Protocolos de Ciberseguridad para un Gestor Documental en Aplicaciones Móviles y Desktop con Azure

La gestión segura de documentos en plataformas digitales exige la implementación de un marco integral de ciberseguridad que abarque desde el ciclo de desarrollo hasta la protección de la infraestructura en la nube. Un gestor documental moderno que opera en ambientes móviles y de escritorio debe garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y conformidad normativa. Este documento detalla los componentes esenciales que deben implementarse para lograrlo, utilizando Azure como plataforma de referencia.

1. DevSecOps: Seguridad desde el Ciclo de Vida del Desarrollo

Integración de Seguridad en CI/CD:

- Escaneo automático de dependencias y código fuente (SAST) en cada *push* al repositorio (Ej: SonarQube, GitHub Advanced Security, Snyk).
- Análisis de seguridad en tiempo de ejecución (DAST) mediante pruebas dinámicas automatizadas.
- Revisión de configuraciones en archivos `IaC` (Terraform, Bicep, ARM Templates) para prevenir despliegues inseguros.

Principios clave:

- *Shift-Left Security:* abordar la seguridad desde las etapas iniciales del desarrollo.
- *Automatización de pruebas de seguridad* en cada *build* y *release*.
- *Firmado de código* y *control de integridad* para asegurar binarios móviles (.apk, .ipa) y desktop.

2. Control de Acceso: Roles, Permisos y Autenticación

Modelo de Seguridad Basado en Roles (RBAC):

- Definición granular de roles: Admin, Editor, Lector, Auditor, entre otros.
- Control de acceso a documentos y carpetas con políticas de herencia.
- Auditoría completa de cambios, accesos y operaciones sobre documentos.

Autenticación y Autorización:

- Uso de OAuth 2.0 y OpenID Connect (OIDC) con Azure Active Directory B2C.
- Autenticación multifactor (MFA) obligatoria para usuarios administrativos o sensibles.
- Integración con proveedores de identidad federada (Google, Microsoft, SAML).
- Expiración y renovación de tokens con scopes específicos por operación (lectura, escritura, eliminación).

Just-in-Time Access (JIT):

- Acceso temporal a recursos críticos o confidenciales bajo aprobación explícita.
- Útil para auditores, soporte técnico o integradores temporales.

3. Cifrado y Protección de Datos

En tránsito (TLS):

- Uso obligatorio de TLS 1.2 o superior en todas las comunicaciones cliente-servidor y servidor-servidor.
- Certificados gestionados por Azure Key Vault con rotación automática.

En reposo:

- Cifrado de datos en Blob Storage con claves gestionadas por el cliente (CMK) en Azure Key Vault.
- Cifrado transparente de bases de datos (TDE) en PostgreSQL/Azure SQL.
- Control de acceso a claves criptográficas mediante RBAC y políticas de acceso temporal.

Protección contra fuga de datos (DLP):

- Políticas para detectar contenido sensible (PII, contraseñas, claves) en documentos.
- Restricciones de descarga o reenvío para ciertos roles.

4. Seguridad de Red y Aislamiento

Perímetro seguro con Azure:

- Aislamiento de redes por entorno (Dev, QA, Prod) mediante VNets separadas.
- Segmentación interna con NSGs (Network Security Groups) y reglas de acceso explícitas.
- Integración con Azure Private Link para evitar exposición pública de servicios internos.

Firewall y WAF:

- Uso de Azure Firewall para control centralizado del tráfico.
- Azure Application Gateway con Web Application Firewall activado (protección OWASP top 10).
- Reglas de geo-restricción y reputación IP para proteger aplicaciones públicas.

Protección contra DDoS:

- Activación de Azure DDoS Protection (standard) en recursos críticos como el frontend móvil y backend del gestor documental.

5. Gestión de Identidades y Sesiones

Sesiones seguras:

- Control de tiempo de vida de tokens JWT con renovaciones rotativas.
- Verificación de revocación de sesión en cada endpoint sensible.
- Identificadores únicos de sesión con trazabilidad completa.

Zero Trust Architecture:

- Validación contextual (identidad, dispositivo, ubicación, comportamiento).
- Reautenticación cuando se detecten anomalías (login sospechoso, cambios de IP frecuentes).

6. Supervisión, Auditoría y Respuesta a Incidentes

Logging estructurado y centralizado:

- Envío de logs a Azure Monitor, Log Analytics y Sentinel.
- Registros de accesos, modificaciones, intentos fallidos, uso de roles, etc.

Auditoría continua:

- Activación de diagnósticos para todos los recursos (Storage, SQL, Key Vault, App Services).
- Reportes periódicos de cumplimiento y actividad.

Respuesta a incidentes:

- Configuración de alertas en tiempo real ante comportamientos anómalos (Azure Defender).
- Playbooks automáticos con Logic Apps para bloquear IPs, revocar tokens, o activar modos de aislamiento.

7. Normativas y Cumplimiento

Normas recomendadas:

- ISO/IEC 27001: Sistema de Gestión de Seguridad de la Información (SGSI).
- GDPR/CCPA: Protección de datos personales y derecho al olvido.
- HIPAA (si se manejan datos médicos): Seguridad y privacidad en datos de salud.

- OWASP MASVS (Mobile Application Security Verification Standard): Para garantizar seguridad en apps móviles.
- OWASP SAMM: Modelo para madurez de seguridad en desarrollo.

Prácticas adicionales:

- Revisión manual de seguridad por cada *release* mayor.
- Pentesting semestral externo e interno (simulaciones de ataque controlado).
- Control de librerías de terceros con monitoreo de vulnerabilidades CVE.

8. Seguridad en Aplicaciones Móviles y de Escritorio

Móviles:

- Revisión de permisos de apps (cámara, almacenamiento, localización).
- Protección contra *reverse engineering* con ofuscación y detección de entornos *rooted/jailbroken*.
- Verificación de integridad de APK/IPA antes de ejecución.
- Uso de almacenamiento seguro para tokens (Secure Storage o Keystore).

Desktop (Windows/macOS/Linux):

- Firma digital del instalador y binarios.
- Restricciones de ejecución con AppLocker o políticas de endpoint.
- Sandboxing para aislamiento del componente que interactúa con documentos locales.