Forcepoint

Un día en la vida de los datos sensibles

Una empleada. Una mañana ordinaria. Una explosión exponencial del riesgo de datos. Así es como sucede y cómo detenerlo

El Riesgo Ya Está Aquí

53%

DE LOS INCIDENTES INTERNOS SON ACCIDENTALES O NEGLIGENTES

DTEX 2026 of Insider Risks

13%

DE LOS INCIDENTES SE CONTIENEN EN MENOS DE 30 DÍAS

DTEX 2026 Cost of Insider Risks

Más de 200 Días

TIEMPO PROMEDIO DE RESOLUCIÓN DE INCIDENTES INTERNOS (MALICIOSOS Y ACCIDENTALES)

IBM 2026 Cost of a Data Breach Report

$19,5 Millones

COSTO ANUAL PROMEDIO TOTAL DE LOS INCIDENTES INTERNOS

DTEX 2026 Cost of Insider Risks

Te presentamos a María

María es una representante de ventas que se prepara para una reunión de alto impacto con un socio. Está haciendo su trabajo. No intenta causar un incidente de seguridad. **Observa qué les sucede a los datos sensibles mientras se alista.**

Salesforce → Excel

María genera un reporte de sus principales cuentas estratégicas en Salesforce y lo descarga como archivo Excel. Los datos incluyen nombres de cuentas, contactos y cifras de ingresos.

PII regulada, PI y datos de cuentas estratégicas salen de un entorno CRM controlado.

Excel → Nube

Sube el archivo a una plataforma de colaboración para compartirlo con su equipo. SharePoint. Box. OneDrive. No importa cuál.

Los datos críticos ahora existen en múltiples ubicaciones, accesibles para cualquier persona con permisos.

Excel → IA pública

María usa una herramienta de IA pública para resumir tendencias y crear puntos de discusión. Sube el archivo Excel directamente al prompt.

Los datos críticos han sido subidos a una Shadow AI con un prompt riesgoso.

Resultado de IA → Slack

Comparte el resumen generado por IA con su equipo en Slack. Nuevo contenido que incluye elementos de datos críticos se propaga en un canal de colaboración.

El nuevo contenido que incluye elementos de datos críticos se difunde a través de un canal de colaboración.

Slack → Correo electrónico externo

María envía el resumen por correo electrónico a un socio fuera de la organización.

Los datos críticos se exportan a través del canal más riesgoso, sin controles de acceso ni auditoría.

¿Qué acaba de ocurrir?

PII. Propiedad intelectual. Información estratégica. En un solo día, todo eso ha explotado en plataformas de colaboración, almacenamiento en la nube, herramientas de IA y límites de confianza externos. Alice no tenía intención de causar un problema. Simplemente intentaba trabajar de forma más inteligente y rápida. Eso es lo que hace que el riesgo interno sea tan difícil de gestionar: la mayoría no es malicioso. Es humano.

Un Nuevo Enfoque: Seguridad Que Sigue A Los Datos

Proteger los datos sensibles requiere un enfoque continuo que se adapte en tiempo real. No una lista de verificación. No un conjunto de políticas estáticas. Un ciclo. **Forcepoint llama a este enfoque Data Security Everywhere.**

Descubrir
Establecer visibilidad sobre los datos sensibles dondequiera que se encuentren

Clasificar
Identificar el tipo, el uso empresarial y el nivel de sensibilidad de los datos

Priorizar
Enfocar la atención donde el riesgo es mayor

Proteger los datos sensibles no es una lista de verificación. **Es un ciclo continuo.**

Proteger
Aplicar políticas de manera consistente en todos los canales para reducir el riesgo

Remediar
Abordar las vulnerabilidades antes de que se conviertan en brechas

Forcepoint Data Security Cloud

Los cinco pasos se conectan en una plataforma unificada: Forcepoint Data Security Cloud. Una plataforma. Un conjunto de políticas. Visibilidad completa en cada entorno donde los datos viven, se mueven y se utilizan.

Más información

Forcepoint