Política de Seguridad DLP (Prevención de Pérdida de Datos)

1. Introducción al DLP

La **Prevención de Pérdida de Datos (DLP)** es una estrategia de seguridad diseñada para evitar la fuga, uso no autorizado o filtración de información sensible dentro de una organización.

TechCorp Inc. implementa un sistema DLP para proteger **datos financieros, información de clientes y propiedad intelectual**, asegurando el cumplimiento de regulaciones como **GDPR, ISO 27001 y otras normativas de seguridad**.

2. Clasificación de Datos

Para una gestión eficiente de la seguridad, los datos se clasifican en cuatro categorías:

Datos Públicos: Información sin restricciones, accesible a todos los empleados y, en algunos casos, al público en general. Ejemplo: comunicados de prensa, información de marketing.
Datos Internos: Información de uso exclusivo dentro de la empresa, accesible solo para empleados autorizados. Ejemplo: documentación interna, informes de desempeño.
Datos Sensibles: Información altamente confidencial que solo puede ser accedida por personal autorizado bajo estrictas medidas de seguridad. Ejemplo: datos financieros, credenciales de acceso, registros de clientes.
Datos Críticos: Información estratégica o vital para la continuidad del negocio, cuya exposición podría causar un impacto grave en la empresa. Ejemplo: claves de infraestructura, planes de negocio, información legal confidencial.

3. Acceso y Control

El acceso a los datos se rige por el **Principio del Menor Privilegio**, garantizando que cada usuario solo tenga permisos sobre la información estrictamente necesaria para su función.

Accesos restringidos: Los empleados solo pueden acceder a los archivos y bases de datos que sean necesarios para sus tareas.

Revisión periódica de permisos: Los permisos de acceso serán revisados cada **trimestre** para eliminar accesos innecesarios.
Autenticación multifactor (MFA): Requerida para el acceso a **datos sensibles** y sistemas críticos.
Accesos temporales: En casos donde sea necesario, se otorgará acceso temporal, con aprobación y registro detallado.

4. Monitoreo y Auditoría

Para garantizar el cumplimiento de la política DLP, se implementan las siguientes medidas de monitoreo:

Registros de actividad: Se registran accesos, descargas y modificaciones en archivos sensibles.
Alertas de seguridad: Se configuran notificaciones automáticas en caso de intentos de acceso no autorizados o actividades sospechosas.
Auditorías regulares: Se realizarán auditorías semestrales para revisar el cumplimiento de la política DLP.
Soluciones SIEM y herramientas DLP: Se emplearán herramientas como **Splunk, Microsoft Purview o Symantec DLP** para monitorear el uso de datos sensibles en la organización.

5. Prevención de Filtraciones

Para evitar la exfiltración o filtración de datos sensibles, TechCorp aplicará:

Cifrado de datos: Todo documento clasificado como **sensible** deberá estar cifrado tanto en tránsito como en reposo.
Restricciones en dispositivos externos: Se bloqueará la transferencia de archivos sensibles a **USB, correos personales o plataformas no autorizadas**.
Protección en la nube: Se aplicarán políticas de acceso a plataformas en la nube como **Google Drive, OneDrive y AWS**, asegurando que solo usuarios autorizados puedan compartir documentos.
DLP en correos electrónicos: Se implementarán filtros para detectar y bloquear el envío de información confidencial fuera del dominio corporativo.

6. Educación y Concientización

Los empleados recibirán formación continua sobre la importancia de la seguridad de datos y buenas prácticas:

Capacitaciones obligatorias: Se realizarán sesiones trimestrales para sensibilizar a los empleados sobre **ataques de phishing, protección de datos y uso seguro de la información corporativa**.
Simulaciones de ataques: Se llevarán a cabo pruebas de phishing para evaluar la respuesta de los empleados y reforzar las medidas de seguridad.
Políticas visibles: Se publicarán las políticas de seguridad en la intranet y se enviarán recordatorios periódicos sobre las mejores prácticas.

7. Conclusión

La implementación de esta política de **Prevención de Pérdida de Datos (DLP)** permite a TechCorp Inc. mitigar riesgos asociados a la filtración de información confidencial, proteger los activos digitales de la empresa y garantizar el cumplimiento de regulaciones de seguridad.

El compromiso de todos los empleados es clave para el éxito de esta estrategia de seguridad.