Informe de Políticas de Seguridad: Principio de menor privilegio, uso de Microsoft 365

Fecha: 05 de Marzo de 2024
Elaborado por: Pablo Sánchez Martín
Empresa: TechCorp Solutions

1. Introducción

La **Prevención de Pérdida de Datos (DLP, Data Loss Prevention)** es un conjunto de estrategias y herramientas diseñadas para evitar la fuga, pérdida o exposición no autorizada de información sensible dentro de una organización. Su implementación es crucial para proteger datos confidenciales, cumplir con normativas y evitar brechas de seguridad que puedan comprometer la reputación y operaciones de la empresa.

En entornos corporativos donde se utilizan herramientas de colaboración como **Microsoft 365**, el DLP juega un papel fundamental al controlar el intercambio de información, restringir la divulgación de datos sensibles y garantizar que los empleados cumplan con las políticas de seguridad establecidas. Mediante la configuración de reglas y políticas adecuadas, es posible prevenir que documentos críticos sean compartidos de forma indebida, reforzando así la seguridad sin afectar la productividad.

2. Clasificación de Datos

Para mejorar la gestión de los permisos y el acceso a documentos en Microsoft 365, TechCorp Solutions clasifica sus datos de la siguiente manera:

1. Documentos Públicos: Información general de la empresa, accesible por cualquier empleado, código de conducta, procedimientos, comunicados de prensa.

2. Documentos Internos: Presupuestos departamentales, informes de reuniones, comunicación interna.

3. Documentos Sensibles: Datos de empleados y clientes, estado financiero, contratos con proveedores, propiedad intelectual.

La correcta clasificación de los documentos en Microsoft 365 (One 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 One Drive se gestionará de la siguiente manera:

● Se crearán grupos de trabajo con acceso únicamente a su espacio en One Drive.
● Cada usuario tendrá acceso a una carpeta propia dentro del espacio de su grupo.
● Las altas y bajas de personal serán gestionadas de inmediato para tener los permisos actualizados.
● Los documentos compartidos con otros departamentos tendrán que ser autorizados por el responsable correspondiente.
● La petición deberá especificar el tipo de permisos que se necesita, Solo Lectura, Edición…
● Los espacios personales no se pueden compartir de forma general, solo documentos en particular.

● Se impide compartir los documentos con personas fuera de la empresa.

4. Monitoreo y Auditoría

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

● Se registrará el acceso de cada usuario a cada documento.
● Alertas al intentar acceder a documentos que no han sido compartidos con el usuario.
● Alerta por cada documento descargado en el equipo.

5. Prevención de Filtraciones

Para prevenir la filtración de datos sensibles desde One Drive, se aplicarán las siguientes medidas:
● Únicamente se pueden compartir documentos con empleados de la empresa previa autorización.
● Los documentos etiquetados con la etiqueta “protección máxima” solo se podrán descargar previa autorización.
● Se establece marca de agua en los documentos individual para cada usuario propietario de ese documento.

6. Educación y Concientización

Es fundamental que el personal comprenda la importancia de las políticas de seguridad en el uso de One Drive:
● Formacion para nuevos empleados del uso de One Drive
● Recursos o “píldoras” formativas disponibles en la nube de formación sobre el uso de One Drive
● Formación Obligatoria: Una vez al año, se realizará un test a los empleados sobre diversas funciones de One Drive y ciberseguridad en la empresa, las preguntas comprenderán diversas áreas, por cada respuesta incorrecta se tendrá que volver a realizar la formación de ese área.
● Se enviarán periódicamente, por los medios de comunicación de la empresa, recordatorios sobre buenas prácticas en el uso de las aplicaciones.
● Se establecerá un canal de comunicación donde se resolverá cualquier duda con respecto al uso y buenas prácticas en el uso de las aplicaciones.

7. Conclusión

La correcta aplicación del Principio del Menor Privilegio en el uso de One 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.