# La guía definitiva para la protección de datos

Forcepoint

Folleto

## Descripción general del panorama

De alguna manera, la relación entre la seguridad de datos y el rendimiento comercial es tan antigua como el comercio en sí. Después de todo, la forma más simple de obtener una ventaja competitiva es la capacidad de una empresa de evitar que se divulgue su "receta secreta", es decir, un proceso exclusivo, propiedad intelectual crítica o incluso una receta literal.

Pero hoy, el problema es infinitamente más complejo. Se calcula que el 90 % de los datos globales se creó en tan solo dos años.[1] Además, la proliferación de los dispositivos móviles, las relaciones lejanas entre cliente y contratista, los empleados remotos e itinerantes y otros aspectos agravan ese efecto, ya que los datos están almacenados y se accede a ellos en más lugares, por parte de más personas, en cualquier momento.

Inmediatamente después de este cambio en el rol de los datos en el lugar de trabajo, las fugas de datos de alto perfil han ayudado a crear un nuevo caso comercial para la seguridad de datos. El impacto financiero es un factor, por supuesto; el costo promedio de una fuga de datos es de USD 3,26 millones.[2] Pero, en términos claros y simples, los incidentes de seguridad de datos pueden causar un daño crítico a la marca de la compañía y la confianza de sus clientes.

Durante mucho tiempo, las industrias altamente reguladas como la de la atención médica y los servicios financieros se han regido por leyes que establecen la protección de los datos confidenciales. Sin embargo, más recientemente, un mayor escrutinio público y conciencia sobre la seguridad de datos han contribuido a incentivar una nueva legislación para abordar de qué manera las empresas pueden recolectar, procesar y almacenar datos. La Ley de Protección de Datos Personales de Malasia, la Normativa General de Protección de Datos de la Unión Europea (GDPR), los Principios de Privacidad Australianos, la Ley de Privacidad del Consumidor de California, y la lista sigue. Y es suficiente para hacer que una organización, ya sea que esté sujeta o no a las normas vigentes, piense de manera crítica sobre la protección de datos.

**$3,26 millones**

Costo promedio de una fuga de datos[2]

**2.600-10.000**

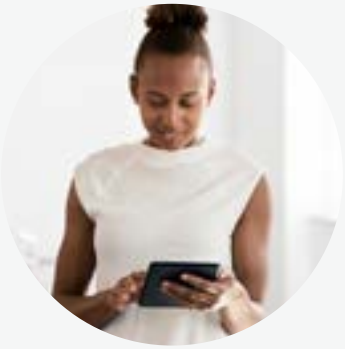
Cantidad de registros confidenciales en una fuga promedio[2]

**68 %**

Porcentaje de fugas de datos que pasan inadvertidas por meses[2]

En medio de todo esto, algo quedó claro: Darles poder a las compañías y los empleados para desempeñarse en el entorno comercial actual exige un cambio en la manera en que pensamos en la seguridad de datos. En el constante estado de cambio que se ha vuelto nuestra nueva realidad, las políticas reactivas ya no son suficientes para mantenernos a salvo. Exploremos cómo tomar una postura proactiva sobre la protección de datos, y por qué es la opción segura para las empresas en la actualidad.


**Se calcula que el 90 % de los datos globales se creó en tan solo dos años.[1]**



## Elevar el rol de la seguridad de datos

Para muchos equipos de seguridad de datos los días consisten en ciclos eternos de recibir una alerta, investigarla y reparar el daño. Una y otra vez. ¿El problema? Las políticas inflexibles a menudo señalan actividad de bajo riesgo, lo que da como resultado alertas de "falsos positivos". Investigar estos falsos positivos implica una inmensa carga para los equipos de seguridad de datos, quienes ya tienen más tareas y responsabilidades a su cargo que el ancho de banda con el que cuentan para llevarlas a cabo.

La tecnología de protección de datos que puede leer el contexto que rodea la actividad cibernética puede disminuir esta carga para los equipos de seguridad de datos y ayudarlos a centrar sus investigaciones en incidentes que realmente conlleven una amenaza, dejando de lado aquellos que no presentan un riesgo real para la empresa. Y, al priorizar su tiempo de manera más inteligente, el equipo de seguridad puede hacer evolucionar su rol dentro de una organización de simplemente aplicar reglas a dirigir en forma proactiva la empresa hacia un futuro más seguro y eficiente.

### Empoderar el crecimiento profesional

Los expertos en seguridad de datos que no están sobrepasados con alertas falsas tienen la capacidad de entrenar y guiar a otros empleados, contribuyendo así con su desarrollo profesional y trayectoria profesional.

### Empoderar el crecimiento comercial

Los profesionales de la seguridad que son capaces de encontrar eficiencias en sus propias cargas de trabajo pueden ayudar a señalar oportunidades para el crecimiento de la compañía a través de un uso más inteligente de los datos. (O bien, señalar comportamientos de datos que puedan impedir el crecimiento del negocio).

### Empoderar la transformación digital

La optimización de las investigaciones basadas en la comprensión del contexto de los incidentes relacionados con los datos brinda a los equipos el tiempo necesario para optimizar sus políticas y procedimientos para adaptarse a la cultura de datos impulsados por la nube, lo que permite una transformación digital más rápida y ofrece una ventaja competitiva a la empresa.

# Proteger los datos en los sitios en donde se realiza el trabajo

**La prevención contra la pérdida de datos protege los datos en tres puntos de acceso: en su red, en los dispositivos finales y, cada vez más, en la nube. Y eso podría ser suficiente, si las personas que acceden a esos datos se mantuvieran dentro de esos perímetros. Pero, cada vez más, no lo hacen y tan pronto se cruza el perímetro, se infringen las políticas de protección de datos. Eso significa que ya no es suficiente cumplir con las reglas. Analicemos qué se puede hacer para superar esto.**

## Implicaciones de la transformación a la nube

No hay que preguntarse "si" habrá una migración a la nube. Sino "cuándo" sucederá. Las demandas de contar con fuerzas laborales, clientes y socios estratégicos remotos solo aceleran los plazos, y requieren una adopción más rápida de la nube. ¿Un ejemplo? El 87 % de las compañías actuales dependen de empleados que acceden a sus aplicaciones comerciales móviles desde sus teléfonos inteligentes personales[3] , algo que se conoce como "traiga su propio dispositivo" o BYOD. Además, casi un cuarto de los trabajadores millenials dicen que han descargado archivos de la compañía en esos dispositivos e instalado aplicaciones en la nube de terceros ("traiga su propia nube" o BYOC) sin notificar a TI o al liderazgo ejecutivo. Estos comportamientos crean lo que se conoce como "Shadow IT", y demuestran que una empresa no siempre tiene control sobre cuándo y cómo pasan a la nube. Pero sin importar el ritmo, las políticas de seguridad arraigadas luchan por estar a la altura mientras se adaptan para satisfacer las nuevas demandas.

Un motivo es que los proveedores de aplicaciones en la nube tienden a priorizar la portabilidad, la accesibilidad y la facilidad de uso, no necesariamente la seguridad de los datos que se hicieron portables, accesibles y fáciles de usar. Se centran en un modelo de responsabilidad compartida en el que ellos protegen la infraestructura, pero dejan que los clientes se encarguen de proteger los datos que comparten en la infraestructura. Eso significa que, dada la naturaleza transitoria y móvil del trabajo en la actualidad, es su responsabilidad crear una protección de datos que acompañe al personal donde quiera que este vaya.

## Los seres humanos son el nuevo perímetro

¿Cómo puede mantener seguros los datos cuando las personas los utilizan más allá de sus líneas de defensa? Se requiere un nuevo perímetro: los seres humanos en sí mismos.

La protección de datos centrada en las personas permite que los datos se localicen en un entorno seguro al cual las personas pueden acceder desde el lugar en el que trabajan. Además, vincular la seguridad de datos a la identidad de una persona permite crear políticas que consideren el nivel de riesgo personal y proporcionen datos sobre la intención; por ejemplo, un incidente relacionado con un empleado confiable de larga data puede ser una preocupación menor que uno relacionado con un proveedor de reputación dudosa o un exempleado insatisfecho. Finalmente, supervisar la seguridad de datos a nivel de las personas proporciona visibilidad sobre cómo los utilizan en los diferentes dispositivos y aplicaciones, y brinda contexto que puede ayudar a los equipos de seguridad a identificar mejor las amenazas y a aprender de ellas.

# Creando un caso comercial para la protección de datos

**La protección de datos centrada en las personas se adapta bien a la realidad dinámica de los negocios de la actualidad, pero, ¿qué valor tiene para sus negocios? Para responder esta pregunta, refutaremos el mito que acosa a todos los equipos de seguridad de datos: que la protección es enemiga de la productividad. Con la implementación de las herramientas y los procesos adecuados, una puede fortalecer a la otra.**

### Respuestas específicas

Las tácticas tradicionales de prevención contra la pérdida de datos simplemente pueden bloquear acciones riesgosas, por ejemplo, un archivo confidencial de la compañía que se guarda en una unidad flash personal. Y, si dicha acción fuera realizada por un exempleado insatisfecho o un contratista a corto plazo, esa respuesta tiene sentido. Sin embargo, la mayoría de las veces, esto no es así; puede tratarse de un ejecutivo de la compañía que simplemente desea crear una copia de respaldo de un archivo importante o pasarlo a una computadora nueva. Pero las políticas tradicionales de seguridad de datos no pueden notar la diferencia, por lo que aplican bloqueos generales en forma rutinaria a actividades cibernéticas totalmente inocuas, y dificultan la productividad de la empresa en el proceso.

Detectar riesgos al nivel de las personas permite considerar el contexto y la intención detrás de una acción, lo que posibilita respuestas de seguridad específicas, y no generales. Esto no solo reduce las interrupciones en los flujos de trabajo de los empleados, sino que también disminuye la carga de investigaciones de los equipos de seguridad, y les permite colaborar con el progreso en lugar de obstruirlo.

### Menor vulnerabilidad

Incluso un empleado sin malas intenciones puede frustrarse con políticas de seguridad generales que le impidan realizar su trabajo. Por eso (aún sin malas intenciones) pueden intentar buscar un atajo, burlando levemente las reglas para poder atravesar el bloqueo de seguridad. En el último ejemplo, tal vez dividan el archivo en segmentos más pequeños y los envíen por correo electrónico a una computadora personal para poder guardarlos en la unidad finalmente.

Esto crea dos problemas: Primero, esta secuencia de acciones puede activar una alarma incluso más urgente que un intento de guardar un archivo en una unidad portátil, ya que indica que la persona está intentando eludir las medidas de seguridad. Probablemente se deberá investigar el caso, lo que requiere tiempo y recursos. Pero tal vez lo más preocupante es que los atajos como este, aunque sean inocentes, pueden introducir nuevas vulnerabilidades que debilitan las políticas de seguridad que las señalaron en un principio. La protección de datos centrada en las personas permitiría contar con políticas adecuadas más flexibles que detendrían esta espiral descendente antes de su comienzo.

### Postura proactiva

Como pueden confirmar cualquier maestro, dueño de una mascota o profesional de seguridad de datos, evitar un "lío" en primer lugar es más eficiente que limpiarlo después.

Con las pistas contextuales y el conocimiento conductual que proporcionan los datos centrados en las personas, es posible detener las verdaderas amenazas antes de que causen daño, a la vez que la compañía desempeña sus actividades en el más alto nivel. Los empleados pueden trabajar sin tener que lidiar con políticas de seguridad sumamente inflexibles. Los equipos de seguridad de datos ocupados pueden clasificar correctamente las alertas y centrarse en la resolución de los incidentes que presentan un riesgo real. Es seguridad de datos, sin riesgos.

## El nuevo estándar para la protección de datos

La naturaleza en evolución de las amenazas de seguridad plantea la necesidad de que modifiquemos nuestra mentalidad para mantener los datos protegidos, y eso incluye aceptar que el cambio es, y siempre será, constante. Es por eso que nuestros principios fundamentales para la protección de datos se crean teniendo en cuenta las necesidades del futuro:

**1. Una cultura de seguridad de datos preventiva, y no correctiva**

El rol de los equipos de seguridad de datos pasará de aplicar políticas de seguridad en forma retroactiva a dirigir a sus organizaciones y colegas hacia nuevos comportamientos de uso de datos más seguros.

**2. Evaluación de riesgos centrada en las personas**

El uso de datos móviles y dinámicos exige una seguridad capaz de dar cuenta de la única constante: el usuario. Esto permite tener una seguridad flexible que se adapte a medida que cambia el comportamiento y nivel de riesgo de una persona.

**3. Visión holística de los datos**

Mantener una visibilidad completa de los datos a medida que se mueven fuera de su red, por los dispositivos finales o hacia la nube brinda pistas contextuales sobre la intención, y ayuda a fundamentar respuestas de seguridad adecuadas.

**4. Políticas constantes independientes del entorno**

Establecer su perímetro de seguridad a nivel de las personas garantiza que los datos están protegidos sin importar dónde se los almacene o desde dónde se acceda a ellos.

### ¿Listo para ver lo que viene en el camino hacia la protección de datos proactiva?

› **Vea nuestra infografía**
9 pasos para proteger sus datos con éxito.

1. IBM Marketing Cloud, "10 Key Marketing Trends for 2017" (10 tendencias de marketing clave para 2017)
2. Ponemon Institute, "U.S. Cost of a Data Breach Study" (Estudio sobre el costo de una fuga de datos en los EE. UU.), 2017
3. Syntonic, "BYOD Usage in the Enterprise" (Uso de BYOD en la empresa), 2016

Forcepoint

**forcepoint.com/contact**

## Acerca de Forcepoint

Forcepoint es la compañía líder en ciberseguridad de protección de datos y usuarios, encargada de proteger a organizaciones a la vez que impulsa la transformación digital y el crecimiento. Las soluciones de Forcepoint se adaptan en tiempo real a la manera en que las personas interactúan con los datos, y proporcionan un acceso seguro a la vez que permiten que los empleados generen valor. Con sede en Austin, Texas, Forcepoint crea entornos seguros y fiables para miles de clientes en todo el mundo.