Forcepoint

9 pasos para proteger sus datos con éxito

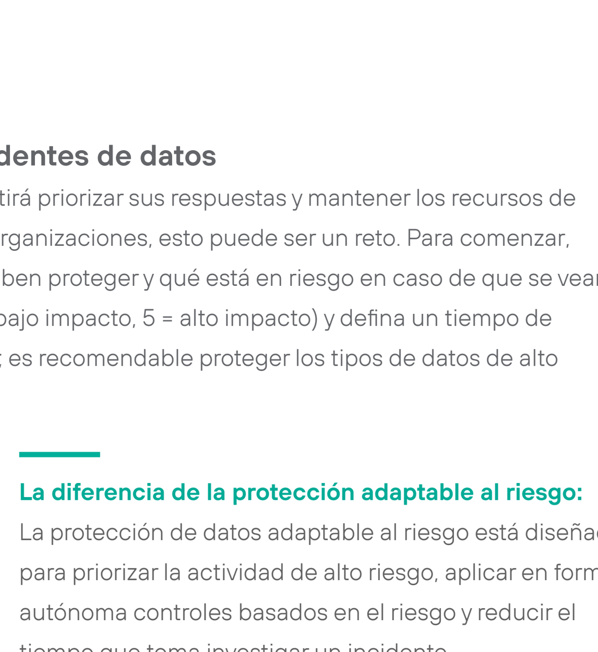
Para proteger sus datos, es necesario comprender los riesgos a los que estos se exponen y cómo tomar medidas si tales riesgos se concretan.

Pero, ¿cómo mantiene el equilibrio entre lo que su organización necesita para funcionar y lo que requiere para mantener los datos a salvo?

Estos nueve pasos le enseñarán a implementar controles de protección de datos que son eficaces, prácticos y medibles para el día a día, e identificar oportunidades para fortalecer su solución con protección de datos adaptable al riesgo.

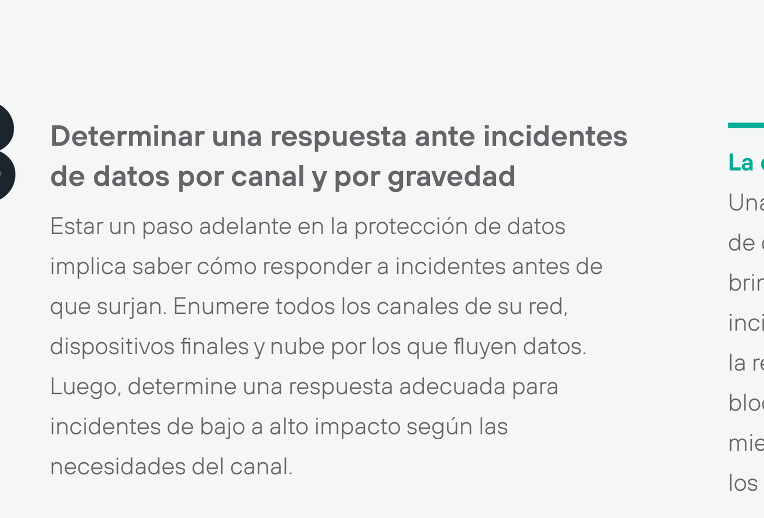
1 Crear un perfil de riesgo de la información

Un perfil de riesgo lo ayuda a comprender lo que necesita de su solución de protección de datos. Primero, indique los riesgos que desea mitigar y enumere los tipos de datos con los que se relacionan, agrupándolos por tipo de dato, según sea necesario. Luego, defina las redes, los dispositivos finales y canales de la nube por los que se podrían perder datos junto con los controles que actualmente utiliza para protegerlos.



2 Crear una tabla de gravedad y respuesta ante incidentes de datos

Relacionar cada tipo de datos con su impacto comercial le permitirá priorizar sus respuestas y mantener los recursos de seguridad enfocados en donde son más eficaces. Para algunas organizaciones, esto puede ser un reto. Para comenzar, analice con los propietarios de los datos qué tipos de datos se deben proteger y qué está en riesgo en caso de que se vean comprometidos. Luego, clasifíquelos en una escala del 1 al 5 (1 = bajo impacto, 5 = alto impacto) y defina un tiempo de respuesta aceptable para cada uno según la gravedad del riesgo; es recomendable proteger los tipos de datos de alto riesgo en primer lugar.



La diferencia de la protección adaptable al riesgo:
La protección de datos adaptable al riesgo está diseñada para priorizar la actividad de alto riesgo, aplicar en forma autónoma controles basados en el riesgo y reducir el tiempo que toma investigar un incidente.

3 Determinar una respuesta ante incidentes de datos por canal y por gravedad

Estar un paso adelante en la protección de datos implica saber cómo responder a incidentes antes de que surjan. Enumere todos los canales de su red, dispositivos finales y nube por los que fluyen datos. Luego, determine una respuesta adecuada para incidentes de bajo a alto impacto según las necesidades del canal.

La diferencia de la protección adaptable al riesgo:
Una solución adaptable al riesgo da cuenta del nivel de riesgo de cada ser humano que entra en contacto con sus datos, brindándole el control para ajustar las respuestas a los incidentes según los riesgos individuales. Por ejemplo, adaptar la respuesta a solo auditoría para usuarios de bajo riesgo y a bloqueo para los de alto riesgo solamente garantiza que cada miembro de su equipo pueda hacer su trabajo sin comprometer los datos o afectar la productividad del usuario.

Canales	Nivel 1 Bajo	Nivel 2* Bajo-Medio	Nivel 3 Medio	Nivel 4* Medio-Alto	Nivel 5* Alto	Notas
Correo electrónico	Encriptar	Eliminar adjuntos de correo electrónico	Poner en cuarentena	Poner en cuarentena		Encriptación Proxy para bloquear
Web						Inspección de SSL
Web segura						Proxy para bloquear
FTP	Auditar	Auditar/Notificar	Bloquear/Notificar	Bloquear/Alertar	Bloquear	Instalar agente de impresora DLP
Impresora en red						
Personalizado						
Aplicaciones en la nube			Poner en cuarentena con nota	Poner en cuarentena		

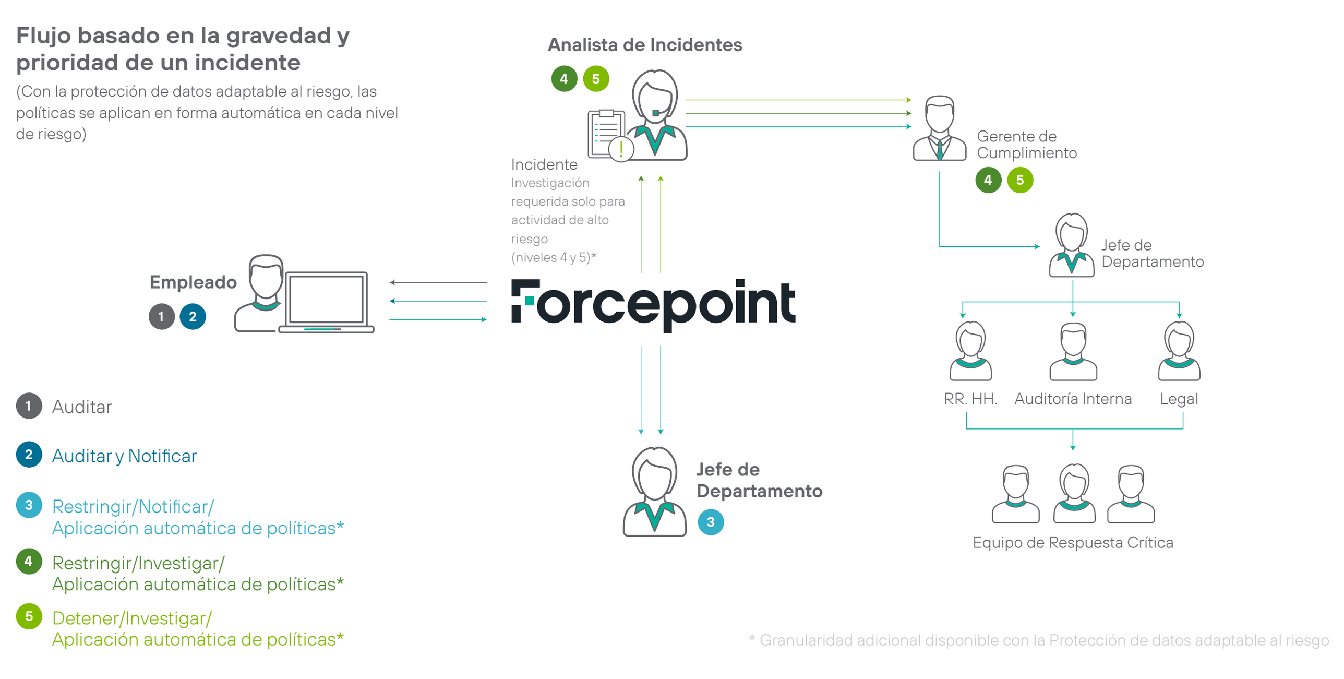
* Granularidad adicional disponible con la Protección de datos adaptable al riesgo

4 Establecer un flujo de trabajo de incidentes

Asegúrese de que su equipo de seguridad pueda entrar en acción en el momento en que se detecta el incidente al definir en forma clara el flujo de trabajo de respuesta para incidentes de bajo a alto riesgo. Para incidentes de menor impacto, automatice siempre que sea posible. Esto liberará ancho de banda para la reparación práctica de incidentes de mayor impacto.

La diferencia de la protección adaptable al riesgo:
Una solución adaptable al riesgo le permite analizar los incidentes sobre la base del nivel de riesgo individual, sin la necesidad de consultar a un analista de incidentes para determinar la mejor acción a seguir. Es posible que los incidentes relacionados con individuos de bajo riesgo no presenten una amenaza para su empresa, por lo que permitirles que continúen con su trabajo (con protecciones adicionales como la encriptación para la transferencia de archivos por USB o la eliminación automática de adjuntos de correo electrónico) puede mantener la productividad en funcionamiento.

Los administradores pueden emplear el mismo método proactivo con las personas e incidentes de alto riesgo al bloquear o restringir de forma automática acciones específicas hasta que un analista de incidentes lleve a cabo una investigación.



5 Asignar roles y responsabilidades

Incremente la estabilidad, escalabilidad y eficiencia operativa del programa de protección de datos al definir quién es quién en su equipo. Asigne roles clave como administradores técnicos, analistas de incidentes, investigadores forenses y auditores, y conceda los derechos y acceso adecuados a cada quien.

6 Comenzar un proyecto en modo de monitoreo

Una vez que instale su solución de protección de datos en red, un período de monitoreo le permitirá identificar patrones en su actividad y establecer un punto de referencia para ayudarlo a reconocer el comportamiento normal de los usuarios. Una vez finalizado este período, analice el comportamiento observado y presente sus hallazgos a su equipo ejecutivo, junto con recomendaciones sobre cómo mitigar los riesgos. Luego, puede poner esas recomendaciones en práctica, monitorear su éxito y presentarlas a los ejecutivos nuevamente.

La diferencia de la protección adaptable al riesgo:
Con una solución adaptable al riesgo, analizar incidentes en modo de solo auditoría (en lugar del modo de aplicación escalonada) resaltará la reducción de incidentes que requieren investigación, sin comprometer sus datos. Además, observará más incidentes positivos sin sobrecargar los recursos para abordar amenazas falsas.

7 Cambiar a una protección proactiva

Lo que descubrió en el modo de monitoreo le proporcionará el nivel de confianza que necesita para pasar al modo de bloqueo para los eventos de alto riesgo, o según su plan de respuestas ante incidentes. A medida que implemente la protección de datos en los dispositivos finales y las aplicaciones autorizadas en la nube, podrá monitorear, analizar, informar, optimizar y volver a informar sus hallazgos al equipo ejecutivo.

8 Integrar los controles de protección de datos en toda su empresa

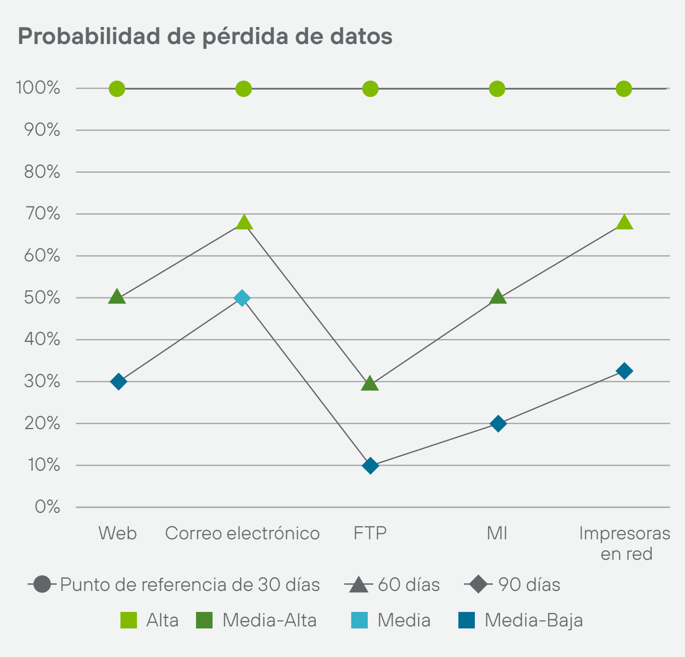
Cuando delegue responsabilidades a los líderes de seguridad en los distintos departamentos, piense en la "eficiencia". Por ejemplo, los propietarios de los datos ya son responsables en caso de una pérdida de datos, por lo que nombrarlos administradores de incidentes los ayuda a comprender cómo los demás usan los datos y a evaluar su riesgo, eliminando idas y vueltas innecesarias.

Comience a delegar responsabilidades al hacer que el equipo de seguridad organice una reunión inicial para presentar los controles de protección de datos a otros. Luego, realice una capacitación para los nuevos miembros del equipo, y establezca un período durante el cual los ayudará con la respuesta ante incidentes para que se sientan cómodos con sus procesos. También podría evaluar la posibilidad de ofrecer un asesoramiento en tiempo real para reforzar esos procesos.

9 Realizar un seguimiento de los resultados de la reducción de riesgos

Ya comenzó a prepararse para esto en el Paso 6; esto es lo que falta: Agrupe los incidentes relativos por criterio como gravedad, canal, tipo de datos y normativa. Luego, establezca sus períodos de monitoreo y reducción de riesgos para que tengan la misma duración (pruebe con dos semanas cada uno para comenzar) para preservar la integridad de sus resultados.

Probabilidad de pérdida de datos



Número de Incidentes en 90 días

Incidentes	Correo electrónico	Web	FTP	MI	Impresora en red
Punto de referencia de 30 días	150	200	50	10	45
60 días	100	100	15	5	30
Reducción de riesgos durante 60 días	33 %	50 %	70 %	50 %	33 %
90 días	76	60	5	2	15
Reducción de riesgos durante 90 días	49 %	70 %	90 %	80 %	67 %

Objetivos

60 días **Reducción de más del 25 %**

90 días **Reducción de más del 50 %**

La diferencia de la protección adaptable al riesgo:
Con un enfoque adaptable al riesgo, puede proporcionar una comparación de los incidentes capturados en el modo de solo auditoría (todos los incidentes) frente a los incidentes que requieren investigación con aplicación escalonada. El resumen debe mostrar la cantidad de incidentes para cada nivel de riesgo de 1 a 5, comparado con los que realmente requieren una investigación (niveles de riesgo 4 y 5).

Ya sea que tome un enfoque tradicional o aumente su seguridad con protección de datos adaptable al riesgo, esta fórmula demostrada lo ayudará a tener éxito.

¿Quiere ver la protección adaptable al riesgo en acción?

Descúbrala aquí

Forcepoint