Manual de Buenas Prácticas de Seguridad para Super Apps Financieras

1. Introducción

Este manual establece las buenas prácticas de seguridad esenciales para el desarrollo, operación y mantenimiento de una super app financiera. Su propósito es asegurar la confidencialidad, integridad y disponibilidad de los datos sensibles gestionados por la plataforma.

2. Principios Fundamentales de Seguridad

• Minimización de privilegios: cada usuario y servicio debe operar con el nivel mínimo de acceso necesario.

• Seguridad por defecto: todas las configuraciones deben partir desde un estado seguro.

• Defensa en profundidad: aplicar múltiples capas de seguridad para reducir el impacto de fallos.

• Registro y monitoreo: toda actividad relevante debe quedar registrada para investigación y auditoría.

• Automatización: usar procesos automáticos para despliegues y controles de seguridad.

3. Gestión de Identidades y Accesos (IAM)

• Implementar autenticación multifactor (MFA) para administradores y usuarios de alto riesgo.

• Utilizar protocolos estándar: OAuth 2.0, OpenID Connect, SAML.

• Adoptar roles (RBAC) o políticas basadas en atributos (ABAC) para accesos complejos.

• Limitar intentos fallidos de inicio de sesión y habilitar alertas.

• Revisar permisos cada 90 días.

4. Seguridad de Contraseñas

• Longitud mínima de 12 caracteres.

• Fomentar el uso de passphrases.

• Almacenar contraseñas usando hashing seguro: Argon2, bcrypt o scrypt.

• Prohibido almacenar contraseñas en texto plano.

• Forzar MFA en lugar de exigir cambios periódicos innecesarios.

5. Seguridad de Aplicaciones

• Validar y sanitizar toda entrada del usuario.

• Usar HTTPS obligatorio (TLS 1.2+).

• Implementar Content Security Policy (CSP).

• Reducir superficie de ataque deshabilitando endpoints o módulos innecesarios.

• Revisar dependencias con herramientas como Dependabot o Snyk.

6. Gestión de APIs

• Utilizar gateways con autenticación fuerte.

• Firmar solicitudes sensibles.

• Limitar tráfico mediante rate limiting y throttling.

• Deshabilitar CORS abiertos.

• Registrar accesos a cada endpoint crítico.

7. Cifrado de Datos en Tránsito y en Reposo

• TLS 1.2+ con suites modernas.

• Cifrar datos sensibles en bases de datos (AES-256-GCM recomendado).

• Rotar llaves criptográficas cada 6–12 meses.

• Administrar secretos mediante Vault, AWS Secrets Manager o GCP Secret Manager.

8. Gestión de Infraestructura Segura

• Aplicar parches de seguridad periódicos.

• Segmentar redes internas y limitar acceso mediante firewall.

• Usar contenedores o máquinas virtuales aisladas.

• Habilitar logs: sistema, autenticación, API y eventos críticos.

• Configurar backups automáticos con pruebas de restauración.

9. Seguridad en CI/CD

• Integrar análisis estático (SAST) y análisis dinámico (DAST).

• Escanear dependencias.

• Firmar imágenes de contenedores.

• Aplicar reglas para evitar despliegues no autorizados.

10. Gestión de Incidentes

• Definir roles: líder, comunicaciones, analista.

• Establecer un flujo claro: detección → contención → erradicación → recuperación → post-mortem.

• Mantener checklist y documentación disponible.

• Realizar simulacros de incidentes.

11. Concienciación del Equipo

• Entrenamiento trimestral en phishing.

• Políticas claras de uso de dispositivos y contraseñas.

• Campañas con ejemplos reales.

• Reporte obligatorio de anomalías.

12. Conclusión

La seguridad debe integrarse desde el inicio del desarrollo de una super app. El cumplimiento de estas buenas prácticas reduce significativamente el riesgo de brechas y fortalece la confianza del usuario.