Informe de Política Integral de Prevención de Pérdida de Datos (DLP)
Fecha: 10 de julio de 2025
Elaborado por: Javier Martinez
Empresa: TechCorp Inc

1. Introducción

La Prevención de Pérdida de Datos (DLP) es el conjunto de prácticas y tecnologías que impiden la divulgación, modificación o destrucción no autorizada de información sensible. En esta organización el objetivo es proteger los datos en sus tres estados críticos — en reposo, en movimiento y en uso — cumplir con marcos regulatorios (GDPR, HIPAA, PCI-DSS) y mantener la confianza de clientes y socios. Para lograrlo se aplican controles técnicos y de gobierno basados en el principio del menor privilegio y en la clasificación formal de la información.

---

2. Clasificación de Datos

Se establecen cuatro niveles de sensibilidad:

- **Pública**: información que puede difundirse sin impacto (p. ej., notas de prensa).
- **Interna**: datos operativos de uso exclusivo del personal (p. ej., manuales de proceso).
- **Confidencial**: PII, propiedad intelectual o estrategias de negocio cuyo acceso requiere cifrado y control estricto.
- **Regulada**: información sujeta a normas sectoriales (PCI, historiales clínicos) que exige salvaguardas adicionales.

Para automatizar la etiquetación y heredarla a correo, SharePoint y OneDrive se emplea **Microsoft Information Protection (MIP)**. MIP detecta contenido sensible mediante plantillas predefinidas, aplica la etiqueta correspondiente y, si el documento se envía fuera de la organización, obliga a cifrarlo o bloquea el envío.

---

3. Acceso y Control (Principio del Menor Privilegio)

- Los usuarios reciben únicamente los permisos imprescindibles para cumplir sus funciones.
- Bitácoras de Active Directory y las etiquetas de MIP se revisan cada trimestre; cualquier cambio de puesto desencadena la revocación inmediata de privilegios.

- El acceso temporal a información confidencial requiere solicitud formal y expirará al cerrar la tarea.
- Solamente los responsables directos de un documento poseen derechos de edición; los demás disponen, como máximo, de lectura.

Para reforzar el control se utiliza **BitLocker** en todos los discos Windows. BitLocker cifra con AES-256, protege la clave mediante TPM y almacena las claves de recuperación en Azure AD, de modo que incluso si un dispositivo se extravía nadie sin autorización podrá leer su contenido.

---

4. Monitoreo y Auditoría

- El agente **Symantec DLP Endpoint** vigila en tiempo real operaciones locales (copiar, pegar, impresión, capturas de pantalla) y registra cada intento de exfiltración.
- En la red, sensores DLP conectados al proxy y al firewall inspeccionan los flujos salientes; cualquier archivo etiquetado como Confidencial se bloquea o se cifra automáticamente.
- El Security Operations Center recibe alertas inmediatas y tiene como meta contener un incidente en menos de cuatro horas. Auditorías semestrales validan permisos y reglas, y los hallazgos alimentan mejoras continuas.

---

5. Prevención de Filtraciones

- **Datos en reposo** se protegen con BitLocker y copias de seguridad cifradas administradas por un HSM o KMS con rotación anual de llaves.
- **Datos en movimiento** viajan a través de **Cisco AnyConnect**, que crea túneles TLS 1.3/IPsec AES-256 y verifica la postura de los equipos antes de conceder acceso remoto. Para transferencias puntuales se exige SFTP o HTTPS con certificados Let’s Encrypt renovados de forma automática.
- **Datos en uso** quedan cubiertos por Symantec DLP Endpoint: impide capturas de pantalla, bloquea pegado de texto sensible en aplicaciones no autorizadas y añade marcas de agua para rastreo forense. Los sistemas reciben parches de microcódigo y SO contra vulnerabilidades como Meltdown y Spectre tan pronto como se publican.

Estas medidas, combinadas, aseguran que la información sensible permanezca cifrada, vigilada y controlada en todo momento de su ciclo de vida.

---

6. Educación y Concientización

- Cada nuevo empleado completa el primer día un módulo que explica las etiquetas de MIP, el cifrado de correo y las buenas prácticas de acceso remoto.
- Se envían micro-lecciones mensuales y se ejecutan simulaciones de fuga (por ejemplo, intento de copiar archivos a un USB) cada trimestre; el objetivo es que menos del 5 % de los usuarios reincida en la misma infracción.
- Las capacitaciones incluyen casos reales de filtraciones provocadas por compartir enlaces “con cualquiera” y demuestran cómo evitarlas.

---

7. Conclusión

La combinación de clasificación automatizada mediante Microsoft Information Protection, cifrado integral con BitLocker, tránsito seguro con Cisco AnyConnect y control granular de datos en uso gracias a Symantec DLP Endpoint proporciona una defensa holística frente a la fuga de información. El principio del menor privilegio, refuerzo educativo y auditorías periódicas completan un ecosistema que minimiza el riesgo y facilita el cumplimiento normativo. Con esta política, la organización protege su activo más valioso — la información — y consolida la confianza de sus partes interesadas.