Seguridad de Datos y Encriptación en Entidades Financieras

Protección estructural de activos e información personal

La digitalización total acarrea la responsabilidad legal e imperativa de salvaguardar terabytes de datos sumamente sensibles (imágenes de DNI, reportes de historial crediticio y datos bancarios) frente a vulnerabilidades, inyecciones de código y ciberataques maliciosos.

1. Cifrado en Reposo y en Tránsito (AES-256 / SSL)

Toda la información viaja desde la computadora o celular del promotor hacia los servidores de elCobrador bajo canales seguros mediante cifrado HTTPS/TLS (Transport Layer Security). Esto mitiga ataques tipo "Man in the Middle". Adicionalmente, información sensible como contraseñas u OTPs (Tokens) jamás se almacenan en texto plano en la base de datos, sino que sufren algoritmos de Hashing irreversibles (como Bcrypt/Argon2) protegiendo a los usuarios incluso en escenarios extremos de contingencia.

2. Respaldo Deslocalizado (Geo-Backups) y Restauración

Las estrategias de recuperación ante desastres (Disaster Recovery) exigen que los respaldos no existan únicamente en el centro de datos principal. La arquitectura de elCobrador realiza respaldos automatizados de la base de datos (Dumps) con frecuencia diaria e inter-diaria. Estas copias se envían cifradas hacia infraestructuras en zonas geográficas separadas. En caso de una falla catastrófica del servidor primario, se reconstruye el último snapshot para retomar la operatividad comercial sin pérdida irreversible de flujos de fondos.

3. Cumplimiento de la Ley de Protección de Datos (Ley 25.326)

La manipulación de bases de datos de perfiles crediticios está fuertemente legislada. El sistema incorpora mecanismos de anonimización parcial para el manejo cotidiano y protege los accesos mediante auditorías de roles estrictas, garantizando que un operador que se desvincule de la empresa no pueda "exportar" o llevarse la cartera de clientes. Las vistas y descargas masivas están deshabilitadas o registradas perimetralmente, y la entidad mantiene plena custodia digital sobre sus bases para cumplir con las exigencias del Hábeas Data.

Conclusión: Abordar el crédito B2B/B2C requiere cimientos inexpugnables. La política de seguridad informática profunda es la garantía invisible para el crecimiento sostenido de toda organización crediticia.