MEDIDAS DE SEGURIDAD PARA LOS USUARIOS DE TARJETA DE CRÉDITO Y DÉBITO

CARTILLA TEMÁTICA 408

INCORPORADAS EN LA TARJETA

- Reglas de seguridad definidas en el chip de las tarjetas.
- Procedimientos criptográficos sobre los datos críticos y claves almacenadas en el chip.
- Métodos de autenticación de datos.
- Mecanismos para aplicar instrucciones sobre el chip de las tarjetas en respuesta a una transacción en línea.

RESPECTO A LOS USUARIOS

- Entregar la tarjeta al titular o persona autorizada.
- Obligar cambiar la primera clave antes de realizar la primera operación.
- Permitir al usuario cambiar la clave o número secreto, las veces que lo requiera.
- Servicio de notificaciones para todos los usuarios para que se les informe de las operaciones realizadas con sus tarjetas inmediatamente después de ser registradas por la empresa.

MONITOREO Y REALIZACIÓN DE OPERACIONES

- Sistemas de monitoreo de operaciones.
- Análisis sistemático de la información histórica de las operaciones.
- Límites y controles en los diversos canales de atención.
- Requerir la presentación de DNI.
- En el caso de operaciones de retiro o disposición de efectivo, requerir la clave secreta del usuario.

SEGURIDAD DE LA INFORMACIÓN

- Configuración de cortafuegos, enrutadores y similares.
- Políticas para evitar el uso de clave secreta y parámetros de seguridad predeterminados.
- Políticas de almacenamiento, retención y eliminación de datos, y manejo de llaves criptográficas.
- Mecanismos de cifrado para la transmisión de los datos del usuario en redes públicas.
- Software y programas antivirus.
- Sistemas informáticos y aplicaciones seguras.
- Políticas que restrinjan el acceso a los datos de los usuarios solo al personal autorizado.
- Políticas de asignación de identificador único a cada persona que acceda a través de software a datos de usuarios.
- Controles de acceso físico para proteger los datos de los usuarios.
- Registrar y monitorear todos los accesos a los recursos de red y a los datos de los usuarios.
- Análisis de vulnerabilidades periódicos a la red interna y pruebas de penetración externas e internas.
- Lineamientos y procedimientos de seguridad de la información específicos.

EN NEGOCIOS AFILIADOS

- Procedimientos de aceptación de las operaciones, incluyendo la verificación de validez de la tarjeta, identificación del usuario y la firma de ser aplicable.
- No guardar o almacenar en bases de datos manuales o computarizadas la información de la tarjeta.
- Cumplir con los requerimientos de seguridad.

BASE LEGAL: **RESOLUCIÓN SBS N° 6523-2013, REGLAMENTO DE TARJETAS DE CRÉDITO.**

MEDIDAS DE SEGURIDAD PARA LOS USUARIOS DE TARJETAS DE CRÉDITO Y DÉBITO

MEDIDAS DE SEGURIDAD PARA LOS USUARIOS DE TARJETAS DE CRÉDITO Y DÉBITO

I. TARJETA DE CRÉDITO Y DÉBITO

1. RESOLUCIÓN SBS N° 6523-2013, REGLAMENTO DE TARJETAS DE CRÉDITO

Artículo 3.- Tarjeta de crédito

La tarjeta de crédito es un instrumento de pago que puede tener soporte físico o representación electrónica o digital y que está asociado a una (1) línea de crédito, otorgada por la empresa emisora. De acuerdo con lo establecido en el respectivo contrato, a través de la tarjeta de crédito, el titular (o usuario) puede realizar el pago por bienes, servicios u obligaciones, así como hacer uso de los servicios adicionales conforme a lo establecido en este reglamento.

Artículo 4.- Tarjeta de débito

La tarjeta de débito es un instrumento de pago que puede tener soporte físico o representación electrónica o digital, que permite realizar operaciones con cargo a depósitos previamente constituidos en la empresa emisora. A través de la tarjeta de débito el titular puede realizar el pago de bienes, servicios u obligaciones, efectuar el retiro de efectivo o realizar transferencias, a través de los canales puestos a disposición por la empresa emisora u otros servicios asociados, dentro de los límites y condiciones pactados.

II. MEDIDAS DE SEGURIDAD

1. RESOLUCIÓN SBS N° 6523-2013, REGLAMENTO DE TARJETAS DE CRÉDITO

Artículo 15.- Medidas de seguridad incorporadas en las tarjetas

Las tarjetas deberán contar con un circuito integrado o chip que permita almacenar y procesar la información del usuario y sus operaciones, cumpliendo estándares internacionales de interoperabilidad para el uso y verificación de las tarjetas, así como para la autenticación de pagos; para lo cual deberá cumplirse como mínimo con los requisitos de seguridad establecidos en el estándar EMV, emitido por EMVCo. Al respecto, las empresas deberán aplicar, entre otras, las siguientes medidas:

1. Reglas de seguridad definidas en el chip de las tarjetas, que deben ser utilizadas para verificar la autenticidad de la tarjeta, validar la identidad del usuario mediante el uso de una clave o firma u otros mecanismos de autenticación.
2. Aplicar procedimientos criptográficos sobre los datos críticos y claves almacenadas en el chip de las tarjetas, así como sobre aquellos existentes en los mensajes intercambiados entre las tarjetas, los terminales de punto de venta, los cajeros automáticos y las empresas emisoras.
3. En caso las empresas emisoras permitan la autorización de operaciones fuera de línea, deben aplicar un método de autenticación de datos que brinde adecuadas condiciones de seguridad, sin afectar la calidad y el rendimiento del servicio provisto al usuario. Dichas

operaciones se realizarán conforme a los límites y condiciones pactadas con el cliente, que incluirán por ejemplo límites al número de operaciones consecutivas procesadas fuera de línea.

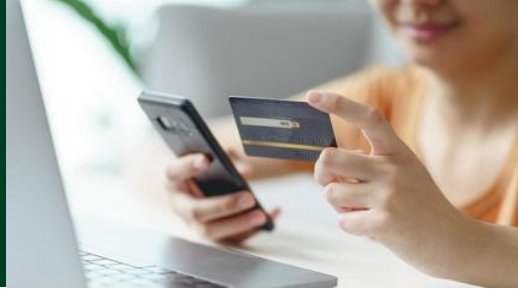
4. Disponer de mecanismos para aplicar instrucciones sobre el chip de las tarjetas en respuesta a una transacción en línea, a fin de modificar los límites establecidos según perfiles de riesgo, así como bloquear o deshabilitar aquellas tarjetas que hayan sido extraviadas o sustraídas.

El procesamiento de transacciones en línea haciendo uso del chip de las tarjetas u otros mecanismos debe incluir como mínimo la solicitud de autorización realizada, la respuesta a la solicitud, la cual debe ser generada desde el sistema autorizador de la empresa, así como la indicación de haber aprobado o declinado la transacción generada; ello salvo en caso de excepción previsto contractualmente, donde corresponda la aprobación a la marca. Cuando la operación sea realizada haciendo uso del chip u otro mecanismo sin contacto, la autenticación de la tarjeta debe utilizar criptografía dinámica, de manera que pueda verificarse que no hubo alteración de la transacción entre la tarjeta y el terminal. Cuando se utilice otro soporte distinto a la tarjeta física, además de asegurar mecanismos de autenticación, debe evitar exponer el número de la tarjeta.

Artículo 16.- Medidas de seguridad respecto a los usuarios

Las empresas deben adoptar, como mínimo, las siguientes medidas de seguridad con respecto a los usuarios:

1. Entregar la tarjeta y, en caso corresponda, las tarjetas adicionales al titular, excepto cuando este haya instruido en forma expresa que se entreguen a una persona distinta, previa verificación de su identidad y dejando constancia de su recepción.
2. En caso la empresa genere la primera clave o número secreto de la tarjeta, esta deberá ser entregada según las condiciones del numeral anterior, obligando su cambio antes de realizar la primera operación que requiera el uso de dicha clave.
3. En caso de que se utilice la clave como método de autenticación, permitir que el usuario pueda cambiar dicha clave o número secreto, las veces que lo requiera.
4. Para las operaciones que se realicen con cargo a la línea de crédito o a los depósitos previamente constituidos, la empresa debe habilitar y brindar un servicio de notificaciones para todos los usuarios para que se les informe de las operaciones realizadas con sus tarjetas inmediatamente después de ser registradas por la empresa, mediante la utilización de alguno de los siguientes mecanismo de comunicación directa tales como mensajes de texto, correo electrónico, llamadas, entre otros, que pueden ser pactados con los titulares; debiendo este servicio estar activo desde el momento de la contratación del producto. Para este servicio, las empresas pueden establecer mecanismos a través de los cuales los usuarios puedan configurar o limitar las



notificaciones sobre la base de umbrales o variables como montos mínimos, entre otros. Los titulares pueden solicitar la habilitación o deshabilitación de este servicio, en cualquier momento, a través de los mecanismos establecidos por las empresas, los cuales no podrán ser más complejos que los ofrecidos al momento de la celebración del contrato.

5. Poner a disposición de los usuarios, la posibilidad de comunicar a la empresa que realizarán operaciones con su tarjeta desde el extranjero, antes de la realización de estas operaciones.
6. En los casos de micropago, las operaciones deben encontrarse sujetas a un monto máximo.

Artículo 17.- Medidas de seguridad respecto al monitoreo y realización de las operaciones

Las empresas deben adoptar como mínimo las siguientes medidas de seguridad con respecto a las operaciones con tarjetas que realizan los usuarios:

1. Contar con sistemas de monitoreo de operaciones, que tengan como objetivo detectar aquellas operaciones que no corresponden al comportamiento habitual de consumo del usuario.
2. Implementar procedimientos complementarios para gestionar las alertas generadas por el sistema de monitoreo de operaciones.
3. Identificar patrones de fraude, mediante el análisis sistemático de la información histórica de las operaciones, los que deberán incorporarse al sistema de monitoreo de operaciones.
4. Establecer límites y controles en los diversos canales de atención, que permitan mitigar las pérdidas por fraude.
5. Requerir al usuario la presentación de un documento oficial de identidad, cuando sea aplicable, o utilizar un mecanismo de autenticación de múltiple factor. La Superintendencia podrá establecer, mediante oficio múltiple, montos mínimos a partir de los cuales se exija la presentación de un documento oficial de identidad.
6. En el caso de operaciones de retiro o disposición de efectivo, según corresponda, u otras con finalidad informativa sobre las operaciones realizadas u otra información similar, deberá requerirse la clave secreta del usuario, en cada oportunidad, sin importar el canal utilizado para tal efecto.

Artículo 18.- Medidas en materia de seguridad de la información

Son exigibles, a las empresas, las normas vigentes emitidas por la Superintendencia sobre gestión de seguridad de la información y de continuidad del negocio.

Asimismo, en torno al almacenamiento, procesamiento y transmisión de los datos de las tarjetas que emitan, las empresas deberán implementar los siguientes controles específicos de seguridad:

1. Implementar y mantener la configuración de cortafuegos o firewalls, enrutadores y equipos similares que componen la red interna, adoptando configuraciones estandarizadas y restringiendo permisos para evitar accesos no autorizados.

2. Implementar políticas para evitar el uso de clave secreta y parámetros de seguridad predeterminados provistos por los proveedores de servicios de tecnología.
3. Implementar políticas de almacenamiento, retención y de eliminación de datos, así como para el manejo de llaves criptográficas, que permitan limitar la cantidad de datos a almacenar y el tiempo de retención a lo estrictamente necesario según requerimientos legales, regulatorios y de negocio.
4. Implementar mecanismos de cifrado para la transmisión de los datos del usuario en redes públicas.
5. Implementar y actualizar software y programas antivirus en computadores y servidores.
6. Mantener sistemas informáticos y aplicaciones seguras; para el caso de software provisto por terceros, establecer procedimientos para identificar vulnerabilidades y aplicar actualizaciones; para el caso de desarrollos de sistemas propios, adoptar prácticas que permitan reducir las vulnerabilidades de seguridad de dichos sistemas.
7. Implementar políticas que restrinjan el acceso a los datos de los usuarios solo al personal autorizado, reduciéndolo al estrictamente necesario.
8. Implementar políticas de asignación de un identificador único a cada persona que acceda a través de software a los datos de los usuarios.
9. Implementar controles de acceso físico para proteger los datos de los usuarios, restringiéndolo únicamente a personal autorizado, propio o de terceros.
10. Registrar y monitorear todos los accesos a los recursos de red y a los datos de los usuarios.
11. Efectuar análisis de vulnerabilidades periódicos a la red interna y pruebas de penetración externas e internas, así también luego de cambios significativos en la red o sistemas informáticos.
12. Implementar lineamientos y procedimientos de seguridad de la información específicos, incluyendo un programa formal de capacitación en seguridad de la información, en función a las responsabilidades del personal, controles aplicables a los proveedores de servicios y un plan de respuesta a eventos de violación de seguridad que sea probado anualmente.

Las mencionadas implementaciones deberán efectuarse siguiendo las recomendaciones técnicas del estándar de la industria de tarjetas, PCI DSS o equivalentes

Artículo 19.- Medidas de seguridad en los negocios afiliados

Las empresas deben adoptar las medidas de seguridad apropiadas para determinar la validez de la tarjeta, así como para dar cumplimiento a las condiciones de uso señalados en el Reglamento, por parte de los operadores o establecimientos afiliados.

En ese sentido, cuando las empresas suscriban contratos con los operadores o establecimientos afiliados, deberán asegurarse de incluir como obligaciones de estos, de ser el caso, los siguientes aspectos:

1. Contar con procedimientos de aceptación de las operaciones,

incluyendo entre otros la verificación de la validez de la tarjeta, la identidad del usuario, y la firma en caso de ser aplicable.
2. No guardar o almacenar en bases de datos manuales o computarizadas la información de la tarjeta, más allá de utilizarla para solicitar la autorización de una operación.
3. Cumplir con los requerimientos de seguridad del presente Reglamento, en lo que les sea aplicable.

El cumplimiento de lo dispuesto en el presente artículo no exime de responsabilidad a la empresa por las pérdidas generadas en las operaciones no reconocidas que se hayan realizado bajo alguno de los supuestos establecidos en el segundo párrafo del artículo 23 del Reglamento.

(…)

Artículo 21.- Mecanismo de comunicación a disposición de los usuarios

Las empresas deberán contar con infraestructura y sistemas de atención, propios o de terceros, que permitan a los usuarios comunicar el extravío o sustracción de la tarjeta o de su información, los cargos indebidos y las operaciones que los usuarios no reconozcan. Dicha infraestructura deberá encontrarse disponible las veinticuatro (24) horas del día, todos los días del año.

Se deberán registrar las comunicaciones de los usuarios, de tal forma que sea posible acreditar de manera fehaciente su fecha, hora y contenido. Por cada comunicación, se deberá generar un código de registro a ser informado al usuario como constancia de la recepción de dicha comunicación. Asimismo, se deberá enviar al titular de las tarjetas una copia del registro de la comunicación efectuada, a través de medios físicos o electrónicos, según elección del propio usuario.

La información referida a los mecanismos de comunicación establecidos por la empresa, para dar cumplimiento a lo dispuesto en los párrafos precedentes, deberá encontrarse publicada en la parte inicial de la página web de la empresa, en las oficinas y en cualquier otro medio a criterio de la empresa, siempre que sea fácilmente identificable.

Lo expuesto en el presente artículo resulta aplicable, sin perjuicio de las demás exigencias establecidas por el marco normativo vigente en materia de atención de reclamos.

Artículo 22.- Seguimiento de operaciones que pueden corresponder a patrones de fraude

Las empresas deben contar con procedimientos para el seguimiento de operaciones que puedan corresponder a patrones de fraude, los cuales deben incluir por lo menos los siguientes aspectos:

1. Mecanismos para la comunicación inmediata al usuario sobre las posibles operaciones de fraude.
2. Acciones para proceder con el bloqueo temporal o la cancelación definitiva de la tarjeta, en caso sea necesario.

#ContribuyendoAlConocimientoDelPersonalPolicial