

# Informe de Políticas de Seguridad DLP

## Prevención de Pérdida de Datos en la organización



# Índice

<b>1. Introducción al Data Loss Prevention (DLP)</b>	<b>3</b>
1.1 Concepto General de DLP	3
1.2 Importancia dentro de la Organización	3
1.3 Rol en la Protección de Datos Confidenciales	4
<b>2. Clasificación de Datos</b>	<b>4</b>
2.1 Marco de Clasificación	4
2.2 Categorías de Clasificación	4
2.3 Criterios de Clasificación	5
<b>3. Acceso y Control</b>	<b>5</b>
3.1 Principio del Menor Privilegio	5
3.2 Políticas de Acceso Basadas en Roles	5
3.3 Flujo de Revisión de Permisos	5
<b>4. Monitoreo y Auditoría</b>	<b>6</b>
4.1 Reglas de Monitoreo	6
4.2 Herramientas de Monitoreo y Auditoría	6
4.3 Procedimiento de Auditoría	7
<b>5. Prevención de Filtraciones</b>	<b>7</b>
5.1 Tecnologías de Protección	7
5.2 Herramientas DLP Específicas	7
5.3 Procedimiento de Respuesta a Filtraciones	7
<b>6. Educación y Concientización</b>	<b>8</b>
6.1 Programa de Capacitación	8
6.2 Frecuencia y Modalidad	8
6.3 Riesgos Asociados por Incumplimiento	8
<b>7. Implementación y Cumplimiento</b>	<b>8</b>
7.1 Cronograma de Implementación	8
7.2 Responsabilidades	9
<b>8. Revisión y Mejora</b>	<b>9</b>

# 1. Introducción al Data Loss Prevention (DLP)

## 1.1 Concepto General de DLP

Data Loss Prevention (DLP) es un conjunto de tecnologías, procesos y políticas diseñadas para prevenir la pérdida, filtración o uso no autorizado de datos confidenciales de una organización. DLP no solo detiene el acceso no autorizado, sino que también monitorea, registra y alerta sobre intentos de transferencia de información sensible[1].

## 1.2 Importancia dentro de la Organización

En la era digital, los datos constituyen uno de los activos más valiosos de cualquier organización. Los riesgos incluyen:

- **Pérdida financiera:** Robo de propiedad intelectual, datos de clientes o financieros
- **Daño reputacional:** Vulneraciones de privacidad que erosionan la confianza
- **Cumplimiento normativo:** Incumplimiento de RGPD, HIPAA u otras regulaciones
- **Continuidad del negocio:** Interrupciones causadas por brechas de seguridad

Las políticas DLP mitigan estos riesgos mediante la implementación de controles que garantizan que solo el personal autorizado acceda a datos sensibles según lo requiera su rol.

## 1.3 Rol en la Protección de Datos Confidenciales

DLP opera en tres niveles:

- **Prevención:** Evita la transferencia de datos sensibles a través de controles técnicos
- **Detección:** Identifica intentos de acceso o movimiento no autorizado
- **Respuesta:** Genera alertas y registros para investigación forense

# 2. Clasificación de Datos

## 2.1 Marco de Clasificación

La organización clasifica los datos en función de su sensibilidad, criticidad e impacto potencial en caso de divulgación. Esta clasificación determina los controles de acceso y protección aplicables.

## 2.2 Categorías de Clasificación

Categoría	Descripción	Ejemplos
Datos Públicos	Información que puede divulgarse libremente sin riesgo. No requiere protección especial.	Información de marketing, contenido web público
Datos Internos	Información para uso interno únicamente. Acceso restringido a empleados de la organización.	Políticas internas, procedimientos, anuncios
Datos Sensibles	Información crítica cuya divulgación causaría daño significativo. Acceso estrictamente limitado.	Datos financieros, información de clientes, secretos comerciales, contraseñas

## 2.3 Criterios de Clasificación

Cada empleado es responsable de clasificar correctamente los datos que genera. Los criterios incluyen:

- Impacto de divulgación:** ¿Qué daño causaría si se filtrara?
- Requisitos legales:** ¿Exigen regulaciones protección específica?
- Valor comercial:** ¿Es información competitiva?
- Relevancia del rol:** ¿Necesita el empleado acceso para su función?

# 3. Acceso y Control

## 3.1 Principio del Menor Privilegio

El Principio del Menor Privilegio (PMP) es fundamental en nuestra estrategia de seguridad. Cada usuario recibe únicamente los permisos necesarios para ejecutar sus funciones específicas, ni más ni menos.

**Beneficios del PMP:**

- Limita el daño potencial en caso de compromiso de una cuenta
- Reduce la probabilidad de acceso accidental a datos no autorizados
- Facilita la auditoría y el cumplimiento
- Minimiza la superficie de ataque

## 3.2 Políticas de Acceso Basadas en Roles

El acceso a datos se otorga según el rol del usuario:

Rol	Nivel de Acceso	Datos Autorizados
Administrador	Total	Todos los datos (con auditoría)
Gerente de Departamento	Elevado	Datos de su departamento + internos
Empleado Estándar	Moderado	Datos públicos + internos relevantes
Contratista/Proveedor	Limitado	Solo datos públicos + datos específicos del proyecto

### **3.3 Flujo de Revisión de Permisos**

Proceso de solicitud inicial:

1. El empleado nuevo solicita acceso a través del sistema de gestión de identidades
2. Su gerente directo aprueba o rechaza según responsabilidades
3. El propietario del dato (data owner) valida la justificación empresarial
4. TI provisiona acceso con los permisos mínimos requeridos
5. Se registra la decisión en logs de auditoría

Revisión periódica:

1. Trimestralmente, cada gerente revisa permisos de su equipo
2. Se eliminan accesos no utilizados o no justificados
3. Se documenta la revisión en el sistema de cumplimiento
4. Anualmente se realiza auditoría externa de accesos

Responsables de revisión:

- Gerente Directo: Valida necesidad del rol
- Propietario del Dato: Autoriza acceso a datos específicos
- Administrador de TI: Implementa y documenta cambios
- Oficial de Cumplimiento: Audita y reporta

## **4. Monitoreo y Auditoría**

### **4.1 Reglas de Monitoreo**

Se establecen reglas automáticas para detectar actividades sospechosas con datos sensibles:

- Acceso a más de 100 registros en 5 minutos
- Descarga en lote de información sensible
- Acceso desde ubicación geográfica inusual

- Acceso fuera de horario laboral sin justificación
- Múltiples intentos fallidos de autenticación

## 4.2 Herramientas de Monitoreo y Auditoría

Herramienta	Funcionalidad	Proveedor
SIEM (Security Information Event Management)	Correlaciona eventos de seguridad en tiempo real	Splunk, IBM QRadar
DLP (Data Loss Prevention)	Monitorea transferencias de datos sensibles	Symantec, Forcepoint
PAM (Privileged Access Management)	Gestiona y audita acceso administrativo	BeyondTrust, Delinea
Cloud Access Security Broker (CASB)	Monitorea uso de servicios en la nube	Microsoft Defender, Netskope

## 4.3 Procedimiento de Auditoría

1. **Recopilación:** Las herramientas SIEM y DLP registran todas las actividades con datos sensibles
2. **Análisis:** Análisis semanal de eventos para identificar anomalías
3. **Investigación:** El equipo de seguridad investiga eventos críticos dentro de 24 horas
4. **Escalamiento:** Incidentes confirmados se escalan a dirección y recursos humanos
5. **Documentación:** Todos los hallazgos se registran para auditoría externa

# 5. Prevención de Filtraciones

## 5.1 Tecnologías de Protección

- **Cifrado en tránsito (TLS/SSL):** Protege datos durante transferencia entre sistemas
- **Cifrado en reposo:** Almacenamiento encriptado de bases de datos y archivos
- **Tokenización:** Reemplaza datos sensibles con tokens no reversibles

- **Enmascaramiento de datos:** Oculta información sensible en reportes y desarrollos

## 5.2 Herramientas DLP Específicas

### Google Workspace DLP:

- Detecta y bloquea transferencias de datos sensibles por correo o Drive
- Notifica al usuario del intento bloqueado

### Restricción de dispositivos USB:

- Desactivar puertos USB para usuarios no autorizados
- Implementada mediante políticas de grupo en Windows

### Watermarking digital:

- Marca documentos sensibles para rastrear filtración
- Vincula documento a usuario específico

## 5.3 Procedimiento de Respuesta a Filtraciones

1. **Detección:** Alerta automática de herramienta DLP
2. **Contención:** Aislamiento inmediato de cuenta/dispositivo comprometido
3. **Investigación:** Análisis de logs para determinar alcance
4. **Notificación:** Comunicación a stakeholders según gravedad (RGPD 72h)
5. **Remediación:** Reset de credenciales, cambio de contraseñas asociadas

# 6. Educación y Concientización

## 6.1 Programa de Capacitación

Todos los empleados reciben formación obligatoria en políticas de seguridad:

### Contenidos de capacitación:

- Clasificación correcta de datos
- Identificación de intentos de phishing y ingeniería social
- Uso seguro de dispositivos y contraseñas

- Procedimientos de reportar incidentes de seguridad
- Consecuencias legales del incumplimiento de políticas

## 6.2 Frecuencia y Modalidad

Público	Frecuencia	Modalidad
Empleados nuevos	Al ingreso	Curso obligatorio en línea
Todos los empleados	Anual	Repaso de 30 minutos
Personal técnico	Semestral	Formación avanzada
Directivos	Trimestral	Sesiones ejecutivas

## 6.3 Riesgos Asociados por Incumplimiento

- **Riesgos organizacionales:** Pérdida de datos críticos, daño reputacional, pérdidas financieras
- **Riesgos legales:** Multas RGPD (hasta €20 millones), acciones civiles, demandas de clientes
- **Riesgos personales:** Despido por causa, responsabilidad penal en casos graves, antecedentes legales