Pay

CONTÁCTAME

ESCANÉAME

Checklist Simple PCI V4.0.

Identidad y accesos

- Activa MFA (doble verificación) para todos los usuarios con acceso administrativo y a datos de tarjeta.
- Revisa usuarios y accesos al menos cada 90 días, elimina cuentas que no se usan.
- Usa contraseñas fuertes y gestiona caducidad y bloqueo por intentos fallidos.
- Separa funciones: quien desarrolla no despliega en producción sin revisión.

Inventario y alcance (scoping)

- Lista todos los sistemas, apps, redes y servicios que tocan datos de tarjeta o pueden afectarlos.
- Dibuja un diagrama de flujo: dónde entran, por dónde viajan y dónde se almacenan los datos.
- Identifica qué está "en alcance" y aísla lo que no necesita estarlo (segmentación de red).

Protección de datos de tarjeta

- No almacenes PAN si no es necesario, si debes, enmascara y cifra.
- Usa tokenización: guarda los datos reales en un "cofre" seguro del proveedor y usa tokens en tu app.
- Cifra datos en tránsito (TLS 1.2+ o superior) y en reposo.
- Controla y elimina datos temporales o logs con PAN.

Seguridad de aplicaciones y scripts

- Controla los scripts del checkout: inventario, integridad y alertas ante cambios.
- Limita scripts a lo necesario y con motivos documentados.
- Integra seguridad en el ciclo de vida: revisión de diseño, gestión de secretos, pruebas estáticas/dinámicas.
- Establece un "check de seguridad" obligatorio antes de publicar.

Gestión de vulnerabilidades y parches

- Mantén inventario de software, librerías y componentes.
- Evalúa vulnerabilidades al menos mensualmente y tras cambios importantes.
- Aplica parches con fechas objetivo según criticidad (críticos: lo antes posible).
- Usa anti-malware/EDR donde aplique y monitorea.

Monitoreo y registros

- Activa logs en sistemas clave: accesos, cambios, intentos fallidos, actividades de admin.
- Protege y centraliza logs, conserva según política (p. ej., mínimo 1 año, 3 meses en línea).
- Implementa alertas para eventos críticos y revisa diariamente lo relevante.

Controles de red

- Firewalls en perímetros y entre zonas, solo puertos/servicios necesarios.
- Desactiva servicios inseguros, usa configuraciones seguras (hardening).
- Segmenta el entorno de datos de tarjeta del resto de la red.

Pruebas y verificación

- Haz pruebas más frecuentes donde hay más cambios o riesgo.
- Escaneos ASV externos trimestrales y tras cambios significativos.
- Pruebas de penetración internas y externas al menos anuales y tras cambios mayores.
- Verificación de cambios: checklist, aprobación y rollback.

Gestión de proveedores

- Evalúa a terceros que procesan o pueden afectar datos de tarjeta.
- Obtén su estatus PCI (AOC, SAQ) o evidencia equivalente.
- Define responsabilidades de seguridad en contratos.

Políticas y documentación

- Documenta políticas de seguridad, gestión de accesos, clasificación de datos y retención.
- Si adaptas un requisito (Customized Approach), explica el objetivo, tu método y guarda pruebas.
- Mantén procedimientos simples: qué se hace, quién lo hace y cómo se prueba.

Respuesta a incidentes

- Plan escrito para incidentes (contactos, pasos, contención, comunicación).
- Prueba el plan al menos anual (simulacro).
- Define cómo notificar a bancos, marcas y clientes si aplica.

Concienciación y formación

- Capacita al personal al ingresar y al menos anual (phishing, manejo de datos, políticas).
- Entrenamiento específico para admin y desarrolladores.

Físico y dispositivos

- Control de acceso físico a áreas y equipos con datos de tarjeta.
- Protección de POS y terminales, inspecciones contra manipulación.
- Gestión de medios (copias, discos) con cifrado y destrucción segura.

Criptografía y claves

- Usa algoritmos aprobados, gestiona ciclo de vida de claves (creación, rotación, almacenamiento).
- Separación de funciones para manejo de claves.

Gobernanza y mejora continua

- Asigna responsables claros de cada control.
- Revisión ejecutiva periódica del programa PCI y del plan de riesgos.
- Métricas: tiempos de parcheo, hallazgos abiertos, cumplimiento de MFA, resultados de escaneos.

Checklist rápido de arranque (esta semana)

- Activa MFA para todos los administradores.
- Dibuja el mapa de datos y el alcance.
- Vigila y limita los scripts del checkout.
- Define un plan de pruebas por riesgo y un calendario.

1️⃣ **Grupo de ayuda gratis PayOk:** Fintech, Adquirencia, Pagos Electrónicos, Gestión Riesgos, Medios de Pago, PBCFT y Compliance.

2️⃣ **Newsletter Radar Financiero Adquirencia PayOk**

3️⃣ **Sígueme con un click en LinkedIn**

4️⃣ **Tarjeta digital de contacto**