Datos filtración hoja de trabajo

Resumen del incidente: Un gerente de ventas compartió con su equipo el acceso a una carpeta de documentos internos durante una reunión. La carpeta contiene archivos relacionados con un nuevo producto aún no anunciado públicamente. También incluía análisis de clientes y materiales promocionales. Tras la reunión, el gerente no revocó el acceso a la carpeta interna, pero advirtió al equipo que esperará la aprobación antes de compartir los materiales promocionales.

Durante una videollamada con un socio comercial, un miembro del equipo de ventas olvidó la advertencia de su gerente. El representante de ventas quería compartir un enlace a los materiales promocionales para que el socio pudiera distribuirlos a sus clientes. Sin embargo, accidentalmente compartió un enlace a la carpeta interna. Posteriormente, el socio comercial publicó el enlace en las redes sociales de su empresa, creyendo que se trataba de los materiales promocionales.

Control	Mínimo privilegio
Asuntos)	*¿Qué factores contribuyeron a la fuga de información?* ***Error humano interno**: el gerente no limitó ni revocó los accesos a tiempo.* ***Desobediencia de directrices**: el colaborador de marketing ignoró la advertencia de esperar autorización.* ***Confusión en el manejo de la información**: el socio comercial no verificó el contenido antes de publicarlo.* ***Ausencia de controles técnicos**: falta de políticas de expiración automática de enlaces y clasificación de la información.*

Revisar	*¿Qué aborda NIST SP 800-53: AC-6?* ***Definición**: Establece que los usuarios deben contar únicamente con los privilegios estrictamente necesarios para cumplir sus funciones.* ***Discusión**: El acceso indebido a información sensible se produce cuando no se restringen privilegios y no existen mecanismos de control y monitoreo.* ***Mejoras sugeridas**:* ● *Limitar accesos temporales a carpetas y documentos.* ● *Segmentar accesos según roles y departamentos.* ● *Implementar seguimiento y auditoría de permisos.* ●
Recomendación(es)	*¿Cómo se podría mejorar el principio del mínimo privilegio en la empresa?* ***Políticas claras y capacitación**: reforzar la cultura de seguridad con políticas de protección de datos, capacitaciones periódicas y consecuencias definidas ante incumplimientos.* ***Gestión de accesos**: aplicar control granular en carpetas y subcarpetas, con privilegios limitados por rol y caducidad automática de permisos.* ***Clasificación y etiquetado de la información**: diferenciar documentos públicos, internos, confidenciales y restringidos para evitar confusiones.* ***Tecnologías de seguridad**: implementar herramientas como DLP (Data Loss Prevention), monitoreo de accesos y alertas automáticas para detectar y prevenir fugas.*

Justificación	*¿Cómo podrían estas mejoras abordar los problemas?* *Las medidas propuestas permiten:* ● ***Prevenir incidentes similares** mediante control de accesos temporales y segmentados.* ● ***Reducir la dependencia del factor humano** al automatizar restricciones de permisos.* ● ***Asegurar la trazabilidad** con auditorías y monitoreo en tiempo real.* ● ***Reforzar la cultura organizacional** al capacitar al personal sobre políticas internas y normativas legales.* *En conjunto, estas acciones fortalecen el principio de mínimo privilegio, aseguran un control más estricto de la información sensible y reducen significativamente el riesgo de fugas futuras.*

Instantánea del plan de seguridad

El NIST Ciberseguridad FEl marco de seguridad (CSF) utiliza una estructura jerárquica, similar a un árbol, para organizar la información. De izquierda a derecha, describe una función de seguridad general y luego se vuelve más específica al ramificarse en una categoría, una subcategoría y controles de seguridad individuales.

Función	Categoría	Subcategoría	Referencia(s)
Proteger	PR.DS: *Seguridad de datos*	PR.DS-5: *Protecciones contra fugas de datos.*	NIST SP 800-53: AC-6

En este ejemplo, los controles implementados que utiliza el fabricante para protegerse contra fugas de datos se definen en NIST SP 800-53, un conjunto de pautas para proteger la privacidad de los sistemas de información.

Nota: Las referencias suelen incluir hipervínculos a las directrices o normativas a las que se refieren. Esto facilita obtener más información sobre cómo implementar un control específico. Es habitual encontrar múltiples enlaces a diferentes fuentes en las columnas de referencias.

Instituto Nacional de Estándares y Tecnología (NIST)SP 800-53: AC-6

El NIST desarrolló el SP 800-53 Proporcionar a las empresas un personalizable Plan de privacidad de la información. Es un recurso completo que describe una amplia gama de categorías de control. Cada control proporciona información clave:

- **Control:**Una definición del control de seguridad.
- **Discusión:**Una descripción de cómo se debe implementar el control.
- **Mejoras de control:**Una lista de sugerencias para mejorar la eficacia del control.

AC-6	**Mínimo privilegio**
	Control: Solo se debe proporcionar a los usuarios el acceso mínimo y la autorización necesarios para completar una tarea o función.
	Discusión: Los procesos, las cuentas de usuario y los roles deben implementarse según sea necesario para lograr el mínimo privilegio.La intención es evitar que un usuario opere con niveles de privilegio superiores a los necesarios para lograr los objetivos comerciales.
	Mejoras de control: • Restrinja el acceso a recursos confidenciales según el rol del usuario. • Revocar automáticamente el acceso a la información después de un período de tiempo. • Mantener registros de actividad de las cuentas de usuario aprovisionadas. • Auditar periódicamente los privilegios de los usuarios.

Nota: En la categoría de controles de acceso, la norma SP 800-53 incluye el privilegio mínimo en sexto lugar, es decir, AC-6.