Implementación políticas de seguridad

DLP o Data Loss Prevention, en español prevención de pérdida de datos, sirve para garantizar que los usuarios no envíen información delicada o crítica fuera de la red corporativa. El término describe productos de software que ayudan a un administrador de redes a controlar los datos que los usuarios pueden transferir. Los productos de DLP usan reglas de negocio para clasificar y proteger la información confidencial y crítica, para que los usuarios no autorizados no puedan intercambiar datos de manera accidental o malintencionada, cosa que podría poner en riesgo a la organización. Por ejemplo, si un empleado intenta reenviar un correo electrónico empresarial fuera del dominio corporativo o cargar un archivo corporativo a un servicio de almacenamiento en la nube para el consumidor, como Dropbox, el empleado no recibirá autorización.

Un DLP es una herramienta que tiene como finalidad prevenir las fugas de información cuyo origen está dentro de la propia organización, de una manera activa y sin perder productividad. Estas herramientas suelen incorporar inteligencia artificial que les permite aprender sobre el tipo de documentos confidenciales que se utilizan y qué acciones llevan a cabo los usuarios sobre los mismos, para volverse cada vez más efectivas en la prevención de fugas de información.

Los DLP monitorizan la red de la organización para evitar las fugas de información antes de que se lleguen a producir. Una vez que detectan una posible fuga, alertan al usuario para que sea consciente de que la acción que está realizando atenta contra la confidencialidad de la empresa o contra una política de seguridad que vela por ella. Estas acciones tienen como objetivo concienciar a los miembros de la organización.

La monitorización de recursos por parte de un DLP no se limita exclusivamente a la red interna de la organización, ya que estas herramientas son capaces de extender su supervisión a dispositivos móviles, tanto Android como iOS. Los DLP son capaces de comprobar a qué correos corporativos se ha accedido. Además, tienen capacidad de comprobar y detener la transmisión de datos confidenciales desde la organización a aplicaciones de almacenamiento en la nube o redes sociales.

Políticas DLP

A) Identificar los datos que la política pretende proteger principalmente.

La mayoría de las veces, los datos se clasifican según su vulnerabilidad y factores de riesgo. Invertir tiempo en entender los datos y clasificarlos puede conducir a una mayor comprensión de la organización.

B) Establecer criterios para evaluar proveedores de Data Loss Prevention

Elegir soluciones DLP puede ser desalentador. Pero crear un marco de evaluación con las preguntas correctas puede ayudar a tomar una decisión de compra informada.

C) Definir claramente los roles de las personas que estarán involucradas en la prevención de pérdida de datos.

No se trata solo de quién monitoreará el uso de datos y establecerá las reglas. La segregación de responsabilidades ayuda a prevenir el mal uso.

D) Empezar por lo más sencillo. Elija un tipo específico de datos o riesgo para abordar.

El objetivo es asegurar los datos más críticos y obtener una ganancia medible temprano, luego construir sobre eso.

E) Obtener la aceptación del liderazgo de la organización.

Cada jefe de departamento o unidad tiene un papel en la configuración de una política de prevención de pérdida de datos que se alinea con la cultura corporativa. Esta es una estrategia que afecta a todos los departamentos y funciones.

F) Formar a todos los empleados de la organización sobre cómo y por qué se implementó la política de prevención de pérdida de datos.

Muchos ejecutivos ven a los empleados como el eslabón más débil en la prevención de pérdida de datos, pero no ven la formación en Seguridad como una prioridad.

G) Documentar cuidadosamente los procesos de Data Loss Prevention.

Una política escrita debe centrarse en los datos que se protegen.

H) Establecer y compartir métricas para el éxito.

Las métricas de prevención de pérdida de datos determinarán el retorno de la inversión de políticas y soluciones. También pueden ayudar a determinar la eficiencia.

I) Anticipar soluciones a los límites.

Si las reglas de correo electrónico impiden que se adjunten archivos grandes, ¿los empleados encontrarán otras formas de transferir archivos? **Examine los flujos de trabajo para asegurarse de que las políticas de prevención de pérdida de datos no interfieran con el trabajo legítimo de los empleados.**

J) Evaluar cuántos datos se necesitan.

Determine qué tipo de datos se necesitan y por qué. No guarde datos innecesarios. Los datos inexistentes no se pueden perder.

J) Monitorear el uso de datos antes de bloquearlos.

Configure herramientas de prevención de pérdida de datos para reportar primero sobre la pérdida de datos confidenciales. Asegúrese de que las reglas que bloquean la transferencia de datos no interrumpan el flujo de trabajo.

Clasificación de datos

Datos altamente confidenciales información que, si se hace pública, pone a la empresa en peligro de acción legal, incumplimiento normativo o pérdida financiera. Esto se refiere especialmente a la información de identificación personal, pero también a los registros de la empresa y otras categorías de datos que se consideran confidenciales según la industria.
Datos confidenciales internos: información que, si se revela, puede suponer un riesgo para las operaciones de la empresa. Esto incluyen datos de ventas, información de clientes, salarios de empleados, etc.
Datos internos: información que, si bien no es confidencial, no está disponible públicamente, como organigramas, estrategias de marketing, etc.
Datos disponibles al público: información a la que todas las personas dentro y fuera de la organización tienen acceso, por ejemplo, descripciones de productos, direcciones de empresas, etc.

Acceso y Control

El **principio del menor privilegio** establece que cada usuario debe tener solo los permisos necesarios para realizar su trabajo, ni más ni menos. Esto ayuda a minimizar el impacto de posibles violaciones de seguridad al reducir el acceso innecesario a información sensible. Para implementar este principio, es fundamental definir políticas claras de acceso y establecer un flujo continuo de revisión y ajustes de permisos.

Políticas de Acceso Basadas en el Principio del Menor Privilegio:

- **Control de acceso basado en roles (RBAC)**: Los permisos deben asignarse a roles, no a individuos. Los roles deben estar definidos en función de las tareas y responsabilidades del empleado. Por ejemplo, un empleado del departamento de recursos humanos tendría acceso a la información de los empleados, pero no a los datos financieros.
- **Revisión de permisos**: Los permisos de acceso deben revisarse periódicamente para asegurarse de que siguen siendo apropiados. Las revisiones deben realizarse al menos una vez cada trimestre.
- **Flujo de Revisión de Permisos**:
    - **Roles responsables**: El **Responsable de Seguridad de la Información (CISO)** supervisará la política general, mientras que los **Responsables de Departamentos** revisarán y validarán los accesos específicos dentro de su área.
    - **Método de revisión**: Los accesos se revisarán mediante informes generados por herramientas de gestión de identidades y accesos (IAM) que detallan quién tiene acceso a qué sistemas y datos.
    - **Revisión por separación de roles**: Las revisiones deben realizarse por un grupo de usuarios distinto al responsable de la asignación inicial de permisos, garantizando la imparcialidad.

Monitoreo y Auditoría

El monitoreo y la auditoría son esenciales para detectar actividades sospechosas y para asegurar el cumplimiento de las políticas de acceso.

Reglas de Monitoreo:

- **Monitoreo de actividades sensibles**: Toda actividad que involucre datos sensibles debe ser registrada y monitoreada. Esto incluye acceso, modificación, exportación o eliminación de datos sensibles.
- **Herramientas de Monitoreo y Auditoría**:
    - **SIEM (Security Information and Event Management)**: Herramientas como Splunk, IBM QRadar o ArcSight se usarán para correlacionar eventos y generar alertas sobre accesos no autorizados o actividades sospechosas.
    - **DLP (Data Loss Prevention)**: Soluciones DLP como Symantec DLP, McAfee Total Protection, o Forcepoint serán implementadas para monitorear y bloquear la transferencia no autorizada de datos sensibles fuera de la red corporativa.
    - **Registro de auditoría**: Toda actividad debe quedar registrada en un sistema de auditoría, con detalles sobre el usuario, la actividad, la hora y la naturaleza del acceso.

Auditoría de Actividades:

- Las auditorías deben realizarse trimestralmente por parte de un equipo independiente, con revisiones ad hoc si se detecta alguna actividad sospechosa.
- Los informes de auditoría deben ser revisados por el CISO y el comité de seguridad para evaluar las brechas de seguridad y la necesidad de ajustes en las políticas.

Prevención de Filtraciones

La prevención de filtraciones de datos sensibles es crucial para proteger la integridad y privacidad de la información confidencial de la organización.

Estrategias de Prevención:

- **Cifrado de datos**: Todos los datos sensibles deben ser cifrados tanto en reposo como en tránsito. Se utilizarán estándares de cifrado como AES-256 para garantizar que los datos sean ininteligibles para personas no autorizadas.
- **Uso de DLP**: Además de monitorear, las herramientas DLP también bloquearán intentos de transferencia de datos sensibles sin autorización, ya sea por correo electrónico, USB, o aplicaciones de mensajería.
- **Autenticación multifactor (MFA)**: Se implementará MFA para acceder a sistemas que contengan información crítica, evitando accesos no autorizados incluso si las credenciales son comprometidas.

Educación y Concientización

La capacitación y la concientización sobre la seguridad son fundamentales para evitar errores humanos y aumentar la cultura de seguridad dentro de la organización.

Plan de Capacitación:

- **Formación inicial**: Todos los empleados recibirán capacitación en políticas de seguridad, manejo de datos sensibles y cómo prevenir ataques comunes como phishing.
- **Capacitación continua**: Se realizarán sesiones de actualización periódicas para mantener al personal al tanto de nuevas amenazas, técnicas de seguridad y cambios en las políticas internas.
- **Simulacros de seguridad**: Se realizarán simulacros de incidentes de seguridad, como intentos de phishing o filtración de datos, para mejorar la respuesta del personal ante incidentes reales.
- **Campañas de concientización**: Campañas de comunicación continuas reforzarán la importancia de la seguridad, promoviendo buenas prácticas como el uso de contraseñas fuertes y el reporte inmediato de incidentes de seguridad.

Ejemplo Dropbox creación DLP

Paso 1: Requisitos Previos

Antes de comenzar con la implementación de una política de DLP en Dropbox, asegúrate de contar con:

1. **Cuenta de Dropbox Business**: Solo las cuentas de Dropbox Business o Dropbox Enterprise permiten gestionar políticas de seguridad como DLP.
2. **Acceso de Administrador**: Necesitarás privilegios de administrador para configurar las políticas de seguridad.
3. **Un Servicio de DLP Compatible**: Aunque Dropbox tiene algunas funciones básicas de protección de datos, es recomendable integrar una herramienta de **Data Loss Prevention (DLP)** de terceros para una mayor efectividad. Algunas opciones populares incluyen **Microsoft Purview**, **Symantec DLP**, **McAfee DLP**, o **Nightfall**.
4. **Conocimiento de los Datos Sensibles**: Debes conocer qué tipo de datos sensibles quieres proteger (números de tarjetas de crédito, datos de salud, información personal identificable, etc.).

Paso 2: Habilitar la Integración DLP con Dropbox

1. Iniciar sesión en el Admin Console de Dropbox

- Accede a tu cuenta de **Dropbox Business** y ve a la sección **Admin Console**.

2. Conectar Dropbox con un Servicio DLP de Terceros

- En el panel izquierdo, selecciona la opción **Security** (Seguridad).
- Busca la sección **Connected Apps** (Aplicaciones Conectadas) o **Data Protection** (Protección de Datos).
- Selecciona la opción de **Integración DLP**.

Por ejemplo, si usas **Microsoft Purview** (anteriormente conocido como Microsoft Information Protection):

- Inicia sesión con tu cuenta de **Microsoft 365**.
- Autoriza a Microsoft Purview para que pueda escanear y aplicar políticas de protección en los archivos de Dropbox.

Para otras herramientas DLP, el proceso será similar: tendrás que autenticar y dar acceso al servicio de DLP para que interactúe con los archivos en Dropbox.

Paso 3: Crear y Configurar una Regla de DLP

1. Crear una Nueva Política DLP

Una vez que hayas conectado tu herramienta de DLP, deberías crear una nueva política de protección de datos. A continuación, te doy un ejemplo para **proteger números de tarjetas de crédito**.

Ejemplo: Proteger Datos de Tarjetas de Crédito

- **Paso 1:** Inicia sesión en la plataforma de DLP que hayas conectado (por ejemplo, **Microsoft Purview**).
- **Paso 2:** Ve a la sección de **Políticas** o **Data Loss Prevention**.
- **Paso 3:** Crea una nueva política o regla de DLP.
    - Selecciona el **tipo de datos** que quieres proteger. En este caso, elige **números de tarjetas de crédito**.
    - En **Microsoft Purview**, esto se puede hacer utilizando plantillas predefinidas como "**Credit Card Number**" o puedes crear expresiones regulares personalizadas.

2. Definir los Condiciones para Detectar Datos Sensibles

La herramienta DLP utilizará expresiones regulares para buscar patrones que coincidan con los **números de tarjetas de crédito**. Aquí hay una expresión regular común utilizada para detectar números de tarjetas de crédito:

- \b[3456]\d{3}[\s-]?\d{4}[\s-]?\d{4}[\s-]?\d{4}\b

Esta expresión regular buscará:

- Números que comienzan con 3, 4, 5, o 6 (que son los primeros dígitos válidos para tarjetas de crédito).
- Un formato con 16 dígitos, permitiendo espacios o guiones entre ellos.

3. Configurar el Alcance de la Política

Decide en qué parte de Dropbox quieres aplicar esta política. Por ejemplo:

- **Documentos y Archivos en Dropbox**: Aplica la regla a todos los archivos que se carguen en Dropbox.
- **Directorios Específicos**: Si solo deseas aplicar la regla a carpetas específicas (como una carpeta de pagos), puedes configurarlo para que solo esa carpeta esté sujeta a esta regla.

4. Establecer las Acciones a Tomar

Una vez que la herramienta DLP detecte datos sensibles, puedes configurar las acciones que tomará:

- **Bloquear la carga**: Si un archivo contiene un número de tarjeta de crédito, el sistema bloqueará automáticamente la carga del archivo en Dropbox.
- **Notificación al usuario**: Puedes configurar para que el usuario que intenta cargar el archivo sea notificado que contiene datos sensibles, informándole sobre la violación de la política.
- **Notificación al administrador**: Los administradores también pueden recibir una notificación cada vez que un archivo es bloqueado o marcado como sospechoso.
- **Cifrado adicional**: Si prefieres no bloquear el archivo, puedes cifrarlo de manera que solo los usuarios autorizados puedan acceder al contenido.

Puedes establecer reglas adicionales, como permitir que solo los administradores suban ciertos archivos si contienen datos sensibles.

Paso 4: Monitorear y Validar las Políticas

1. Probar las Políticas DLP

Una vez que hayas configurado la política DLP, realiza pruebas para asegurarte de que funciona correctamente.

- Intenta cargar un archivo de texto con un número de tarjeta de crédito (puede ser algo como: 1234-5678-9012-3456).
- Dropbox, con la integración de DLP, debería bloquear la carga del archivo y notificarte.

2. Revisión de Alertas y Registros

Accede a los registros de actividad en el **Admin Console** de Dropbox y en la plataforma DLP:

- **Alertas**: Si se bloquea un archivo, deberías recibir una alerta.
- **Registros de Actividad**: Puedes revisar quién intentó cargar el archivo, qué tipo de archivo era, y qué acción tomó la política de DLP.

Paso 5: Ajustar la Configuración según Necesidad

Conforme vayas usando la herramienta, es probable que encuentres **falsos positivos** (archivos legítimos que son bloqueados por error) o necesites ajustar los umbrales de sensibilidad. Puedes:

- Modificar las expresiones regulares.
- Cambiar el tipo de archivos que deseas que sean analizados.
- Ajustar las acciones de las políticas (por ejemplo, permitir excepciones bajo ciertas condiciones).

Paso 6: Monitoreo Continuo y Actualización de Políticas

La protección de datos es un proceso continuo. Asegúrate de:

- Revisar los informes de **compliance** y **auditoría** regularmente.
- Actualizar las reglas conforme cambien las normativas de privacidad o los tipos de datos sensibles que manejas.

Políticas de dispositivos USB en Windows

Políticas de Grupo (GPO) para Control de Dispositivos USB

Ubicación en **Editor de directivas de grupo** (gpedit.msc o gpmc.msc en un dominio):

Configuración del equipo → Plantillas administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos
Restricción de Instalación de Dispositivos

- **"Impedir la instalación de dispositivos extraíbles"**
  - Bloquea por completo el uso de dispositivos de almacenamiento USB.
- **"Impedir la instalación de dispositivos no descritos por otras configuraciones de directiva"**
  - Solo se permitirán dispositivos explícitamente autorizados.
- **"Impedir la instalación de dispositivos con una clase de instalación coincidente"**
  - Bloquea tipos de dispositivos específicos (almacenamiento, impresoras, cámaras, etc.).

Excepciones y Permisos

- **"Permitir la instalación de dispositivos que coincidan con cualquiera de estos ID de dispositivo"**
  - Permite solo dispositivos específicos mediante su ID de hardware.
- **"Permitir la instalación de dispositivos de una clase de instalación específica"**
  - Se permite una categoría de dispositivos (ejemplo: solo teclados y ratones).
- **"Permitir a los administradores anular las restricciones de instalación de dispositivos"**
  - Solo administradores pueden instalar dispositivos bloqueados.

Políticas de Almacenamiento Extraíble

Ubicación:

Configuración del equipo → Plantillas administrativas → Sistema → Acceso de almacenamiento extraíble

Bloqueo de Lectura y Escritura

- **"Denegar acceso de escritura en dispositivos de almacenamiento extraíbles"**
  - Permite leer archivos desde un USB, pero impide copiar archivos a él.
- **"Denegar acceso de lectura en dispositivos de almacenamiento extraíbles"**
  - Bloquea totalmente el acceso a USBs conectados.

Restricciones Adicionales

- **"Denegar acceso a CD y DVD"**
  - Bloquea el uso de unidades ópticas.
- **"Denegar acceso a dispositivos de cinta"**
  - Bloquea almacenamiento en cinta magnética.
- **"Denegar acceso a dispositivos WPD (dispositivos portátiles como smartphones y cámaras)"**
  - Restringe teléfonos, cámaras y otros dispositivos MTP.

Políticas de Seguridad de BitLocker para USB

Ubicación:

Configuración del equipo → Plantillas administrativas → Componentes de Windows → Cifrado de unidad BitLocker → Unidades de datos extraíbles

Requerir Cifrado en USBs

- **"Requerir el uso de BitLocker en unidades extraíbles"**
  - Obliga a cifrar unidades USB antes de poder usarlas.
- **"Denegar el acceso a unidades extraíbles sin BitLocker"**
  - Bloquea los USB sin cifrado.
- **"Permitir solo lectura en dispositivos sin BitLocker"**
  - Permite leer desde USBs sin cifrar, pero no escribir en ellos.

Políticas de Restricción de Hardware Específico

Ubicación:

Configuración del equipo → Plantillas administrativas → Sistema → Instalación de dispositivos
Restringir o Permitir Dispositivos por Hardware

- **"Denegar la instalación de dispositivos que coincidan con estos ID de hardware"**
  - Se pueden listar dispositivos específicos para bloquearlos.
- **"Permitir solo la instalación de dispositivos USB con ID aprobados"**
  - Permite únicamente dispositivos específicos.
- **"Aplicar restricciones incluso si el dispositivo ya está instalado"**
  - Desactiva USBs ya conectados previamente.

Auditoría y Monitoreo del Uso de USB

Si necesitas **auditar** los dispositivos USB usados en tu sistema, puedes activar la auditoría con GPO:

Ubicación:

Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Directiva de auditoría

- **Habilitar Auditoría de Acceso a Dispositivos Extraíbles**
  - Registra eventos cada vez que se conecta un USB.
  - Puedes visualizar los eventos en el **Visor de eventos** (eventvwr.msc):
    - Registros de Windows → Seguridad → ID de evento 4663 o 4656
