VARONIS

# Librar una batalla diferente

El enfoque único de Varonis con respecto a la ciberseguridad

# Introducción

A medida que las organizaciones se transforman y se basan cada vez más en los datos, almacenan más información en repositorios locales y en la nube a la que los empleados acceden desde cualquier lugar con teléfonos, tabletas y computadoras portátiles. El perímetro de seguridad está mucho menos definido y los puntos finales son intercambiables: actualmente, muy pocos datos se alojan únicamente en su teléfono o computadora portátil.

Esta transformación digital ha cambiado por completo el modelo de seguridad tradicional que se centró en el perímetro y los puntos finales. En lugar de enfocarse en la seguridad desde afuera hacia adentro, las organizaciones están empezando a pensar en ella desde adentro hacia afuera, es decir, en la seguridad centrada en los datos en primer lugar.

La protección de los datos es intuitivamente simple, pero inmensamente compleja.

¿Por qué la protección de datos es intuitivamente simple?

Diría que si puede responder de forma afirmativa a estas tres preguntas, y si puede hacerlo de forma continua, sus datos están seguros:

1. ¿Sabe **dónde se almacenan sus datos importantes?**
2. ¿Sabe si **solo las personas adecuadas tienen acceso a ellos?**
3. ¿Sabe si **esas personas están usando los datos correctamente?**

Es simple, ¿no?

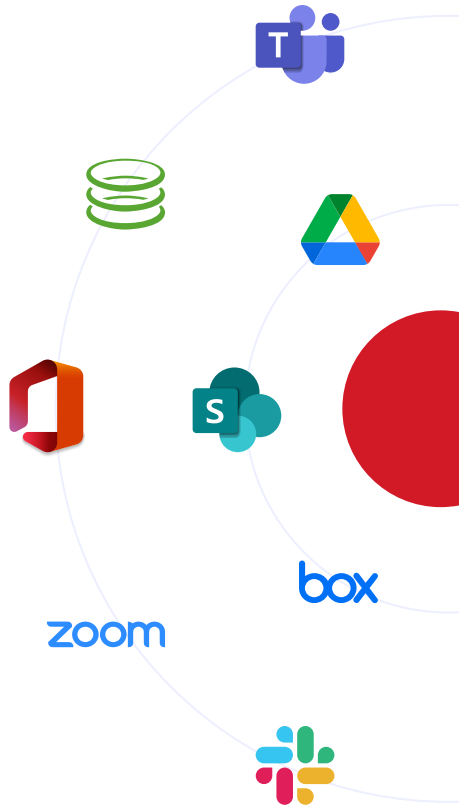
Estas son las tres dimensiones fundamentales de la protección de datos: importancia, accesibilidad y uso. Si trabaja en TI o seguridad de TI, sabe que comprender estas dimensiones no es para nada sencillo.

Es probable que también sepa que, si no puede responder afirmativamente a estas preguntas, o si no puede responderlas en absoluto, estas darán paso a otras preguntas que tienen consecuencias urgentes para los CISO, el personal de cumplimiento, las juntas directivas y las partes interesadas:

- ¿Dónde se alojan nuestros datos confidenciales y regulados?
- ¿Dónde permiten demasiado acceso y se encuentran en mayor riesgo?
- ¿Cuál es el radio de ataque potencial para una cuenta o un empleado que han sido vulnerados?
- ¿Cómo sabríamos si se robaron, cifraron o eliminaron datos?
- ¿Podemos eliminarlos?

Cada vez es más difícil responder a estas preguntas a medida que el volumen de datos crece tanto en los almacenes locales como en los de la nube, en las aplicaciones y en los repositorios de datos, ya que cada uno de estos cuenta con su propio modelo de seguridad. Hacer que la protección de los datos funcione correctamente en un solo sitio ya es bastante complicado, y lo es mucho más si hay que hacerlo en varios sitios a la vez.

# ¿Dónde se supone que deben alojarse nuestros datos?




En los últimos años, la cantidad de sitios en los que podemos alojar datos se ha disparado, y es frecuente que los usuarios accedan a sus datos desde diferentes dispositivos y puntos finales. Los puntos finales ahora funcionan principalmente como puertas de enlace hacia los sitios en los que verdaderamente se alojan los datos, que ahora suele ser una aplicación en la nube.

En la actualidad, la mayoría depende de una combinación de aplicaciones e infraestructura en la nube para operar, además de su infraestructura local. Cada vez es más inusual que una organización no autorice el uso de Microsoft 365, Box, Google Drive o Slack para la colaboración; GitHub o Jira para crear código fuente; AWS, Azure o Google Cloud para descargar cómputo o almacenamiento; o que no permita el uso de una solución CRM como Salesforce.com.

# ¿Dónde se alojan los datos importantes?

Incluso en el ámbito de estas aplicaciones autorizadas, la superficie es muy amplia y difícil de visualizar y evaluar en términos de riesgo. Algunas organizaciones optan por concentrar sus esfuerzos al pedirles a los empleados que etiqueten los archivos, o al utilizar la automatización para identificar o clasificar los datos regulados o confidenciales con la esperanza de poder priorizar los esfuerzos de protección de los datos.

Sin duda tiene sentido dividir un problema enorme en piezas más pequeñas, pero el problema se ha vuelto tan grande que incluso estas piezas más pequeñas pueden ser abrumadoras.

La mayoría de las organizaciones se sorprenden con la cantidad de archivos y registros confidenciales que encuentran. Miles de archivos aquí, miles o decenas de miles allá, y la lista será diferente mañana y pasado mañana.

Aquellos que lleguen a este punto sin un plan de acción claro pueden quedarse atascados sobre qué hacer a continuación. Algunos evalúan un enfoque de fuerza bruta, como trasladar todo lo que encuentran a otro lugar, como un repositorio local, eliminar todo lo posible o encriptar todo, de modo de restringir el acceso únicamente a los empleados o a un pequeño grupo que acaba de heredar un gran problema.

Sin embargo, estos enfoques no resuelven realmente el problema central: garantizar que solo las personas adecuadas puedan acceder a los datos. Este enfoque se conoce como principio de privilegios mínimos de acceso, o ahora, más popularmente como Zero Trust (confianza cero).

Para garantizar que el acceso sea el correcto para todos los datos, ya sean confidenciales o de otro tipo, primero debe poder ver quién tiene acceso a ellos; eso es casi siempre más difícil de responder de lo que la gente cree, en especial en lo que respecta a la nube.

# ¿Quién tiene acceso a nuestros datos importantes? ¿Quién *debería* tener acceso?

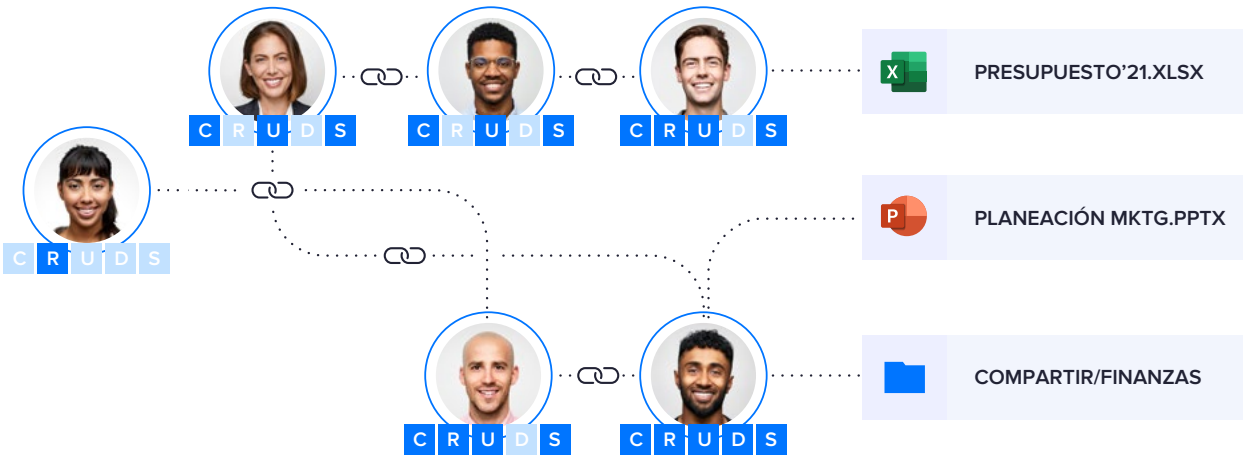
Al no comprender qué datos están regulados o son confidenciales, no debería sorprendernos que las decisiones en torno a quién debería tener acceso a ellos deban tomarse sin un contexto muy importante. Lo que a menudo sorprende es lo difícil que es ver quién tiene acceso en primer lugar.

El acceso a los datos se maneja mediante permisos o listas de control de acceso. La lógica es bastante uniforme en todas las aplicaciones y los repositorios de datos:

- Hay un **objeto,** como un archivo, una carpeta o un registro.
- Hay **identidades digitales** que corresponden a usuarios, cuentas y grupos de usuarios y cuentas que pueden hacer cosas con esos objetos.
- Hay una **descripción de las acciones que pueden realizar,** como crear, compartir, eliminar, etc.

Aunque la lógica es casi la misma, ya sea que se refiera a Slack, Box, SharePoint Online o a sistemas de archivos locales o UNIX, las implementaciones son diferentes:

- Los objetos son similares, pero hay diferentes tipos de objetos según la aplicación (por ejemplo, archivos, sitios, registros, buckets).
- Los usuarios/las cuentas y los grupos se almacenan en varios lugares; en la nube, cada repositorio de datos suele tener su propia base de datos de usuarios y grupos. A veces, se conectan con otras cuentas (como una cuenta Okta), y a veces hay cuentas personales y corporativas a las que se debe hacer un seguimiento. Cada una de estas aplicaciones puede asignar atributos a objetos de usuarios y de grupos, como el título, el rol y la ubicación.






VARONIS

Lo que pueden hacer se describe de manera diferente en cada aplicación, aunque en su mayoría incluyen crear, leer, actualizar, eliminar y compartir.

Además de estas diferencias, calcular los derechos efectivos para un objeto o usuario determinado puede ser muy complejo y varía mucho entre repositorios. Para determinar los derechos efectivos sobre un objeto determinado se deben considerar múltiples atributos, que incluyen lo siguiente:

- **Permisos específicos para objetos.** Como se mencionó anteriormente, cada objeto tiene una lista de control de acceso que enumera entidades de usuario, grupo o rol. El rango de posibilidades es amplio: en los permisos UNIX básicos, por ejemplo, hay tres permisos posibles (lectura, escritura y ejecución) para tres usuarios/grupos (raíz, propietario, grupo); en SharePoint Online, hay 33 permisos posibles que se agrupan en siete niveles predeterminados (puede crear otros adicionales), y estos niveles de permisos se pueden asignar a **muchos** usuarios y grupos en los objetos.
- **Relaciones de grupos.** Los grupos pueden contener usuarios u otros grupos "anidados". Para determinar los permisos efectivos para un objeto o un usuario, se deben calcular estas relaciones. En algunos casos, los grupos en un servicio de directorio pueden referirse a usuarios y grupos en otros servicios de directorio, lo que hace que este cálculo sea más complejo. Por ejemplo, SharePoint Online tiene grupos locales que pueden contener usuarios y grupos en Azure AD.
- **Herencia jerárquica.** En muchos repositorios de datos, los permisos fluyen de forma descendente en la jerarquía, por lo que todos los objetos dentro de una carpeta "heredarán" las entradas de control de acceso de sus carpetas principales. Algunos repositorios, aunque no todos, le permiten detener la herencia en los objetos derivados. Box, por ejemplo, solo admite la adición de entradas de control de acceso en objetos derivados, por lo que este nunca puede contar con menos autorizaciones que su(s) objeto(s) principal(es).
- **Roles y jerarquías de roles.** Se puede otorgar acceso a objetos en función de un rol. Los roles pueden contener otros roles y se asignan de manera diferente en diferentes aplicaciones. Por ejemplo, en AWS, los roles se suelen asumir según sea necesario, mientras que en Salesforce, los roles tienden a asignarse de manera más estática.
- **Configuraciones de todo el sistema.** Algunas configuraciones afectan el acceso a todos los objetos. En Google Drive, por ejemplo, la configuración de uso compartido de enlaces anula todos los permisos y posibilita que todo el dominio pueda acceder a cada objeto recientemente creado. En Salesforce, los "ajustes predeterminados para toda la organización" (OWD) establecen un acceso de nivel básico para todos los objetos.

Para visualizar el acceso, todos estos atributos y relaciones funcionales se deben calcular con anterioridad y normalizar en todos los repositorios de datos y las aplicaciones. Sin este tipo de automatización, resulta totalmente imposible determinar quién tiene acceso a un objeto, o a qué usuario o cuenta tiene acceso (es decir, el radio de ataque potencial eficaz), debido a la cantidad de tiempo que implica esta tarea, lo que perjudica las actividades cotidianas que van desde la respuesta a incidentes hasta la solución de problemas y los informes de auditoría.

# ¿Comprender la actividad de acceso es más fácil que comprender los permisos?

No, no lo es.

Al evaluar la seguridad de los datos, existen varios tipos de eventos que se relacionan directamente con la protección de los datos.

- **Eventos de acceso a datos.** Las actividades más relevantes para la seguridad implican la interacción directa con los datos, es decir, cuando los usuarios crean, leen, cambian/actualizan, eliminan o comparten datos. Lamentablemente, cada aplicación y repositorio de datos tiene su propia forma de registrar (o no) la manera en que los usuarios interactúan de forma directa con los datos. En los registros de Salesforce, por ejemplo, la actividad de acceso a los datos incluye información sobre a qué objeto se accedió.
- Los **cambios de control de acceso y los cambios de configuración** que afectan la accesibilidad de los datos también son muy importantes. Los cambios de control de acceso también se informan de manera diferente y están incompletos sin información sobre el usuario y los grupos a los que hacen referencia. Por ejemplo, muchos sistemas que registran permisos solo registran que se modificó una lista de control de acceso (ACL), no qué entradas se modificaron. Además, es posible que el sistema de archivos o la aplicación no registren los cambios en los objetos a los que se hace referencia en la ACL; quizá estos deban registrarse en el servicio de directorio (por ejemplo, Azure Active Directory). Los cambios de configuración son igualmente complejos, incluso con respecto a la accesibilidad de los datos. Los cambios de GPO en el Directorio Activo pueden afectar todo tipo de cosas importantes, como las políticas de contraseñas y la funcionalidad de los puntos finales. GitHub, por ejemplo, registra los cambios en la accesibilidad de los repositorios de código, pero no indica cuáles fueron los cambios.
- Los **eventos de autenticación** pueden proporcionar un contexto significativo sobre qué usuarios se conectaron a la aplicación o al repositorio de datos, desde dónde y con qué tipo de autenticación (por ejemplo, de uno o múltiples factores). Los eventos de autenticación varían entre los servicios de directorio y las aplicaciones.
- **Eventos del perímetro.** En la infraestructura local, las señales del perímetro del DNS, las puertas de enlace de la VPN y los proxies proporcionan información sobre conexiones inusuales dentro y fuera del entorno. Los eventos de dispositivos de perímetro son voluminosos y no son uniformes; puede resultar tentador comenzar a extraer la telemetría de muchos lugares, pero debe tener cuidado de no romper la relación señal/ruido. Lo que resulta más práctico es la telemetría, que es relevante desde la perspectiva de los datos, como el DNS para ver la infiltración y el proxy web para ver la exfiltración. Consulte **Cinco maneras en que su SIEM está fallando** para obtener más información.

Debido a que los repositorios de datos y las aplicaciones describen estos eventos de manera tan diferente, es muy difícil responder preguntas sobre ellos. Tan solo comprender a qué datos accedió un empleado en un día determinado, o qué cambios en el control de acceso realizó un administrador, se convierten en proyectos de investigación en lugar de ser simples consultas.

# ¿Qué sucede con las alertas?

Sin un flujo de eventos uniforme y normalizado, las alertas basadas en reglas representan un desafío, y las alertas basadas en el comportamiento se limitan a una sola aplicación o se descartan por completo de la ecuación. A la hora de modelar el comportamiento para desarrollar perfiles, los eventos también se deben enriquecer para que la IA tenga un conjunto significativo de aspectos para evaluar. Por ejemplo, si desea crear una alerta simple basada en umbrales para que se active cuando alguien accede a más de mil archivos u objetos, o los elimina o actualiza, en un período de 5 minutos, sin un flujo de eventos uniforme y confiable, es probable que tenga que crear una alerta para cada aplicación. Si quisiera que esa alerta se dispare cuando el número total de eventos supere las 1000 operaciones de archivos en un período de 5 minutos en todos los repositorios, esta ya sería una consulta bastante compleja.

Si quiere algo un poco más avanzado, como obtener una alerta si se accede a mil archivos confidenciales en un período de 5 minutos en los repositorios de datos, deberá enriquecer los eventos con información sobre la confidencialidad de los archivos antes de alertar a los procesos de lógica. Ya puede comenzar a entender cuán importantes son los eventos limpios y enriquecidos en las alertas basadas en umbrales; y lo son aún más para las alertas basadas en IA.

Los flujos de eventos limpios y enriquecidos son fundamentales para desarrollar puntos de referencia conductuales, o perfiles de tiempo de paz, que la IA puede evaluar para detectar anormalidades. Estos perfiles centrados en datos producen alertas con relaciones señal/ruido muy altas. Por ejemplo, cuando un ejecutivo que normalmente accede a una docena de archivos en una semana (y muy pocos de ellos son importantes) comienza a acceder a docenas de archivos importantes a los que ni él ni sus colegas suelen acceder, tal vez desde un dispositivo que nunca ha sido asociado con ese usuario o desde una ubicación que no suele visitar, esto merece atención inmediata.

El análisis del comportamiento requiere un comportamiento relevante, enriquecido y confiable para realizar un análisis. Por eso, las tecnologías de seguridad que analizan flujos ruidosos y poco confiables inevitablemente fallan.

# Sin las tres dimensiones, **decididamente fracasará**

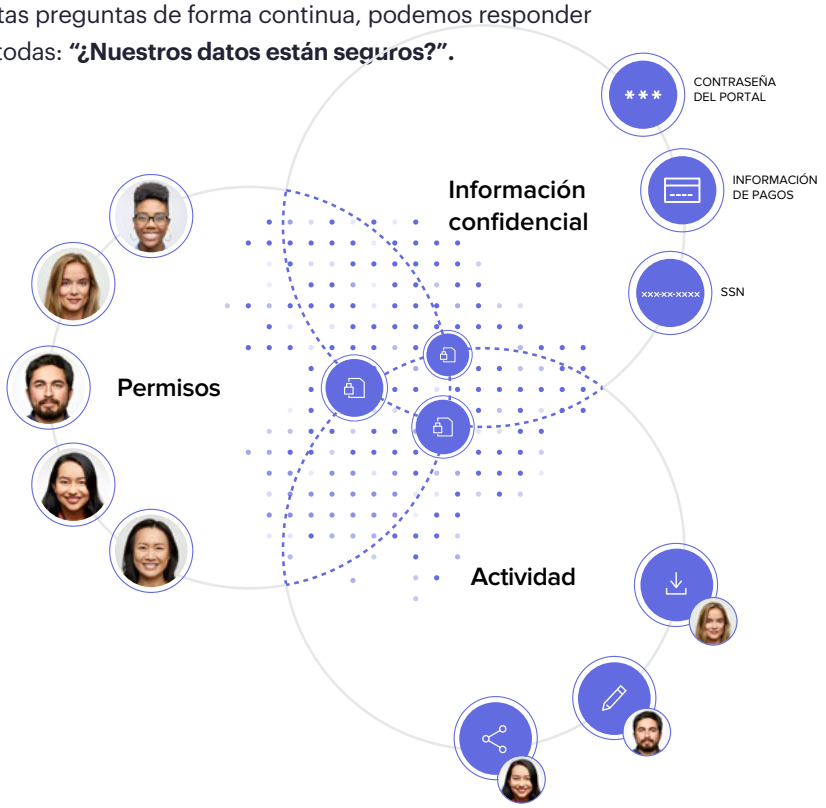
Cuando no se puede ver alguna de las tres dimensiones que hemos analizado hasta el momento (confidencialidad, permisos y actividad), muchos comienzan a pensar que pueden arreglárselas con una o dos. Sin embargo, si exploramos las diferentes combinaciones, muy pronto nos daremos cuenta de cuánto más poderoso es contar con todas las dimensiones juntas.

Como mencioné anteriormente, si solo sabe qué datos son confidenciales, no sabrá dónde están concentrados ni expuestos sin la dimensión de los permisos. Sin la actividad, nunca sabría cómo corregir de forma segura cualquier exposición que encuentre, o si se están robando datos confidenciales o incluso con quién debe hablar al respecto. Si solo observa la actividad, podrá ver qué datos fueron robados después de una vulneración, o incluso recibirá alertas sobre algunos cambios en el comportamiento, pero no sabrá qué tan confidenciales eran los datos, quién más estaba en condiciones de acceder a ellos, o si siquiera estaban expuestos incorrectamente a todos los miembros de la empresa (o en Internet).

A la hora de proteger los datos, se necesita cada una de estas dimensiones para responder a las preguntas críticas que fueron el punto de partida para este documento:

1. ¿Sabe **dónde se almacenan sus datos importantes?**
2. ¿Sabe si **solo las personas adecuadas tienen acceso a ellos?**
3. ¿Sabe si **esas personas están usando los datos correctamente?**

Cuando podemos responder afirmativamente a estas preguntas de forma continua, podemos responder afirmativamente a la pregunta más importante de todas: **“¿Nuestros datos están seguros?”.**






VARONIS

VARONIS

# ¿Está listo para experimentar la diferencia de Varonis?

Reduzca su riesgo sin asumir ninguno. Comuníquese con nuestro equipo para saber qué aspectos se analizarán en su evaluación de riesgos sobre los datos **gratuita**.

**Contáctenos**

ACERCA DE VARONIS

Varonis es pionera en seguridad y análisis de datos, y libra una batalla diferente de la que enfrentan las empresas de ciberseguridad convencionales. Varonis se centra en proteger los datos empresariales in situ y en la nube: archivos y correos electrónicos importantes; información confidencial de clientes, pacientes y empleados; registros financieros; planes estratégicos y de productos; y otra propiedad intelectual.

La Plataforma de seguridad de datos Varonis detecta amenazas internas y ataques cibernéticos al analizar la información, la actividad de la cuenta y el comportamiento del usuario; evita y limita que se produzcan incidentes restringiendo el acceso a datos importantes y obsoletos; y mantiene la seguridad de forma eficiente mediante la automatización. Con énfasis en la seguridad de los datos, Varonis puede aplicarse a una variedad de casos de uso que incluyen control, cumplimiento, clasificación y análisis de amenazas. Varonis comenzó a operar en 2005 y cuenta con miles de clientes en todo el mundo, entre los que se incluyen líderes de la industria de muchos sectores, como tecnología, consumo, venta minorista, servicios financieros, atención médica, fabricación, energía, medios de comunicación y educación.