Informe de Políticas de Seguridad: Prevención de Pérdida de Datos (DLP) - Aplicando el Principio del Menor Privilegio

Fecha: 19 de febrero de 2026
Elaborado por: Luis Gómez
Empresa: Google LLC

1. INTRODUCCIÓN

La prevención de pérdida de datos o DLP, es una estrategia de seguridad que tiene como objetivo proteger la información confidencial y sensible de una organización en contra de accesos no autorizados, filtraciones, robo y fuga de información en general. Se puede definir como un conjunto de herramientas, procesos y políticas diseñadas para identificar, monitorear y proteger los datos en sus tres estados (en movimiento, en uso y en reposo).

La implementación de esta estrategia es fundamental para cualquier organización ya que busca proteger los activos de información valiosos, como propiedad intelectual, información financiera, datos de clientes, entre otros. Su importancia radica en que la pérdida o filtración de estos datos puede significar daños financieros, sanciones regulatorias, pérdida de reputación y confianza de los clientes y/o socios comerciales y en general, tener un impacto negativo en la salud o el crecimiento de la organización.

En este informe, se establece un marco de políticas de DLP que aplican el Principio del Menor Privilegio, garantizando que el personal tenga acceso únicamente a la información estrictamente necesaria para el desempeño de sus funciones laborales, siendo esta la forma recomendada en la que debe de tratarse la data de la empresa.

2. CLASIFICACIÓN

Para implementar efectivamente esta estrategia y gestionar los permisos de accesos de forma correcta, se ha decidido clasificar los datos en las siguientes categorías, basadas en su nivel de sensibilidad.

2.1 Datos Públicos

Información destinada al consumo público general que no representa un riesgo para la organización si se exfiltra. Tales como:

- Material de marketing y comunicados de públicos.

- Información corporativa básica disponible en medios web o RRSS.
- Folletos y documentación pública.

Nivel de acceso: Cualquier empleado y público externo.

2.2 Datos Internos

Información operativa y administrativa de uso interno que, si se expone, podría causar daños de nivel intermedio a la organización. Incluye:

- Políticas internas y procedimientos.
- Documentación de proyectos no sensibles.
- Informes de desempeño individuales o por departamento.
- Comunicaciones internas de la empresa.

Nivel de acceso: Todos los empleados activos de Google LLC.

2.3 Datos Sensibles

Información altamente confidencial y sensible, una divulgación no autorizada podría causar daños significativos a la organización, incluyendo pérdidas financieras o tener repercusión reputacional. Tales como:

- Información financiera y estados contables no públicos.
- Datos personales de empleados y clientes.
- Contratos, acuerdos legales y documentación regulatoria.
- Propiedad intelectual y planes estratégicos.
- Información de investigación y desarrollo.
- Credenciales de acceso y contraseñas.

Nivel de acceso: Siguiendo el principio del menor privilegio, a esta información solo debe de tener acceso el personal estrictamente necesario, que la necesite para llevar a cabo sus tareas laborales.

3. ACCESO Y CONTROL

3.1 Acceso según necesidades operativas.

- Los empleados tendrán acceso únicamente a los datos y sistemas necesarios para poder desempeñar sus funciones laborales.
- Se evitará el acceso general a datos sensibles, incluso dentro del mismo departamento.
- Los permisos se otorgarán de forma individual, diferenciando entre lectura, edición, ejecución y descarga/compartición de la información.

3.2 Flujo de Revisión de Permisos

Responsables de la Revisión:

- **Data Owners o Propietarios de los datos:** Gerentes de departamento responsables de autorizar el acceso a los datos específicos de su área.
- **Oficial de Seguridad de la Información (CISO):** Responsable de la supervisión general y aprobación de accesos a datos altamente sensibles de la organización.
- **Equipo de TI y Seguridad:** Responsables de la implementación técnica y de la verificación de cumplimiento de las políticas y reglas de forma específica.

Proceso de Revisión:

- **Revisión periódica:** Evaluación de todos los permisos de acceso a datos sensibles e internos de forma periódica, trimestralmente.
- **Revisión ante Cambios de Rol:** Verificación de cuando un empleado cambia de posición o departamento en la compañía.
- **Revisión de Desincorporación (Off-boarding):** Revocación automática de accesos dentro de las 24 horas siguientes a la terminación de la relación laboral, para evitar que los accesos queden abiertos.
- **Auditoría de Accesos Temporales:** En caso de necesitarse accesos temporales, debe de haber una verificación semanal de estos para asegurarse que finalicen cuando sea pertinente.

3.3 Accesos Temporales

- Cuando se requiera acceso temporal a datos sensibles (por apoyo entre departamentos, proyectos específicos, un empleado cubriendo a otro en ausencias

médicas o vacaciones), este será concedido mediante autorización formal por escrito del Propietario de Datos correspondiente, vía email obligatoriamente, copiado al CISO y a demás responsables.
- Los accesos temporales deben de tener una fecha de expiración automática configurada en el sistema.
- Se realizará una revisión post-proyecto o post-ausencia para confirmar la revocación de estos permisos temporales.

3.4 Control de Dispositivos y Medios Extraíbles

Como parte de la política de DLP, se implementarán las siguientes restricciones:

- **Bloqueo de forma predeterminado:** Los puertos USB estarán deshabilitados por defecto en todas las terminales de la organización, esta es una práctica que ha demostrado ser efectiva para evitar la propagación de virus/malware y la fuga de información.
- **Autorización por Necesidad**: El uso de dispositivos USB solo se habilitará mediante solicitud formal, justificada y aprobada por el supervisor directo y el departamento de Seguridad de la Información vía correo interno de la compañía.
- **Monitoreo de Actividad:** Todas las operaciones de lectura/escritura en dispositivos USB autorizados serán registradas y auditadas.
- **Escaneo de Contenido:** Los archivos transferidos a memorias USB serán analizados automáticamente por el sistema DLP de Endpoint para detectar cualquier posible transferencia de datos sensibles.

4. MONITOREO Y AUDITORÍA

- Implementación del Sistema de monitoreo (SIEM) Wazuh para la correlación y registro de Logs, en conjunto con un DLP empresarial Purview para descubrimiento de datos y políticas en EndPoints para control de hardware como unidades extraíbles USB.
- Implementación de alertas inteligentes para comportamientos anómalos, tales como descargas masivas, accesos fuera de horario o desde localizaciones/IPs desconocidas.
- Establecimiento de una política de retención de al menos 12 meses para la información sensible, en conjunto con auditorias de integridad, cumplimiento y pruebas de penetración para corroborar la seguridad de esta.

5. PREVENCIÓN DE FILTRACIONES

Para mitigar las posibles filtraciones de datos, se aplicarán las siguientes medidas:

- **Protocolo de encriptación:** Toda la información en movimiento o en reposo, estará encriptada bajo algoritmos vigentes y seguros.
- **Aseguramiento de EndPoints:** Todos los discos estarán encriptados con Bitlocker y se deshabilitarán funciones que pueden presentar un riesgo para la seguridad de la información, como el Print-Screen, el copiado/pegado de información sensible y el acceso no autorizado de almacenamiento en la nube.
- **Control de egreso:** Implementación de inspección de paquetes a nivel de red y DLP de correo electrónico con una cuarentena automatizada para bloquear información sensible antes de que salga del control de la empresa.

6. EDUCACIÓN Y CONCIENTIZACIÓN

- **Entrenamiento en On-boarding y periódico:** Implementación de inducciones de seguridad obligatorias para los nuevos ingresos y sesiones de refrescamiento en el manejo seguro de datos y ataques de ingeniería social.
- **Simulación de campañas de Phishing:** Ejecución de ejercicios prácticos y ejemplos de la vida real en cuando a correos de phishing para fortalecer la intuición de los empleados en este tema.
- **Entrenamiento continuo:** Divulgación de boletines mensuales de seguridad digital y sistemas de recompensas para empleados que demuestren un manejo seguro de la información.