2º Reunión: CICLO DE CAPACITACIÓN Y CONCIENTIZACIÓN EN CIBERSEGURIDAD DOCUMENTAL. CPCECABA, CABA, 2017.

Seguridad en las transacciones electrónicas.

Diego Sebastian Escobar.

CICLO DE CAPACITACIÓN Y CONCIENTIZACIÓN EN CIBERSEGURIDAD DOCUMENTAL

2º Reunión: Seguridad en las transacciones electrónicas

Exposición

Dr. C.P. y L.A. Diego Sebastián Escobar

Coordinación
Dra. C.P. Maria Cecilia Pavicich

consejo
Profesional de Ciencias Económicas de la Ciudad Autónoma de Buenos Aires

Los canales electrónicos

Los canales electrónicos que son utilizados en la república Argentina se encuentran definidos en la Comunicación A 4609 y A 5374 / 6017 del Banco Central.

- Cajeros Automáticos (ATM).
- Terminales de Autoservicio (TAS).
- Banca Móvil (BM).
- Banca Telefónica (BT).
- Banca por Internet (BI).
- Puntos de Venta (POS).
- Plataformas de pagos móviles (PPM)

Factores de autenticación de los usuarios

"Algo que sabe"	• Contraseña, dato personal, entre otros.
"Algo que tiene"	• Tarjeta TC/TD, Token, tarjeta de coordenadas.
"Algo que es"	• Características biométrica.

El impacto en los sistemas de registros contables

Sistema de Información Contable

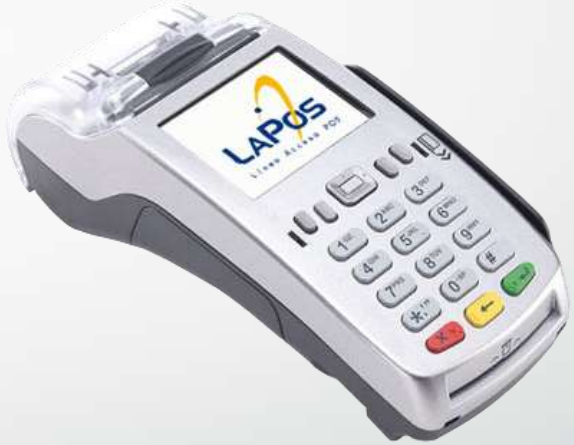
Las empresas que utilizan sistemas de cobro de tarjeta de crédito y débito tienen 2 posibilidades integrar las POS sistema de información:

- Implementar sus propios sistemas de POS.
- Contratar servicios de empresas proveedoras de POS, como POSNET (FIRST DATA) o LaPOS (Prisma).

Sistemas propios

Canales electrónicos

LAPOS
Línea Acceso POS



POSNET
Una compañía de First Data

¿Qué normas debería cumplir el SIC?

Para aquellas empresas que decidan **implementar un sistema propio** de cobro de tarjetas de crédito deben cumplir con las Normas PCI - DSS, desarrolladas por el consorcio de empresas emisoras.

¿Qué normas debería cumplir el SIC?

Norma de seguridad de datos de la PCI: descripción general de alto nivel

Desarrolle y mantenga redes y sistemas seguros.	**1.** Instalar y mantener una configuración de firewall para proteger los datos del titular de la tarjeta **2.** No utilizar contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores
Proteger los datos del titular de la tarjeta	**3.** Proteja los datos del titular de la tarjeta que fueron almacenados **4.** Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas
Mantener un programa de administración de vulnerabilidad	**5.** Utilizar y actualizar con regularidad los programas o software antivirus **6.** Desarrolle y mantenga sistemas y aplicaciones seguras
Implementar medidas sólidas de control de acceso	**7.** Restrinja el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa. **8.** Identifique y autentique el acceso a los componentes del sistema. **9.** Restringir el acceso físico a los datos del titular de la tarjeta
Supervisar y evaluar las redes con regularidad	**10.** Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas **11.** Pruebe con regularidad los sistemas y procesos de seguridad.
Mantener una política de seguridad de información	**12.** Mantenga una política que aborde la seguridad de la información para todo el personal.

¿Qué cuidados tener como usuarios en los canales electrónicos?

Ingeniería Social

Phishing

Conclusión

Proteger la información confidencial de la organización = Proteger el negocio

Utilización de las tecnologías para la seguridad
+
Educación de los usuarios

Proteger los activos de información del negocio

Cualquier incidente de seguridad podría impactar
- ✓ En la imagen de la organización
- ✓ En la confianza de los clientes
- ✓ En la continuidad del negocio
- ✓ En incumplimiento de normativas legales/regulatorias

La **seguridad corporativa** otorga un valor agregado

¡Muchas gracias!