Listas de verificación

Listas para diseño seguro

Listas para evaluación de seguridad posterior

Criterio	Preguntas	Sí	No	No aplica
Exposición mínima de datos y operaciones	¿Los endpoints exponen únicamente los campos estrictamente necesarios (sin información sensible innecesaria)?			
	¿Existen controles para evitar que un cliente solicite más datos de los permitidos (ej. sobreexposición por **overfetching**)?			
	¿Se han limitado las operaciones (métodos HTTP) a las que realmente necesita la API?			
Comportamiento según el contexto	¿Cada operación solo puede ejecutarse en el contexto correcto (ej. eliminación restringida a usuarios con permisos válidos)?			
	¿Se validan parámetros y estado antes de ejecutar operaciones críticas?			
Integridad de los datos	¿Los datos de entrada pasan por validaciones estrictas (tipos, rangos, formatos, valores permitidos)?			
	¿Las respuestas de la API incluyen mecanismos para garantizar integridad (ej. firmas digitales, checksums, hash)?			
	¿Se previenen ataques de inyección mediante validación y sanitización de entradas?			
Prevención de fugas por protocolo o infraestructura	¿Toda comunicación está protegida con HTTPS/TLS y certificados válidos?			
	¿Se configuran headers de seguridad adecuados (ej. Strict-Transport-Security, X-Content-Type-Options)?			
	¿Los mensajes de error, cabeceras y logs evitan exponer información sensible del servidor o la infraestructura?			

Criterio	Preguntas	Sí	No	No aplica
Limitación de acceso con scopes de seguridad	¿Se implementa control de acceso basado en scopes o roles siguiendo el principio de mínimo privilegio?			
	¿Cada endpoint valida de manera consistente los tokens de autenticación y autorización?			
	¿Se previene el acceso no autorizado a recursos de otros usuarios (ej. mediante validación de IDs de usuario)?			
Manejo seguro de errores	¿Los mensajes de error no revelan información técnica interna (stack traces, queries, paths)?			
	¿Los códigos de estado HTTP son consistentes (ej. 401 para no autorizado, 403 para prohibido, 500 solo para fallos internos)?			
	¿Se registran los errores de manera interna para auditoría, sin exponer detalles al cliente?			