáptese rápidamente a los cambios de su entorno.

Productos de Protección de Datos:

- **IBM Security Guardium Data Protection Platform**

  Descubra, clasifique, monitoree y controle el acceso a los datos con una misma plataforma. IBM Security Guardium ayuda a garantizar la seguridad, privacidad e integridad de sus datos críticos en una amplia gama de entornos, desde bases de datos hasta plataformas BigData, nube, sistemas de archivos y más.

- **IBM Security Data Risk Manager**

  Lo que no se conoce puede hacerle daño. Identifique y ayude a detener los riesgos potenciales para los datos sensibles empresariales, que pueden afectar los procesos comerciales, las operaciones y la posición competitiva. IBM Data Risk Manager proporciona a los ejecutivos y a sus equipos, un centro de control de riesgos de datos consumibles, que ayuda a descubrir, analizar y visualizar los riesgos comerciales relacionados con los datos para que puedan tomar medidas para proteger sus negocios.

Identity & Access Management

En GBM, creemos que la seguridad es mejor cuando está trabajando detrás de escena para proporcionar un acceso sin interrupciones y solo interviene cuando algo está mal. Una fuerte postura en seguridad y una experiencia digital positiva no tienen que ser mutuamente excluyentes. Usted logra ambos con IBM IAM, ya que nuestra seguridad silenciosa va a funcionar para usted y sus clientes.

- **Asegure su negocio:** con las soluciones IBM IAM asegurará su negocio, al garantizar que las personas adecuadas tengan el acceso correcto. Podrá verificar discretamente la identidad de un usuario cuando inicie sesión y durante toda su sesión. Con capacidades analíticas únicas, podrá tomar decisiones más inteligentes e informadas para modificar el acceso de los usuarios, al descubrir valores atípicos y combinaciones tóxicas de derechos de acceso.

- **Habilite la transformación digital:** con IBM IAM podrá habilitar rápidamente el acceso a recursos y aplicaciones, ya sea en la nube, en las instalaciones o en una nube híbrida. Ya sea que proporcione acceso a aplicaciones para consumidores o para empleados, podrá ofrecer la experiencia perfecta que esperan sus usuarios.

- **Establezca confianza:** las regulaciones van y vienen; hoy fue SOX, GDPR y PSD2, y mañana será otra cosa. Con IBM IAM podrá gestionar de forma centralizada certificaciones de acceso, dentro y fuera de la organización, y violaciones de separación de funciones, de modo que esté preparado para cumplir con las últimas regulaciones.

Productos de Gestión de Identidades y Accesos:

- **IBM Security Identity Governance & Intelligence**

  IBM Security Identity Governance and Intelligence (IGI) faculta a las empresas y las TI para que trabajen juntas a fin de cumplir con los objetivos de seguridad y normativos en todas las aplicaciones y datos empresariales. IGI cubre la administración del ciclo de vida del usuario empresarial, la evaluación y mitigación de riesgos de acceso, la certificación, la administración de contraseñas, así como potentes análisis e informes para permitir que las empresas tomen las decisiones correctas sobre el acceso empresarial.

- **IBM Security Access Manager**

  En un mundo de entornos de administración de acceso altamente fragmentados, IBM Security Access Manager lo ayuda a simplificar el acceso de sus usuarios. Esta solución le ayuda a lograr un equilibrio entre facilidad de uso y seguridad mediante el acceso basado en riesgos, inicio de sesión único, control de gestión de acceso integrado, federación de identidades y su capacidad de autenticación de múltiples factores móviles. Recupere el control de la administración de acceso con IBM Security Access Manager.

- **IBM Security Privileged Identity Manager**

  IBM Security Privileged Identity Manager protege, automatiza y hace el seguimiento del uso de identidades privilegiadas para frustrar las amenazas internas y mejorar la seguridad en toda la empresa, incluidos los entornos de nube. La opción de dispositivo virtual y la interfaz de usuario rediseñada hace que IBM Security Privileged Identity Manager sea muy fácil de instalar y de gestionar.

  La herramienta opcional Privileged Session Recorder registra las actividades de punto final del usuario privilegiado para mejorar la visibilidad y la conformidad de seguridad.

  Otro componente opcional, IBM Security Privileged Identity Manager for Applications, protege las credenciales entre aplicaciones y realiza el seguimiento de su uso, que permite el gobierno de esas credenciales de aplicación bajo políticas de gestión de contraseñas.

Mobile Security

La velocidad a la que la tecnología móvil está cambiando, ha creado lagunas peligrosas en la seguridad, y los ciberdelincuentes han aprovechado. En la empresa móvil de hoy, las líneas se difuminan entre los activos personales y los corporativos. Las organizaciones de TI tienen que hacer mucho más que simplemente proteger un dispositivo de propiedad corporativa. De hecho, la protección de los datos personales a menudo es una regulación impuesta por el gobierno.

Desbloquee el potencial de la movilidad empresarial abordando todo el espectro de riesgos móviles, habilitando transacciones confiables e implementando un enfoque inteligente e integrado con las soluciones de seguridad móvil de IBM.

- Proteja los dispositivos móviles, desde los activos de propiedad de la empresa hasta los BYOD, contra el acceso no autorizado y la fuga de datos.
- Asegure el contenido y la colaboración, y resguarde las aplicaciones y los datos.
- Identifique las tendencias de seguridad móvil para abordar rápidamente las posibles amenazas.

Productos de Seguridad Móvil:

- **IBM MaaS360:**

  Cognitive UEM es el futuro de la gestión y la seguridad de los dispositivos móviles.

  Administrar los puntos finales más sus usuarios y datos es una tarea que consume mucho tiempo con las soluciones convencionales de gestión de dispositivos móviles (MDM) y gestión de empresas móviles (EMM).

  Los líderes de TI están recurriendo a un enfoque de administración de puntos finales cognitivos unificados (UEM) que consolida la administración de teléfonos inteligentes, tabletas, computadoras portátiles, equipos de escritorio, dispositivos *wearables* y IoT, junto con sus datos y aplicaciones.

Application Security

La investigación, incluida la llevada a cabo por IBM X-Force Research, revela consistentemente que las aplicaciones web y móviles son las más vulnerables a los ataques. Las organizaciones necesitan probar continuamente su software y aplicaciones en toda su cartera al principio del ciclo de vida del desarrollo. Para reducir costos y construir un ecosistema de TI fuerte y seguro, las pruebas y la verificación deben realizarse lo antes posible.

Las soluciones de prueba de seguridad de aplicaciones IBM brindan protección preventiva para mejorar la seguridad de las aplicaciones móviles y web, proteger las aplicaciones del uso malicioso y ayudarlo a remediar los posibles ataques en el futuro.

- Mejore la administración del programa de seguridad de aplicaciones y fortalezca los esfuerzos de cumplimiento regulatorio.
- Evalúe el código de software y las aplicaciones web y móviles en busca de vulnerabilidades.
- Use una única consola para administrar las pruebas de aplicaciones, los informes y las políticas.

Productos de Seguridad en Aplicaciones:

- **IBM Security AppScan**

  IBM Security AppScan y Application Security on Cloud mejoran la seguridad de las aplicaciones web y móviles, mejoran la gestión de los programas de seguridad de las aplicaciones y refuerzan el cumplimiento de las normativas. Probar aplicaciones web y móviles antes de su implementación, puede ayudarlo a identificar riesgos de seguridad, generar informes y corregir recomendaciones.

Advanced Fraud Protection

IBM combina un enfoque cognitivo de la tecnología y la inteligencia de seguridad avanzada con la experiencia de seguridad humana para descubrir conocimientos sobre el panorama de amenazas, por lo que se puede pasar menos tiempo investigando falsos positivos y más tiempo centrándose en mejorar la experiencia del cliente.

Los productos de IBM Trusteer ayudan a muchos de los proveedores de servicios financieros más grandes y líderes del mundo a abordar el fraude de identidad digital mediante la detección de actividades delictivas sofisticadas desde el inicio de una transacción. Con Trusteer, los bancos y las instituciones financieras pueden dejar entrar a los clientes adecuados y ayudar a evitar la actividad fraudulenta.

- Aumente la satisfacción del cliente mediante el uso de análisis de comportamiento y biometría de comportamiento para ayudar a identificar y denegar la actividad no autorizada.
- Adapte continuamente la inteligencia y las protecciones de amenazas en evolución con capas de tecnología cognitiva y análisis avanzados.
- Reduzca el tiempo y el costo asociados con la investigación de falsos positivos a través de una administración simplificada del ciclo de vida con servicios basados en la nube.

Productos de Protección contra Fraude Avanzado:

- **IBM Trusteer**

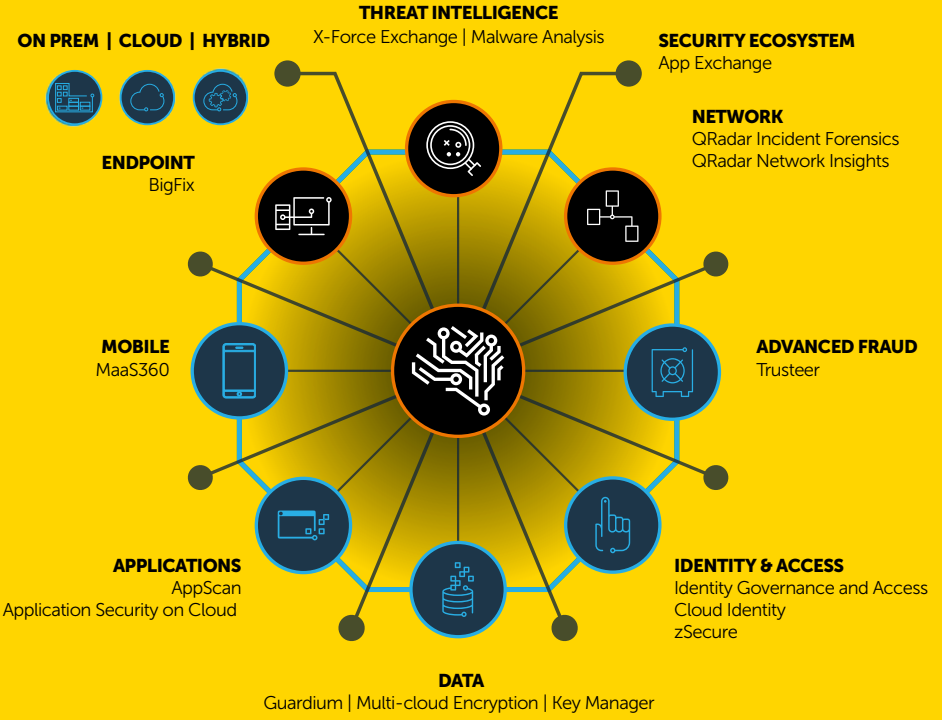
  Con IBM Trusteer Fraud Prevention se combina la inteligencia avanzada y la cognitiva con la experiencia humana para tener una visión más precisa del panorama de las amenazas, de modo que se pueda dedicar menos tiempo a investigar falsos positivos y más tiempo a la experiencia del cliente.

Integrated and Intelligent Security Immune System

Lo hemos escuchado una y otra vez: cuando se trata de amenazas de ciberseguridad, nadie es inmune. La conversación ha cambiado de enfoque en "si lo atacan" a "qué tan rápido puede responder".

Como seres humanos, hemos afinado sistemas inmunes adaptativos listos para ayudarnos a luchar contra todo tipo de ataques que, de otra manera, amenazarían para destruirnos. Este sistema inmune está compuesto de células, tejidos y órganos que trabajan juntos para defendernos contra los ataques de invasores o "seres extraños". Es inteligente, organizado y eficiente, con capacidad de reconocer al instante un invasor y tomar medidas para bloquear su entrada o destruirlo.

Pero cuando miramos a la ciberseguridad, la tradicional estrategia de defensa está fragmentada. Es por eso que, hoy en día, tiene mucho sentido un **sistema inmune de seguridad**, donde todos los componentes de seguridad trabajen de forma conjunta para prevenir, detectar y responder a las amenazas que acechan a las organizaciones.


THREAT INTELLIGENCE
X-Force Exchange | Malware Analysis
ON PREM | CLOUD | HYBRID
SECURITY ECOSYSTEM
App Exchange
NETWORK
QRadar Incident Forensics
QRadar Network Insights
ENDPOINT
BigFix
MOBILE
MaaS360
ADVANCED FRAUD
Trusteer
APPLICATIONS
AppScan
Application Security on Cloud
IDENTITY & ACCESS
Identity Governance and Access
Cloud Identity
zSecure
DATA
Guardium | Multi-cloud Encryption | Key Manager

Soluciones adicionales de seguridad

Simplifique la complejidad de la seguridad, mantenga los negocios más protegidos y aumente la productividad de las TI con las siguientes soluciones. Los servicios de GBM lo ayudan a integrar tecnologías como Cisco, migrando desde otras herramientas y optimizando soluciones existentes para obtener la mayor seguridad posible.

Protección para redes frente a Ransomware

El Ransomware es software malicioso, o malware, que cifra la información contenida en el ordenador de una persona, como documentos, fotos y música y no libera estos archivos hasta que el usuario pague una tarifa (o rescate) para desbloquearlos y recuperarlos.

No deje que su empresa sufra ataques y pierda la información, para esto Ransomware Defense incluye:

- **Protección de la capa de DNS:** protege los dispositivos adentro y afuera de la red corporativa. Bloquea las solicitudes DNS antes de que un dispositivo siquiera pueda conectarse a sitios que alojan ransomware.
- **Protección de terminales:** supervisa constantemente todo el comportamiento de los archivos para descubrir ataques furtivos, detecte, bloquee y corrija problemas con malware avanzado en todos los terminales.
- **Protección contra amenazas provenientes del correo electrónico:** bloquea el ransomware que llega a través del spam y de los mensajes de correo electrónico de suplantación de identidad. Incluso identifica las URL y los adjuntos maliciosos del correo electrónico. Mitigue los ataques antes de que se propaguen.
- **Segmentación sofisticada**: acelera las operaciones de seguridad y aplica de manera uniforme las políticas en cualquier lugar de la red.
- **Defensas avanzadas para ataques avanzados:** bloquea amenazas y mitiga rápidamente aquellas que traspasan sus defensas con el primer firewall de nueva generación (NGFW) centrado en amenazas del sector.

Breach Readiness

Está solución lo ayuda a prepararse, gestionar y recuperarse de las filtraciones de datos y los ataques a la red. Nuestro experimentado equipo utiliza la inteligencia de amenazas de Talos y la tecnología de seguridad más actual para responder a los ataques y reducir el daño y la exposición.

Secure Office365

Detecta cuentas en la nube comprometidas e información privilegiada maliciosa, monitorea cuentas de usuarios privilegiados y obtiene visibilidad y control sobre la información sensible. Proporciona la inteligencia de uno de los equipos de detección de amenazas más grandes del mundo, junto con las sólidas funciones que necesita para proteger a sus usuarios con Microsoft Office 365.

Secure Data Center

Brinda protección integrada en arquitecturas virtuales, físicas, en la nube y en SDN.

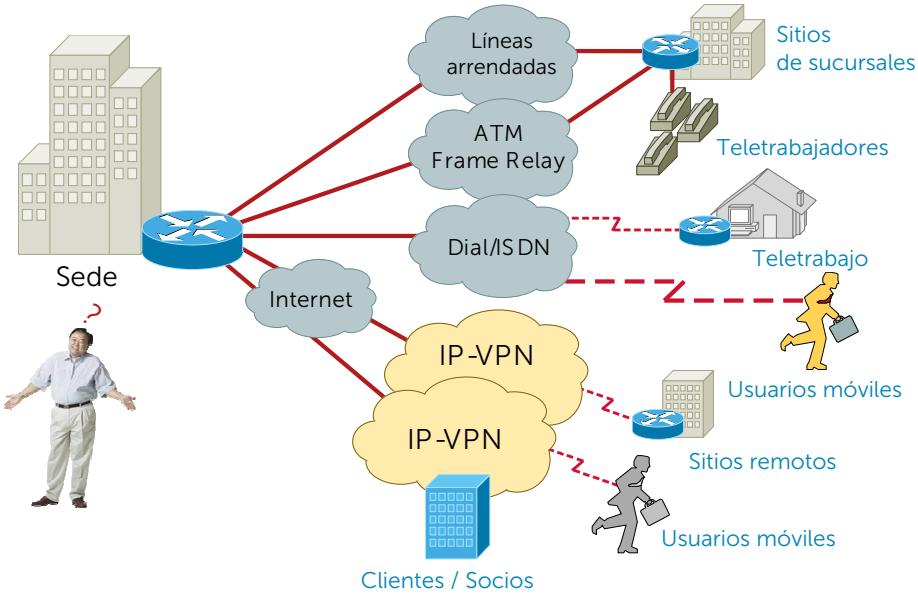
Beneficios:

- **Confianza para competir**
  La seguridad se convierte en un motor de crecimiento para nuevas oportunidades de negocios.
- **Protección avanzada contra amenazas**
  Obtenga la última inteligencia y defensa para una mejor seguridad.
- **Inteligencia de seguridad**
  El análisis en la industria lo mantiene informado y protegido.

Network Visibility

Detecta rápidamente amenazas, acceso seguro y segmentación definida por software. Reduce el riesgo, convierte su red en un sistema de seguridad con soluciones diseñadas para interoperar y proporcionar protección en varias capas y

btiene una visibilidad profunda, es decir utiliza los datos en tiempo real para garantizar el acceso y detectar actividades sospechosas.




#makeIT
secure
Tenemos la solución para cada reto tecnológico de su empresa
TRANSFORMACIÓN DIGITAL
SMART SERVICES
CONSULTING
SEGURIDAD
INFRASTRUCTURE EXPERTS
www.gbm.net | mercadeo@gbm.net | GBMCorp
Contacte a la oficina GBM de su país y marque la extensión 3840 (Contact Center)
GBM
as a Service