DIARIO DIGITAL DEV / RECURSO DE LECTURA

Adjuntos en un portal: qué validar antes de dejarlos disponibles

El portal debe recibir el archivo con acceso restringido, comprobar formato y contenido según reglas acordadas, obtener los resultados exigidos y autorizar su uso para personas y procesos definidos. Un análisis pendiente, fallido o sin resultado mantiene la restricción. Cada sustitución requiere una decisión vinculada al contenido nuevo.

Evidencia que pedir al proveedor

[ ] Matriz de formatos, controles y resultados pendientes.

[ ] Pruebas de acceso antes y después de habilitar.

[ ] Correspondencia entre versión, contenido y decisión.

[ ] Sustitución y resultado antiguo ensayados.

[ ] Responsables de seguimiento y recuperación definidos.

Próximas acciones

1. Elegir un adjunto representativo y definir quién podrá usarlo.

2. Acordar estados, controles y política de sustitución con TI y el área responsable.

3. Pedir un ensayo de aceptación con fallas controladas antes de aprobar la entrega.

Notas para tu equipo

_____

_____

_____

_____

Artículo y fuentes

https://www.digital-dev.cl/blog/portal-empresarial-adjuntos-disponibles-validacion/

OWASP: File Upload Cheat Sheet
https://cheatsheetseries.owasp.org/cheatsheets/File_Upload_Cheat_Sheet.html

Microsoft Learn: On-upload malware scanning
https://learn.microsoft.com/en-us/azure/defender-for-cloud/on-upload-malware-scanning

Microsoft Learn: Understand malware scanning results
https://learn.microsoft.com/en-us/azure/defender-for-cloud/understand-malware-scan-results

Microsoft Learn: Set up automated remediation for malware detection
https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-storage-configure-malware-scan

Microsoft Learn: Introduction to malware scanning
https://learn.microsoft.com/en-us/azure/defender-for-cloud/introduction-malware-scanning