Informe de Políticas de Seguridad: Control de Acceso a Google Drive Aplicando el Principio del Menor Privilegio

Fecha: 04 de Octubre de 2024
Elaborado por: [Nombre del Responsable de Seguridad]
Empresa: TechCorp Solutions

---

1. Introducción

Google Drive es una herramienta comúnmente utilizada en **TechCorp Solutions** para almacenar, compartir y colaborar en documentos de trabajo. Sin embargo, sin un control adecuado, puede convertirse en una fuente de riesgo de **pérdida de datos** o **accesos no autorizados**.

Este informe propone una política de seguridad que limita y controla el uso de Google Drive mediante el **Principio del Menor Privilegio**, asegurando que los empleados solo tengan acceso a los documentos necesarios para el cumplimiento de sus funciones.

---

2. Clasificación de Datos

Para mejorar la gestión de los permisos y el acceso a documentos en Google Drive, **TechCorp Solutions** clasifica sus datos de la siguiente manera:

1. **Documentos Públicos:** Información general de la empresa, accesible por cualquier empleado.
2. **Documentos Internos:** Información confidencial que solo puede ser accedida por el personal autorizado.
3. **Documentos Sensibles:** Datos altamente confidenciales (contratos, acuerdos legales, datos financieros) que están restringidos a los niveles directivos o personal autorizado bajo estricta necesidad.

La correcta clasificación de los datos en Google Drive es esencial para definir los niveles de acceso y compartirlos solo con el personal autorizado.

---

3. Acceso y Control (Aplicando el Principio del Menor Privilegio)

En línea con el **Principio del Menor Privilegio**, el acceso a Google Drive se gestionará de la siguiente manera:

- **Acceso Restringido:** Los empleados tendrán acceso **solo** a los documentos y carpetas necesarios para sus tareas diarias. Se evitará el acceso generalizado a carpetas sensibles.
- **Revisión de Permisos:** Los permisos de acceso a los archivos y carpetas de Google Drive serán revisados trimestralmente para asegurarse de que solo el personal activo y autorizado conserve acceso.
- **Acceso Temporal:** Cuando se requiera acceso temporal a documentos sensibles, este será concedido bajo autorización formal y se eliminará una vez que el proyecto o tarea esté finalizado.
- **Permisos de Edición Limitados:** Solo los responsables directos tendrán permisos de edición. El resto de los empleados podrán tener permisos de solo lectura si es necesario para sus funciones.

---

4. Monitoreo y Auditoría

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

- **Registro de Actividades:** Se utilizarán las funciones de Google Workspace para registrar y monitorear quién accede a qué documentos, cuándo y qué acciones realiza (edición, descarga, compartir).
- **Alertas de Seguridad:** Se configurarán alertas automáticas para detectar y notificar al departamento de seguridad cuando se compartan documentos sensibles fuera de la organización o se concedan permisos de acceso inadecuados.
- **Auditorías Regulares:** Se realizarán auditorías trimestrales para revisar el acceso a documentos sensibles y detectar posibles incumplimientos de las políticas de seguridad.

---

5. Prevención de Filtraciones

Para prevenir la filtración de datos sensibles desde Google Drive, se aplicarán las siguientes medidas:

- **Desactivación de Compartir con Cualquiera:** La opción de compartir archivos o carpetas con "cualquier persona con el enlace" será deshabilitada de manera predeterminada para los documentos clasificados como sensibles.
- **Compartir Controlado:** Solo se podrá compartir documentos sensibles con empleados o socios externos previamente aprobados, y el acceso se controlará mediante permisos de lectura, sin opción de descarga o copia.

- **Protección con Etiquetas:** Los documentos más sensibles se protegerán con etiquetas de "Confidencial" o "Solo para uso interno", y solo podrán ser descargados con permisos especiales.

---

6. Educación y Concientización

Es fundamental que el personal comprenda la importancia de las políticas de seguridad en el uso de Google Drive:

- **Capacitaciones Obligatorias:** Se impartirán capacitaciones trimestrales para que el personal esté al tanto de las políticas de uso de Google Drive y cómo manejar documentos sensibles de manera segura.
- **Concientización sobre Riesgos:** Durante las capacitaciones, se presentarán ejemplos de incidentes comunes relacionados con el mal uso de Google Drive (como compartir documentos accidentalmente con terceros no autorizados) y las mejores prácticas para evitarlos.

---

7. Conclusión

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