

# Tarjetas con Chip EMV: El nuevo estándar en seguridad de tarjetas.



COMPAÑÍA LATINOAMERICANA  
DE APLICACIONES INFORMÁTICAS

## ¿En qué vamos sobre EMV?

A raíz de las numerosas vulnerabilidades de seguridad y funcionalidad que tienen las tarjetas de crédito y débito convencionales de banda magnética, los emisores de tarjetas adoptan cada vez con mayor frecuencia el uso de la plataforma tecnológica EMV, que, entre otras ventajas, permite que el dialogo tarjeta-terminal gane capacidad de decisión sobre el resultado de la operación, amplía la lista de servicios factibles y generará eficiencia en el back office. Las nuevas entidades financieras de la región tienen EMV no como meta sino como su punto de partida.

Según nuestra experiencia, obtenida en conjunto con varios de nuestros clientes, encontramos que una de las principales problemáticas que enfrentan las instituciones financieras para implementar EMV es la dificultad de, dentro de todo el mar de información que se recibe, identificar cuáles son los cambios que deben realizar en sus sistemas y procesos actuales. Es por ello que **CLAI** orientará su próximo evento de capacitación en exponer de manera clara cuál es el impacto real de implementar EMV en la institución financiera.

**CLAI** se ha mantenido a la vanguardia de la innovación tecnológica, ofreciendo soluciones integrales para cubrir las necesidades del mercado. Mediante su producto **AUTORIZA7®**, ofrece las herramientas necesarias para la personalización, emisión y administración de tarjetas chip EMV, así como para la configuración, monitoreo y administración de terminales con capacidad para aceptar dichas tarjetas.

**AUTORIZA7®** también provee todas las herramientas necesarias para la realización del ciclo completo de la transacción (crédito/débito) EMV, incluyendo en esto la totalidad de los procesos criptográficos correspondientes, que se soportan en el módulo **Az-CRIPTO/EMV** el cual ofrece rutinas que detectan clonación de tarjetas, validan la autenticidad del autorizador y permiten cambiar datos dentro del chip de manera posterior a la emisión de la tarjeta. Adicionalmente con **Az-AUTHORIZER** la entidad financiera cuenta con una herramienta que le provee todas las nuevas validaciones necesarias minimizando el impacto en sus sistemas actuales.



## V Evento BIANUAL TRANSACCIONAL Panamá 2010

Del 08 al 11 de setiembre de 2010 se celebrará la V edición del Evento BIANUAL Transaccional de CLAI, en donde se presentarán conferencias sobre las tendencias actuales y sobre las innovaciones tecnológicas en los medios de pago.

El evento se realizará en la Ciudad de Panamá y contará con la participación de conferencistas internacionales expertos en la materia y con la asistencia de especialistas de más de catorce países de las Américas.

Se abordarán temas como:

- Nuevas tendencias en la evolución del mercado EMV.
- Evaluación del impacto en los negocios de emisores y de adquirentes debido a la adopción de la tecnología EMV.
- Normas y estándares PCI.
- Uso de herramientas que ayuden a cumplir con las normativas y a mantener la competitividad ante las nuevas tendencias del mercado.



# NORMAS Y ESTANDARES

Toda entidad que participe en el procesamiento, transferencia o almacenamiento de información de tarjetas de crédito y débito debe cumplir los requerimientos que establece PCI



El PCI "Security Standards Council" creó, entre otras, la Normativa de Seguridad de Datos de la Industria de Tarjetas de Pago con el objetivo de fomentar y mejorar la seguridad de los datos del titular de la tarjeta.

El objetivo es desarrollar, mejorar, difundir y asistir en la implantación de estándares de seguridad para las tarjetas de pago.

A través de PCI se pretende ayudar a las organizaciones a adoptar un enfoque proactivo en la protección de los datos de las tarjetas de los clientes. La aplicación del PCI no solo se centra en las instituciones financieras, sino también en comercios y proveedores de servicios.

## Que exige la normativa

Descripción general de los 12 requerimientos de PCI DSS:

### Cree y mantenga una red segura:

1. Proteja los datos con un Firewall cuya configuración se mantenga correctamente.
2. Nunca utilice valores por defecto en contraseñas y parámetros de seguridad.

### Proteja los datos de los titulares de tarjetas:

3. Proteja los datos almacenados de cada titular.
4. En las transmisiones de datos por redes públicas cifre la información sensible, como por ejemplo los datos de los titulares.

### Mantenga un Programa de Gestión de Vulnerabilidades:

5. Utilice un anti-virus permanentemente actualizado.
6. Desarrolle y mantenga sistemas y aplicaciones seguras.

### Despliegue medidas de control de acceso robustas:

7. Restrinja el acceso a los datos a quienes lo tengan atribuido por su actividad.
8. Asigne identificadores únicos a cada persona que disponga de acceso informático.
9. Restrinja el acceso físico a los datos de los titulares.

### Monitoree y compruebe las redes regularmente:

10. Registre y monitoree cualquier acceso a recursos de red y a datos de titulares.
11. Compruebe regularmente los sistemas y los procesos de seguridad.

### Mantenga una política de seguridad de la información:

12. Mantenga una política que contemple la seguridad de la información

## Noticia:

Una vez más **CLAI** y **AUTORIZA7®** se mantienen a la vanguardia en logros tecnológicos y de negocios para beneficio de nuestros clientes.

**AUTORIZA7®** es el primer Switch Transaccional en Latinoamérica certificado con la red PULSE para atención regional de clientes Dinners y Discover.

