Recomendaciones de seguridad para el comercio (Tomado Incocrédito www.incocredito.com.co)

1. **TRANSACCIONES PRESENCIALES:**

- En una transacción con tarjeta siempre debe haber presencia del titular de la tarjeta, la tarjeta de crédito y el documento de identidad.
- Solicite y verifique el documento de identidad y la tarjeta de crédito antes de la transacción.
- Revise las características de seguridad tanto del documento de identidad como de la tarjeta.
- Confronte los datos del documento de identidad contra los de la tarjeta.
- Valide en el comprobante diligenciado los 4 últimos números de la tarjeta, fecha de vencimiento, tipo de tarjeta, franquicia o marca.
- Verifique que la firma en el comprobante coincida con la firma registrada en el panel de la tarjeta.
- Verifique que el número de cédula en el comprobante coincida con el del documento de identidad.
- Cuando en su establecimiento se requiera el mantenimiento de los datafonos, tenga presente que sólo las personas autorizadas por Credibanco o Redeban Multicolor pueden tener acceso a la terminal, para lo cual se deben contactar a los números telefónicos autorizados para confirmar la identidad del funcionario.
- Lleve un control de las visitas realizadas para el mantenimiento de datafonos. No permita que personas extrañas manipulen o abran las terminales o que estas sean retiradas temporalmente del establecimiento así sea por corto tiempo.
- Mantenga al personal de su establecimiento capacitado.
- Verifique que el número realzado que aparece en el anverso de la tarjeta sea igual al registrado en bajo relieve en el reverso de la misma
- No retirar los sellos de seguridad del dispositivo
- Ingresar a www.incocredito.com.co para encontrar más información sobre prevención del fraude.

2. **VENTAS NO PRESENCIALES (INTERNET):**

- La página Web del comercio debe ser una página segura certificada por una empresa idónea y reconocida.
- La información del tarjeta habiente debe viajar por un canal dedicado (VPN) o Red privada virtual (Virtual Private Network).
- La información debe ser encriptada con software de alto nivel y reconocimiento, la norma PCI DSS exige la utilización de Triple DES o AES.
- Se recomienda certificarse con los sistemas de tarjetas para realizar transacciones seguras por Internet.
- Se sugiere hacer validaciones con el cliente vía telefónica.
- Se recomienda contar con un servicio de atención telefónica 7 x 24 y una línea nacional para atender las inquietudes del cliente.
- Es importante que en el establecimiento se tengan definidas políticas de facturación, cambios, reembolsos y cancelaciones.
- Es recomendable contar con antivirus para evitar la instalación de troyanos o virus que faciliten el robo de información.

3. RECOMENDACIONES EN SERVICIO DE DOMICILIOS

- Se recomienda asignar un datafono exclusivo por cada domiciliario.
- Desarrollar e implementar un proceso diario de validación del inventario de datafonos asignados al punto de venta.
- Garantizar la custodia de estos dispositivos en horarios no hábiles.

4. RECOMENDACIONES EN EL CONTROL DE LA INFORMACIÓN:

- La administración de la información de los tarjetahabientes debe estar en áreas seguras.
- Es importante realizar seguimiento estricto al manejo y control de información en servidores y equipos de cómputo.
- No se debe almacenar información Financiera de tarjetahabientes o bases de datos que puedan comprometer al comercio como punto de compromiso por fuga de información.
- Cumplir con estándares de seguridad información como PCI.

5. RECOMENDACIONES ANTE UN POSIBLE FRAUDE:

- Verifique la autenticidad de la tarjeta y el documento de identidad.
- Ante alguna irregularidad de aviso al jefe inmediato y/o personal de seguridad del almacén.
- Si tiene certeza absoluta de la irregularidad contacte al Centro de información de INCOCREDITO.
- Una vez confirmado el fraude INCOCREDITO coordinará con la autoridad la captura y judicialización.