La Guía Práctica para Ejecutivos sobre Prevención contra Pérdida de Datos

Forcepoint

Whitepaper

forcepoint.com

Índice

02 El problema
02 Un punto de partida
03 De la visión a la implementación
03 DLP práctica y medible
04 La fórmula del riesgo de la pérdida de datos
04 La regla 80/20 del DLP
05 La estrategia de ejecución y metodología de DLP de Forcepoint
05 La adquisición de valor
06 ¿Qué sucede con los datos en reposo y el cumplimiento?
07 Los nueve pasos para alcanzar el éxito
07 Paso 1: Crear un perfil de riesgo de la información
08 Paso 2: Crear una tabla de gravedad del impacto y respuesta
09 Paso 3: Determinar la respuesta ante incidentes basándose en la gravedad y el canal
10 Paso 4: Crear un diagrama de flujo de trabajo de incidentes
11 Paso 5: Asignar roles y responsabilidades
12 Paso 6: Establecer el marco técnico
13 Paso 7: Aumentar la cobertura de los controles de DLP
14 Paso 8: Integrar los controles de DLP al resto de la organización
15 Paso 9: Realizar un seguimiento de los resultados de la reducción de riesgos
16 Conclusión

El problema

Ha habido mucha confusión en el mercado respecto de los controles de prevención contra la pérdida de datos (DLP). Existen numerosos factores que contribuyen a esto, principalmente, la falta de comprensión en la comunidad de proveedores sobre cómo funciona la seguridad de datos o qué comunica el riesgo a una empresa. Se establecieron procesos poco prácticos, se generaron cuellos de botella operativos y la amenaza constante del robo y la pérdida de datos persistió. Como resultado, las organizaciones que quieren proteger sus datos confidenciales y cumplir con las leyes y regulaciones suelen mostrarse escépticas y no saben a quién acudir. Algunas quedaron marcadas por implementaciones nada exitosas.

Es importante reconocer que no es la tecnología detrás de los controles de DLP lo que en última instancia determina su éxito, sino que la estrategia de ejecución y metodología del proveedor determinarán tanto su experiencia como los resultados. Este whitepaper brinda orientación y claridad sobre lo siguiente: explica distinciones importantes y brinda consejos sobre cómo evaluar a un proveedor potencial; brinda perspectivas valiosas sobre las tendencias de la fuga de datos; ofrece un proceso de nueve pasos y fácil de seguir para implementar y ejecutar una estrategia de protección de datos de manera práctica, medible y adaptable al riesgo; y, por último, proporciona numerosas "mejores prácticas en la práctica" para evitar peligros comunes y eliminar la mayoría de los desafíos operativos que dificultan las implementaciones de DLP.

Un punto de partida

Todos los controles de DLP deben cumplir los dos primeros objetivos de la siguiente lista. Sin embargo, una solución de DLP más avanzada también debe contar con la tercera capacidad.

1. Brindan la habilidad de identificar los datos.

→ Datos en movimiento (desplazándose por la red)

→ Datos en uso (usándose en el dispositivo final)

→ Datos en reposo (inactivos en almacenamiento)

→ Datos en la nube (en uso, en movimiento y en reposo)

2. Identifican los datos como descritos o registrados.

→ Descritos: Plantillas de políticas y clasificadores listos para usar ayudan a identificar los tipos de datos. Esto resulta útil cuando se busca contenido como información de identificación personal (PII).

→ Registrados: Datos registrados con el sistema para crear una "huella", lo que permite la coincidencia total o parcial de información específica como la propiedad intelectual (IP).

3. Adoptan un enfoque de DLP adaptable al riesgo

→ La DLP adaptable al riesgo diferencia las soluciones de prevención contra la pérdida de datos de los otros conjuntos de herramientas de DLP. Derivada del enfoque estratégico continuo de riesgo adaptable y de evaluación de confianza (CARTA) de Gartner, el DLP adaptable al riesgo aporta flexibilidad y proactividad a DLP. Se ajusta y aplica de manera autónoma políticas de DLP basándose en el riesgo que un individuo implica para una organización en un momento determinado.

Para ilustrar cómo funcionan las dos primeras capacidades, a un control de DLP se le indica:

→ Qué buscar (por ej., números de tarjetas de crédito)

→ El método para identificar la información (descrita/registrada)

→ Dónde buscarla (por ej., en la red, en un dispositivo final, en almacenamiento, en la nube)

Lo que sucede después de que un control de DLP identifica la información depende de: a) el riesgo depende de la tolerancia al riesgo del propietario de los datos; b) las opciones de respuesta disponibles cuando se detecta la pérdida de datos; y c) si la solución es adaptable al riesgo.

Punto de partida

De la visión a la implementación

Si bien todos los controles de DLP ofrecen capacidades similares, es importante entender que no todos los proveedores comparten la misma visión respecto de cómo la DLP ayuda a abordar el problema de la pérdida de datos. Por lo tanto, su primer paso es comprender la estrategia de ejecución y metodología de cada proveedor que está evaluando.

Al preguntarle a un proveedor: "¿Cuál es su metodología?", lo que está preguntando en verdad es "¿Cuál es su visión respecto de cómo esta herramienta ayudará a resolver el problema de la pérdida de datos?". Esta es una pregunta importante pero que rara vez se hace. La respuesta le permite entender la visión de un proveedor, lo que a la vez le ayuda a identificar sus capacidades únicas y la dirección en la que la estrategia de desarrollo de sus productos probablemente se dirija. Para los responsables de la toma de decisiones, saber por qué los proveedores hacen lo que hacen está mucho más relacionado con su éxito y felicidad a largo plazo que saber qué es lo que hacen.

La metodología de un proveedor también tiene una fuerte influencia en su estrategia de ejecución o implementación. Por ejemplo, si la metodología de un proveedor comienza por evaluar los datos en reposo, y la de otro se inicia al evaluar los datos en movimiento usando controles adaptables al riesgo, entonces sus estrategias de ejecución difieren enormemente. La manera en que un proveedor ejecuta los controles de DLP importa porque afecta tanto su costo total de propiedad (TCO) como su adquisición de valor esperada, lo que es crucial para tomar la decisión de compra correcta y establecer debidamente las expectativas de las partes interesadas.

Cabe destacar lo siguiente: debe evitar aplicar la metodología de un proveedor a la tecnología de otro. La metodología define e impulsa la estrategia de desarrollo tecnológica de un proveedor, de modo que al combinar los dos aspectos corre el riesgo de invertir en una tecnología que no satisfaga sus necesidades a largo plazo.

DLP práctica y medible

Si asistió a una conferencia o leyó un artículo sobre las mejores prácticas de DLP, probablemente esté familiarizado con la metáfora de "no intente hervir el océano". Esto significa que no puede ejecutar un programa de DLP completo de una sola vez. Esta no es una mejor práctica útil ya que no ayuda a descubrir qué hacer y cúando hacerlo. En algunos aspectos, "no hervir el océano" suena más como una advertencia que como una mejor práctica.

Desafortunadamente, muchas mejores prácticas publicadas no siempre son prácticas. La falta de recursos, financieros u otros, y demás problemas organizativos suelen hacer que no se sigan las mejores prácticas y, por lo tanto, resulten inútiles. Existe mayor valor en las mejores prácticas en la práctica, que tienen en cuenta el costo, los beneficios y el esfuerzo que implica seguirlas, y pueden medirse para determinar si usted y su organización pueden o deben adoptarlas.

Para que su control de DLP sea medible y práctico a la hora de gestionar y mitigar la pérdida de datos, hay dos cosas que debe conocer y comprender:

1. Para ser medible, tiene que conocer y aplicar la fórmula del riesgo de la pérdida de datos. Si bien es similar a otros modelos de cálculo del riesgo, la fórmula del riesgo de la pérdida de datos presenta una diferencia sustancial, que explicaremos a continuación.
2. Para ser práctico, debe entender en dónde es más probable que experimente una fuga de datos de alto impacto y usar la regla 80/20 para enfocar su atención y recursos.

La fórmula del riesgo de la pérdida de datos

La fórmula de cálculo del riesgo básica que la mayoría conocemos es:

Riesgo = Impacto x Probabilidad
El desafío con la mayoría de los modelos de riesgo es determinar la probabilidad de que ocurra una amenaza. Esta probabilidad es crucial para determinar si se gastará dinero en una solución de prevención de amenazas o si se ignorará esa inversión y se aceptará correr el riesgo.

La diferencia con la fórmula del riesgo de la pérdida de datos es que no se lidia con un dato desconocido. Reconoce el hecho de que la pérdida de datos es inevitable y, por lo general, involuntaria. Lo que es aún más importante: la fórmula del riesgo permite medir y mitigar el riesgo a un nivel cómodo para su organización.

Por lo tanto, la métrica utilizada para hacer un seguimiento de la reducción en el riesgo de los datos y el retorno de inversión (ROI) de los controles de DLP es el índice de ocurrencia (RO).

Riesgo = Impacto x Índice de ocurrencia (RO)
El RO indica con qué frecuencia, a lo largo de un período determinado, se utilizan o transmiten datos de una manera que exponga a dichos datos a pérdida, robo o compromiso. El RO se mide antes y después de la ejecución de los controles de DLP para demostrar en qué medida se redujo el riesgo.

Por ejemplo, si comienza con un RO de 100 incidentes en un período de dos semanas, y logra reducir esa cantidad a 50 incidentes en un plazo de dos semanas tras la implementación de los controles de DLP, entonces habrá reducido la probabilidad de un incidente de pérdida de datos (fuga de datos) en un 50 %.

Una consideración importante es que si una de las soluciones de DLP que está comparando tiene tecnología adaptable al riesgo, es probable que muestre un RO menor. Esto se debe a que la DLP adaptable al riesgo es mucho más precisa a la hora de identificar las interacciones de los usuarios riesgosos con los datos, por lo que produce una menor cantidad de falsos positivos y un RO total menor. Esto presenta una ventaja por sobre las soluciones de DLP tradicionales. Sin embargo, también hace que comparar la reducción del riesgo sea más difícil.

Para contemplar esto, se recomienda que se revise y verifique cada incidente producido por tecnología que no es adaptable al riesgo para determinar que no sea un falso positivo. Tenga en cuenta que solo porque los datos identificados coincidan con la regla de DLP creada, eso no significa necesariamente que los datos estén infringiendo una política. También se debe inspeccionar la intención y el contexto del incidente de pérdida de datos para garantizar que sea de hecho un verdadero positivo.

La regla 80/20 de la DLP

Además de identificar el RO, es importante descubrir dónde es más probable que su organización experimente una fuga de datos de alto impacto. Para hacerlo, necesita estudiar las tendencias de fugas más recientes y luego aplicar la regla 80/20 para determinar dónde comenzar sus esfuerzos de DLP. Un estudio reciente reveló esta información.

Según un estudio de 2018 del Ponemon Institute, el 77 % de las fugas de datos ocurren a causa de empleados internos debido a incidentes en los que se comprometen las credenciales de usuario o se produce una exposición accidental.

Para contar con un programa realmente eficaz que proteja contra la pérdida de datos, debe sentirse confiado respecto de su capacidad para detectar y responder al movimiento de datos a través de la web, el correo electrónico, la nube y los medios extraíbles.

Aquí es donde una solución adaptable al riesgo puede brindar una ventaja. Las soluciones de DLP tradicionales suelen tener problemas para identificar ítems como trastornos en los procesos comerciales o actividad irregular, y ambas cosas pueden generar una pérdida de datos significativa. La DLP adaptable al riesgo entiende el comportamiento de los usuarios individuales y los compara con sus grupos de pares para reforzar los controles de DLP de manera rápida y autónoma cuando la actividad no se alinea con la función laboral del usuario final. Este enfoque proactivo puede reducir el riesgo de exposición y pérdida de datos accidentales.

La estrategia de ejecución y metodología de DLP de Forcepoint

Tener en cuenta las últimas tendencias de fuga de datos y aplicar la fórmula del riesgo de la pérdida de datos son los primeros pasos hacia la creación de una estrategia de prevención contra la pérdida de datos. La metodología de DLP más eficaz se enfoca en entender las intenciones de los usuarios para evitar la pérdida de datos antes de que ocurra. A esto lo denominamos "seguridad cibernética centrada en las personas". La ejecución debe centrarse en brindar la mejor adquisición de valor para demostrar una reducción del riesgo medible.

Adquisición de valor
La adquisición de valor es la diferencia de tiempo entre la implementación de los controles de DLP y la observación de resultados medibles en términos de reducción del riesgo. Dado que el 77 % de las fugas de datos ocurren a causa de empleados (comprometidos o de forma accidental), obtendrá la mejor adquisición de valor con una DLP que se enfoque en los datos en movimiento y los datos en reposo, usando tecnología adaptable al riesgo en segundo plano.

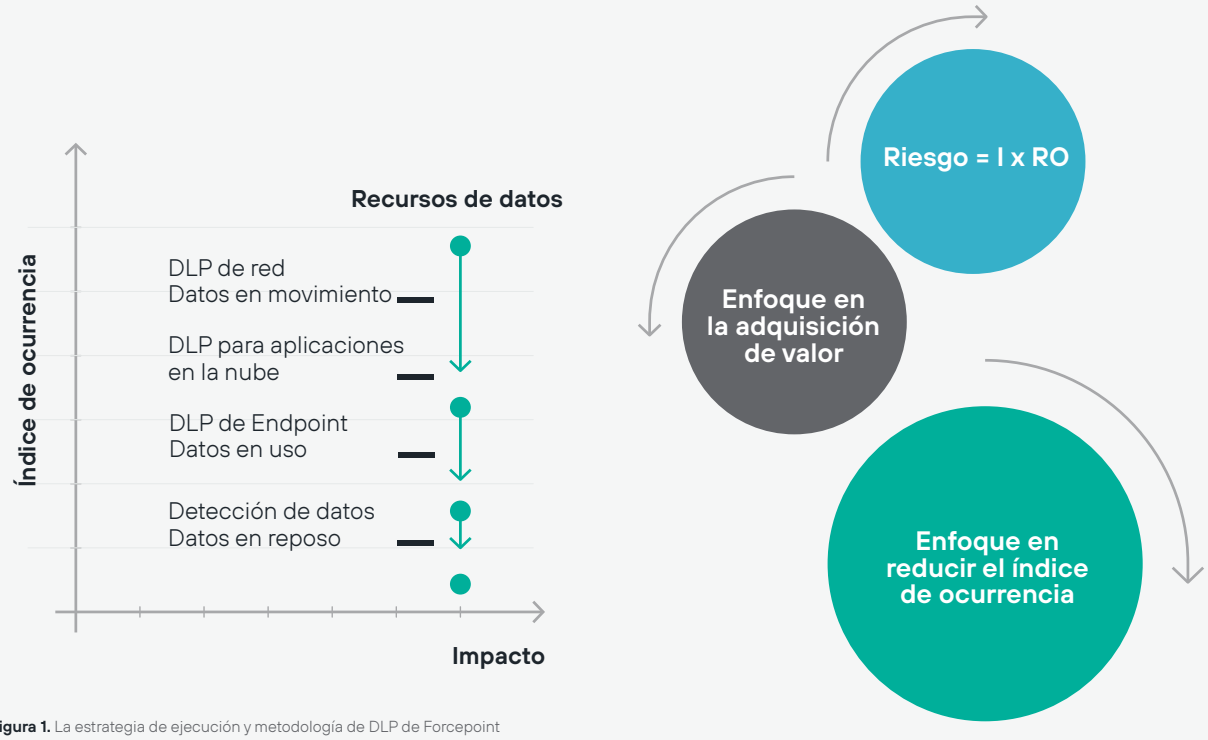


Figura 1. La estrategia de ejecución y metodología de DLP de Forcepoint

Si otros proveedores o líderes de opinión le dijeron que primero enfoque sus controles de DLP en los datos en reposo, ahora debe estar rascándose la cabeza. Ellos suelen decir: "Si no sabe qué tiene ni dónde se encuentra, entonces no podrá protegerlo". Sin embargo, eso no es cierto. De hecho, los controles de DLP están diseñados para hacerlo. O bien los otros proveedores y expertos no entienden cómo evaluar y abordar el riesgo correctamente, o simplemente están repitiendo lo que otros dicen porque parece funcionar para ellos.

¿Por qué debería desafiar la recomendación de comenzar por los datos en reposo? Considere las siguientes preguntas:

1. ¿Conoce alguna organización que haya identificado y protegido con éxito todos sus datos confidenciales?
2. ¿Tiene idea de cuánto tiempo llevará escanear, identificar y proteger cada archivo que contenga información confidencial?
3. ¿Sabe cuánto se reducirá el riesgo como resultado de esta estrategia?

El problema de enfocarse primero en los datos en reposo es que eso significa centrarse en el riesgo implícito, no el riesgo real, y, por lo tanto, no puede medirse en el contexto de la reducción del riesgo. El riesgo implícito significa que se deben cumplir otras condiciones antes de que pueda ocurrir una consecuencia negativa. En el contexto de la pérdida de datos, esas condiciones son:

→ Alguien o algo con intenciones maliciosas debe estar en su red o acceder a sus entornos en la nube.

→ Deben estar buscando sus datos confidenciales.

→ Deben encontrarlos.

→ Deben moverlos.

Esto se aplica a todas las organizaciones y lleva a la pregunta más importante: "¿Qué tan cómodo se siente con la capacidad de su organización de detectar cuando los datos están en movimiento y responder a ello?"

Existen tres canales a través de los cuales ocurre la pérdida de datos, donde usted detecta el riesgo real y responde a él:

→ Canal de red (por ej., correo electrónico, web, FTP)

→ Canal de dispositivo final (por ej., almacenamiento USB impresoras)

→ Canal de nube (por ej., Office 365, Box)

¿Qué sucede con los datos en reposo y el cumplimiento?

Muchas regulaciones requieren que escanee sus datos almacenados en busca de datos en reposo desprotegidos, de modo que es posible que se pregunte por qué la ejecución y metodología de DLP no comienza por ahí. Sin embargo, la verdad es que los auditores están más preocupados por el hecho de que esté cumpliendo ahora más que por si lo hizo en el pasado.

De modo que escanear los datos en reposo es importante para el cumplimiento pero no es el objetivo principal y valor de su control de DLP. Por lo tanto, planifique usar la DLP para la detección de datos y el cumplimiento, pero de una manera práctica y sostenible para su organización.

El mejor lugar donde empezar es usar la DLP para colocar en cuarentena de forma automática archivos a los que no se accedió en los últimos seis meses. Asigne permisos a sus equipos de cumplimiento y legal para que puedan tomar decisiones basándose en las políticas de retención de datos.

Los nueve pasos para alcanzar el éxito con la DLP

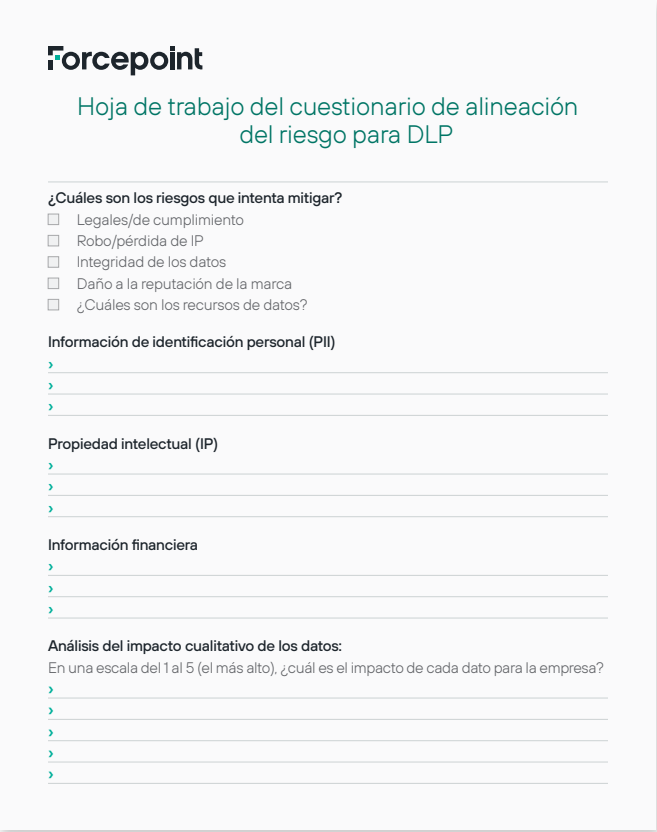
Los siguientes nueve pasos definen un proceso para implementar controles de DLP que su empresa pueda seguir fácilmente y que entreguen resultados medibles. Ya sea que esté en las primeras etapas en su desarrollo de DLP o ya esté bien encaminado, esto detalla los pasos para alcanzar el éxito con las aplicaciones de DLP tradicionales, o para quienes deseen fortalecer su enfoque con DLP adaptable al riesgo.

Paso 1:
Crear un perfil de riesgo de la información

Objetivo: Entender el alcance de sus necesidades de protección de datos.
Descripción general: Crear un perfil de riesgo de la información inicial que incluya:

- → Una declaración de las consecuencias potenciales de la falta de acción.
- → Una descripción de los tipos de datos en el alcance (por ej., PII, IP, datos financieros).
- → Definiciones de los canales de red, dispositivo final y nube en donde puede perderse o robarse información.
- → Una lista de los controles existentes actualmente utilizados para la protección de datos (por ej., encriptación).

1. **Declare el riesgo que quiere mitigar.**
2. **Compile una lista de recursos de datos y agrúpelos por tipo.**
3. **Entreviste a los propietarios de los datos para determinar el impacto.**
4. **Enumere los canales que pueden transmitir información.**


Forcepoint

Hoja de trabajo del cuestionario de alineación del riesgo para DLP

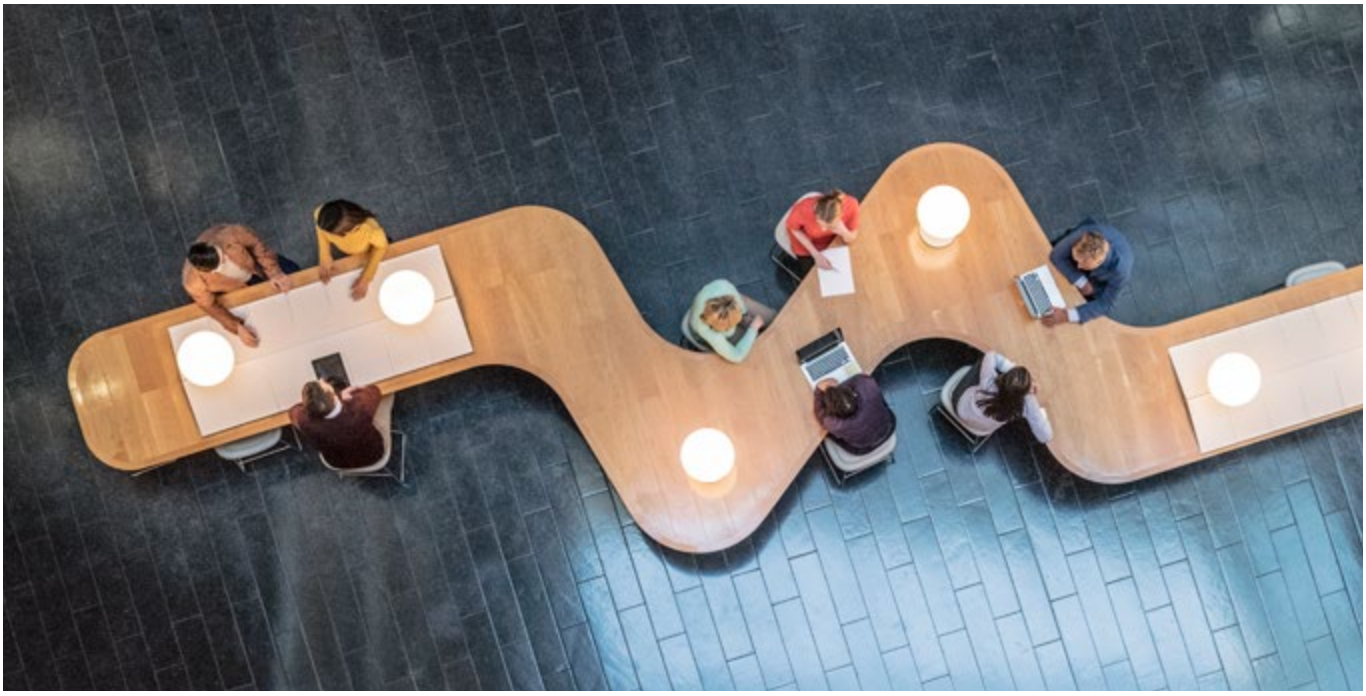
¿Cuáles son los riesgos que intenta mitigar?
- ☐ Legales/de cumplimiento
- ☐ Robo/pérdida de IP
- ☐ Integridad de los datos
- ☐ Daño a la reputación de la marca
- ☐ ¿Cuáles son los recursos de datos?

Información de identificación personal (PII)
›
›
›

Propiedad intelectual (IP)
›
›
›

Información financiera
›
›
›

Análisis del impacto cualitativo de los datos:
En una escala del 1 al 5 (el más alto), ¿cuál es el impacto de cada dato para la empresa?
›
›
›
›
›



Paso 2:
Crear una tabla de gravedad del impacto y respuesta

Objetivo: Determinar los tiempos de respuesta ante incidentes de pérdida de datos según el grado de gravedad.

Descripción general: Hacer que su equipo de implementación de DLP se reúna con los propietarios de los datos para determinar el nivel de impacto en caso de que pérdida, robo o compromiso de los datos. Utilizar el análisis cualitativo para describir el impacto, como una escala del 1 al 5. Esto ayuda a priorizar los esfuerzos de respuesta ante incidentes y se usa para determinar el tiempo de respuesta adecuado.

Opción de DLP adaptable al riesgo: Recuerde que una solución de DLP con un enfoque 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. El resultado es un riesgo de impacto menor y un control más proactivo de datos críticos.

Los pasos descritos más arriba todavía corresponden pero se verán aumentados con la DLP adaptable al riesgo.

Regulaciones			**Paso 1:** Discutir los tipos de datos generales **Paso 2:** Regulaciones relativas (asistente disponible) **Paso 3:** "Identificación": registrados o descritos **Paso 4:** Cantidad o porcentaje para alto, medio, bajo		Leyenda de clasificación del impacto		
Notificación de fuga	HIPPA	PCI/PCI-DSS			5, 4	3, 2	1
			Información de identificación personal (PII)	Identificación	Alto	Medio	Bajo
			VIP PII	R	1	-	-
			PII	D	>100	>25	>2
			PHI	D	>100	>50	>2
			Información financiera	Identificación	Alto	Medio	Bajo
			Tarjetas de crédito	D	>25	>5	>2
			Información de nómina	D	>25	>5	>2
			Propiedad intelectual	Identificación	Alto	Medio	Bajo
			Proyecto X	R	>25 %	>10 %	10 %<
			Documento de diseño	R	>25 %	>10 %	10 %<
			Nombres de usuario y contraseñas	R	>25 %	>10 %	10 %<

1. **Comience por analizar los tipos de datos a proteger.**
2. **Alinee las regulaciones con los tipos de datos identificados.**
3. **Determine cómo identificará los datos.**
4. **Determine la gravedad del impacto y la respuesta ante incidentes.**

Paso 3:
Determinar la respuesta ante incidentes basándose en la gravedad y el canal

Objetivo: Definir qué sucede en respuesta a un incidente de pérdida de datos basándose en su gravedad y canal.

Descripción general: Su organización cuenta con una cantidad limitada de canales a través de los cuales fluye la información. Estos canales se convierten en puntos de verificación de monitoreo que los controles de DLP utilizan para detectar y responder ante la pérdida de datos. Enumere todos los canales de comunicación de su red, en los dispositivos finales y en la nube (es decir, las aplicaciones en la nube autorizadas) en una hoja de trabajo. Luego aplique una respuesta (basándose en la gravedad del incidente) usando una de las opciones de respuesta disponibles en los controles de DLP para ese canal.

También puede aclarar los requisitos adicionales que su organización tenga para entregar la respuesta deseada, como encriptación o inspección de SSL. Por ejemplo, los medios extraíbles son uno de los tres principales vectores para la pérdida de datos. Sin embargo, también son una excelente herramienta para aumentar la productividad.

Una opción para mitigar el riesgo de la pérdida de datos en Box o Google Drive es dejar de compartir automáticamente los archivos que contengan información confidencial que se transfieren al almacenamiento en la nube y se comparten externamente.

Opción de DLP adaptable al riesgo: Una solución de DLP adaptable al riesgo puede brindar a las organizaciones controles de aplicación granulares en todos los canales, lo que aporta flexibilidad para ajustar la respuesta basándose en el nivel de riesgo del usuario (por ej., solo auditoría para los usuarios de riesgo bajo y bloqueo para los usuarios de riesgo alto). Esto permite a los usuarios realizar sus tareas con eficacia, sin que los datos se vean comprometidos.

1. **Elija los datos o tipos de datos.**
2. **Confirme los canales a monitorear.**
3. **Determine la respuesta basándose en la gravedad.**
4. **Señale los requisitos adicionales para la respuesta deseada.**

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

*Granularidad adicional disponible con DLP adaptable al riesgo

Paso 4:
Crear un diagrama de flujo de trabajo de incidentes

Objetivo: Garantizar que se sigan los procedimientos para identificar y responder ante incidentes.

Descripción general: Consulte el diagrama a continuación para ver el proceso en donde se gestionan los incidentes de acuerdo a su gravedad, y para ver qué sucede cuando se detecta un incidente. Para los incidentes de baja gravedad, aplique la automatización siempre que sea posible; esto normalmente incluye notificar a los usuarios y gerentes sobre el comportamiento riesgoso. También puede incluir asesorar a los empleados para facilitar la autocorrección del riesgo.

Los incidentes con un mayor impacto requieren de intervención por parte de un analista de incidentes que investigará y determinará el tipo de amenaza (por ej., accidental, intencional o maliciosa). El analista de incidentes deriva el incidente y su análisis al gerente del programa (por lo general, el responsable de seguridad o cumplimiento), quien determinará qué medidas tomar y a qué equipos incluir.

Opción de DLP adaptable al riesgo: Si elige sacar provecho de una solución adaptativa, no se requiere de la investigación por parte de un analista de incidentes antes de tomar medidas. Los incidentes atribuidos a usuarios de bajo riesgo pueden no significar una amenaza a la organización y, por lo tanto, se les debe permitir continuar para no afectar la productividad. Sin embargo, estas acciones permitidas deben contar con protecciones como requerir encriptación al guardar en una unidad USB o eliminar los adjuntos enviados por correo electrónico.

Para los usuarios de alto riesgo y los incidentes asociados, los administradores pueden tener un enfoque proactivo al restringir o bloquear automáticamente acciones específicas hasta que el analista de incidentes pueda investigar.

Flujo basado en la gravedad y prioridad de un incidente

Con la DLP adaptable al riesgo, las políticas se aplican en forma automática en cada nivel de riesgo

Paso 5:
Asignar roles y responsabilidades

Objetivo: Aumentar la estabilidad, escalabilidad y eficiencia operativa del programa de DLP

Descripción general: Por lo general, existen cuatro roles distintos asignados para ayudar a preservar la integridad de los controles de DLP y aumentar su eficiencia operativa.

→ Administrador técnico

→ Gerente/Analista de incidentes

→ Investigador forense

→ Auditor

Cada rol se define de acuerdo con sus responsabilidades y se asigna a la parte interesada correspondiente. En este punto, es común ver a miembros del equipo de implementación de DLP actuar como los gestores de incidentes. Sin embargo, a medida que los controles de DLP alcanzan la madurez e inspiran un nivel de confianza más alto, estos roles pasarán al propietario de datos correspondiente.

Paso 6:
Establecer el marco técnico

Objetivo: Implementar la DLP de red para medir y comenzar a reducir el riesgo.

Descripción general: El Paso 6 cuenta con dos fases. Durante la fase uno, se establece un punto de referencia para ayudar a su organización a reconocer el comportamiento normal de los usuarios y prevenir fugas de datos de alto impacto. En esta etapa, el rol del control de DLP es básicamente monitorear, bloqueando solo los incidentes de gravedad alta (por ej., datos que se cargan a destinos maliciosos conocidos o descargas masivas de registros desprotegidos en riesgo en una sola transacción).

Este enfoque de solo auditoría también puede realizarse al usar un DLP adaptable al riesgo, configurando cada nivel de riesgo como de solo auditoría. Al obtener una perspectiva más clara sobre el movimiento de datos y el uso dentro de su organización, puede ajustar los controles para aplicar medidas de cumplimiento para los usuarios con riesgo más alto.

Después de la fase de monitoreo inicial, durante la que implementó un control de DLP de red, realice un análisis y presente los hallazgos clave al equipo ejecutivo. Esto debe incluir recomendaciones para las actividades de mitigación del riesgo que pueden reducir el índice de ocurrencia (RO) de los datos en riesgo. Luego, capture los resultados e infórmelos al equipo ejecutivo.

Opción de DLP adaptable al riesgo: Si elige implementar una DLP adaptable al riesgo, puede ejecutar un análisis donde se comparen los incidentes en modo de solo auditoría con los del modo de aplicación escalonada. Estos datos contrastantes destacarán la menor cantidad de incidentes que requieren investigación sin comprometer sus datos. Los resultados observados serán más indicativos de verdaderos positivos. También puede demostrar los beneficios de la automatización, la menor cantidad de recursos que se necesitan para monitorear y gestionar incidentes, y la mayor productividad de los equipos afectados.

✓ El Paso 9 cubre el ROI y el seguimiento de reducción del riesgo en mayor profundidad.

1. **Instalación y configuración**
2. **Monitoreo de red**
3. **Análisis de los resultados**
4. **Resumen ejecutivo 1**
5. **Actividades de mitigación del riesgo** (por ej., activar políticas de bloqueo)
6. **Análisis de los resultados**
7. **Resumen ejecutivo 2**

Fase uno	Lunes	Martes	Miércoles	Jueves	Viernes
Semana 1: Instalación/ Optimización/Entrenamiento					
Semana 2: Monitoreo					
Semana 3: Monitoreo					
Semana 4: Resumen ejecutivo 1					
Semana 5: Mitigación del riesgo					
Semana 6: Resumen ejecutivo 2					

Paso 7:
Ampliar la cobertura del control de DLP

Objetivo: Implementar DLP en los endpoints y las aplicaciones en la nube autorizadas para medir y comenzar a reducir el riesgo.

Descripción general: Ahora está listo para abordar los datos en uso y los datos en reposo. Durante este paso, implementará la DLP en los endpoints y las aplicaciones en la nube autorizadas, monitoreará y analizará sus datos, actualizará al equipo ejecutivo y realizará actividades de mitigación del riesgo como lo hizo en el Paso 6. La principal diferencia es que ahora elegirá responder a los incidentes basándose en los distintos canales y opciones disponibles para los datos en uso, lo que ocurre en los endpoints y las aplicaciones en la nube. (En el Paso 3 determinó la gravedad del incidente y la respuesta de acuerdo con el canal).

Para los datos en reposo, el proceso identifica y prioriza objetivos a escanear, y coloca todo dato obsoleto en cuarentena, en donde los equipos legal y de cumplimiento pueden proceder de acuerdo con las políticas de retención de datos de su organización. En lo que respecta al cumplimiento, se trata de cooperar. Y no solo cooperar sino hacerlo a una velocidad que sea razonable para su organización. Recuerde: nadie recibe un premio por ser el primero.

En caso de que necesite realizar una tarea de detección rápidamente, sepa que puede aumentar temporalmente (o permanentemente) la velocidad a la que se realiza la detección usando agentes de detección locales o configurando varios dispositivos de detección de red.

1. **Implementación y monitoreo en endpoints y aplicaciones en la nube (autorizadas)**
2. **Inicio de los escaneos de detección**
3. **Análisis de los resultados**
4. **Resumen ejecutivo 3**
5. **Actividades de mitigación del riesgo**
6. **Análisis de los resultados**
7. **Resumen ejecutivo 4**

Fase dos	Lunes	Martes	Miércoles	Jueves	Viernes
Semana 7: Implementación en endpoints y aplicaciones en la nube (autorizadas)					
Semana 8: Monitoreo en endpoints y aplicaciones en la nube (autorizadas)/Datos en reposo					
Semana 9: Monitoreo en endpoints y aplicaciones en la nube (autorizadas)/Datos en reposo					
Semana 10: Resumen ejecutivo 3					
Semana 11: Mitigación del riesgo					
Semana 12: Resumen ejecutivo 4					

Paso 8:
Integrar los controles de DLP al resto de la organización

Objetivo: Se delega la gestión de incidentes a partes interesadas clave de las principales unidades de negocio.

Descripción general: Si todavía no hizo participar directamente a los propietarios de los datos y otras partes interesadas clave, este es el momento de hacerlo.

En particular, el rol del gestor de incidentes se adapta mejor a los propietarios de los datos, dado que son los responsables en caso de pérdida de datos. Poner la gestión de incidentes en sus manos elimina a los intermediarios y mejora la eficiencia operativa. Además, les permite evaluar con precisión su tolerancia al riesgo, y entender debidamente cómo otros utilizan sus recursos de datos.

Durante este paso, pida al equipo de implementación de DLP que organice una reunión de lanzamiento para presentar a otros los controles de DLP. Realice una capacitación después de la reunión para que los nuevos miembros del equipo se aclimaten a la aplicación de gestión de incidentes. Antes de delegar las responsabilidades de gestión de incidentes, establezca un período durante el que proporcionará respuesta ante incidentes para que los nuevos miembros del equipo se pongan al día.

1. **Creación y participación en un comité**
2. **Actualización del programa y roles**
3. **Capacitación**
4. **Respuesta antes incidentes asistida**
5. **Resumen ejecutivo 5**
6. **Respuesta ante incidentes por parte del comité**
7. **Resumen ejecutivo 6**

Fase tres	Lunes	Martes	Miércoles	Jueves	Viernes
Semana 13: Selección y notificación					
Semana 14: Actualización del programa y roles					
Semana 15: Capacitación con respuesta asistida					
Semana 16: Resumen ejecutivo 5					
Semana 17: Respuesta ante incidentes por parte del comité					
Semana 18: Resumen ejecutivo 6					

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

Objetivo: Mostrar el ROI al demostrar una reducción del riesgo medible.

Descripción general: Existen dos puntos clave a agregar al proceso de seguimiento de reducción del riesgo que se mencionó por primera vez en el Paso 6. Estos son:

1. Los incidentes relativos deben agruparse juntos.
Los grupos comunes incluyen gravedad, canal, tipo de datos y regulación. Para las organizaciones más grandes, los subgrupos adicionales ayudan a aclarar más el riesgo según ubicaciones geográficas o subsidiarias.

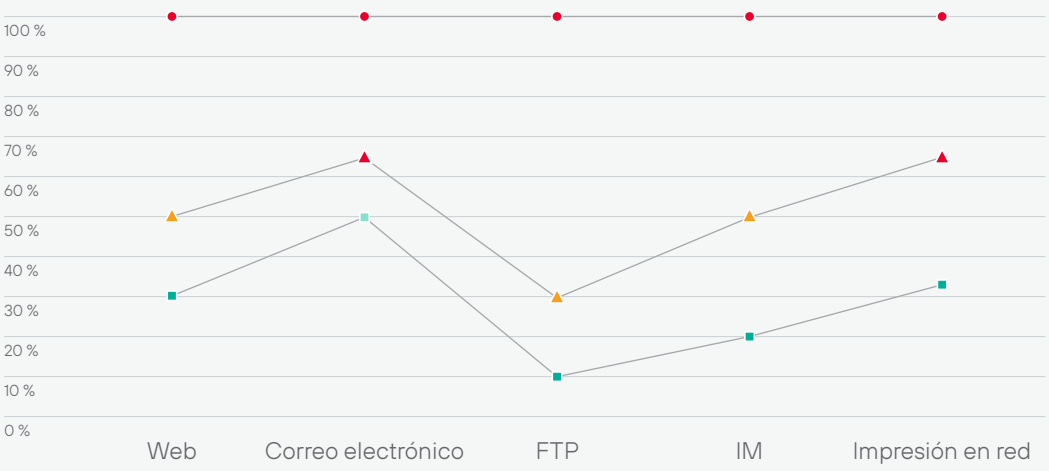
2. Mantener la congruencia entre las fases de reducción del riesgo.
Para preservar la integridad de sus resultados, los períodos de monitoreo y reducción del riesgo deben durar lo mismo. Al comienzo, recomendamos dos semanas para mejorar la adquisición de valor y simplificar el análisis. Sin embargo, usted podrá determinar mejor qué es lo más razonable para su organización.

A continuación hay un ejemplo de cómo se aplica el agrupamiento y se hace seguimiento de la reducción del riesgo. Tenga en cuenta que hay un período constante, un enfoque en los incidentes de riesgo alto y que estos incidentes se agruparon por su canal relativo.

Opción de DLP adaptable al riesgo: Si se decidió por adoptar 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).

Por último, cuando actualice a su equipo ejecutivo sobre el proceso de DLP y sus resultados, recuerde que menos es más. Concéntrese en el panorama general cuando explique los vectores de alto riesgo de su organización y describa las actividades de mitigación del riesgo recomendadas y el costo, los beneficios y el esfuerzo de cada una.

Probabilidad de pérdida de datos



Leyenda del marcador

- Alto
- Moderado
- Bajo
- Aceptable
- Punto de referencia de 30 días
- 60 días
- 90 días

Cantidad de incidentes en 90 días

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

Objetivos

- **60 días** Reducción de más del 25 %
- **90 días** Reducción de más del 50 %

Conclusión

Una implementación de DLP exitosa no se logrará por una nueva parafernalia técnica y no podrá colocarse y apilarse en una central de datos. En cambio, dependerá de su habilidad para:

1. Entender la estrategia de ejecución y metodología de un proveedor de DLP. Su organización se beneficia de comprender de qué manera los distintos proveedores abordan el DLP. Hacerlo le permite determinar las metodologías más prometedoras para su entorno, y qué tecnologías de DLP evaluar. Tener en cuenta a un proveedor que brinde una solución adaptable al riesgo puede sumar ventajas duraderas a una organización, como un aumento en la eficiencia y la productividad. Y no olvide: aplicar la metodología de un proveedor a la tecnología de otro tiene implicancias a largo plazo negativas.

2. Aplicar la fórmula del riesgo de la pérdida de datos. Una vez que su equipo de seguridad comprenda y aplique la fórmula del riesgo de la pérdida de datos, puede colaborar con los propietarios de los datos para identificar y priorizar los recursos de datos. Además, cada actividad de mitigación del riesgo deberá estar diseñada con el único propósito de disminuir el índice de ocurrencia (RO) de la pérdida de datos. El RO es la medición correcta para hacer el seguimiento de la reducción del riesgo y mostrar el ROI de los controles de DLP. Recuerde: preste especial atención al comparar soluciones de DLP tradicionales con una tecnología de DLP adaptable al riesgo para asegurarse de no estar comparando falsos positivos con verdaderos positivos.

3. Aplicar la regla 80/20 para la asignación de recursos. Al entender qué vectores de pérdida de datos implican un mayor riesgo de fuga de datos de alto impacto, su organización puede usar la regla 80/20 para asignar recursos y formular estrategias de protección de datos eficaces.

4. Seguir los nueve pasos para alcanzar el éxito con el DLP. Ya sea que opte por un enfoque de DLP tradicional o uno adaptable al riesgo, nuestro proceso de nueve pasos es una fórmula probada para implementar controles de DLP de manera tal que seguirlos resulte práctico para su negocio y que entreguen resultados aplicables, medibles y adaptables al riesgo.

Forcepoint

forcepoint.com/contact

Acerca de Forcepoint

Forcepoint es la compañía líder en ciberseguridad de protección de datos y usuarios, encargada de proteger a las 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.

© 2020 Forcepoint. Forcepoint y el logotipo de FORCEPOINT son marcas comerciales de Forcepoint.
Todas las demás marcas comerciales utilizadas en este documento son propiedad de sus respectivos dueños.
[Practical-Exec-Guide-to-DLP-Whitepaper-ES] 27OCT2020