ANEXO 5

MEDIDAS DE SEGURIDAD

A. MEDIDAS DE SEGURIDAD PARA LA TRANSMISIÓN, ALMACENAMIENTO Y PROCESAMIENTO DE LA INFORMACIÓN

Los Emisores y Adquirentes distintos a las Instituciones de Crédito, y Agregadores, para la prestación de servicios que correspondan a su naturaleza, deberán implementar medidas o mecanismos de seguridad en la transmisión, almacenamiento y procesamiento de información, a fin de que esta no sea conocida por terceros. Para tales efectos, los Participantes en la Red de Pagos con Tarjeta deberán cumplir con lo siguiente:

1. Asegurar que las TPV y demás dispositivos utilizados para los Pagos con Tarjetas cuenten con lectores que permitan obtener la información de las Tarjetas del circuito integrado o chip cuando estas cuenten con dichos circuitos.

2. Cifrar los mensajes o utilizar medios de comunicación cifrada, en la transmisión de la información sensible (información personal del Tarjetahabiente que contenga nombres, en conjunto con números de Tarjetas, números de cuenta, límites de crédito, saldos o información de Autenticación) de las Tarjetas y sus operaciones, desde el dispositivo donde se origine la transacción hasta la recepción para su autorización por parte de los Emisores.

   Para efectos de lo anterior, deberán utilizar tecnologías que manejen esquemas de cifrado y que requieran el uso de llaves criptográficas para mitigar el riesgo de que terceros accedan a la información de que se trate.

3. Asegurarse que las llaves criptográficas y el proceso de cifrado y descifrado se encuentren instalados en dispositivos de alta seguridad, tales como los denominados HSM (Hardware Security Module), los cuales deberán contar con prácticas de administración que eviten el acceso no autorizado y la divulgación de la información que contienen.

4. Contar con controles para el acceso a las bases de datos y archivos correspondientes a las operaciones y servicios efectuados a través de las Redes de Medios de Pagos, aun cuando dichas bases de datos y archivos residan en medios de almacenamiento de respaldo. Para efectos de lo anterior, deberán ajustarse a lo siguiente:

   a. El acceso a las bases de datos y archivos estará permitido exclusivamente a las personas expresamente autorizadas por el Participante, en función de las actividades que realizan. Al otorgarse dichos accesos, deberá dejarse constancia de tal circunstancia y señalar los propósitos y el periodo al que se limitan los accesos.

   b. Tratándose de accesos que se realicen en forma remota, deberán utilizarse mecanismos de cifrado en las comunicaciones.

   c. Deberán contar con procedimientos seguros de destrucción de los medios de almacenamiento de las bases de datos y archivos que contengan información sensible de los Tarjetahabientes, que prevengan su restauración a través de cualquier mecanismo o dispositivo.

   d. Deberán desarrollar políticas relacionadas con el uso y almacenamiento de información que se transmita y reciba, derivado de los servicios que correspondan, estando obligados a verificar el cumplimiento de sus políticas por parte de sus proveedores y afiliados.

5. Generar registros, bitácoras y huellas de auditoría de las operaciones y servicios realizados en los que conste cuando menos la fecha y hora, datos de la Tarjeta, y demás información que permita identificar el mayor número de elementos involucrados en el acceso y operación de los Pagos con Tarjeta, así como los datos de identificación de la TPV utilizada por el Tarjetahabiente para realizar la operación de que se trate. Dichos registros, bitácoras y huellas de auditoría estarán sujetos a la supervisión de las Autoridades, quienes podrán ordenar correcciones en todo momento.

6. Almacenar la información involucrada en los servicios de procesamiento de Pagos con Tarjetas, incluyendo los registros, bitácoras y huellas de auditoría mencionados en el numeral 5 anterior, de forma segura por un periodo mínimo de ciento ochenta días naturales contados a partir de su

generación y contemplar mecanismos para evitar su alteración, así como mantener procedimientos de control interno para su acceso y disponibilidad. Lo anterior sin perjuicio de lo establecido en las disposiciones que les resulten aplicables.

7. Realizar revisiones de seguridad, enfocadas a verificar la suficiencia en los controles aplicables a la infraestructura de procesamiento y telecomunicaciones para los Pagos con Tarjetas. Las revisiones deberán realizarse al menos de forma anual, o bien, cuando se presenten cambios significativos a dicha infraestructura, debiendo comprender lo siguiente:

    a. Mecanismos de autenticación de los Tarjetahabientes;

    b. Configuración y controles de acceso a la infraestructura de procesamiento y telecomunicaciones;

    c. Actualizaciones requeridas para los sistemas operativos, certificados, llaves y software en general;

    d. Análisis de vulnerabilidades sobre la infraestructura de procesamiento y telecomunicaciones, y sistemas;

    e. Identificación de posibles modificaciones no autorizadas al software original;

    f. Identificación de posibles herramientas o procedimientos que permitan conocer la información de las Tarjetas o de los Tarjetahabientes, así como de cualquier información que de manera directa o indirecta pudiera obtenerse para realizar Pagos con Tarjetas sin conocimiento ni consentimiento del Tarjetahabiente;

    g. Análisis metódico de la infraestructura, certificados, llaves y software en general, con la finalidad de detectar errores, funcionalidad no autorizada o cualquier código que ponga o pueda poner en riesgo la información de los Tarjetahabientes.

8. Contar con medidas preventivas, de detección, disuasivas y procedimientos de respuesta a incidentes de seguridad, controles y medidas de seguridad informática para mitigar amenazas y vulnerabilidades relacionadas con los servicios proporcionados en las Redes de Medios, que puedan afectar a los Participantes en la Red de Pagos con Tarjeta o Tarjetahabientes. Las referidas medidas y procedimientos, deberán ser evaluadas por auditoría internas o externas para determinar su efectividad y, en su caso, realizar las actualizaciones correspondientes. En caso de que se detecte la existencia de vulnerabilidades y riesgos asociados a los servicios mencionados, deberán tomarse medidas de forma oportuna previniendo que los Participantes en la Red de Pagos con Tarjeta o Tarjetahabientes puedan verse afectados.

9. En caso de que la información sensible sea extraída, extraviada o supongan o sospechen de algún incidente que involucre accesos no autorizados a dicha información, deberán:

    a. Enviar por escrito a la Dirección General responsable de su supervisión en la CNBV dentro de los cinco días naturales siguientes al evento de que se trate, la información que se contiene en el Apartado B del Anexo 5 de las presentes disposiciones.

    b. Llevar a cabo una investigación inmediata para determinar si la información ha sido o puede ser mal utilizada, y en este caso deberán notificar esta situación, en los siguientes tres días hábiles, a sus Tarjetahabientes y Participantes en la Red de Pagos con Tarjeta involucrados afectados a fin de prevenirlos de los riesgos derivados del mal uso de la información que haya sido extraída, extraviada o comprometida, debiendo informarle las medidas que deberán tomar. Asimismo, deberán enviar a la Dirección General responsable de su supervisión en la CNBV el resultado de dicha investigación en un plazo no mayor a cinco días naturales posteriores a su conclusión.

B. REPORTE DE EVENTOS DE PERDIDA DE INFORMACIÓN ADMINISTRADA, TRANSMITIDA O PROCESADA POR LOS EMISORES Y ADQUIRENTES DISTINTOS A LAS INSTITUCIONES DE CRÉDITO, Y AGREGADORES

I. Información del Participante

1. Nombre del Participante

2. Dirección de la(s) oficinas(s) o establecimiento(s) donde ocurrió el incidente de seguridad informática

   2.1. Ciudad

   2.2. Estado

   2.3. Código Postal

3. ¿La información involucrada era administrada por terceros? [Sí] [No]

   En caso afirmativo:

   3.1. Nombre del proveedor

   3.2. Dirección del proveedor

   3.3. Contacto

II. Información del incidente de seguridad informática

1. Breve descripción del incidente de seguridad informática
2. Información comprometida

Información personal del Tarjetahabiente		En conjunto con:		
Nombres			Número de tarjetas de débito y crédito	
Domicilios			Números de cuenta	
Teléfonos			Contraseñas o Números de Identificación Personal	
Direcciones de correo electrónico			Límites de crédito	
Otro:_____			Saldos	
			Otro:	

3. Número de Tarjetas afectadas. Especificar el número de Tarjetas que están bloqueadas o suspendidas:

Número de Tarjetas afectadas	Número de Tarjetas afectadas bloqueadas o suspendidas	Comentarios

Anexar al reporte el desagregado de las Tarjetas afectadas de manera digital conforme se indica en el siguiente cuadro:

	Número de Tarjeta afectada	Estado de la Tarjeta afectada (bloqueada, suspendida, activa)	Comentarios

4. Fecha o periodo en que ocurrió el incidente de seguridad informática
5. Monto total en pesos conocido o estimado involucrado en el incidente de seguridad informática, en su caso
6. Clasificación del incidente de seguridad informática:

   a. Intrusión en equipos de cómputo [ ]

b. Tarjetas de crédito [ ]

c. Tarjetas de débito [ ]

d. Robo de identidad [ ]

e. Robo de bases de datos [ ]

f. Otros [ ]

7. Monto del daño en pesos, en su caso
8. Monto recuperado en pesos, en su caso
9. ¿Se ha dado a conocer el incidente de seguridad informática a alguna autoridad local o federal?

   [Sí] [No]

   En caso afirmativo:

   ¿A qué autoridad?

   ¿En qué fecha?

III. Contacto en el Participante

1. Nombre de la persona que está facultada para dar información a la Autoridad
2. Puesto desempeñado
3. Teléfono
4. Correo electrónico

_____