

Guía de estrategias de ventas para soluciones de seguridad



SEGURIDAD: OPORTUNIDAD



Las ciberamenazas se han vuelto complejas y generalizadas. No se pueden erradicar mediante un enfoque de mosaico. Se requiere una nueva barrera impenetrable.

La mayoría de las vulneraciones de datos (48 %) fueron causadas por ataques malintencionados o criminales, el 25 % a causa de empleados o contratistas negligentes (factor humano) y el 27 % involucró fallas en el sistema que incluían fallas tanto de IT como de procesos comerciales.

La probabilidad de una vulneración de datos disminuye a medida que aumenta el tamaño del registro. Para 10,000 registros comprometidos, la estimación es del ~26 %. Para 100,000 registros, la probabilidad es inferior al 1 %.

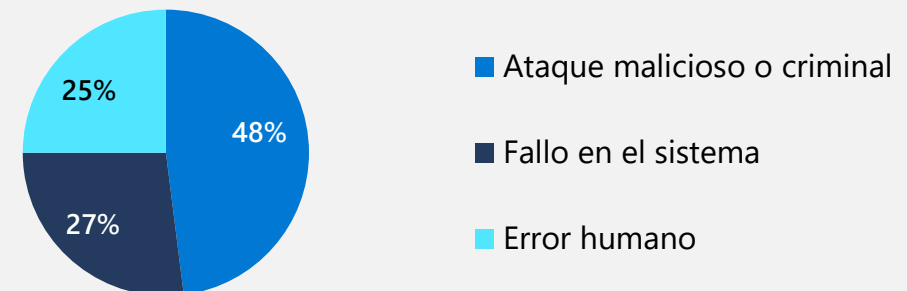
Las ciberintrusiones han aumentado un 400 % en la era del COVID, con impactos particulares en el fraude médico y financiero.

Costo de una vulneración

Una vulneración de datos tiene como consecuencia impactos financieros enormes, de acuerdo con *Ponemon Institute's 2016 Cost of Data Breach Study*. El costo total promedio de perder información corporativa o personal sensible se aproxima a los 4,000 millones de dólares.

Por registro robado, los costos comerciales y de asociación varían según el sector. En 2016, el costo global promedio por registro perdido o robado fue de 158 USD. Las organizaciones de atención médica tenían un costo promedio de 355 USD. Otros costos promedio: educación (246 USD), transporte (129 USD), investigación (112 USD) y sector público (80 USD).

- <https://www.cloudmask.com/blog/the-cost-of-data-security-are-cybersecurity-investments-worth-it>
- <https://www.cloudmask.com/hubfs/IBMstudy.pdf>



SEGURIDAD: PROPUESTA DE VALOR



La seguridad integrada de Microsoft es una solución de defensa empresarial inteligente y unificada que proporciona protección integral contra ataques

Reduzca costos con una solución integrada



Emplee la presencia de seguridad más grande y confiable del mundo.

Asegure los entornos híbridos de manera efectiva

Microsoft Zero Trust

Al implementar **Zero Trust**, Microsoft adopta un enfoque por capas para proteger los datos corporativos y de los clientes. La implementación por fases de **Microsoft Zero Trust** se centra en una identidad de usuario segura, verificación del estado del dispositivo, validación del estado de la aplicación y acceso seguro con menos privilegios a los recursos y servicios corporativos.

La seguridad digital se ha vuelto infinitamente compleja. Los datos se vuelven cada vez más valiosos cada día y son más difíciles de proteger. En lo que se refiere a la administración de la seguridad y la evaluación de amenazas, entre más grande, mejor.

- 1 **Magnitud:** Al unirse a Microsoft Trust Protection (MTP), los clientes repelen más amenazas mediante el acceso al vasto alcance y décadas de experiencia de Microsoft.
- 2 **Ahorre en grande:** el 40 % de las empresas apuntan a una mayor complejidad de la infraestructura como un motor clave de los presupuestos de ciberseguridad. Las soluciones integradas en la nube reducen los costos hasta un 52 %, ofreciendo un TCO más bajo que un enfoque de mosaico.
- 3 **Mayor eficiencia:** Haga que los equipos de seguridad interna sean más eficientes al apoyar al personal en vez de reemplazarlo.
- 4 **Escalar para adaptarse:** La seguridad de la nube de Azure crece junto con la empresa.
- 5 **Estándar del sector:** El enfoque en capas de Microsoft es el mejor en su clase en cinco categorías de soluciones de seguridad.
- 6 **Simplifique y unifique:** Un panel elimina la infraestructura de seguridad de IT adicional para proteger contra todos los escenarios de intrusión.

SEGURIDAD: INFORMACIÓN GENERAL DE LA SOLUCIÓN



Microsoft Threat Protection implementa una amplia gama de tecnologías de seguridad integradas para empresas y pymes. Logre mayor seguridad a menor costo al aprovechar la experiencia y potencia de Microsoft Threat Protection, Azure Security Center y Azure Sentinel

Microsoft Threat Protection (MTP)

- El conjunto de defensa empresarial
- Procesa 6.5 billones de señales diarias
- La mejor protección contra amenazas M365 de su clase
- Recopila datos, identifica amenazas, investiga usando AI, respuesta rápida

Microsoft Threat Protection es un conjunto de defensa empresarial unificada previa y posterior a la vulneración que coordina de forma nativa la detección, prevención, investigación y respuesta en puntos de conexión, identidades, correo electrónico y aplicaciones para proporcionar protección integrada contra ataques sofisticados.



Azure Sentinel

La vista panorámica de toda la empresa que pone en funcionamiento la nube y la inteligencia a gran escala de Microsoft, con décadas de experiencia en seguridad. Al hacer que la detección de amenazas y la respuesta ante ellas sea más rápida e inteligente. Elimina la instalación y el mantenimiento de la infraestructura de seguridad, y escala flexiblemente para satisfacer las necesidades de seguridad, a la vez que reduce los costos de IT.



Azure Security Center

El panel usado por el cliente es nativo de Azure. Proporciona al cliente las herramientas necesarias para tomar posesión de la seguridad de sus datos. La retroalimentación, con precisión de nanosegundos, proporciona supervisión continua para evaluar los niveles de amenaza de los visitantes.

Casos de uso clave



Mejore las operaciones de seguridad
Garantice la seguridad continua basada en la nube, con visibilidad mejorada y reducción de gastos generales



Modernice la arquitectura de seguridad
Use soluciones de seguridad integrales y proactivas que ayuden a proteger su patrimonio digital



Proteja el lugar de trabajo
Implemente una plataforma de productividad de clase mundial que proteja los puntos de conexión y los datos

SEGURIDAD: CLIENTES



- Defensa de alta prioridad
- Mejor postura de seguridad con protección flexible y conectada
- Potencia de un marco integrado

- Transforme la forma en que las personas trabajan entre sí y sus datos
- Ofrezca servicios de seguridad de próxima generación

- Cumplimiento del dispositivo
- Control estricto de identidad y administración del acceso
- Protección avanzada contra amenazas

- Mejore la capacidad de hacer fracasar las amenazas de seguridad.
- Mejore y unifique la protección de identidad en la nube.
- Prevenga filtraciones accidentales de datos.

Productos y servicios:

- Azure Advanced Threat Protection
- Azure Information Protection P2
- Cloud App Security
- Microsoft Defender Advanced Threat Protection

Productos y servicios:

- Azure Active Directory P1
- Enterprise Mobility + Security
- Microsoft Information Protection

Productos y servicios:

- Azure Active Directory
- Azure Multi-Factor Authentication
- Cloud App Security
- Conditional Access
- Enterprise Mobility + Security
- Microsoft 365 E5
- Microsoft Cloud App Security
- Microsoft Defender Advanced Threat Protection

Productos y servicios:

- Azure Active Directory P2
- BitLocker
- Cloud App Security
- Office 365 Advanced Threat Protection P1
- Azure Multi-Factor Authentication

Si dificulta la seguridad, la gente puede evitarla. Con Microsoft 365 obtenemos funcionalidades nativas, visibilidad de nuestro entorno operativo y simplicidad para todos los empleados.

Simon Hodgkinson

Director de seguridad de la información del grupo
BP



Confío en la solución Microsoft 365. Tengo confianza de almacenar nuestros documentos legales en OneDrive y SharePoint. También utilizo las funciones de administración de los derechos de información en Microsoft Information Protection para cifrar los archivos de acuerdo con sus niveles de seguridad. Es un gran activo en mi trabajo.

Frida Rosenholm

Vicepresidenta Senior, Asesora general
Securitas Group



Azure Active Directory detectó los intentos de acceso y luego orquestó la respuesta bloqueando al usuario y pidiéndole que cambiara su contraseña.

Doug Howell

Director de IT
The Little Potato Company



Queríamos aumentar nuestra seguridad para evitar el tipo de eventos que habíamos visto en otros lugares, y tenemos esas funciones avanzadas con Microsoft 365.

Tammy Stringer

Gerente de oficina
DJ Stringer Property Services

