Hoja de trabajo sobre fuga de datos

Resumen del incidente: Un gerente de ventas compartió el acceso a una carpeta de documentos internos únicamente con su equipo durante una reunión. La carpeta contiene archivos asociados con un nuevo producto que no se había 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 esperará 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 hacer circular 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	**Least privilege**
Problema(s)	*Aparte de no mantener limitado el uso de las carpetas para un uso específico (limitar acceso y uso). No se tiene control luego del uso de gestionar esos recursos. También instruir a los trabajadores para tener cuidado con los recursos a compartir.*
revision	*Establece medidas a tomar para asegurar la seguridad de los datos, como limitar el acceso a los datos por parte de los departamentos si no lo necesitan. Por otro lado es tener activo la idea de privilegios mínimos y tener auditorías para mantenerlos siempre actualizados.*

Recomendación(es)	*Primero es establecer directrices con los permisos, otorgar accesos puntuales y luego quitarlos al no ser necesario o separar el uso para otros departamentos para que queden separados los contenidos.*
Justificación	*Principalmente es evitar errores humanos poniendo reglas fáciles de seguir y que limitan acceso, juntos con auditorías para revisar que los permisos están bien administrados , se evitarán muchos errores que pueden terminar en filtraciones.*

Panorama del plan de seguridad

The NIST Cybersecurity Framework (CSF) uses a hierarchical, tree-like structure to organize information. From left to right, it describes a broad security function, then becomes more specific as it branches out to a category, subcategory, and individual security controls.

Function	Category	Subcategory	Reference(s)
Protect	PR.DS: *Data security*	PR.DS-5: *Protections against data leaks*.	NIST SP 800-53: AC-6

In this example, the implemented controls that are used by the manufacturer to protect against data leaks are defined in NIST SP 800-53—a set of guidelines for securing the privacy of information systems.

Note: References are commonly hyperlinked to the guidelines or regulations they relate to. This makes it easy to learn more about how a particular control should be implemented. It's common to find multiple links to different sources in the references columns.

NIST SP 800-53: AC-6

NIST developed SP 800-53 to provide businesses with a customizable information privacy plan. It's a comprehensive resource that describes a wide range of control categories. Each control provides a few key pieces of information:

- **Control:** A definition of the security control.
- **Discussion:** A description of how the control should be implemented.
- **Control enhancements:** A list of suggestions to improve the effectiveness of the control.

AC-6	**Least Privilege**
	Control: Only the minimal access and authorization required to complete a task or function should be provided to users.
	Discussion: Processes, user accounts, and roles should be enforced as necessary to achieve least privilege. The intention is to prevent a user from operating at privilege levels higher than what is necessary to accomplish business objectives.
	Control enhancements: • Restrict access to sensitive resources based on user role. • Automatically revoke access to information after a period of time. • Keep activity logs of provisioned user accounts. • Regularly audit user privileges.

Note: In the category of access controls, SP 800-53 lists least privilege sixth, i.e. AC-6.