POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN — VETEL

Borrador público con referencia a ISO/IEC 27001 y buenas prácticas OWASP

Documento público provisional. VETEL se encuentra en proceso de preparación para auditoría externa. Este texto no acredita certificación, homologación, cumplimiento total ni aval de ISO o de una institución pública.

PRINCIPIOS

Minimización; necesidad de conocer; privilegio mínimo; separación de funciones; cifrado en tránsito; gestión segura de secretos; desarrollo seguro; monitoreo proporcional; continuidad; eliminación verificable; respuesta documentada a incidentes.

ARCHIVOS Y DATOS

VETEL declara el procesamiento local del archivo principal. Esa promesa debe verificarse extremo a extremo en navegador, memoria, temporales, Worker, almacenamiento, registros y terceros. Hasta completar la prueba, la eliminación integral permanece no verificada.

TERCEROS Y CAMBIOS

Los proveedores, APIs, bibliotecas y servicios de nube deben evaluarse por seguridad, privacidad, disponibilidad, ubicación, subencargados, continuidad y notificación de incidentes. Cada cambio requiere análisis de impacto y pruebas.

INCIDENTES

La organización debe habilitar detección, contención, preservación de evidencia, evaluación, comunicación, recuperación, análisis de causa y verificación de acciones. Los detalles explotables y secretos no se publican.

ESTADO

Evaluación de riesgos, Declaración de Aplicabilidad, pentest independiente, matriz de accesos, respaldo, recuperación y monitoreo: pendientes o parciales según la matriz de brechas.

Centro de Estudios Rincón Político · Director Ejecutivo Proyecto VETEL: Dr. Gustavo M. Martin
auditoriavetel.ar · consultora@rinconpolitico.com · +54 358 4332541