



DIPLOMADO EN SEGURIDAD EN ATMS

[HTTPS://CERTISYSNET-SOLUTIONS.COM/CAPACITACION/](https://certisysnet-solutions.com/capacitacion/)



DIPLOMADO + CERTIFICACIÓN

Seguridad en Cajeros Automáticos
(ATMs)

¡Domina los ataques reales contra la infraestructura bancaria automatizada!

Aprende a prevenir, detectar y responder a fraudes y amenazas físicas, lógicas y mixtas en cajeros automáticos con herramientas profesionales, simulaciones realistas y contenido alineado a normas internacionales.

 Modalidad: 100% Online

 Acceso: Ilimitado y de por vida

 Certificación: Diploma profesional con validez internacional

 Inversión: \$6,990 MXN / \$350 USD

 TEMARIO: www.certisysnet-solutions.com/capacitacion

¿Qué incluye tu inscripción?

- ✓ Acceso permanente a la plataforma y actualizaciones
 - ✓ Casos prácticos con simulaciones de ataques reales
 - ✓ Checklists técnicos para auditar cajeros automáticos
 - ✓ Manuales descargables y material complementario
 - ✓ Mentoría directa con expertos certificados
 - ✓ Soporte técnico durante todo el diplomado
 - ✓ Certificación profesional con firma electrónica avanzada
 - ✓ Código único de validación para tu CV
-

Ejes Temáticos Principales

1. Estudio de Fraudes Digitales

- Skimming
- Shimming
- Jackpotting
- Accesos remotos
- Dispositivos alterados
- ✓ Análisis forense aplicado a ATMs
- ✓ Ciclo completo del fraude (intrusión → respuesta)
- ✓ Impacto técnico, operativo y regulatorio
- ✓ Identificación de causas raíz y generación de informes

2. Normativas y Regulaciones Internacionales

- PCI DSS
- SWIFT CSP
- NIST 800-53
- ISO/IEC 27001
- ✓ Auditorías técnicas y de cumplimiento
- ✓ Controles exigidos por organismos certificadores

✓ Diseño de arquitecturas seguras y sostenibles para ATMs

✓ Casos reales de cumplimiento normativo

📌 3. Preparación para la Industria Financiera

✓ Simulación de ataques físicos y lógicos

✓ Respuesta ante incidentes reales

✓ Validación de controles técnicos

✓ Reportes ejecutivos para auditores y gerentes

✓ Checklists desde el primer día

✓ Diagnósticos aplicados en bancos y procesadoras

🧐 ¿A quién va dirigido?

- Pentesters y especialistas en seguridad ofensiva
 - Consultores y auditores de cumplimiento
 - Equipos de TI en bancos y fintechs
 - Analistas de fraude digital
 - Personal de riesgos y operaciones
 - Estudiantes avanzados de ingeniería, informática y ciberseguridad
-

Certificación Profesional

- ✓ Diploma digital con firma electrónica y código único
 - ✓ Válido para procesos ISO, PCI, SWIFT
 - ✓ Aceptado por entes reguladores y empresas
 - ✓ Respaldo técnico de Certisysnet Solutions
-

Métodos de Pago

◆ Pago único:

\$6,990 MXN / \$350 USD → acceso total inmediato

◆ Pago en 2 partes:

1° pago: \$3,500 MXN / \$175 USD → acceso total inmediato

2° pago: \$3,500 MXN / \$175 USD (antes de la entrega del Certificado)

- ✓ Accedes desde el primer pago
- ✓ Recibes el Diplomado al completar el curso
- ✓ Recibes la Certificación profesional al finalizar

 Una vez confirmado tu pago, obtienes acceso inmediato al curso completo y todos los materiales descargables.



<https://certisysnet-solutions.com/capacitacion/>

✉ Escríbenos a services@certisysnet-solutions.com para inscribirte

👉 [Inscríbete ahora!!!](#)

TEMARIO

MÓDULO 1: Fundamentos de Seguridad en Cajeros Automáticos

- 1.1 Historia y evolución de ataques a ATM
- 1.2 Topología y arquitectura lógica/física de cajeros
- 1.3 Tipología de ATM (drive-up, lobby, wall-mounted, island)
- 1.4 Ciclo completo de una transacción financiera
- 1.5 Normativas globales y su aplicación práctica (PCI, EMV, ISO, GDPR)
- 1.6 Comparativa de fabricantes de ATMs y software

MÓDULO 2: Compromiso del PIN y Seguridad del Teclado

- 2.1 Ingeniería social en PIN harvesting
- 2.2 Interceptores electromagnéticos de teclados
- 2.3 Esteganografía en teclados EPP falsificados
- 2.4 Protocolos criptográficos para cifrado de PIN
- 2.5 Teclados biométricos y validación multifactor
- 2.6 Instalación de sensores de integridad y honeypots

MÓDULO 3: Skimming y Robo de Tarjetas

- 3.1 Reverse engineering de dispositivos skimmer
 - 3.2 Técnicas de lectura sin contacto (NFC sniffing)
 - 3.3 Lectura y decodificación de pistas magnéticas
 - 3.4 Exfiltración de datos desde skimmers GSM/Wi-Fi
 - 3.5 Detección de cambios mecánicos en ranura
 - 3.6 Integración de IA para prevención de skimming
-

MÓDULO 4: Trampas de Efectivo y Fraudes de Reversión

- 4.1 Análisis de anomalías en sensores de billetes
 - 4.2 Log manipulation y análisis de transacciones no concluidas
 - 4.3 Estudio de dispositivos cash-trap y pruebas de laboratorio
 - 4.4 Implementación de detección por presión/infrarrojo
 - 4.5 Procedimientos de verificación de entregas
 - 4.6 Revisión de firmware de módulos dispensadores
-

MÓDULO 5: Ataques de Malware y Caja Negra

- 5.1 Análisis estático y dinámico de malware para ATM
- 5.2 Cadenas de infección USB y scripts persistentes

- 5.3 Técnicas anti-debugging y sandboxing
 - 5.4 Manipulación de módulos XFS Manager
 - 5.5 Ejecución remota desde Command & Control
 - 5.6 Simulación de ataques tipo Jackpotting
offline/online
-

MÓDULO 6: Seguridad Física y Manipulación de Cerraduras

- 6.1 Bypass electromagnético de cerraduras electrónicas
 - 6.2 Instalación de cámaras ocultas para ataques físicos
 - 6.3 Modelos de cerraduras más vulnerables y su reemplazo
 - 6.4 Ataques combinados físico-lógicos
 - 6.5 Detección de intento de apertura forzada (sensores de vibración)
 - 6.6 Red team físico: rolplay de intrusiones
-

MÓDULO 7: Fraudes de Extracción Ilimitada de Efectivo

- 7.1 Ataques coordinados con tarjetas clonadas
- 7.2 Simulación de escenarios bancarios globales
- 7.3 Generación masiva de transacciones válidas no autorizadas

7.4 Técnicas de obfuscación de logs en servidores centrales

7.5 Integración con análisis de fraude financiero

7.6 Respuesta bancaria ante ataques tipo “ATM Cashout”

MÓDULO 8: Manipulación de Mensajes de Autorización

8.1 Ingeniería inversa de mensajes ISO 8583

8.2 Suplantación de mensajes de autorización/respuesta

8.3 Redirección de transacciones hacia terminales controladas

8.4 Interferencia activa con routers intermedios (ARP Poisoning)

8.5 Implementación de TLS mutuo y validación de certificados

8.6 Simulación de corrupción de mensaje (bit flipping attack)

MÓDULO 9: Gestión de Crisis y Delitos Asociados

9.1 Desarrollo de escenarios tipo “crisis coordinada”

9.2 Activación de CSIRT financiero

9.3 Análisis post-mortem de brechas

9.4 Simulación con actores internos (fraude interno)

9.5 Integración de simulacros en tiempo real

9.6 Estudio de perfil criminal en delitos contra cajeros

MÓDULO 10: Auditoría Técnica y Cumplimiento Normativo

10.1 Auditoría Red Team vs Blue Team

10.2 Uso de herramientas de compliance automatizado

10.3 Validación de cifrados y tokens EMV

10.4 Simulación de informes para auditorías externas

10.5 Auditoría de logs, firmware, BIOS y configuraciones

10.6 Integración de métricas de madurez de ciberseguridad

MÓDULO 11: Laboratorios Prácticos y Simulación de Ataques

11.1 Emulación de red bancaria y nodo ATM

11.2 Integración con software real o emulado de ATMs

11.3 Simulación de vulnerabilidades físicas, lógicas y mixtas

11.4 Instalación de honeypots ATM

- 11.5 Monitoreo SIEM en tiempo real y correlación
- 11.6 Desarrollo de “Cyber Range ATM”
- 11.7 Emulación ATM

MÓDULO 12: Proyecto Final y Defensa Técnica

- 12.1 Diseño de ataque ofensivo a ATM (plan de ejecución)
- 12.2 Documentación técnica, forense y ejecutiva
- 12.3 Defensa del caso ante panel evaluador
- 12.4 Propuesta de mejoras a sistemas ATM reales
- 12.5 Evaluación integral: pentest, defensa, cumplimiento

Recursos Adicionales

Checklist Avanzado de Seguridad para Cajeros Automáticos (ATMs)

<https://certisysnet-solutions.com/capacitacion/>