UNMSM
Fundación
SAN MARCOS
Por el desarrollo de la Ciencia y la Cultura

DIPLOMADO DE ESPECIALIZACIÓN

GESTIÓN DE LA CIBERSEGURIDAD Y PRIVACIDAD

RESUMEN EJECUTIVO

PRINCIPIOS ACTUALIZADOS SOBRE LA PRIVACIDAD Y LA PROTECCIÓN DE DATOS PERSONALES

JULIO – OCTUBRE 2026

CENCAEP
CAPACITA

RESUMEN EJECUTIVO PRINCIPIOS ACTUALIZADOS SOBRE LA PRIVACIDAD Y LA PROTECCIÓN DE DATOS PERSONALES

Análisis de los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales de la OEA (2021)

1. Contexto Operativo y Alcance del Documento

El presente informe ejecutivo constituye un análisis técnico-normativo del documento oficial «Principios Actualizados sobre la Privacidad y la Protección de Datos Personales», adoptado por el Comité Jurídico Interamericano (CJI) y aprobado por la Asamblea General de la Organización de los Estados Americanos (OEA) mediante la resolución AG/RES. 2974 (LI-O/21). Este instrumento actualiza el marco normativo regional previo de 2012 y 2015, integrando los avances tecnológicos globales y regulaciones de alto estándar como el Reglamento General de Protección de Datos (GDPR).

Desde una perspectiva de Ciberseguridad, Gestión de Riesgos de la Información y Cumplimiento Normativo, el documento sienta las bases operativas para la arquitectura de sistemas seguros, el flujo transfronterizo de datos, la resiliencia ante ciberincidentes y la rendición de cuentas (accountability) tanto en el sector público como en la empresa privada.

> 📌 **Perspectiva Estratégica de Ciberseguridad**
> *El marco de la OEA transiciona del cumplimiento reactivo tradicional hacia un modelo proactivo basado en el riesgo, exigiendo salvaguardias técnicas actualizables, evaluaciones de impacto a la privacidad (PIA/DPIA) y controles rigurosos en la transferencia de datos entre jurisdicciones.*

2. Desglose Estratégico de los 13 Principios de la OEA

Principio 1: Finalidades Legítimas y Lealtad

Alcance Normativo: Los datos personales deben recopilarse únicamente para fines legítimos, transparentes y por medios leales, evitando el fraude, engaño o técnicas de manipulación (e.g., ataques de ingeniería social o captura engañosa de credenciales).

Impacto en Ciberseguridad y Tecnologías de Información: Requiere auditar las fuentes de ingesta de datos y los formularios digitales para garantizar que la recolección no utilice patrones oscuros (dark patterns). En ciberseguridad, restringe el uso de técnicas de monitoreo excesivo o supervisión oculta no justificada legalmente.

Principio 2: Transparencia y Consentimiento

Alcance Normativo: Antes o en el momento de la recolección, se debe informar la identidad del responsable, finalidades, base legal, destinatarios y derechos del titular. El consentimiento debe ser previo, libre, explícito/inequívoco e informado. Se norma el derecho a revocarlo sin efectos punitivos.

Impacto en Ciberseguridad y Tecnologías de Información: Exige la implementación de Portales de Gestión de Consentimiento (CMP), registros de auditoría inmutables que demuestren la trazabilidad de los consentimientos otorgados y revocados, y avisos de privacidad claros y segmentados por perfil de usuario.

Principio 3: Pertinencia y Necesidad

Alcance Normativo: Aplica el principio estricto de minimización de datos: solo se debe capturar e identificar la información mínima indispensable para la finalidad declarada, manteniendo criterios de proporcionalidad.

Impacto en Ciberseguridad y Tecnologías de Información: Directamente alineado con el principio de Mínimo Privilegio y Reducción de la Superficie de Ataque. A menor volumen de datos almacenados, menor es el impacto y la severidad en caso de una filtración de datos (data breach).

Principio 4: Tratamiento y Conservación Limitados

Alcance Normativo: Prohíbe tratar o almacenar datos para fines incompatibles con los originales. Exige definir políticas explícitas de retención y purga, obligando a la destrucción segura o anonimización una vez cumplido el ciclo de vida del dato.

Impacto en Ciberseguridad y Tecnologías de Información: Implementación de mecanismos automatizados de purga de bases de datos, sanitización de almacenamiento, anonimización criptográfica irreversible y control de versiones para evitar que copias de respaldo (backups) retengan datos expirados fuera de control.

Principio 5: Confidencialidad

Alcance Normativo: Prohíbe divulgar o dar acceso a datos personales a terceros no autorizados sin consentimiento explícito o mandato imperativo de la ley. Es el pilar fundamental del secreto profesional y la custodia de datos.

Impacto en Ciberseguridad y Tecnologías de Información: Despliegue de controles de Acceso Basado en Roles (RBAC/ABAC), cifrado en tránsito (TLS 1.3) y cifrado en reposo (AES-256), Prevención de Pérdida de Datos (DLP) y Gestión de Acceso Privilegiado (PAM) para prevenir filtraciones internas o externas.

Principio 6: Seguridad de los Datos

Alcance Normativo: Exige garantizar la Confidencialidad, Integridad y Disponibilidad (Tríada CIA) mediante salvaguardias técnicas, administrativas y organizacionales razonables. Obliga a auditar y actualizar permanentemente estos controles y a gestionar y notificar incidentes de seguridad de datos.

Impacto en Ciberseguridad y Tecnologías de Información: Constituye el corazón operativo de la Ciberseguridad en el documento. Exige implementar un Sistema de Gestión de Seguridad de la Información (SGSI/ISO 27001), monitoreo SOC 24/7, pruebas de penetración periódicas, parches de vulnerabilidades y planes de respuesta a incidentes con notificación mandatoria a las autoridades y afectados.

Principio 7: Exactitud de los Datos

Alcance Normativo: Los datos deben mantenerse exactos, completos y actualizados para que no se altere la veracidad ni se generen decisiones erróneas perjudiciales para el titular.

Impacto en Ciberseguridad y Tecnologías de Información: Requiere controles de calidad de datos (data quality gates), validación de entradas digitales y sanitización de bases de datos para evitar discrepancias que afecten algoritmos de perfilamiento o decisiones automatizadas.

Principio 8: Derechos ARCOP (Acceso, Rectificación, Cancelación, Oposición y Portabilidad)

Alcance Normativo: Otorga a las personas mecanismos sencillos, ágiles y gratuitos para solicitar el acceso, corrección, eliminación, oposición al tratamiento y la transferencia de sus datos estructurados a otro proveedor en formato legible por máquina.

Impacto en Ciberseguridad y Tecnologías de Información: Demanda la construcción de herramientas de automatización de solicitudes ARCOP (Self-Service Privacy Portals), motores de exportación de datos interoperables (JSON/XML) y procesos eficientes de borrado seguro en todos los sistemas primarios y secundarios.

Principio 9: Datos Personales Sensibles

Alcance Normativo: Categoriza datos íntimos (salud, biometría, genética, orientación sexual, religión, ideología, geolocalización, menores) que exigen un nivel reforzado de protección legal y técnica debido al riesgo inminente de discriminación o daño grave.

Impacto en Ciberseguridad y Tecnologías de Información: Exige esquemas de cifrado homomórfico o avanzado, aislamiento de bases de datos sensibles (data vaulting), controles de acceso de autenticación multifactor estricta (MFA) y evaluaciones de impacto de ciberseguridad reforzadas.

Principio 10: Responsabilidad (Accountability), Privacidad desde el Diseño y por Defecto

Alcance Normativo: Obliga a los responsables a demostrar el cumplimiento de los principios mediante controles auditables. Introduce formalmente los marcos de Privacy by Design (PbD) y Privacy by Default (PbD).

Impacto en Ciberseguridad y Tecnologías de Información: Integración del ciclo de vida de desarrollo seguro (DevSecOps), modelos de datos con privacidad predeterminada (las opciones de menor exposición activadas por defecto) y designación obligatoria de un Oficial de Protección de Datos (DPO) o CISO enfocado en privacidad.

Principio 11: Flujo Transfronterizo de Datos y Cooperación Internacional

Alcance Normativo: Facilita la transferencia internacional de datos a jurisdicciones con niveles de protección adecuados, desaconsejando barreras proteccionistas como la localización forzada de datos, pero garantizando cláusulas contractuales tipo y responsabilidad compartida.

Impacto en Ciberseguridad y Tecnologías de Información: Evaluación de Riesgos de Transferencia Transfronteriza (TIA), auditoría de proveedores en la nube (AWS, Azure, GCP) y garantía de cumplimiento de estándares interoperables sin descuidar el cifrado de extremo a extremo en enlaces internacionales.

Principio 12: Excepciones Trazables

Alcance Normativo: Cualquier restricción a los principios debe estar expresamente prevista en la ley y responder exclusivamente a soberanía, seguridad nacional, orden público, combate a la criminalidad o salud pública.

Impacto en Ciberseguridad y Tecnologías de Información: Establecimiento de protocolos estrictos para la atención de requerimientos judiciales o policiales de interceptación y entrega de datos, evitando 'puertas traseras' (backdoors) indeseadas que debiliten la seguridad general del sistema.

Principio 13: Autoridades de Protección de Datos Independientes

Alcance Normativo: Los Estados deben crear órganos de supervisión independientes, dotados de autonomía técnica, operativa y financiera, con capacidad sancionadora y de cooperación transfronteriza.

Impacto en Ciberseguridad y Tecnologías de Información: Establece el interlocutor regulador frente al cual las organizaciones deben reportar vulneraciones de seguridad, consultar evaluaciones de impacto y gestionar inspecciones operativas de auditoría.

3. Matriz de Controles Técnicos de Ciberseguridad Requeridos

Para dar cumplimiento a los directrices de la OEA, la siguiente tabla mapea los dominios técnicos clave y las soluciones de ciberseguridad correspondientes:

Principio OEA	Dominio de Ciberseguridad	Controles Técnicos Obligatorios
Principio 5 y 6 (Confidencialidad y Seguridad)	Protección de Datos & Cryptography	Cifrado AES-256 en reposo, TLS 1.3 en tránsito, Gestión Centralizada de Claves (HSM/KMS), DLP.
Principio 2 y 10 (Consentimiento y PbD)	Gestión de Identidades & Accesos (IAM)	Autenticación Multifactor (MFA), Zero Trust Architecture, RBAC/ABAC, SSO, Gestión de Privilegios (PAM).
Principio 6 y 10 (Seguridad y Rendición de Cuentas)	Monitoreo & Respuesta a Incidentes	SIEM/SOAR con registros de auditoría inmutables, SOC 24/7, Plan de Notificación de Brechas (<72h).

Principio 3 y 4 (Minimización y Conservación)	Gobierno y Gestión del Ciclo de Vida	Scripts automatizados de purga/anonimización, herramientas de descubrimiento de PII, sanitización de discos.
Principio 11 (Flujo Transfronterizo)	Seguridad en la Nube & Terceros	Evaluaciones de riesgo a proveedores (TPRM), cifrado client-side en multicloud, Cláusulas Contractuales Tipo.

4. Recomendaciones de Implementación para C-Level y Equipos de Seguridad

- **Adopción del Modelo Zero Trust:** Asumir que las redes internas están comprometidas y verificar continuamente cada solicitud de acceso a datos personales.
- **Implementación del Ciclo DevSecOps y Privacidad por Diseño:** Integrar pruebas automatizadas de seguridad (SAST/DAST) y revisiones de impacto en la privacidad desde las etapas iniciales de desarrollo de software.
- **Plan de Respuesta ante Brechas de Datos (Data Breach Protocol):** Establecer procedimientos claros para aislar incidentes, mitigar daños y cumplir con la notificación oportuna a las Autoridades de Protección de Datos y a los afectados.
- **Gestión Rigurosa de Riesgos de Terceros (Vendor Risk Management):** Homologar los requisitos de ciberseguridad en la cadena de suministro y proveedores en la nube antes de autorizar transferencias de datos.

- **Auditoría y Cultura Operativa:** Ejecutar revisiones periódicas de cumplimiento, simulacros de incidentes de filtración y capacitaciones continuas contra la ingeniería social.