Informe de políticas de seguridad:
Control de acceso a almacenamiento TI aplicando el principio del menor privilegio

Fecha: 06 de marzo de 2025
Elaborado por: Gisela Ferreira Ruiz
Empresa: TechCorp Inc.

---

1. Introducción

La Prevención de Pérdida de Datos (DLP) es un conjunto de herramientas, procesos y políticas diseñados para detectar y prevenir el uso y transmisión no autorizados de información sensible. En TechCorp Inc., la implementación de DLP es crucial debido a la gran cantidad de datos sensibles que manejamos en todos nuestros departamentos.

El almacenamiento centralizado (nube) es una herramienta comúnmente utilizada en TechCorp Inc. para almacenar, compartir y colaborar en documentos de trabajo. Sin embargo, sin un control adecuado, puede convertirse en una fuente de riesgo significativo para la pérdida de datos confidenciales.

Según nuestro análisis de flujo de datos, existen puntos críticos de riesgo en las transferencias de información entre departamentos, como:

- Transmisión de información de nómina entre RRHH y Finanzas
- Acceso remoto al código fuente por parte del equipo de I+D
- Intercambio de información de clientes entre Ventas y Soporte

Este informe propone políticas de seguridad que limitan y controlan el acceso a la información mediante el **Principio del Menor Privilegio**, asegurando que los empleados solo tengan acceso a los documentos necesarios para cumplir sus funciones específicas.

---

2. Clasificación de datos

Para mejorar la gestión de los permisos y el acceso a documentos en el almacenamiento, TechCorp Inc. clasifica sus datos en tres categorías:

- **Documentos públicos:** Información general de la empresa, material promocional y comunicados de prensa accesibles por cualquier empleado.
- **Documentos internos:** Información confidencial para personal autorizado, incluyendo documentación de proyectos y comunicaciones entre departamentos.
- **Documentos sensibles:** Datos altamente confidenciales como contratos, información financiera, datos de nómina, código fuente e información de clientes, restringidos a directivos o personal específicamente autorizado.

Nuestro análisis por departamento ha identificado los siguientes datos críticos (clasificación ALTA):

- **RRHH:** Información personal de empleados, datos salariales y registros médicos.
- **Finanzas:** Datos bancarios, registros financieros, información fiscal y datos de facturación de clientes.
- **I+D:** Código fuente, algoritmos propietarios, especificaciones de diseño y datos de prueba.
- **Soporte:** Información de clientes, credenciales temporales y grabaciones de llamadas/chats.
- **Ventas:** Base de datos de clientes, contratos y estrategias de precios.

La correcta clasificación es esencial para establecer los niveles de acceso adecuados y garantizar que la información solo sea compartida con el personal autorizado.

---

3. Acceso y control (aplicando el principio del menor privilegio)

En línea con el Principio del Menor Privilegio, el acceso al almacenamiento y datos en TechCorp Inc. se gestionará de la siguiente manera:

- **Acceso restringido:** Los empleados tendrán acceso solo a los documentos y carpetas necesarios para sus tareas diarias. Se implementarán controles de acceso específicos para cada departamento.
- **Revisión de permisos:** Los permisos de acceso serán revisados trimestralmente por el departamento de TI junto con los jefes de cada área para detectar y corregir permisos innecesarios.
- **Acceso temporal:** Para documentos sensibles, el acceso temporal requerirá autorización formal y se eliminará automáticamente al finalizar el proyecto.
- **Permisos limitados:** Solo los responsables directos tendrán permisos de edición completos. Los demás empleados tendrán permisos de solo lectura cuando sea necesario.

Estas medidas garantizarán que cada usuario solo pueda acceder a la información que realmente necesita para realizar su trabajo, reduciendo significativamente el riesgo de exposición de datos sensibles.

---

4. Monitoreo y auditoría

Se implementará una política de monitoreo y auditoría sobre el uso del almacenamiento para detectar accesos no autorizados y malas prácticas:

- **Registro de actividades:** Se utilizarán funciones de registro para monitorear accesos y acciones (edición, descarga, compartir) con marcas de tiempo precisas. Los registros se conservarán por 18 meses.

- **Alertas de seguridad:** Se configurarán alertas automáticas cuando se compartan documentos sensibles externamente, se otorguen permisos inadecuados, se detecten patrones de acceso sospechosos o transferencias masivas de datos.
- **Auditorías regulares:** Se realizarán auditorías trimestrales para revisar accesos a documentos sensibles, examinar patrones anómalos y generar informes para la dirección.

Para casos específicos, se implementarán herramientas como Symantec DLP (para monitorear acceso al código fuente) y Digital Guardian (para proteger información de clientes).

---

5. Prevención de filtraciones

Para prevenir la filtración de datos sensibles, se aplicarán medidas específicas según el estado de los datos:

Para datos en reposo:

- **Cifrado:** Se implementarán BitLocker (Windows) o FileVault (macOS) para proteger los datos almacenados.
- **Controles de acceso:** Se utilizará autenticación multifactor para sistemas con datos sensibles.

Para datos en movimiento:

- **Protección con etiquetas:** Los documentos sensibles tendrán etiquetas de "Confidencial" o "Solo uso interno".
- **Restricción de compartir:** Se deshabilitará la opción "compartir con cualquiera" para documentos sensibles.
- **Cifrado en tránsito:** Se utilizará SSL/TLS y VPN con autenticación multifactor para accesos remotos.

Para datos en uso:

- **Compartir controlado:** Solo se compartirá con personas autorizadas, principalmente con permisos de solo lectura.

Restricción de dispositivos USB:

Como medida crítica para prevenir la filtración de datos, se implementará un control estricto sobre los dispositivos USB:

- **Inventario de dispositivos:** Se mantendrá un registro centralizado de dispositivos USB autorizados, cada uno con identificador único. Solo estos podrán conectarse a equipos corporativos.
- **Control de acceso a puertos USB:** Se utilizará software de control de endpoints configurando los puertos USB en modo "solo lectura" por defecto, requiriendo autorización específica para escritura.

- **Cifrado obligatorio:** Todos los dispositivos autorizados usarán cifrado de hardware, implementando BitLocker To Go en entornos Windows y requiriendo contraseña para acceder a contenidos.
- **Monitoreo de transferencias:** Se registrarán todas las transferencias, configurando alertas para volúmenes inusuales y realizando análisis automáticos de malware.

Estas medidas están diseñadas específicamente para proteger los tres puntos de riesgo identificados en nuestro análisis de flujo de datos de TechCorp, especialmente el punto de riesgo 2 (acceso al código fuente), limitando la capacidad de descargar grandes volúmenes de código a dispositivos externos.

---

6. Educación y concienciación

Es fundamental que todo el personal comprenda la importancia de las políticas de seguridad:

- **Capacitaciones obligatorias:** Se impartirán sesiones trimestrales sobre el uso correcto del almacenamiento, clasificación de datos, identificación de riesgos y mejores prácticas de seguridad.
- **Concienciación sobre riesgos:** Durante las capacitaciones se presentarán ejemplos reales de incidentes y sus consecuencias. Se realizarán simulacros de phishing para evaluar la conciencia de seguridad.
- **Portal de recursos:** Se creará un portal interno con recursos educativos, actualizaciones sobre amenazas y un canal anónimo para reportar posibles violaciones de seguridad.

Estas actividades de formación ayudarán a crear una cultura de seguridad y minimizarán el riesgo de errores humanos, que frecuentemente son la causa de filtraciones de datos.

---

7. Conclusión

La correcta aplicación del **Principio del Menor Privilegio** en el uso del almacenamiento centralizado, junto con una política de seguridad bien definida, garantizará que TechCorp Inc. proteja su información más sensible y minimice los riesgos de accesos no autorizados o pérdida de datos.

Estas políticas están específicamente diseñadas para proteger los puntos de riesgo identificados en nuestro análisis de flujo de datos:

1. Transmisión de información de nómina entre RRHH y Finanzas
2. Acceso remoto al código fuente por parte del equipo de I+D
3. Intercambio de información de clientes entre Ventas y Soporte

Además, asegurarán el cumplimiento con regulaciones como GDPR, PCI-DSS y HIPAA, fundamentales para proteger la información personal, financiera y la propiedad intelectual de la empresa.