### **Hoja de cálculo de fuga de datos**

**Resumen de incidentes:** Un gerente de ventas compartió el acceso a una carpeta de documentos internos con su equipo durante una reunión. La carpeta contenía archivos asociados con un nuevo producto que no se ha anunciado públicamente. También incluía análisis de clientes y materiales promocionales. Después de la reunión, el gerente no revocó el acceso a la carpeta interna, pero advirtió al equipo que esperara la aprobación antes de compartir los materiales promocionales con otros.

Durante una videollamada con un socio comercial, un miembro del equipo de ventas olvidó la advertencia de su gerente. El representante de ventas tenía la intención de compartir un enlace a los materiales promocionales para que el socio comercial pudiera distribuir los materiales a sus clientes. Sin embargo, el representante de ventas compartió accidentalmente un enlace a la carpeta interna. Más tarde, el socio comercial publicó el enlace en la página de redes sociales de su empresa asumiendo que se trataba de los materiales promocionales.

|  |  |
| --- | --- |
| **Control** | **Privilegio mínimo** |
| **Problema(s)** | *¿Qué factores contribuyeron a la fuga de información?* |
| **Revisión** | *¿Qué aborda NIST SP 800-53: AC-6?* |
| **Recomendación(es)** | *¿Cómo se podría mejorar el principio de privilegio mínimo en la empresa?* |
| **Justificación** | *¿Cómo podrían estas mejoras abordar los problemas?* |

### **Instantánea del plan de seguridad**

El marco de ciberseguridad (CSF) del NIST utiliza una estructura jerárquica en forma de árbol para organizar la información. De izquierda a derecha, describe una función de seguridad amplia y, a continuación, se vuelve más específica a medida que se ramifica a una categoría, subcategoría y controles de seguridad individuales.

|  |  |  |  |
| --- | --- | --- | --- |
| **Función** | **Categoría** | **Subcategoría** | **Referencia(s)** |
| **Proteger** | PR.DS: *Seguridad de los 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 las fugas de datos se definen en NIST SP 800-53, un conjunto de directrices para proteger la privacidad de los sistemas de información.

**Nota:** Por lo general, las referencias tienen hipervínculos a las pautas o regulaciones a las que se relacionan. Esto facilita obtener más información sobre cómo se debe implementar un control determinado. Es común encontrar varios enlaces a diferentes fuentes en las columnas de referencias.

### **NIST SP 800-53: AC-6**

El NIST desarrolló SP 800-53 para proporcionar a las empresas un plan de privacidad de la información personalizable. Es un recurso completo que describe una amplia gama de categorías de control. Cada control proporciona algunos datos 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** | **Privilegio mínimo** |
| Control:  Solo se debe proporcionar a los usuarios el acceso y la autorización mínimos necesarios para completar una tarea o función. |
| Discusión:  Los procesos, las cuentas de usuario y los roles deben aplicarse según sea necesario para lograr el privilegio mínimo. La intención es evitar que un usuario opere con niveles de privilegios superiores a los necesarios para lograr los objetivos empresariales. |
| Mejoras en el control:   * Restrinja el acceso a recursos confidenciales en función del rol del usuario. * Revocar automáticamente el acceso a la información después de un período de tiempo. * Mantenga los registros de actividad de las cuentas de usuario aprovisionadas. * Audite regularmente los privilegios de los usuarios. |

**Nota:** En la categoría de controles de acceso, SP 800-53 enumera el sexto privilegio mínimo, es decir, AC-6.