REGLAMENTO INTERNO DE POLÍTICAS DE SEGURIDAD

Materia: Seguridad en Bases de Datos Alumnos:

Jesús Eduardo Rodríguez García - 2058524

Aldo De Jesús Luna Maldonado - 2087570

Christian Domínguez Villanueva - 2118864

Israel Sánchez Hilario - 2094993

Darien Alexander Ñañez Torres - 2119054

Abril Azeneth Alcocer Piñero - 2048108

BANCO CAPIBARAS_MX

Versión: 1.1 (Adaptación Sector Financiero)

Fecha de Emisión: 13 de noviembre de 2025

Departamento Responsable: Dirección de Tecnología e Información (DTI) y Oficial de Seguridad de la Información (CISO)

Contenido

INTRODUCCIÓN Y ALCANCE

Este Reglamento de Políticas de Seguridad establece las directrices y normas obligatorias para la protección de los activos de información, sistemas y recursos tecnológicos del **Banco Capibaras_MX**. Su cumplimiento es crucial para mantener la confianza del cliente y cumplir con las regulaciones bancarias mexicanas.

El objetivo principal es garantizar la **Confidencialidad, Integridad y Disponibilidad (CIA)** de todos los datos sensibles (incluyendo datos personales y transaccionales), mitigando riesgos de seguridad, fugas de información, ataques cibernéticos y fallos operativos, especialmente aquellos derivados de la manipulación de la base de datos.

1. POLÍTICAS DE ACCESO Y AUTORIZACIÓN

El acceso a los recursos de la Organización se basa en el principio del **Mínimo Privilegio (Principio de Privilegios Mínimos)**, esencial para el entorno bancario, asegurando que los usuarios y las aplicaciones solo tengan los permisos estrictamente necesarios para cumplir con sus funciones.

1.1. Autenticación de Usuarios

Requisito	Descripción
Identificación Única	Cada persona (empleado o administrador de sistema) debe tener una cuenta personal e intransferible. Está prohibido compartir credenciales.
Autenticación Multifactor (MFA)	El MFA es **obligatorio** para el acceso a todos los sistemas críticos: servidores, bases de datos (DB), aplicaciones de banca digital y acceso remoto/VPN.
Bloqueo Automático	Las cuentas se bloquearán automáticamente tras 5 intentos fallidos de inicio de sesión.

1.2. Gestión de Permisos sobre la Información y la Base de Datos

Los permisos se categorizan según el Nivel de Sensibilidad de la Información. Es obligatorio aplicar la separación de funciones.

Nivel de Permiso	Definición (Entorno DB)	Requisitos y Contramedidas
Acceso a Aplicaciones (rolClienteApp)	Permite a la aplicación interactuar con la DB a través de procedimientos almacenados.	La aplicación debe conectarse usando un usuario con permisos limitados a EXECUTE sobre procedimientos almacenados y **vistas seguras (vw_ClientePublico)**. **Prohibido** SELECT * directo en tablas.
Lectura (Read)	Visualizar información no sensible o datos de reportes.	Se otorga a usuarios con necesidad de conocimiento. Los datos sensibles (ej. PAN_Enc, RFC, CURP_Enc) solo pueden ser consultados a través de vistas que los excluyan o que requieran desencriptación con privilegios especiales.
Modificación (Modify)	Alterar, editar o actualizar registros transaccionales (ej. Transaccion, Cuenta).	Se otorga solo a usuarios operativos que intervienen directamente. **Todas las modificaciones deben ser realizadas a través de procedimientos almacenados parametrizados** para prevenir inyección SQL.
Eliminación (Delete)	Borrar registros.	**Estrictamente restringido** a la DTI y CISO. Cualquier eliminación requiere aprobación formal y un registro de auditoría. Se prefiere la desactivación lógica (bool Activa) en lugar de la eliminación física.
Acceso Privilegiado (DBA)	Permite administrar la DB (esquemas, usuarios, cifrado, respaldos).	Requiere cuentas únicas, MFA, y debe ser utilizado solo para tareas de administración. Todas las acciones son monitoreadas y auditadas en tiempo real.

1.3. Revisión de Acceso

Se realizará una revisión trimestral de los permisos de acceso y de los roles de aplicación (ej. rolClienteApp) por parte del CISO y la DTI para asegurar la vigencia del Principio de Mínimo Privilegio.

2. GESTIÓN DE RESPALDOS Y RECUPERACIÓN DE DESASTRES

La Organización implementará una estrategia de respaldo para garantizar la disponibilidad y la integridad de los datos financieros.

2.1. Política de Respaldo (Backup)

1. **Frecuencia:** Los datos críticos (Bases de Datos Transaccionales) se respaldarán diariamente (completo) y cada hora (diferencial/log de transacciones). Los sistemas operativos y aplicaciones se respaldarán semanalmente.
2. **Método 3-2-1:** Se requiere mantener un mínimo de **3 copias** de los datos, en **2 tipos diferentes** de medios (ej. disco y cinta), con **1 copia** almacenada fuera de las instalaciones (*off-site*) para protección contra desastres geográficos.
3. **Cifrado:** Todos los respaldos (incluyendo los archivos .mdf y .ldf si se utiliza TDE) almacenados fuera de línea (offline) o fuera de las instalaciones (off-site) deben estar cifrados con claves de cifrado robustas y gestionadas de forma segura.
4. **Verificación:** Se debe realizar una prueba de restauración completa de la base de datos al menos una vez al mes para verificar la integridad y la funcionalidad de los datos respaldados.

2.2. Plan de Recuperación de Desastres (DRP)

1. **Objetivo:** Asegurar la continuidad operativa en caso de un desastre mayor.
2. **RTO y RPO:** El **Tiempo Objetivo de Recuperación (RTO)** para sistemas críticos (banca digital, transacciones) no debe exceder las 4 horas. La **Pérdida de Datos Aceptable (RPO)** no debe exceder 1 hora de transacciones.
3. **Procedimiento:** El DRP debe ser probado y simulado al menos una vez al año, incluyendo la restauración en una infraestructura alternativa (sitio de recuperación secundario).

3. POLÍTICAS DE CIFRADO Y GESTIÓN DE CONTRASEÑAS

Se establecen normas estrictas para proteger las credenciales y los datos sensibles (PAN, CLABE, CURP, RFC, etc.) en tránsito y en reposo.

3.1. Almacenamiento y Hashing de Contraseñas

1. **Hashing:** Las contraseñas de los usuarios (UsuarioSistema.PwdHash) y clientes (Usuario.PasswordHash) en bases de datos **nunca** deben almacenarse en texto plano. Deben ser almacenadas utilizando un algoritmo de *hashing* fuerte y unidireccional (ej. SHA-256 o superior) con una sal (*salt*) única (UsuarioSistema.Salt).
2. **Gestión Centralizada:** Las contraseñas para cuentas privilegiadas (administradores de DB) deben ser almacenadas en un Gestor de Contraseñas Empresarial centralizado y auditado.

3.2. Cifrado de Datos Sensibles (En Reposo)

1. **Cifrado de Columna (Column Encryption):** La información altamente sensible (ej. CURP_Enc, RFC_Enc, PAN_Enc) debe ser cifrada a nivel de columna dentro de la base de datos utilizando llaves simétricas (ej. AES_256), protegidas por certificados y una llave maestra.
2. **Cifrado de Base de Datos (TDE):** Se recomienda la implementación de Transparent Data Encryption (TDE) para cifrar toda la base de datos en reposo, protegiendo los archivos físicos y los respaldos contra el acceso no autorizado a nivel de sistema operativo.
3. **Cifrado de Disco:** Todos los dispositivos que contengan información sensible (portátiles, servidores) deben utilizar cifrado de disco completo (ej. BitLocker, FileVault).

3.3. Cifrado de Datos en Tránsito

Toda la comunicación de red que transporte información financiera o credenciales debe utilizar protocolos seguros (ej. TLS 1.2 o superior, SSH). El acceso a la banca digital se debe realizar exclusivamente bajo HTTPS.

3.4. Requisitos para Contraseñas de Usuario

1. **Longitud Mínima:** 12 caracteres.
2. **Complejidad:** Debe incluir caracteres de al menos 3 de las 4 categorías: mayúsculas, minúsculas, números y símbolos.
3. **Vigencia:** Las contraseñas de usuarios externos deben cambiarse cada 90 días; las de administradores y cuentas privilegiadas, cada 60 días.
4. **Historial:** Prohibición del uso de las últimas 5 contraseñas.

4. PROCEDIMIENTO DE AUDITORÍA Y MONITOREO

El monitoreo continuo es fundamental para detectar actividades anómalas, especialmente la **Escalada de Privilegios** y la manipulación de transacciones.

4.1. Monitoreo de Eventos (Logging)

1. **Registro Obligatorio:** Se deben registrar todos los eventos de seguridad en los sistemas críticos, incluyendo:
    - Intentos fallidos de inicio de sesión (DB, App, OS).
    - **Cambios de permisos y privilegios (DB)**.
    - **Ejecución de procedimientos almacenados sensibles**.
    - Acceso a archivos y bases de datos sensibles.
    - Modificación o eliminación de cualquier registro financiero.
2. **Retención:** Los registros de auditoría (*logs*) se deben almacenar de forma segura (a prueba de manipulaciones) con un periodo de retención mínimo de 2 años, cumpliendo con la normativa financiera.

4.2. Auditoría Periódica

1. **Auditoría de Vulnerabilidades:** Escaneo de vulnerabilidades en la infraestructura de red al menos cada 6 meses.
2. **Pruebas de Penetración (*Penetration Testing*):** Un tercero independiente realizará pruebas de penetración y pruebas específicas de **inyección SQL** al menos una vez al año.
3. **Revisión de Logs:** El CISO revisará los *logs* y las alertas del Sistema de Gestión de Información y Eventos de Seguridad (SIEM) diariamente en busca de patrones de comportamiento sospechoso o accesos con privilegios excesivos.

5. PLAN DE RESPUESTA A INCIDENTES (PRI)

Este plan detalla los pasos a seguir en caso de que se detecte un incidente de seguridad (ej. fuga de datos, ataque de *ransomware*, inyección SQL exitosa, acceso no autorizado).

5.1. Activación y Estructura del Equipo

1. **Equipo de Respuesta a Incidentes (ERI):** Compuesto por miembros de DTI (con enfoque en DB y Red), Asesoría Legal, Dirección Ejecutiva y el Oficial de Seguridad de la Información (CISO).
2. **Contacto:** Todo el personal debe reportar inmediatamente cualquier actividad sospechosa (ej. una transacción anómala, un cambio de saldo injustificado) al ERI.

5.2. Fases de Respuesta al Incidente

El ERI seguirá el siguiente ciclo de respuesta, con especial atención a la integridad de los datos financieros:

Fase	Descripción	Acciones Clave
1. Preparación	Asegurar que los sistemas y el personal estén listos.	Documentación, entrenamiento para ataques específicos (SQLi, Ransomware), herramientas de respuesta forense listas.
2. Detección y Análisis	Determinar el alcance y la causa raíz del incidente.	Monitorear logs transaccionales, aislar sistemas DB afectados, identificar la vulnerabilidad explotada (ej. sin parametrización).
3. Contención	Limitar el daño.	**Aislamiento:** Desconectar los sistemas afectados de la red. Si la DB fue comprometida, aislar las tablas o vistas afectadas. Revocar temporalmente los permisos del usuario o rol comprometido.
4. Erradicación	Eliminar la causa raíz.	Aplicar el *patch* o la corrección de código (ej. implementar la parametrización de consultas) que permitió el ataque. Eliminar el *malware*, cambiar contraseñas comprometidas.
5. Recuperación	Restaurar los sistemas a su estado normal y verificar la integridad de los saldos.	Restaurar datos desde respaldos verificados. Se requiere una doble validación de los saldos y transacciones restauradas. Monitorear el sistema restaurado.

6. Lecciones Aprendidas	Documentar el incidente y las acciones correctivas.	Actualizar políticas, realizar capacitaciones y fortalecer las defensas (ej. crear más vistas seguras).

5.3. Comunicación y Notificación (Fuga o Ataque)

1. **Interna:** La Dirección Ejecutiva y el CISO informarán al personal relevante solo con información aprobada.
2. **Externa (Legal y Regulatoria):** El equipo legal determinará la obligación de notificación a la Comisión Nacional Bancaria y de Valores (CNBV) y a los clientes afectados (si se vieron comprometidos datos personales o financieros) en un plazo no mayor a 72 horas desde el descubrimiento.

ANEXO: CÓDIGO DE CONDUCTA DEL USUARIO

Todo usuario se compromete a:

1. Proteger su contraseña, utilizar MFA y no revelarla.
2. Bloquear su estación de trabajo (Win + L o equivalente) al dejarla desatendida.
3. No instalar software no autorizado ni conectar dispositivos USB de origen desconocido.
4. Mantener el software (navegadores, sistema operativo) actualizado.
5. Ser cauteloso con correos electrónicos y enlaces sospechosos (Phishing), especialmente aquellos que parezcan provenir de la DTI o áreas financieras.

Sanciones: El incumplimiento de estas políticas puede dar lugar a medidas disciplinarias, que van desde una advertencia formal hasta la terminación del empleo y/o acciones legales, incluyendo la responsabilidad por daños y perjuicios al patrimonio del banco o sus clientes.