Medidas de seguridad EN LAS TARJETAS DE CRÉDITO

ANIBAL GALARRETA*

En el Perú, el uso de las tarjetas de crédito se ha incrementado en un marco en el cual la industria viene aplicando medidas de seguridad que permiten minimizar potenciales casos de fraude. El presente artículo describe con fines de difusión las principales medidas adoptadas.

* Jefe de Proyecto de Información y Análisis Económico del BCRP.
anibal.galarreta@bcrp.gob.pe

EVOLUCIÓN DE LAS TARJETAS DE CRÉDITO

Este instrumento de pago registró una tendencia creciente en su uso por parte de la población. El número de tarjetas de crédito en situación activa de julio de 2015 respecto a julio de 2010 creció 30,7 por ciento, alcanzando los 8,0 millones[1] (ver Gráfico 1). Por su parte, el saldo de crédito de consumo con tarjeta de crédito tuvo un crecimiento de 117,4 por ciento en el mismo período, alcanzando los S/17 mil millones[2]. Dicho saldo representa un tercio del crédito de consumo en julio de 2015.

CANALES PARA EL PAGO CON TARJETA DE CRÉDITO

Usualmente, en una transacción de pago con tarjeta de crédito, el cliente entrega su tarjeta al comercio para que la procese vía el punto de venta, viajando la información de la tarjeta y la del pago al sistema procesador, el que se contacta con el banco emisor de la tarjeta para el proceso de autorización de la transacción, que luego de obtenida, se comunica al comercio para que acepte el pago (ver Gráfico 2).

Adicionalmente, la tarjeta se puede utilizar en canales distintos al punto de venta, como son el cajero automático, internet y los dispositivos móviles.

Cabe señalar que en los diversos canales, personas inescrupulosas pueden realizar acciones para llevar a cabo transacciones fraudulentas en perjuicio de los usuarios, como son la clonación, el cambiazo, el *phishing*, el malware y las llamadas y mensajes telefónicos (ver Gráfico 3).

A continuación se describen dichos tipos de fraude:

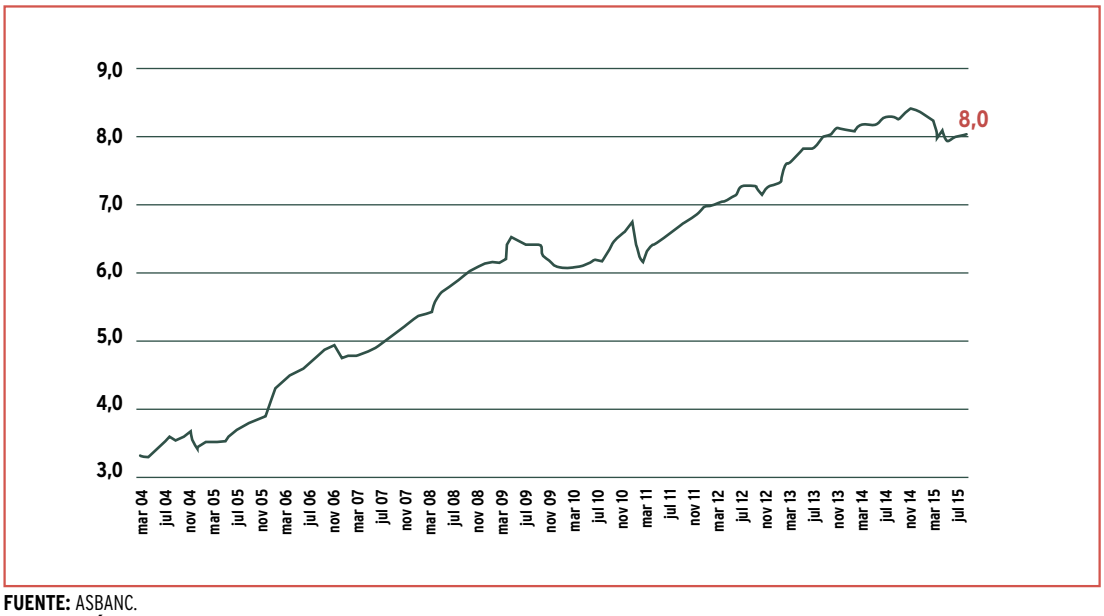
a) Clonación o *skimming*, con un *skimmer*[3], al realizar una transacción desde un punto de venta o un cajero automático se roban datos de la banda magnética de la tarjeta y con esa información se genera una tarjeta falsa. Para concretar el fraude también se debe falsificar la firma del usuario.

b) Cambiazo, un tercero, cambia o roba la tarjeta cuya clave ha observado y con ello realiza retiros de dinero desde cajeros automáticos a nombre del usuario.

c) *Phishing*, se envían correos con enlaces a páginas web falsas, usando el nombre de entidades financieras, para obtener datos personales y de la tarjeta. Las modalidades de *phishing* son: (1) páginas web, (2) formularios de correo electrónico y (3) redes sociales.

d) Malware, programa que se instala en la computadora del usuario, extrae sus datos y los envía automáticamente. Por lo general, se accede a estos programas desde páginas web vinculadas en correos falsos. Los principales tipos de malware son: (1) gusano, (2) virus y (3) troyano.

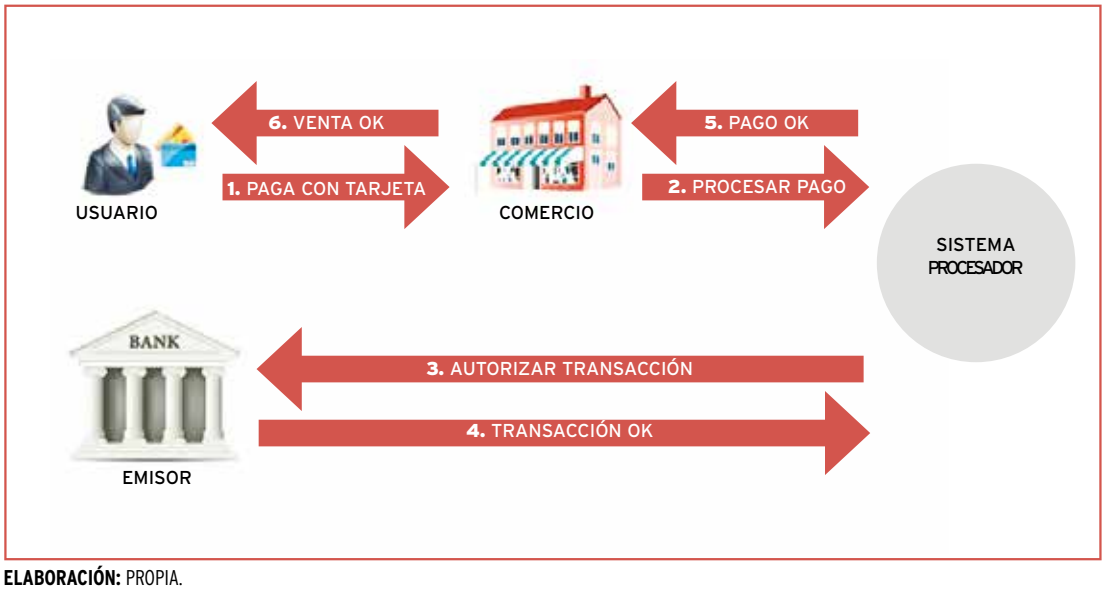
GRÁFICO 1 | **Tarjetas de crédito activas en bancos y financieras** (en millones)



FUENTE: ASBANC.
ELABORACIÓN: PROPIA.

1 SBS: Boletín Estadístico de Banca Múltiple y de Empresas Financieras al 31 de julio de 2015.
2 Notas de Estudios del BCRP N° 52 – 21 de agosto de 2015.
3 Dispositivo portátil de lectura y almacenamiento de datos.

GRÁFICO 2 Flujo de pago con tarjeta de crédito



ELABORACIÓN: PROPIA.

e) Llamadas y mensajes, el fraude a través de llamadas telefónicas se denomina *vishing*[4] y por mensajes de texto *smishing*. Consiste en contactar al usuario para obtener datos personales y de la tarjeta.

Frente a ello, se está aplicando diversas medidas de seguridad para mitigar la ocurrencia de fraudes en tarjetas de pago.

MEDIDAS DE SEGURIDAD EN LAS TARJETAS DE CRÉDITO

Las principales medidas de seguridad implementadas en nuestro mercado para minimizar la ocurrencia de potenciales fraudes son las siguientes:

a) **Uso de tarjetas de crédito con *chip***[5], es una medida efectiva debido a que la tecnología actual no permite la clonación del microprocesador y por ello reduce significativamente este tipo de fraude. Dicha medida se está aplicando por exigencia de las marcas[6]. Por su parte, los adquirientes vienen ofreciendo capacitación a los comercios para la lectura de estas tarjetas.

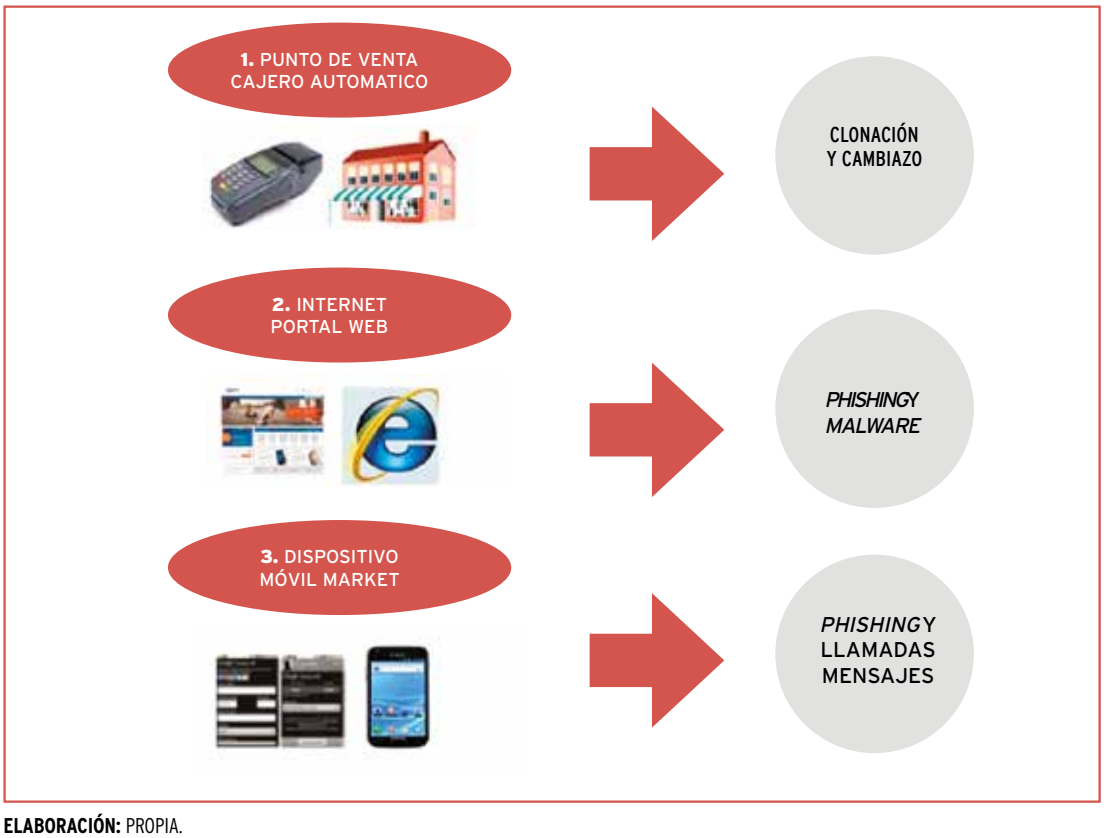
b) **Envío de correos electrónicos y mensajes de alerta**, se envían alertas a una cuenta de correo electrónico o número celular del titular de la tarjeta cada vez que se realiza una transacción. Estas alertas pueden personalizarse para ser activadas cuando la operación supere un monto predeterminado o cuando se realice fuera de alguna zona geográfica. Se está implementando esta medida, en algunos casos a solicitud del usuario, recibiendo éste un mensaje por correo electrónico informando el monto, comercio y fecha de la operación.

> **La industria** está aplicando medidas de seguridad para minimizar potenciales casos de fraude

c) **Bloqueo automático de tarjetas de crédito**, el titular de la cuenta programa el bloqueo automático de su tarjeta de acuerdo a parámetros que ha definido como activadores del bloqueo, tales como un límite de consumo, zona geográfica y hora de la operación. Algunos emisores están aplicando la medida a través de la verificación del consumo por parte del usuario.

4 Este concepto comprende el efecto del phishing pero aplicado a los sistemas de Voice over Internet Protocol (VoIP).
5 De acuerdo al estándar Europay, Mastercard, VISA (EMV).
6 Como por ejemplo, VISA Internacional.

GRÁFICO 3 | Tipos de fraude asociados a los canales



ELABORACIÓN: PROPIA.

d) **Contratación de seguro por eventos de fraude**, cubre eventos de fraude en las tarjetas de pago del titular. Estos seguros se vienen aplicando bajo diversas modalidades. Algunos emisores lo ofrecen como un seguro optativo que cubre todas las tarjetas de pago del usuario contra distintos tipos de fraude. El seguro puede tener cobertura nacional o internacional o proteger una parte o toda la línea de crédito y aplicarse solo a un número de eventos de fraude al año.

e) Mayor difusión de información sobre medidas de seguridad, el conocimiento sobre los riesgos y las medidas de seguridad para mitigarlos aporta a la toma de conciencia del usuario. Al utilizar cuidadosamente las tarjetas y datos personales, se reduce significativamente el riesgo potencial del instrumento de pago. Los emisores y adquirientes vienen informando sobre las medidas de seguridad y los riesgos potenciales a través de sus portales internet y otros medios.

f) Mejor verificación de los comercios al momento de realizar el cobro, la disposición y entrenamiento del personal que opera los puntos de venta en los comercios favorece la seguridad. Reconocer como falsos un DNI o la firma del usuario en el *voucher*, puede impedir que se concrete una operación fraudulenta. Los adquirientes están informando a los comercios sobre el buen uso del medio de pago. Asimismo, a través de líneas telefónicas se ofrece asistencia.

> **Es importante** conocer las medidas de seguridad existentes para mitigar potenciales acciones fraudulentas

CONCLUSIONES

Es importante para las personas, en un contexto en el que el uso de las tarjetas de crédito se está incrementando, conocer las medidas de seguridad existentes para mitigar potenciales acciones fraudulentas.