

1. Introducción al Data Loss Prevention (DLP)

La Prevención de Pérdida de Datos (DLP, por sus siglas en inglés) es un conjunto de estrategias y herramientas que tienen como objetivo evitar que información sensible o confidencial salga de una organización sin autorización. DLP ayuda a proteger datos como información personal, financiera, médica o propiedad intelectual, asegurando que solo personas autorizadas puedan acceder o compartir dicha información. Su implementación es fundamental para cumplir con normativas legales, prevenir ciberataques y mantener la confianza de clientes y colaboradores.

2. Clasificación de Datos

Una parte esencial de cualquier política de DLP es clasificar los datos según su nivel de sensibilidad. Esta clasificación permite aplicar controles específicos a cada tipo de información y minimizar el riesgo de exposición o pérdida.

En nuestra organización, proponemos las siguientes tres categorías de clasificación:

Datos Públicos

Información que puede ser divulgada libremente sin causar daño a la organización. No requiere controles estrictos.

Ejemplos:

- Información publicada en el sitio web institucional
- Comunicados de prensa
- Materiales de marketing

Datos Internos

Información de uso interno, cuyo acceso está limitado al personal autorizado. La divulgación no intencionada podría causar problemas operativos menores.

Ejemplos:

- Procedimientos internos
- Políticas de recursos humanos
- Información operativa de uso diario

Datos Sensibles o Confidenciales

Información crítica cuya exposición no autorizada podría causar daño significativo, violar regulaciones o comprometer la seguridad de la organización.

Ejemplos:

- Datos personales de empleados o usuarios
- Información financiera
- Documentación legal
- Contraseñas y credenciales

3. Acceso y Control

El acceso a los datos debe estar restringido estrictamente con base en el **principio del menor privilegio**. Esto significa que cada empleado o colaborador solo debe tener acceso a la información que necesita para cumplir con sus responsabilidades laborales, y nada más.

Política de Acceso Basada en Roles (RBAC)

La organización establecerá un esquema de permisos basado en roles. Cada rol tendrá asignado un conjunto específico de accesos:

Rol	Tipo de Acceso a Datos	Justificación
Dirección	Datos Sensibles, Internos	Toman decisiones estratégicas
Recursos Humanos	Datos Sensibles	Manejan información personal de empleados
Personal Técnico	Datos Internos	Gestión operativa y soporte
Administrativos	Datos Internos, Públicos	Actividades de gestión y coordinación
Visitantes/Externos	Solo Datos Públicos	Sin necesidad de información interna

Flujo de Revisión de Permisos

1. **Asignación inicial:** Se otorgan accesos mínimos al nuevo usuario según su rol.
2. **Solicitudes de acceso adicionales:** Deben ser justificadas y aprobadas por un supervisor.
3. **Revisión periódica de permisos:** Cada 3 meses se auditarán los accesos para identificar permisos innecesarios o caducados.
4. **Revocación inmediata:** En caso de cambio de rol, baja laboral o conducta sospechosa, se revocarán los accesos críticos de inmediato.

4. Monitoreo y Auditoría

La organización establecerá procedimientos de monitoreo continuo y auditoría para asegurar el cumplimiento de las políticas de DLP (Prevención de Pérdida de Datos), detectar accesos no autorizados y responder ante incidentes.

Objetivos del Monitoreo

- Detectar comportamientos anómalos o no autorizados relacionados con datos sensibles.
 - Verificar el uso correcto de los permisos asignados.
 - Auditar el acceso y transferencia de datos confidenciales.
-

Herramientas de Monitoreo

Se utilizarán las siguientes herramientas y tecnologías, dependiendo del entorno:

Herramienta / Tecnología	Función Principal
SIEM (Ej. Wazuh, Splunk)	Recopilación y análisis centralizado de logs
Windows Event Viewer	Registro de eventos de acceso, cambios en políticas
DLP Software (Ej. Symantec DLP)	Detección de movimientos sospechosos de datos
Registros de Actividad (Logs)	Revisión manual o automática de acceso a archivos

Auditoría de Actividades

Se llevará a cabo una **auditoría mensual** de:

- Archivos sensibles accedidos.
- Transferencias realizadas desde o hacia dispositivos externos.
- Cambios en permisos de acceso a carpetas críticas.
- Fallos de autenticación y accesos denegados.

5. Prevención de Filtraciones

Para evitar la fuga de datos sensibles dentro de la organización, se aplicarán medidas de prevención que combinan controles técnicos, políticas organizativas y herramientas de protección.

Tecnologías y Controles Aplicados

Medida	Descripción
Cifrado de datos	Todos los datos sensibles serán cifrados en reposo (disco) y en tránsito (red).
Bloqueo de dispositivos USB	Se restringirá el acceso a dispositivos de almacenamiento extraíbles.

Bloqueo de servicios de nube	Se limitará el uso de plataformas como Dropbox, Google Drive o WeTransfer si no están autorizadas.
Filtrado de contenido	Se usarán filtros para bloquear el envío de información sensible por correo o mensajería.

Políticas Organizativas

- Está prohibido transferir archivos sensibles fuera de la red corporativa sin autorización explícita.
- Solo el personal con autorización formal puede compartir o imprimir documentos clasificados como “Sensibles”.
- Se revisarán los permisos de forma periódica para minimizar el acceso innecesario.

Herramientas Sugeridas

- **BitLocker o VeraCrypt:** Para cifrado de disco completo.
- **Group Policy Editor:** Para bloquear puertos y dispositivos externos.
- **Firewall y Antivirus Corporativo:** Para bloquear conexiones o procesos sospechosos.
- **Google Workspace / Microsoft 365 Admin:** Para control de flujos de datos y aplicaciones en la nube.

6. Educación y Concientización

Uno de los pilares más importantes para una política DLP efectiva es que el personal esté bien informado sobre cómo manejar datos sensibles y cómo evitar incidentes de seguridad. Una tecnología excelente puede fallar si las personas no están capacitadas.

Plan de Capacitación

Actividad	Frecuencia	Objetivo
Capacitación en ciberseguridad básica	Cada 6 meses	Reconocer amenazas comunes (phishing, malware, etc.)


Entrenamiento específico en DLP	Anualmente	Enseñar cómo clasificar, proteger y manejar datos sensibles
Simulacros de fuga de datos	Trimestral	Evaluar la respuesta ante incidentes

Contenidos Clave del Programa

- Qué son los datos sensibles y cómo reconocerlos.
- Cómo manejar datos personales según normativas (como GDPR).
- Buenas prácticas: uso seguro del correo, contraseñas, navegación web.
- Qué hacer y a quién reportar en caso de incidente o pérdida de información.

Herramientas y Recursos

- Manuales y guías en PDF accesibles desde la intranet.
- Videos educativos cortos con ejemplos reales.
- Cuestionarios interactivos para validar conocimientos.

 **Compromiso institucional:** La organización se compromete a fomentar una cultura de seguridad activa, donde todos los colaboradores entiendan que proteger la información es una responsabilidad compartida.