



# 3 PASOS PARA MEJORAR SU ESTRATEGIA DE DATOS DE CIBERSEGURIDAD



CHAMPION  
GUIDES

EBOOK

# ÍNDICE

- 3** Introducción
- 4** Paso 1: Tome el control de sus datos
- 6** Paso 2: Lleve a cabo una búsqueda proactiva de amenazas en todos sus datos
- 7** Paso 3: Fomente la colaboración con el equipo de datos
- 9** Conclusión: Un buen programa de ciberseguridad requiere una estrategia de datos moderna
- 10** Acerca de Snowflake

# INTRODUCCIÓN

Las organizaciones de seguridad pueden beneficiarse de las inversiones existentes en plataformas de datos para afrontar mejor las amenazas y reducir los riesgos para la empresa.

¿Puede un mejor acceso a los datos resolver una contradicción multimillonaria en el sector de la ciberseguridad? Según **Gartner**<sup>®</sup>, en 2021 se gastaron aproximadamente 150 400 millones de dólares en tecnología y servicios de gestión de riesgos y seguridad de la información en todo el mundo. Hace apenas 15 años, esa cifra era de tan solo 3500 millones, según informaba **Cybersecurity Ventures**. Aun así, las infracciones de ciberseguridad han alcanzado niveles récord y los riesgos nunca habían sido tan altos. **IBM** estima que una sola filtración de datos cuesta a las organizaciones 4,2 millones de dólares de media, la cifra más alta en los 17 años que IBM lleva informando sobre filtraciones de datos.

Esta contradicción entre la inversión y los resultados es consecuencia de una creciente asimetría entre los autores de las amenazas y los equipos que las defienden. Los cibercriminales se han adaptado rápidamente a las nuevas tendencias empresariales, como la infraestructura dinámica en la nube, las cadenas de suministro de software interconectadas y una plantilla que trabaja, sobre todo, fuera de la oficina. Así, aprovechan la escala y complejidad de sus objetivos para acceder sin ser detectados hasta que alcanzan sus objetivos. Mientras tanto, los equipos de seguridad tratan de entender el nuevo entorno empresarial y el panorama de amenazas con ayuda de soluciones obsoletas.

Al tiempo que los defensores se quedaban atrás en la carrera por garantizar la seguridad de la empresa, otros departamentos disfrutaban de toda una serie de ganancias derivadas de la innovación en la pila de

datos moderna. En este sentido, ha surgido una oportunidad para que los defensores superen a sus adversarios si tratan la ciberseguridad como si fuera un problema de datos. Las organizaciones de ciberseguridad que tendrán éxito serán aquellas capaces de movilizar los datos sin limitaciones entre distintas fuentes y a lo largo del tiempo, con todas las ventajas que aportan los avances en plataformas y análisis de datos.

En el centro de esta nueva estrategia se encuentra la adopción de un data lake de seguridad centralizado, impulsado por una moderna plataforma de datos en la nube. Un data lake de seguridad permite a las organizaciones eliminar las limitaciones tradicionales de visibilidad y coste relativas a la cantidad de datos que es posible introducir, almacenar y conservar, y durante cuánto tiempo. También es esencial que sea compatible con lenguajes de análisis estándar (por ejemplo, SQL y Python), ya que esto posibilita la colaboración entre analistas de seguridad, como expertos en la materia, analistas de datos para elaboración de informes de autoservicio y científicos de datos para modelos de comportamiento y aprendizaje automático. Además, la compatibilidad con controles de acceso exhaustivos y con el intercambio de datos seguro hace posible la colaboración en el interior de la organización, entre homólogos del sector y con terceros proveedores de datos, todos ellos aspectos cruciales de los data lakes de seguridad actual.

En las páginas siguientes, compartiremos tres pasos probados que puede seguir para realizar con éxito la transición a una estrategia de ciberseguridad basada en datos.

# PASO 1: TOME EL CONTROL DE SUS DATOS

Controlar los datos significa tener plena libertad para introducir y retener tantos datos como desee, libertad para analizar conjuntos de datos, ya sean recientes o históricos, y libertad para elegir las soluciones de seguridad que le apoyarán en su misión de proteger su empresa.

## DESAFÍO: LAS SOLUCIONES DE SIEM TRADICIONALES LIMITAN LA LIBERTAD Y EL CONTROL DE LOS DATOS

La mayoría de los equipos de seguridad utilizan una solución de gestión de eventos e información de seguridad (SIEM) para la detección de amenazas y la respuesta a incidentes. SIEM es la fuente de verdad del programa de seguridad. Sin embargo, las SIEM heredadas se integran verticalmente y requieren el uso de sus propias bases de datos integradas. Como era de esperar, estos proveedores no han logrado mantener el rendimiento y la escalabilidad de las plataformas de datos en la nube de uso general, que funcionan como una pila de datos independiente para la ciberseguridad, apartada del resto de la empresa.

Como consecuencia, los equipos de seguridad deben lidiar con analíticas rudimentarias y silos de datos fragmentados. A veces se pueden examinar algunos datos de seguridad, pero no se pueden combinar fácilmente con datos contextuales, que podrían incluir datos empresariales o cualquier otro dato que proporcione a los equipos de seguridad más contexto sobre una posible amenaza. Los datos de seguridad por sí solos no son suficientes para evaluar a fondo las posibles amenazas.

Además, los elevados costes de licencia de las SIEM tradicionales obligan a sus usuarios a almacenar cada vez más datos de seguridad en otros lugares, especialmente en contenedores en la nube que solo resuelven el problema del almacenamiento. Este enfoque conlleva procesos engorrosos y una sobrecarga cuando hay que integrar estos conjuntos de datos para el análisis, lo que alarga los tiempos de respuesta durante una infracción y no admite casos de uso clave, como la búsqueda de amenazas y la inteligencia contra amenazas. Aspectos relacionados con la gobernanza de datos agravan los problemas de proliferación de datos en forma de niveles de almacenamiento autogestionados.



## SOLUCIÓN: CENTRALÍCELOS EN UN DATA LAKE DE SEGURIDAD CREADO PARA LA NUBE

Un data lake de seguridad moderno es un repositorio en el que los registros y otros conjuntos de datos se almacenan en un espacio económico y casi ilimitado, donde se pueden analizar rápidamente. Los data lakes modernos están diseñados para proporcionar un acceso centralizado y seguro a los datos de una organización. Cuando las organizaciones centralizan sus datos de seguridad en una única plataforma, se pueden obtener multitud de ventajas inmediatas, entre las que se incluyen:

- **La capacidad de introducir y retener petabytes de registros de eventos de forma rentable**
- **La oportunidad de integrar datos de seguridad con datos empresariales y de aplicaciones para contextualizar y, en última instancia, automatizar las operaciones de seguridad**
- **La libertad de realizar investigaciones sin saber por adelantado qué registros de datos pueden ser relevantes ni tener que recuperar datos históricos de archivos de reserva**
- **La capacidad de controlar qué proveedores tienen acceso a los distintos conjuntos de datos**
- **La flexibilidad para migrar soluciones de seguridad sin tener que mover los datos recopilados**

Un data lake de seguridad moderno permite a equipos de toda la empresa acceder a una fuente única de verdad para diferentes casos de uso relacionados con la ciberseguridad: detección de amenazas y respuesta, gestión de vulnerabilidades, automatización de la conformidad y elaboración de informes de riesgo para juntas directivas.

Además de habilitar y acelerar las iniciativas de los programas de seguridad, un data lake de seguridad moderno puede fomentar el ahorro de costes y la eficiencia presupuestaria. Un almacenamiento económico con compresión en reposo implica menores costes de almacenamiento. Aún más importante es la potencia de procesamiento flexible y casi infinita que proporcionan las principales plataformas de datos en la nube. Ya no es necesario hacer un aprovisionamiento excesivo de recursos. Las plataformas que combinan elasticidad informática con sistemas de tarificación por consumo permiten a los clientes pagar únicamente por los recursos que necesitan, cuando los necesitan. En el contexto de la ciberseguridad, donde a menudo se necesita un poco de potencia pero ocasionalmente mucha más, ese modelo libera totalmente el presupuesto de seguridad para otros usos.

La implementación de un data lake de seguridad moderno y creado para la nube puede resultar transformadora para una organización. Al alojar los datos en una única plataforma, sus equipos de seguridad tienen la oportunidad de simplificar la pila de tecnología, consolidar almacenes de datos dispares y posibilitar analíticas avanzadas con diferentes casos de uso. Las funciones de gobernanza y la auditoría centralizada proporcionan garantías, mientras que las oportunidades de colaboración de datos impulsan a los saturados equipos de seguridad para que tengan éxito en sus iniciativas críticas durante años.



# PASO 2: LLEVE A CABO UNA BÚSQUEDA PROACTIVA DE AMENAZAS EN TODOS SUS DATOS

El panorama de las amenazas está evolucionando rápidamente, y las empresas dependen cada vez más de terceros en las cadenas de suministro y en la infraestructura basada en SaaS. Para mitigar el riesgo resultante para la empresa, es necesario adoptar una postura pesimista en la que se asume que los ataques ocurrirán. Por desgracia, la mayoría de los equipos de seguridad siguen un enfoque de “castillo y foso”, en el cual las amenazas que atraviesan las defensas iniciales pueden persistir dentro del entorno durante meses. Este peligroso statu quo se debe en gran medida a limitaciones impuestas por las soluciones SIEM heredadas.

## **DESAFÍO: LOS CAZADORES DE AMENAZAS NO TIENEN ACCESO A LOS DATOS Y LAS ANALÍTICAS QUE NECESITAN**

Aunque la detección básica de amenazas se puede realizar en tiempo real a medida que se recopilan los registros de eventos, la detección avanzada y la búsqueda proactiva de amenazas requieren una combinación de conjuntos de datos entre distintas fuentes y marcos temporales. Los autores de las amenazas, especialmente una vez que han puesto pie en el entorno, tienen una ventaja importante y un montón de sitios donde esconderse. Esto es lo que hace que los cazadores de amenazas sean tan valiosos para los programas de seguridad empresarial.

Lamentablemente, los cazadores de amenazas no pueden tener éxito si no obtienen respuesta a sus

preguntas. Cuando los datos se almacenan en silos en varios sistemas de origen, se guardan en sistemas de reserva o se pierden a causa de las políticas de retención, los cazadores de amenazas no pueden utilizarlos. Los cazadores de amenazas también se ven frenados cuando sus consultas tardan horas en ejecutarse, sus búsquedas devuelven mensajes de error crípticos “sin memoria” o tienen que batirse por los recursos con otros equipos.

Por último, la mayoría de los productos de seguridad heredados restringen las consultas a lenguajes de búsqueda propios o a técnicas rudimentarias grep/regex. Esto conlleva una curva de aprendizaje para los nuevos miembros del equipo e impide a los cazadores de amenazas expresar correctamente sus hipótesis en forma de código.

## **SOLUCIÓN: OFREZCA A LOS CAZADORES DE AMENAZAS UNA PLATAFORMA DE DATOS EN LA NUBE QUE ADMITA ANALÍTICAS A ESCALA**

Para posibilitar la búsqueda proactiva de amenazas, es clave contar con una arquitectura de datos creada para la nube que se apoye en un data lake de seguridad y elimine los silos de datos. Una vez establecida, los analistas de seguridad experimentados pueden empezar a descubrir rápidamente las amenazas latentes utilizando técnicas analíticas estándar y universales. Con un motor de consulta suficientemente eficaz, los cazadores de amenazas pueden trabajar con meses o años de datos medidos en petabytes.

Incluso los miembros con menos experiencia del equipo de operaciones de seguridad pueden participar en colaboración con analistas de datos de

toda la empresa. Aunque los analistas de datos nunca podrían ayudar en la búsqueda de amenazas en un entorno de nicho, exclusivamente de seguridad, son expertos en convertir la lógica empresarial en SQL dentro de la plataforma de datos de la empresa con la que están familiarizados. Hablaremos más sobre esto más adelante.

Las plataformas de datos en la nube que ofrecen un data marketplace con listas de inteligencia frente a amenazas permiten obtener más beneficios en la búsqueda de tales amenazas. Estos marketplace de datos basados en una moderna tecnología de data sharing permiten a los proveedores inteligencia frente a amenazas y a los organismos de investigación publicar indicadores de compromiso (indicators of compromise, IOC) y otros productos para un uso casi instantáneo. Los equipos de seguridad que utilizan las fuentes de inteligencia de este modo son capaces de aplicar automáticamente y sin problemas IOC actualizados a sus datos de registro. De este modo, los cazadores de amenazas y las herramientas de automatización pueden detectar de forma fiable a los agentes maliciosos conocidos sin la sobrecarga que conllevan las integraciones de API o la búsqueda manual de indicadores en un portal.

Las formas en que este enfoque faculta a los cazadores de amenazas son representativas de la gran oportunidad que presenta la ciberseguridad para coordinarse con la estrategia de datos de toda la empresa: A medida que surjan nuevas capacidades y metodologías de análisis de datos, los defensores reducirán cada vez más la ventaja de los ciberdelincuentes.

# PASO 3: FOMENTE LA COLABORACIÓN CON EL EQUIPO DE DATOS

La división que crece más rápido en muchas empresas es el equipo de datos. Analistas de datos, ingenieros de datos y científicos de datos son agentes clave para el departamento de marketing, el financiero y otros departamentos de una organización. Hoy en día, los responsables de la seguridad están poniendo en marcha tecnologías y procesos que permiten detectar las amenazas y reducir el riesgo a través de la colaboración entre los equipos de seguridad y de datos.

**DESAFÍO: LOS EQUIPOS DE SEGURIDAD DEDICAN DEMASIADO TIEMPO A TAREAS NO ASOCIADAS A LA SEGURIDAD, INCLUIDA LA RECOPILACIÓN DE DATOS Y LA GENERACIÓN DE INFORMES PARA LAS PARTES INTERESADAS**

Cuando su equipo se ve desbordado tratando de estar a la altura los atacantes, no tiene sentido que dedique tiempo a algo que no requiera su experiencia. En lugar de analizar las alertas o investigar las amenazas, muchos equipos de seguridad dedican gran parte de su tiempo a buscar datos, actualizar hojas de cálculo o reavivar clústeres de búsqueda.

La seguridad también desempeña un papel importante en las certificaciones y auditorías que las empresas deben mantener para vender a sus clientes. Esto puede convertirse en una gran carga cuando implica la participación de los equipos de ciberseguridad en interminables reuniones entre partes interesadas en los ámbitos de cumplimiento de normativas, TI, DevOps y liderazgo.

A partir de tres décadas y dos enfoques muy diferentes para permitir un análisis de datos eficaz, ha surgido la plataforma de datos moderna. Esta representa la potencia del almacenamiento de datos, la flexibilidad de las soluciones de big data y la elasticidad de la nube a un coste menor que el de las soluciones anteriores.



## **SOLUCIÓN: ESTABLEZCA UNA ASOCIACIÓN ENTRE LOS ANALISTAS DE SEGURIDAD Y LOS PROFESIONALES DE LOS DATOS PARA PROTEGER LA EMPRESA JUNTOS**

Revise las distintas formas en que el equipo de seguridad invierte su tiempo. ¿Qué tareas no requieren su experiencia en la materia? De estas tareas, ¿cuáles se ocupan principalmente de la preparación, el análisis y la elaboración de informes sobre los datos? Involucra a sus compañeros del equipo de datos en un debate abierto sobre estas áreas de colaboración.

Por ejemplo, recopilar los registros de RR. HH. para enriquecimiento en la detección y respuesta puede ser una tarea del flujo de datos de la que se pueden encargar mejor los ingenieros de datos. Medir el rendimiento del SLA relativo a los parches de seguridad es algo sencillo para los analistas de datos. E identificar movimientos inusuales de los archivos contando con los registros de actividad adecuados puede ser un juego de niños para los científicos de datos.

La integración de los datos de seguridad con el resto de la organización sienta las bases para una alianza entre los equipos de seguridad y los profesionales de los datos. Esta colaboración puede mejorar enormemente la capacidad de una organización para lograr análisis de seguridad de alta fidelidad, a la vez que se aprovecha al máximo el talento de la empresa.

Los informes de inteligencia empresarial (BI) de autoservicio pueden ser una forma excelente de eliminar reuniones y de sacar a los equipos de seguridad de la ruta crítica de procesos rutinarios de la empresa. Por ejemplo, un programa típico de gestión de parches puede implicar que los ingenieros de seguridad evalúen el riesgo de las vulnerabilidades detectadas y que los analistas de cumplimiento prioricen la corrección de esas vulnerabilidades. Esa priorización podría basarse en el lugar en el que se dan los problemas (producción orientada al cliente vs. entorno de pruebas interno, por ejemplo) y en el tiempo que llevan existiendo. Estas consideraciones se derivan de los marcos de cumplimiento a los que la empresa debe adherirse para poder seguir prestando servicio a sus clientes.

Los paneles de control prácticos que aplican la lógica empresarial y conjuntos de datos contextuales a los problemas de seguridad de forma automática y oportuna ofrecen a los equipos responsables de la corrección la posibilidad de solucionar los problemas sin necesidad de reuniones. Las actualizaciones de estado también se eliminan cuando cualquier persona autorizada puede ver el estado más reciente en la herramienta de BI empresarial. Los analistas de datos hacen esto sistemáticamente para otros departamentos, lo que significa que puede llevar esta transformación digital a su equipo de seguridad.

Este enfoque hace que la ciberseguridad pase de ser una práctica reactiva y compartimentada a un sistema de amplia colaboración para resolver problemas con soluciones basadas en datos.

# CONCLUSIÓN: UN BUEN PROGRAMA DE CIBERSEGURIDAD REQUIERE UNA ESTRATEGIA DE DATOS MODERNA

Ahora conoce tres pasos demostrados para mejorar su estrategia de datos de ciberseguridad. Se trata de una parte esencial para proteger a una organización moderna en la nube frente a las ciberamenazas.

Para alcanzar el éxito, los analistas de seguridad necesitan un data lake de seguridad moderno, habilitado por una plataforma de datos en la nube y ofrecido como servicio para acceder rápidamente a los datos relevantes en una ubicación central. Esto es aplicable tanto a grandes empresas en expansión como a ágiles empresas emergentes. Una sola infracción puede significar el fin para cualquier tipo de organización.

Recuerde que sus equipos de ciberseguridad no deben seguir operando por su cuenta, sin acceso a las herramientas de datos y a la experiencia que ahora están presentes prácticamente en cualquier empresa. Los responsables de la seguridad pueden sentar las bases para que el equipo aproveche la experiencia de otras divisiones de la organización y, así, centrarse en los componentes de ciberseguridad de los que nadie más se encargará.

Si sigue los tres pasos descritos en este ebook, puede pasar de una gestión reactiva de la ciberseguridad a apoyar cada vez más los enfoques proactivos, como la búsqueda de amenazas y la elaboración de informes de autoservicio. Con el tiempo, un enfoque basado en datos permitirá a su equipo de ciberseguridad alcanzar todo su potencial y convertir con éxito las inversiones en seguridad en una mayor garantía para su empresa y sus clientes.





## ACERCA DE SNOWFLAKE

Snowflake permite a cualquier organización movilizar sus datos con Snowflake Data Cloud. Los clientes utilizan el Data Cloud para unificar, descubrir y compartir datos de forma segura, impulsar las data applications y ejecutar diversos workloads analíticos y de inteligencia artificial (IA) y aprendizaje automático (machine learning, ML). Independientemente de la ubicación de los datos o de los usuarios, Snowflake ofrece una experiencia de datos única que abarca varias nubes y regiones geográficas. Miles de clientes de numerosos sectores, incluidas 590 de las empresas que figuran en Forbes Global 2000 (G2K) (2022), a fecha de 30 de abril de 2023, utilizan Snowflake Data Cloud para impulsar sus negocios. Más información en [snowflake.com](https://www.snowflake.com)



©2022 Snowflake Inc. Todos los derechos reservados. Snowflake, el logotipo de Snowflake y el resto de nombres de productos, funciones y servicios de Snowflake mencionados en este documento son marcas registradas o marcas comerciales de Snowflake Inc. en Estados Unidos y otros países. El resto de logotipos o nombres de marcas mencionados o utilizados en este documento se usan únicamente con fines identificativos, y pueden ser las marcas comerciales de sus respectivos titulares. Snowflake puede no estar asociado con, patrocinado o apoyado por cualquiera de dichos titulares.

---

### CITAS

<sup>1</sup> Conforme a las previsiones de Gartner, el gasto en gestión de riesgos y seguridad mundial superará la cifra de 150 000 millones de dólares en 2021

<sup>2</sup> El gasto en ciberseguridad global superará el 1,75 billones de dólares entre 2021 y 2025