


# LA CIBERSEGURIDAD EN CAJEROS AUTOMÁTICOS

## UNA TAREA PENDIENTE

ARTÍCULO DE OPINIÓN

THE # NEXTGENBANK®

**AURIGA**  
the banking e-evolution

 [www.aurigasp.com](http://www.aurigasp.com)

Año tras año se generan millones de pérdidas en las instituciones financieras de todo el mundo debido a la vulnerabilidad de los cajeros automáticos y su sistema de control. Según reportes de los últimos cinco años el impacto de ataques en México asciende hasta los USD 5,000 millones de dólares al año, solo superado por Brasil (alrededor de 8 mil millones). En general, se estima un crecimiento del impacto del cibercrimen en todo el mundo de hasta USD 6 billones para 2021.

Los ataques son tanto físicos (skimming o gases explosivos para atentar contra la caja negra) como lógicos (malware, skimming de software, black box). De hecho, el efectivo actúa como incentivo, sumando a la información confidencial (tarjetas de crédito y débito y números PIN) que también se pueden convertir en cash. Se calcula que cada ataque dirigido a un ATM ocasiona de media una pérdida de USD 50,000.

Uno de los puntos débiles de los ATMs es su deficiente monitoreo y la escasa protección de la información que contienen. Otro, es el gran número de agentes involucrados en la ciberseguridad, lo que puede aumentar potencialmente el riesgo de accesos no autorizados. Además, estos equipos normalmente son monitoreados por proveedores externos para su mantenimiento y soporte, generando graves lagunas en el control de la seguridad.

Son muchos los desafíos a los que se enfrentan las instituciones financieras para que los cajeros estén operativos 24/7. Por un lado, necesitan minimizar la carga de desarrollo de software y el mantenimiento del hardware, así como cuidar la visibilidad y el control sobre los cambios en ambos. Por otro, las políticas de seguridad deben aplicarse y respetarse garantizando la visibilidad y la gestión integradas del estado de la seguridad.

## ¿POR QUÉ LOS CAJEROS AUTOMÁTICOS DE LATINOAMÉRICA ESTÁN EXPUESTOS?

Una de las razones es que el hardware y el software heredado en las redes de cajeros automáticos son demasiado caros y difíciles de actualizar. Esto los pone en una posición muy insegura. Tanto es así que alrededor del 40% de estos dispositivos en todo el mundo funcionan con sistemas operativos obsoletos.





Cuando esto sucede se hacen más vulnerables. Muchos de ellos todavía dependen del sistema operativo Windows XP o 7, que ya no son actualizados por Microsoft y no proporcionan parches de seguridad para protegerse contra nuevas amenazas.

Estas debilidades han generado cuantiosas pérdidas económicas en el mundo. Por ejemplo, la familia Ploutus de malware de cajeros, descubierta por primera vez en México en 2013, ha acumulado una pérdida de 450 millones de dólares (398 millones de euros) a nivel mundial.

Uno de los principales vectores de ataque es la capa XFS, la interfaz estándar diseñada para permitir que el software de varios proveedores se ejecute en ATMs de fabricantes y en otro hardware. La capa XFS usa API estándar para comunicarse con las aplicaciones de autoservicio. Este middleware no tiene un proceso integrado de autenticación, lo que hace posible que los delincuentes implementen el malware en dispositivos de hardware como cajeros automáticos para retirar efectivo y dispensar dinero (jackpotting) o para robar números de tarjetas (skimming de software).

## RECOMENDACIONES PARA BANCOS CON RIESGO DE ATAQUES A CAJEROS AUTOMÁTICOS

Como vemos, la tecnología genérica de protección de endpoints no es suficiente para asegurar estas terminales. Los bancos necesitan una solución de seguridad centralizada que proteja, monitoree y controle sus redes de cajeros automáticos, además de que sea fácil de gestionar desde un solo lugar y que pueda detener cualquier actividad fraudulenta.

Por ello deben contar con varias capas de protección en una única plataforma como, por ejemplo, la que brinda Lookwise Device Manager (LDM), una de las soluciones más innovadoras de Auriga.

Las diferentes capas son:

- **Lista blanca de aplicaciones:** la capa que previene la ejecución de malware o software no autorizado definiendo una lista blanca de procesos que pueden ejecutarse en el cajero automático.
- **Cifrado de disco completo de todos los discos duros y volúmenes:** un imprescindible para cualquier banco que quiera proteger su red de ATMs, ya que sin esto los ciberdelincuentes pueden robar hardware y realizar ingeniería inversa para introducir malware en el disco duro y luego reemplazarlo en otra sucursal del banco.
- **Protección de la integridad del sistema de ficheros** para bloquear cualquier intento de modificar un archivo crítico, a no ser que el proceso de actualizaciones de software esté predefinido.
- **Protección de hardware:** evita la conexión de hardware fraudulento, bloqueando dispositivos que no estén incluidos en la lista blanca.

Está claro que cualquier solución integral se complementa con consultorías especializadas para comprobar los planes y procesos de seguridad, lo que idealmente incluye pruebas de penetración de la red de cajeros automáticos, técnicas de evaluación de vulnerabilidades, equipos azules, equipos rojos y pruebas de rendimiento del centro de operaciones de seguridad de un banco.

Asimismo, la inteligencia de amenazas cibernéticas (CTI por sus siglas en inglés) se puede emplear como un sistema de advertencia temprana para detectar y contener potenciales amenazas antes de que escalen.

A pesar de que las instituciones bancarias son conscientes del entorno de amenazas, es recomendable diseñar un plan robusto de continuidad de negocio y de recuperación ante desastres. Esto abarca el tipo de respuesta que se tendrá ante determinados incidentes o cómo restaurar rápidamente los datos y sistemas afectados con el menor impacto posible sobre las operaciones.

Para aplicarlo es clave la estrecha cooperación entre los desarrolladores de software y las organizaciones financieras. De este modo, se asegura la integración adecuada entre proveedores de hardware, software y soluciones de seguridad para cajeros automáticos y las compañías que los gestionan. Estos deben tener en consideración todos los elementos cuando definan el alcance y la interconectividad de la solución con las piezas del software y el hardware que componen la red.

Finalmente, es importante que los bancos no pierdan de vista ni un segundo todas las amenazas que hay en su entorno para evitar futuros ciberataques en su contra. Es clave que investiguen constantemente y se adelanten a las maniobras de los delincuentes, que no se cansan de desarrollar nuevos métodos para vulnerar los sistemas informáticos de los cajeros automáticos.

ARTÍCULO DE OPINIÓN

THE # NEXTGENBANK



Auriga Latin America, S.de R.L.de C.V.  
Rio Pánuco 108, Cuauhtémoc, 06500,  
Ciudad de México, México  
[www.aurigaspa.com](http://www.aurigaspa.com)  
[mexicocity@aurigaspa.com](mailto:mexicocity@aurigaspa.com)