Certisysnet ATM Risk & Security Standard (CARSS)

Versión 1.0 – Marzo 2025

Estándar de Riesgo y Seguridad para Cajeros Automáticos

Autor:
Certisysnet Solutions – División de Seguridad ATM

Descripción:
El estándar CARSS establece controles técnicos, físicos y operativos para la protección integral de cajeros automáticos (ATMs) frente a amenazas cibernéticas, ataques físicos, fraudes financieros y violaciones normativas.
Su contenido ha sido desarrollado en colaboración con expertos en ciberseguridad, cumplimiento normativo y prevención de delitos financieros en entornos críticos.

Propósito:
Fortalecer las prácticas de seguridad y auditoría en la operación de cajeros automáticos, alineándose con marcos globales como PCI DSS, ISO/IEC 27001 y el NIST Cybersecurity Framework.

Certisysnet ATM Risk & Security Standard (CARSS) v1.0

Fecha de emisión: Marzo 2025

Fecha de emisión: Marzo 2025

Control 1: Compromiso del PIN y Seguridad del Teclado (PIN Compromise & Keypad Security)

1.1 Fundamentos Teóricos

1.1.1 Métodos de Obtención del PIN

Shoulder Surfing

Observación directa del usuario al ingresar el PIN.

Factores que facilitan el ataque

- Ausencia de PIN shield.
- Falta de conciencia del usuario sobre cubrir el teclado.
- Cámaras de vigilancia mal posicionadas.
- Inexistencia de señalización de privacidad o advertencia.

Impacto potencial

- Compromiso directo del PIN, especialmente cuando se combina con skimming.
- Acceso no autorizado a cuentas y retiro fraudulento de efectivo.

Controles recomendados

- Instalación obligatoria de blindaje físico (PIN shield).
- Campañas visuales de concientización para cubrir el teclado.
- Ubicación estratégica de cámaras de seguridad.
- Auditorías periódicas para detectar dispositivos ocultos.

Keypad Overlay

Dispositivos falsos colocados sobre el teclado real.

Factores que facilitan el ataque

- Teclados sin sensores de manipulación.
- Falta de inspecciones físicas diarias.
- Desconocimiento técnico del personal de mantenimiento.

Impacto potencial

- Registro y robo del PIN ingresado por el usuario.
- Riesgo aumentado si se combina con skimming.
- Difícil detección sin revisión física directa.

Controles recomendados

- Inspecciones periódicas físicas del teclado.
- Verificación con luz UV o sensores RF.
- Alerta interna por manipulación mecánica del teclado.

1.1.2 Protección del PIN

Cifrado en hardware
Protección de los datos ingresados en el teclado mediante módulos criptográficos certificados (PCI PTS, 3DES, AES).

Factores que facilitan el ataque

- Uso de teclados no certificados.
- Sistemas sin cifrado de extremo a extremo (E2EE).

Impacto potencial

- Intercepción del PIN en texto claro dentro del ATM o en tránsito.

Controles recomendados

- Uso de teclados certificados con cifrado activo.
- Validación de integridad criptográfica.

PIN Shielding
Dispositivos físicos que bloquean la vista del teclado.

Factores que facilitan el ataque

- ATM sin protección visual.
- Blindajes rotos, ausentes o mal instalados.

Impacto potencial

- Vulnerabilidad a shoulder surfing.

Controles recomendados

- Instalación obligatoria de blindaje.
- Revisión física semanal del estado del escudo.

Tiempo de expiración del PIN
Restricción del tiempo de validez del PIN ingresado.

Factores que facilitan el ataque

- PIN almacenado temporalmente sin límite de sesión.
- Falta de limpieza de memoria o timeout.

Impacto potencial

- Reutilización del PIN capturado por sniffers o ataques MitM.

Controles recomendados

- Configurar tiempo límite de ingreso de PIN.
- Reinicio del proceso tras superar el umbral de tiempo.

1.2 Inspección y Auditoría

1.2.1 Revisión de CCTV y Seguridad Perimetral

Inspección de ángulos de visión de las cámaras de seguridad

- Verificación de cobertura completa del área del teclado.

Identificación de puntos ciegos o zonas vulnerables

- Mapeo visual de zonas sin cobertura donde un atacante podría operar.

Validación de almacenamiento y acceso seguro a grabaciones

- Asegurar que los videos estén protegidos y solo accesibles a personal autorizado.

1.2.2 Inspección del Teclado PIN

Identificación de superposiciones falsas en el teclado

- Inspección visual táctil con protocolo definido.

Uso de luz ultravioleta para detectar adhesivos ocultos

- Búsqueda de sustancias fluorescentes no visibles a simple vista.

Pruebas con detectores de radiofrecuencia para identificar dispositivos de transmisión

- Uso de escáners de señales o medidores de espectro.

Inspección térmica con cámaras IR para detectar trazos de calor en el teclado

- Detectar secuencias presionadas segundos después del uso del ATM.

1.3 Pruebas de Ataque

1.3.1 Sniffing de PIN

Captura de tráfico de red con herramientas como Wireshark

- Escuchar el tráfico ATM-host para interceptar PIN no cifrados.

Revisión de logs internos del ATM en busca de almacenamiento accidental de PINs

- Validación de memoria temporal y registros del sistema.

Uso de osciloscopio en la línea de datos entre el teclado y la CPU del ATM

- Análisis de señales eléctricas para reconstruir secuencias de teclas.

1.3.2 Ataques de Fuerza Bruta

Simulación de múltiples intentos de PIN incorrecto

- Evaluar protecciones contra repetición sistemática de intentos.

Evaluación del umbral de bloqueo tras intentos fallidos

- Comprobación de límites definidos por configuración bancaria.

Ataques de relay utilizando hardware como Proxmark3 para interceptar teclas presionadas

- Captura remota de las entradas físicas del teclado.

1.4 Medidas de Mitigación

Instalación de protectores físicos sobre el teclado PIN

- Reforzar protección visual del usuario.

Implementación de teclados con cifrado interno de extremo a extremo (E2EE)

- Evitar manipulación del PIN dentro del sistema ATM.

Monitoreo en tiempo real de intentos de PIN incorrecto con alertas automáticas

- Integrar sistemas de monitoreo para generar alarmas ante patrones de ataque.

Control 2: Robo de Tarjetas y Skimming (Card Theft & Skimming)

2.1 Fundamentos Teóricos

2.1.1 Tipos de ataques

Skimmers físicos (Bluetooth, GSM, USB)
Dispositivos adheridos a la ranura del lector de tarjetas para capturar la información de la banda magnética. Los skimmers modernos pueden transmitir datos en tiempo real mediante tecnologías inalámbricas como Bluetooth, GSM o USB.

Factores que facilitan el ataque

- Falta de inspecciones periódicas del lector de tarjetas.
- Lector de tarjetas sin mecanismos de detección de manipulación.
- Usuarios que no verifican la ranura antes de insertar su tarjeta.

Impacto potencial

- Robo de datos de la banda magnética para clonar tarjetas.
- Uso de datos robados para transacciones fraudulentas.

Controles recomendados

- Implementación de detectores activos de skimming.
- Uso de lectores con protección contra dispositivos no autorizados.
- Educación a los usuarios sobre inspección visual de ranuras.

Shimmers (Dispositivos insertados en la ranura de tarjetas con chip **EMV**)
Los shimmers son pequeños circuitos insertados en la ranura del lector de tarjetas con chip EMV, capturando datos de la transacción.

Factores que facilitan el ataque

- Falta de revisión interna del lector de tarjetas.
- Dispositivos de detección de skimming inactivos o desactualizados.
- Uso de tarjetas con chips vulnerables a ataques de relay.

Impacto potencial

- Intercepción de la comunicación entre la tarjeta y el lector.
- Extracción de datos para replicar transacciones fraudulentas.

Controles recomendados

- Uso de tarjetas con protecciones contra relay.
- Instalación de sensores de manipulación en la ranura.
- Implementación de validaciones adicionales en las transacciones.

Ataques de relay en tarjetas NFC (Transacciones sin contacto interceptadas)
Los atacantes utilizan dispositivos intermedios para capturar y retransmitir la comunicación de una tarjeta NFC a un terminal de pago remoto.

Factores que facilitan el ataque

- Uso de tarjetas NFC sin mecanismos de protección avanzada.
- Falta de autenticación secundaria en transacciones sin contacto.
- Presencia de dispositivos no autorizados en el entorno del ATM.

Impacto potencial

- Uso fraudulento de tarjetas sin contacto.
- Transferencias no autorizadas de fondos en tiempo real.

Controles recomendados

- Implementación de protección contra relay en tarjetas y terminales.
- Configuración de límites estrictos en pagos sin autenticación.
- Uso de monitores de frecuencia para detectar dispositivos relay.

2.2 Inspección y Auditoría

2.2.1 Inspección del Lector de Tarjetas

Revisión física del lector con inspección manual y cámaras endoscópicas

- Evaluación detallada del lector en busca de modificaciones externas o internas.
- Uso de herramientas endoscópicas para inspeccionar el interior del lector.

Uso de detectores de radiofrecuencia para identificar skimmers activos

- Escaneo periódico del ATM para detectar dispositivos de transmisión ocultos.
- Análisis de anomalias en la señal electromagnética del lector.

Inspección con herramientas de rayos X para detectar hardware oculto

- Revisión avanzada del hardware interno del lector.
- Identificación de componentes anómalos adheridos a los circuitos.

2.3 Pruebas de Ataque

2.3.1 Captura de Datos de Tarjetas

Uso de lectores MSR605X para clonar tarjetas insertadas

- Simulación de ataque con dispositivos de lectura de banda magnética.
- Evaluación de protecciones implementadas contra clonado de tarjetas.

Ataques de relay con Proxmark3 para interceptar datos de tarjetas NFC

- Uso de hardware especializado para interceptar comunicaciones NFC.
- Validación de vulnerabilidades en la autenticación de pagos sin contacto.

Simulación de fraude con tarjetas clonadas en el ATM

- Prueba de transacciones fraudulentas utilizando tarjetas duplicadas.
- Análisis de detección y tiempo de respuesta de seguridad bancaria.

2.4 Medidas de Mitigación

Implementación de detección activa de skimming con sensores de campo eléctrico

- Integración de sensores para identificar cambios en el campo eléctrico del lector.
- Activación de alertas ante modificaciones sospechosas en la estructura del ATM.

Cifrado de extremo a extremo en los datos de la tarjeta

- Uso de cifrado en tiempo real para evitar intercepción de datos en tránsito.
- Implementación de tecnologías EMV y TLS para proteger la información.

Instalación de sensores en la ranura de tarjetas para detectar alteraciones

- Uso de mecanismos de detección activa para alertar sobre inserción de dispositivos ilegales.
- Implementación de barreras físicas y tecnológicas en la ranura del lector.

Control 3: Trampa de Efectivo y Fraude de Reversión de Transacciones (Cash Trapping & Reversal Fraud)

3.1 Fundamentos Teóricos

3.1.1 Métodos de ataque

Trampas mecánicas en la ranura del dispensador (bloqueo de billetes)
Los atacantes instalan dispositivos físicos en la salida del dispensador de billetes para bloquear el retiro del dinero por parte del usuario. Posteriormente, cuando el cliente se retira, el atacante recupera los billetes atrapados.

Factores que facilitan el ataque

- Ausencia de sensores en la ranura del dispensador.
- Falta de revisión diaria del hardware externo.
- Diseño del ATM sin mecanismos de bloqueo interno de billetes.

Impacto potencial

- Pérdida de efectivo para el usuario.
- Riesgo reputacional para la entidad financiera.

Controles recomendados

- Revisión física frecuente de la ranura de salida.
- Uso de cámaras para monitorear actividad en el dispensador.
- Instalación de compuertas motorizadas con cierre automático.

Manipulación de sensores para registrar una transacción fallida
El atacante interfiere con los sensores que validan la entrega de billetes, provocando que el ATM marque la transacción como fallida a pesar de haber entregado el efectivo.

Factores que facilitan el ataque

- Acceso físico al área de los sensores.
- Falta de cifrado o autenticación entre sensores y CPU.
- Diseños obsoletos sin redundancia de sensores.

Impacto potencial

- Doble acreditación del monto: efectivo entregado y saldo no debitado.
- Generación de falsos reportes de fallo para extraer más dinero.

Controles recomendados

- Protección física y lógica de los sensores.
- Implementación de validación cruzada entre sensores y cámaras.
- Monitoreo de inconsistencias entre registro de billetes y registros de software.

Simulación de cortes de energía para engañar al ATM
El atacante provoca una interrupción momentánea del suministro eléctrico o realiza reinicios forzados del equipo durante una transacción, generando condiciones anómalas para forzar una reversión del dinero.

Factores que facilitan el ataque

- Falta de respaldo energético confiable (UPS).
- ATM sin sistema de autoauditoría de estado durante reinicio.
- Ausencia de logs forenses en el firmware del dispensador.

Impacto potencial

- Generación de transacciones reversadas de forma no legítima.
- Oportunidad para retirar billetes en el momento del reinicio.

Controles recomendados

- Implementación de sistemas de respaldo energético ininterrumpido.
- Validación de estado de transacción tras reinicio forzado.
- Revisión periódica de logs del sistema ante reinicios inesperados.

3.2 Inspección y Auditoría

3.2.1 Inspección del Dispensador de Efectivo

Revisión física con linterna y cámara térmica

- Detección de dispositivos ocultos y componentes adheridos en la ranura de dispensación.
- Inspección de calor residual que indique manipulación reciente.

Pruebas de dispensación con billetes de prueba

- Ensayo manual y automatizado para verificar operación correcta del dispensador.
- Evaluación de fallos de entrega o desvío físico del dinero.

Análisis de sensores de detección de efectivo

- Verificación del funcionamiento de sensores ópticos y de presión.
- Confirmación de registros precisos sobre el paso de cada billete.

3.3 Pruebas de Ataque

3.3.1 Simulación de Reversión de Transacciones

Simulación de corte de energía durante una transacción

- Evaluación de la respuesta del ATM frente a reinicios abruptos.
- Verificación de la consistencia de los registros en el sistema.

Manipulación del dispensador con herramientas no invasivas

- Ensayo de técnicas para interferir con la entrega de efectivo.
- Análisis de las capacidades de respuesta del hardware.

Análisis de reversión de transacciones con sniffing de red

- Monitoreo del tráfico de red durante eventos de transacción fallida.
- Identificación de debilidades en la comunicación ATM-host.

3.4 Medidas de Mitigación

Instalación de dispensadores con compuertas motorizadas

- Impide el acceso físico a los billetes en caso de fallo.
- Automatiza la retracción del efectivo si no se detecta retiro.

Implementación de alertas de detección de manipulación

- Activación de eventos cuando se detectan fallos mecánicos reiterados.
- Notificaciones automáticas al centro de monitoreo de seguridad.

Monitoreo en tiempo real de reversión de efectivo

- Integración de sistemas que detectan patrones anómalos en la entrega de dinero.
- Correlación con eventos de energía, reinicio o error de sensores para validar autenticidad de la reversión.

Control 4: Ataques de Malware y Cajas Negras (Malware & Black Box Attacks)

4.1 Fundamentos Teóricos

4.1.1 Definición y Clasificación de Malware para ATMs

Malware orientado a extracción de efectivo
Incluye programas diseñados para forzar la dispensación de billetes sin necesidad de tarjeta o autenticación válida.

- *Ploutus*: Permite el control remoto del dispensador mediante comandos externos.
- *Cutlet Maker*: Ejecuta dispensaciones usando solo un código generado por el atacante.
- *ATMitch*: Brinda control total del ATM, incluyendo acceso al sistema operativo y hardware.

Malware de intercepción de datos
Enfocado en capturar datos sensibles como PINs o números de tarjeta durante transacciones.

- *Suceful*: Intercepta datos de tarjetas y pulsaciones del teclado.
- *Tyupkin*: Permite retiros sin tarjeta usando comandos programados y ventanas de tiempo ocultas.

Malware de persistencia y backdoors
Busca mantener acceso prolongado al ATM modificando el sistema de arranque o inyectando puertas traseras.

- Modificaciones al BIOS o firmware del ATM.
- Instalación de backdoors en sistemas de administración remota.

4.1.2 Métodos de Infección y Persistencia

Infección a través de dispositivos físicos

- Uso de USBs maliciosos con carga automática de malware.
- Conexión de dispositivos como Raspberry Pi o BeagleBone Black para mantener acceso persistente o actuar como punto de comando.

Ataques de red y acceso remoto

- Compromiso del software de administración del ATM mediante explotación de vulnerabilidades conocidas.
- Infección de servidores bancarios centrales que distribuyen software a múltiples ATMs.

4.2 Inspección y Auditoría

4.2.1 Revisión de Seguridad del Sistema Operativo

- Identificación del sistema operativo utilizado (Windows XP Embedded, Windows 7/10 IoT, Linux, etc.).
- Análisis de logs para detectar procesos sospechosos o cargas maliciosas.
- Verificación de la integridad de archivos del sistema utilizando herramientas de checksum (SHA256, MD5).

4.2.2 Inspección de Hardware y Conectividad

- Revisión de todos los puertos USB, seriales y de administración en busca de dispositivos extraños.
- Análisis del tráfico de red con herramientas como Wireshark para detectar conexiones externas sospechosas.
- Escaneo de puertos y servicios activos con Nmap para identificar software no autorizado.

4.3 Pruebas de Ataque

4.3.1 Inyección de Malware en el ATM

- Simulación de infección usando dispositivos USB con exploits creados en Metasploit.
- Pruebas con herramientas físicas como Rubber Ducky o Bash Bunny para automatizar ejecución de comandos.
- Validación de persistencia del malware con análisis de memoria activa utilizando Mimikatz, Process Hacker o similares.

4.3.2 Ataque de Caja Negra (Black Box Attack)

- Conexión de dispositivos externos (Raspberry Pi, Teensy, BeagleBone) a interfaces internas del ATM.
- Emulación de comandos de control directo al dispensador para extraer efectivo.
- Intentos de acceso a la consola de administración a través de ingeniería inversa o default credentials.

4.4 Medidas de Mitigación

Implementación de whitelisting para limitar ejecución de software no autorizado

- Permitir únicamente programas firmados y verificados.
- Rechazo automático a ejecutables desconocidos.

Bloqueo de puertos físicos no utilizados (USB, RJ-45, serial)

- Sellado físico o desactivación por BIOS/UEFI.
- Monitoreo continuo de actividad en puertos activos.

Uso de Secure Boot y cifrado en disco completo (BitLocker o TPM)

- Evita ejecución de código no firmado en el arranque.
- Protege la integridad del sistema incluso ante robo físico.

Segmentación de red y uso de VPN cifradas para comunicación ATM-banco

- Aísla al ATM del resto de la red bancaria.
- Garantiza confidencialidad e integridad en la transmisión de datos.

Fecha de emisión: Marzo 2025

Control 5: Seguridad Física y Ataques a Cerraduras (Physical Security & Lock Manipulation)

5.1 Fundamentos Teóricos

5.1.1 Tipos de Cerraduras Utilizadas en ATMs

Cerraduras mecánicas estándar

- Llaves de perfil alto como las utilizadas por fabricantes como Sargent & Greenleaf o Abloy.
- Cilindros de doble seguridad con pines anti-ganzuado y protección contra bumping.

Cerraduras electromagnéticas

- Sistemas controlados por energía eléctrica con autenticación dual.
- Apertura mediante tarjetas RFID, contraseñas o biometría (huella, iris).

Cerraduras electrónicas y de combinación

- Permiten cambio de clave en tiempo real.
- Algunas integran registros de apertura, notificaciones de acceso y monitoreo remoto.

5.1.2 Métodos de Ataque a Cerraduras

Lock Picking (ganzuado convencional y herramientas avanzadas)

- Uso de ganzúas, tensores y decodificadores para manipular pines internos.
- Acceso sin dañar la cerradura.

Llave Bumping

- Inserción de bump keys especialmente cortadas que transmiten un golpe a los pines para alinearlos temporalmente.

Bypass con herramientas de deslizamiento (shims, feeler gauges)

- Acceso sin manipular el mecanismo interno mediante deslizamiento de piezas.

Ataques a cerraduras electromagnéticas

- Uso de imanes de neodimio para desactivar solenoides.
- Inyecciones de corriente para forzar la apertura.

5.2 Inspección y Auditoría

5.2.1 Evaluación de la Integridad Física del ATM

- Revisión visual de la carcasa en busca de señales de acceso forzado.
- Inspección de bisagras, tornillos, y placas de blindaje de los compartimentos críticos.

5.2.2 Pruebas de Resistencia de Cerraduras

- Ejecución de pruebas controladas de apertura forzada (force attacks).
- Pruebas con ganzúas tradicionales, eléctricas y bump keys en laboratorio o entorno controlado.

5.3 Pruebas de Ataque

5.3.1 Simulación de Lock Picking y Llave Bumping

- Evaluación de cerraduras con herramientas como Bogotá Rakes, Hook Picks, Tubular Picks.
- Uso de bump hammer para evaluar tiempos de apertura con técnicas no destructivas.

5.3.2 Simulación de Ataque con Herramientas de Impacto

- Evaluación de resistencia estructural utilizando martillos de seguridad.
- Simulación de apertura con herramientas hidráulicas o palancas de presión.

5.4 Medidas de Mitigación

Reemplazo de cerraduras mecánicas por cerraduras electrónicas con autenticación dual

- Uso de combinación de PIN + RFID, o PIN + biometría.
- Cambio remoto de claves ante sospechas de manipulación.

Implementación de sensores de vibración y movimiento

- Detección temprana de intentos de apertura forzada.
- Activación de alarmas locales o remotas.

Blindaje con placas de acero reforzado en compartimentos críticos

- Refuerzo del compartimento de efectivo y electrónica interna.
- Dificulta significativamente el acceso físico sin generar ruido o tiempo elevado.

Control 6: Extracción Ilimitada de Efectivo (Unlimited Operations Cash-Out)

6.1 Fundamentos Teóricos

6.1.1 Métodos de Cash-Out Fraudulento

Uso de malware para activar comandos de dispensación de efectivo
Malware especializado se instala en el sistema del ATM y permite enviar comandos para dispensar billetes sin autenticación legítima. Este tipo de software malicioso puede ejecutarse local o remotamente y ha sido utilizado en ataques como los relacionados con Ploutus o Cutlet Maker.

Manipulación de la base de datos del banco para aumentar saldos ficticios
Al comprometer sistemas centrales del banco, los atacantes alteran los registros de cuenta para reflejar saldos inflados que luego permiten retiros no legítimos desde los ATMs.

Acceso a la administración remota del ATM para ejecutar retiros no autorizados
El acceso no autorizado a la consola de administración del ATM permite ejecutar directamente comandos de dispensación de efectivo, sin intervención del cliente.

6.2 Inspección y Auditoría

- Revisión de logs de transacciones en busca de anomalías: Detección de patrones irregulares, retiros consecutivos en tiempos reducidos o valores máximos recurrentes.
- Verificación de alertas de retiros inusuales o múltiples en corto tiempo: Cruce de información en los sistemas de detección de fraude y control de límites dinámicos por perfil de usuario.

6.3 Pruebas de Ataque

6.3.1 Simulación de Ataques de Cash-Out

- Intento de extracción masiva con malware (Ploutus, Cutlet Maker): Pruebas controladas en entornos de laboratorio donde se simula la ejecución de malware para dispensar efectivo.
- Simulación de cash-out a través de inyección de comandos remotos: Ejecución de órdenes de dispensación sin intervención física mediante control remoto del ATM.

6.4 Medidas de Mitigación

Implementación de límites de retiro dinámicos según comportamiento del usuario

- Los límites se ajustan automáticamente con base en el comportamiento histórico del cliente, el monto promedio de transacciones y patrones geográficos.
- Desencadena alertas o bloqueos temporales ante conductas inusuales.

Fecha de emisión: Marzo 2025

Monitoreo en tiempo real con algoritmos de detección de fraude

- Análisis basado en inteligencia artificial para detectar patrones sospechosos.
- Correlación de eventos entre diferentes ATMs para identificar posibles ataques coordinados.

Control 7: Manipulación de Mensajes de Autorización (Authorization Message Manipulation)

7.1 Fundamentos Teóricos

7.1.1 Definición y Riesgos

Manipulación de los mensajes de autorización enviados entre el ATM y el procesador bancario
Consiste en interceptar y alterar las solicitudes o respuestas de autorización que validan operaciones como retiros, consultas o autenticaciones. Estas comunicaciones normalmente se basan en protocolos como ISO 8583.

Alteración de los valores de autorización para modificar montos de retiro o validaciones de PIN
El atacante puede modificar campos como montos, códigos de autorización o parámetros de validación para ejecutar transacciones no autorizadas o superar controles de seguridad.

Posibilidad de generar transacciones fraudulentas sin detección inmediata
La manipulación ocurre en tiempo real y puede pasar inadvertida si no existen sistemas robustos de monitoreo y validación de integridad.

7.1.2 Métodos de Ataque

Interceptación de Tráfico de Red

- Ataques Man-in-the-Middle (MitM) entre el ATM y el procesador bancario.
- Uso de herramientas como Ettercap, Wireshark y MITMf para analizar o modificar el tráfico en vivo.

Falsificación de Mensajes de Autorización

- Generación de respuestas falsas desde un nodo controlado por el atacante.
- Modificación de campos sensibles como montos, autorizaciones o códigos de aprobación.
- Inyección de comandos a través de protocolos vulnerables como ISO 8583 sin cifrado ni autenticación.

Ataques a la Infraestructura de Red

- Redireccionamiento de tráfico mediante técnicas como DNS Spoofing o ARP poisoning.
- Compromiso de servidores intermediarios mediante explotación de vulnerabilidades conocidas o desactualización de sistemas.

7.2 Inspección y Auditoría

7.2.1 Análisis de Seguridad en la Comunicación

- Verificación del uso de cifrado robusto como TLS 1.2+, SSL/TLS con cifrado simétrico fuerte (AES, 3DES).
- Inspección de logs de transacciones buscando inconsistencias en tiempos, origen, destino y campos alterados.
- Medición del tiempo de respuesta en solicitudes de autorización: los retrasos pueden indicar interceptación o manipulación.

7.2.2 Escaneo de Infraestructura de Red

- Escaneo de puertos y servicios abiertos con Nmap para identificar servicios expuestos.
- Evaluación del nivel de cifrado en enlaces entre ATM y backend con herramientas como SSL Labs.
- Identificación de segmentos no protegidos mediante técnicas de ARP Spoofing o monitoreo de tráfico en red local.

7.3 Pruebas de Ataque

7.3.1 Simulación de Intercepción de Datos

- Uso de Wireshark o tcpdump para capturar mensajes ISO 8583.
- Reproducción de un escenario de ataque Man-in-the-Middle para modificar valores de autorización en tiempo real.

7.3.2 Manipulación de Mensajes de Respuesta

- Creación y envío de respuestas falsas a transacciones utilizando herramientas como Scapy o Socat.
- Intentos de ejecución de transacciones sin validación de PIN mediante manipulación del código de respuesta.

7.4 Medidas de Mitigación

Implementación de autenticación mutua entre el ATM y el procesador bancario

- Utilización de certificados digitales y validación de identidad bidireccional.

Uso de HSM (Hardware Security Modules) para cifrado seguro de transacciones

- Protección física y lógica de claves criptográficas.
- Firmado y verificación de integridad de cada mensaje transmitido.

Segmentación de red con VLANs y uso de firewalls para evitar ataques MitM

- Aislamiento de la red del ATM respecto a otros sistemas internos o de usuarios.
- Reglas estrictas en firewalls de capa 3 y 7 para controlar el flujo de datos.

Implementación de monitoreo de integridad en mensajes de autorización

- Hashing o firma digital de los mensajes antes de ser transmitidos.
- Validación cruzada entre registros locales y remotos para detectar inconsistencias.

Control 8: Gestión de Crisis y Manejo de Delitos (Crisis & Crime Management)

8.1 Fundamentos Teóricos

8.1.1 Importancia de la Respuesta a Incidentes

Prevención de pérdidas económicas derivadas de fraudes en ATMs
Una respuesta rápida y eficaz puede detener ataques en curso y evitar la extracción masiva de efectivo o la propagación del fraude.

Coordinación con fuerzas de seguridad y equipos forenses en incidentes de fraude permite capturar evidencia, preservar la escena del delito digital y facilitar la judicialización de los responsables.

Minimización del impacto reputacional en la institución financiera
La respuesta oportuna y transparente mitiga daños en la confianza de los clientes y las autoridades regulatorias.

8.1.2 Tipos de Delitos Relacionados con ATMs

Fraudes electrónicos
Incluyen skimming, cash-out y manipulación de mensajes de autorización para ejecutar transacciones no legítimas.

Ataques físicos
Ganzuado, uso de explosivos, corte estructural del cajero, o extracción total con vehículos.

Ataques híbridos
Combinan malware con acceso físico para aumentar el impacto del ataque y el acceso a componentes críticos.

8.2 Inspección y Auditoría

8.2.1 Evaluación de Protocolos de Respuesta a Incidentes

- Análisis de tiempos de detección y contención de incidentes.
- Revisión de los procedimientos de escalamiento dentro del banco.
- Evaluación de las políticas de cierre inmediato o puesta fuera de línea de ATMs comprometidos.

8.2.2 Coordinación con Equipos de Seguridad

- Identificación clara de los responsables de respuesta ante incidentes.
- Protocolos definidos de comunicación con autoridades locales, cuerpos policiales y fiscales.

- Realización de simulacros de ataque para validar la efectividad de la respuesta y los canales de escalamiento.

8.3 Pruebas de Ataque

8.3.1 Simulación de Fraude en ATM

- Ejecución controlada de un ataque de cash-out con malware en entorno aislado.
- Medición de tiempo de detección y reacción del SOC (Security Operations Center).

8.3.2 Evaluación de Tiempo de Respuesta

- Monitoreo del ciclo completo desde la detección hasta la contención.
- Pruebas internas de comunicación y gestión de incidentes con diferentes niveles de severidad.

8.4 Medidas de Mitigación

Implementación de SIEM (Security Information and Event Management)

- Correlación en tiempo real de eventos desde múltiples fuentes (ATM, red, endpoints).
- Generación de alertas automáticas y activación de playbooks de respuesta.

Creación de protocolos de respuesta inmediata con equipos de seguridad forense

- Manuales de actuación ante incidentes según tipo de ataque.
- Acceso inmediato a herramientas de análisis forense y aislamiento de activos.

Simulación de ataques de forma periódica para entrenar a los equipos de respuesta

- Red team / blue team exercises.
- Simulación de escenarios complejos: fraudes combinados, indisponibilidad de red, acceso físico forzado

Control 9: Evaluaciones Regulares y Cumplimiento Normativo (Auditing & Compliance)

9.1 Fundamentos Teóricos

9.1.1 Normativas Aplicables a la Seguridad de ATMs

PCI DSS (Payment Card Industry Data Security Standard)

- Requiere el cifrado de los datos sensibles de las transacciones (como PAN y PIN).
- Exige controles estrictos para proteger la infraestructura de red contra accesos no autorizados, así como pruebas de seguridad regulares.

ISO 27001 (Gestión de Seguridad de la Información)

- Establece políticas para controlar accesos físicos y lógicos en entornos críticos como ATMs.
- Incluye procesos de auditoría continua, análisis de riesgos, y planes de respuesta a incidentes documentados y probados.

NIST Cybersecurity Framework

- Proporciona guías para identificar, proteger, detectar, responder y recuperar en contextos de ciberseguridad bancaria.
- Aporta lineamientos claros para aplicar controles técnicos, organizativos y de monitoreo en sistemas transaccionales.

9.2 Inspección y Auditoría

9.2.1 Evaluación de Controles de Seguridad

- Validación del cumplimiento con requisitos de PCI DSS e ISO 27001 mediante revisiones documentales y técnicas.
- Confirmación de la presencia de cifrado en datos sensibles tanto en tránsito (TLS/SSL) como en reposo (disco, bases de datos).
- Revisión de mecanismos de autenticación (biometría, tokens, MFA) y gestión de accesos privilegiados.

9.2.2 Auditoría de Seguridad Física

- Inspección de cerraduras, sensores, y puntos de acceso físico a los compartimentos internos del ATM.
- Evaluación del blindaje estructural del ATM contra vandalismo o extracción forzada.

Fecha de emisión: Marzo 2025

- Simulaciones de ataques físicos y verificación de la resistencia ante intentos de acceso no autorizado.

9.3 Pruebas de Ataque

9.3.1 Simulación de Auditoría Interna

- Ejecución de pruebas de penetración (pentesting) en la red de ATMs, incluyendo escaneos de vulnerabilidades, ataques dirigidos a interfaces administrativas, y validación de hardening del sistema operativo del ATM.
- Intentos controlados de acceso a la consola de administración y manipulación del software del ATM.

9.3.2 Evaluación de Cifrado en Comunicaciones

- Análisis de los certificados SSL/TLS para determinar versiones, algoritmos de cifrado y vigencia.
- Pruebas de downgrade attack para evaluar si el ATM acepta protocolos de cifrado obsoletos o inseguros.

9.4 Medidas de Mitigación

Implementación de auditorías regulares con equipos de seguridad externos

- Revisiones trimestrales o semestrales realizadas por terceros certificados que aporten una visión imparcial de las vulnerabilidades.

Aplicación de segmentación de red estricta con monitoreo de anomalías

- Separación lógica y física de las redes de ATMs respecto a otras redes corporativas.
- Uso de IDS/IPS para identificar tráfico sospechoso.

Revisión de políticas de seguridad y gestión de acceso en sistemas ATM

- Actualización periódica de las políticas internas de seguridad y revisión de logs de acceso.
- Gestión centralizada de credenciales y revisión de sesiones administrativas.