ENTRUST
SECURING A WORLD IN MOTION

5 RAZONES

PARA INCORPORAR UN HSM NSHIELD PARA LA IMPLEMENTACIÓN DE AZURE

1 USTED ES LA PERSONA RESPONSABLE POR LOS DATOS DE SUS CLIENTES

El modelo de responsabilidad compartida muestra que, independientemente de cómo se entregue el servicio en la nube, los datos siempre son responsabilidad del cliente.

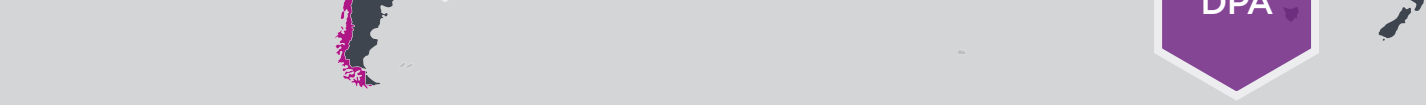
	Infraestructura como servicio (IaaS)	Plataforma como servicio (PaaS)	Software como servicio (SaaS)
Responsabilidad del cliente	Datos	Datos	Datos
	Aplicación	Aplicación	Aplicación
	Tiempo de ejecución	Tiempo de ejecución	Tiempo de ejecución
	Middleware	Middleware	Middleware
	Sistema operativo	Sistema operativo	Sistema operativo
Responsabilidad del proveedor	Virtualización	Virtualización	Virtualización
	Servidores	Servidores	Servidores
	Almacenamiento	Almacenamiento	Almacenamiento
	Redes	Redes	Redes

Fuente: https://gallery.technet.microsoft.com/Shared-Responsibilities-81d091

2 LAS BRECHAS A DATOS ESTÁN INCREMENTANDO

El número presentado de registros de consumidores expuestos que contienen información de identificación personal (PII) aumentó significativamente de 197,6 millones a 446,5 millones en 2018, un aumento del 126%. Es probable que el número total real de registros expuestos sea mayor, dado que solo la mitad de las infracciones informadas revelan el número.

Los datos expuestos del consumidor se dispararon un 126% en 2018



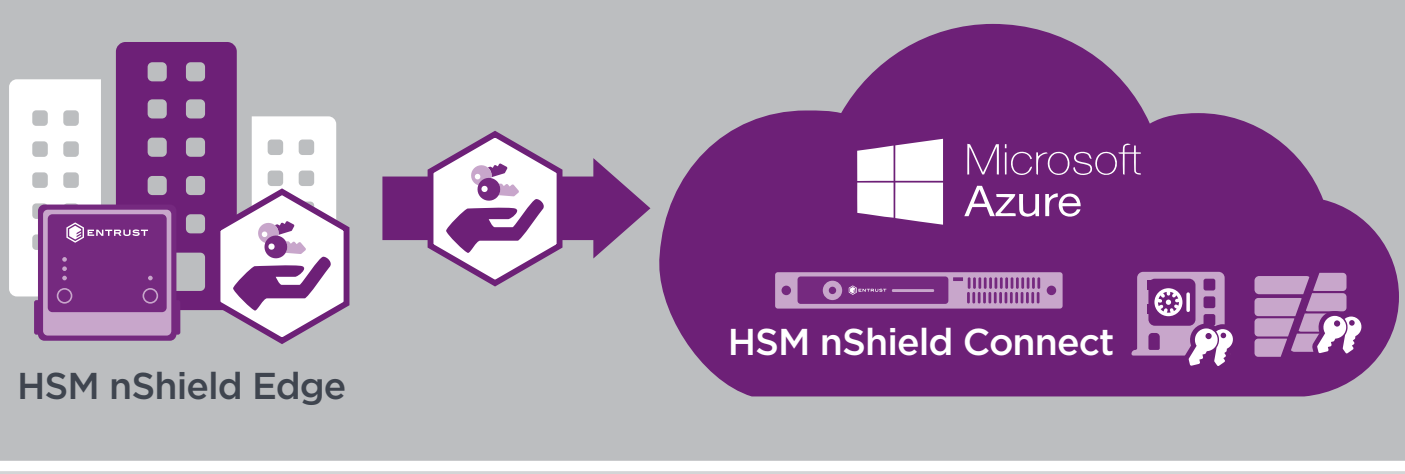
Fuente: Centro de recursos para el robo de identidades www.idtheftcenter.org/2018-data-breaches

3 USTED NECESITA CUMPLIR CON LAS REGULACIONES EN MATERIA DE CUMPLIMIENTO

Se están aplicando nuevas regulaciones de privacidad en todo el mundo, lo que significa que las empresas enfrentan una mayor responsabilidad, rendiciones y multas más severas. Los módulos de seguridad de hardware (HSMs) nShield® garantizan que esté utilizando las mejores prácticas.

4 USTED MANTIENE EL CONTROL SOBRE SUS CLAVES

Con traer su propia clave (BYOK) puede controlar y proteger los datos en la nube utilizando claves criptográficas de forma segura. Usted genera sus propias claves in situ, las claves se transfieren de forma segura a los HSMs en la nube y Azure usa las claves para proteger las aplicaciones y los datos, pero no puede verlos ni hacer un mal uso de ellas.



5 USTED AGREGA UNA RAÍZ DE CONFIANZA A SU NUBE

Los HSMs nShield proporcionan un entorno reforzado y resistente a manipulaciones indebidas para el procesamiento criptográfico seguro, la generación y protección de claves, el cifrado, la gestión de claves HSMs y más, proporcionando:

- Una capa adicional de seguridad para crear una plataforma de aplicaciones segura
- Aislamiento de operaciones y claves criptográficas
- Autenticación de usuario sólida mediante tarjetas inteligentes
- Controles duales reforzados y separación de funciones
- Generación de claves certificadas de alto rendimiento
- Potente aceleración y descarga criptográfica
- Certificación FIPS 140-2 L3

Haga clic para ver nuestro video *Traiga su propia clave con Entrust y Microsoft Azure*

Aprenda más en
entrust.com/HSM

ENTRUST
SECURING A WORLD IN MOTION

Entrust es una marca comercial registrada y/o una marca de servicio de Entrust Corporation en Estados Unidos y/o en otros países. ©2020 Entrust Corporation. Todos los derechos reservados.