Marzo, 10 de 2025



Políticas DLP de TechCorp Inc.

REALIZADO POR:

WILSON JAVIER MENDEZ

# Introducción al Data Loss Prevention (DLP)

Actualmente la información es uno de los activos más valiosos para cualquier organización. Desde datos financieros hasta información personal de clientes y empleados, o incluso proyectos de servicios que no han sido lanzados al mercado.

La protección de estos recursos es fundamental para garantizar la continuidad del negocio, cumplir con normativas legales y mantener la confianza tanto de los empleados como de los clientes.

### 

### ¿Qué es el Data Loss Prevention (DLP)?

El Data Loss Prevention, o Prevención de Pérdida de Datos, es un conjunto de herramientas, políticas y procedimientos diseñados para identificar, monitorear y proteger la información confidencial dentro de una organización. El objetivo principal del DLP es prevenir la fuga o el acceso no autorizado a datos sensibles, ya sea de manera accidental o intencional. Esto se logra mediante la identificación de datos críticos, la implementación de controles de seguridad y la monitorización constante de los flujos de información.

### Importancia del DLP en las Organizaciones

La implementación de un sistema DLP es esencial para cualquier organización que maneje información sensible. No solo ayuda a evitar pérdidas financieras y daños a la reputación derivados de brechas de seguridad. DLP permite a las empresas:

* Proteger la Propiedad Intelectual
* Garantizar la privacidad
* Mejorar la gestión de riesgos

## Clasificación de Datos

### Datos Públicos:

* -Políticas de Empresas.
* -Empleados.
* -Productos y Servicios de la empresa.
* -Contactos.
* -Datos publicados en sitios web.
* -Información de Marketing.

### Datos Internos:

* Comunicaciones Internas
* Herramientas de Trabajo.
* Información de Redes y servicios
* Manuales de Procedimientos Internos
* Empleados de la empresa.

### Datos Sensibles:

* Nóminas
* Información personal e empleados
* Información sobre la Propiedad Intelectual
* Contratos Laborales
* Usuarios y contraseñas.
* Estrategias de Marketing.
* Datos sensibles de Clientes.
* Contratos con otras empresas.
* Contratos Laborales de Empleados.
* Información Bancaria.
* Datos Financieros de la Empresa.

# Políticas de Acceso y Control

* Los permisos de Acceso deberán ser asignados por roles y responsabilidades de cada empleado.
* Cada rol tendrá un conjunto predefinido de permisos que se ajusten a las tareas específicas del puesto.
* Ejemplo de estos roles son:

**Desarrollador:** Acceso a repositorios de códigos y herramientas de desarrollo.

**Analista de Finanzas:** Acceso a sistemas e información de financieros de la empresa.

**Soporte al cliente:** Acceso a sistemas de comunicación con los clientes y bases de conocimiento.

**Recursos Humanos:** Acceso a herramientas y datos de empleados.

**Ventas y Marketing:** Acceso a herramientas de Comunicación con otros departamentos, base de datos con información de finanzas y mercados competitivos.

* Acceso a datos calificados como sensibles (como por ejemplo, información personal tanto de clientes, como empleados, propiedad intelectual), estará restringido a personal específico que necesite esta información para realizar

su trabajo..

* Acceso Temporal, en casos excepcionales, se podrá otorgar acceso temporal a ciertos recursos o sistemas, si el empleado lo necesita.
* Se deberá justificar y enviar una solicitud, esta debe ser aprobada por el jefe de cada departamento.
* Todos los usuarios deberán autentificarse mediante credenciales únicas.
* Estas Credenciales deberán ser revisadas por el departamento de TI.
* En el caso de acceso a información sensible deberá requerir autenticación de doble factor..
* Renovación de Usuarios y contraseñas cada 3 meses.
* Una vez despiden o hay un cambio de empleado en un puesto específico de trabajo, se cambiarán los usuarios, y se le hará un usuario específico a ese nuevo empleado.
* Se eliminará el usuario que ya no se necesite, guardando sólo la información necesaria si se requiere.

# Políticas de monitoreo y Auditoría

* Monitoreo Continuo:
  + Todos los accesos y transacciones relacionadas con datos sensibles serán monitoreados en tiempo real.
  + Se establecerán alertas automáticas para actividades inusuales, como intentos de acceso fuera del horario laboral, accesos por fuerza bruta, descargas masivas de datos etc.
* Registro de Actividades;
  + Se mantendrá un registro detallado de los logs de todas las actividades relacionadas con datos sensibles, incluyendo:
    - Acceso a sistemas y bases de datos.
    - Intentos fallidos de autenticación.
    - Transferencias, modificaciones o eliminaciones de datos.
* Control de Transferencia de Datos:
  + Se monitorearán todas las transferencias de datos Sensibles.
  + Se bloquearán automáticamente Transferencias no autorizadas.
* Se utilizarán herramientas de análisis de comportamiento para detectar patrones anómalos en el uso de datos sensibles.

## Reglas de Auditoría

* Se realizan auditorías periódicas trimestrales.
* Las auditorías incluyen una revisión de permisos de acceso.
* Cualquier alerta generada por el sistema de monitoreo será investigada de inmediato por el equipo de Seguridad de TI.
* Se documentará todos los incidentes, incluyendo la causa, el impacto y las acciones correctivas.
* La auditoría verificará el cumplimiento estricto de las normativas antes dichas DLP.

## Herramientas de Monitoreo y Auditoría

Sistemas SIEM (Security Information and Event Management)

La Herramienta propuesta: WAZUH

Herramientas DLP

* Para Controles de acceso a datos en reposo: Active Directory, OpenLDAP
* Para datos en movimiento: Cisco AnyConnect, Cisco ASA
* Para datos en uso: Microsoft Purview Information Protection.

Para evitar la filtración de datos implementaremos cifrado de datos utilizando herramientas como:

* BitLocker
* AWS KMS

Educación y Concienciación

* Auditorías por departamentos dando charlas y explicando los riesgos que puede tener no cumplir estrictamente con las normas y políticas.
* Concienciación de que los ciberataques pueden ser muy destructivos en muchas razones si no se implementan buenas prácticas de seguridad.
* Clases didácticas sobre los ciberataques más comunes según el Top de MITRE.
* Pruebas de que lo implementado en las charlas está siendo eficaz, como pruebas de phishing y ataques monitoreados por la empresa.
* Pequeños cursos obligatorios de pocas horas donde al final tienen que responder un cuestionario.