EL COMITÉ DE NORMAS DEL BANCO CENTRAL DE RESERVA DE EL SALVADOR,

CONSIDERANDO:

I. Que el artículo 2, inciso segundo de la Ley de Supervisión y Regulación del Sistema Financiero, establece que para el buen funcionamiento del Sistema de Supervisión y Regulación Financiera se requiere que los integrantes del sistema financiero y demás supervisados cumplan con las regulaciones vigentes y la adopción de los más altos estándares de conducta en el desarrollo de sus negocios, actos y operaciones, de conformidad a lo establecido en la referida Ley, en las demás leyes aplicables, en los reglamentos y en las normas técnicas que se dicten para tal efecto.

II. Que el artículo 7 de la Ley de Supervisión y Regulación del Sistema Financiero, establece las entidades que están sujetas a la supervisión de la Superintendencia del Sistema Financiero.

III. Que el artículo 35, literales d) y g) de la Ley de Supervisión y Regulación del Sistema Financiero, establece que los directores, gerentes y demás funcionarios que ostenten cargos de dirección o administración en los integrantes del sistema financiero, están obligados a cumplir y velar porque las entidades adopten y actualicen políticas y mecanismos para la gestión de riesgos, debiendo entre otras acciones, identificarlos, evaluarlos, mitigarlos y revelarlos acordes a las mejores prácticas internacionales. En dichas políticas se deberán incluir las medidas que se adoptarán para prevenir posibles incumplimientos a requerimientos regulatorios y las que adoptarán en el evento de que haya incurrido en ellos, debiendo definir en ambas situaciones los parámetros que orientarán la actuación y los responsables de implementarlas. Asimismo, deben velar porque las entidades cumplan con un eficiente funcionamiento de los sistemas de registro, tratamiento, almacenamiento, transmisión, producción, seguridad y control de los flujos de información.

IV. Que el artículo 56, literal l) de la Ley de Bancos, establece que los bancos podrán celebrar operaciones y prestar servicios con el público mediante el uso de equipos y sistemas automatizados, estableciendo en los contratos respectivos las bases para determinar las operaciones y servicios cuya prestación se pacte; los medios de identificación del usuario y las responsabilidades correspondientes a su uso; y los medios por los que se hagan constar la creación, transmisión, modificación o extinción de derechos y obligaciones inherentes a las operaciones y servicios de que se trate. Cuando estas operaciones se realicen mediante contratos de adhesión, los modelos de dichos contratos deberán ser previamente depositados en la Superintendencia, quien podrá, mediante decisión fundamentada, en un plazo no mayor a treinta días a partir de la fecha del depósito del modelo, requerir los cambios

necesarios, cuando contengan cláusulas que se opongan a la legislación o cuando se consideren violatorios a los derechos del cliente. En todo caso el Banco estará obligado a explicar al cliente las implicaciones del contrato, previo a su suscripción.

V. Que el artículo 63 de la Ley de Bancos y el artículo 41 de la Ley de Bancos Cooperativos y Sociedades de Ahorro y Crédito establecen que los bancos y los bancos cooperativos, respectivamente, deberán elaborar e implantar políticas y sistemas de control que les permitan manejar adecuadamente sus riesgos financieros y operacionales.

VI. Que el artículo 155 de la Ley de Bancos Cooperativos y Sociedades de Ahorro y Crédito establece que las Sociedades de Ahorro y Crédito se sujetarán a las disposiciones de la Ley de Bancos, en los términos ahí señalados, siendo aplicable lo establecido en el artículo 63 de la Ley de Bancos.

VII. Que el artículo 99 de la Ley de Supervisión y Regulación del Sistema Financiero establece que, el Banco Central de Reserva en virtud de dicha Ley, es la institución responsable de la aprobación del marco normativo técnico que debe dictarse de conformidad a esta Ley y demás leyes que regulan a los supervisados. En el cumplimiento de esta responsabilidad, el Banco Central de Reserva deberá velar por que el marco normativo aplicable al sistema financiero se revise periódicamente procurando su actualización oportuna.

VIII. Que para acercar los servicios financieros a las personas, se vuelve necesario la penetración de la banca por medio de los canales digitales, lo que permite una sostenida adopción de nuevos esquemas de pago, los cuales constituyen un medio dinámico y novedoso para las personas que realizan operaciones en el sistema financiero, volviéndose un complemento de los canales que utilizan instrumentos tradicionales.

IX. Que es necesario contar con normas técnicas que establezcan las condiciones y requisitos que las instituciones financieras deberán observar para realizar operaciones y prestar sus servicios por medio de canales digitales, en concordancia con las mejores prácticas internacionales y las características específicas del mercado salvadoreño.

POR TANTO,

en virtud de las facultades normativas que le confiere el artículo 99 de la Ley de Supervisión y Regulación del Sistema Financiero,

ACUERDA, emitir las siguientes:

NORMAS TÉCNICAS SOBRE MEDIDAS DE CIBERSEGURIDAD EN CANALES DIGITALES

CAPÍTULO I
OBJETO, SUJETOS Y TÉRMINOS

Objeto

Art. 1.- El objeto de las presentes Normas es regular las medidas de ciberseguridad de las entidades financieras, por medio de los cuales se recopila, procesa, transmite y se almacena la información de los productos y servicios financieros que las referidas entidades ofrecen a sus clientes en canales digitales.

Asimismo, los términos utilizados en las presentes Normas tendrán el mismo significado establecido en las "Normas Técnicas para la Gestión de la Seguridad de la Información" (NRP-23).

Sujetos

Art. 2.- Los sujetos obligados al cumplimiento de las disposiciones establecidas en las presentes Normas son:

a) Los bancos constituidos en El Salvador;
b) Las sucursales de bancos extranjeros establecidas en El Salvador;
c) Las sociedades de ahorro y crédito;
d) Los bancos cooperativos; y
e) Las federaciones conformadas por bancos cooperativos y también por sociedades de ahorro y crédito regulados por la Ley de Bancos Cooperativos y Sociedades de Ahorro y Crédito.

Términos

Art. 3.- Para efectos de las presentes Normas, los términos que se indican a continuación tienen el significado siguiente:

a) **Afiliación o suscripción:** incorporación de productos y servicios financieros, por parte del cliente, para efectos de realizar operaciones o transacciones en canales digitales;
b) **Autenticación:** conjunto de técnicas y procedimientos tecnológicos utilizados para verificar la identidad de un usuario de canales digitales (1);
c) **Autenticación dinámica:** método de autenticación, que consiste en generar un código para un medio electrónico de pago, diferente en cada transacción, y firmarlo con su clave privada;
d) **Autenticación estática:** método que consiste en generar un código para un medio

electrónico de pago, en la fase de personalización de este, que se graba en el chip del mismo y no cambia nunca. Puede ser validado por un terminal;

e) **Banca Móvil:** canal digital que utiliza un dispositivo móvil para tener acceso a servicios y transacciones financieras asociados a cuentas de depósito, líneas de crédito o cuentas de ahorro con requisitos simplificados;

f) **Banca por Internet:** canal digital asociado a cuentas de depósito, líneas de crédito o cuentas de ahorro con requisitos simplificados, que utiliza un portal transaccional para tener acceso a servicios y transacciones financieras;

g) **Banca Telefónica:** canal digital asociado a cuentas de depósitos, líneas de crédito o cuentas de ahorro con requisitos simplificados, que utiliza un dispositivo telefónico para tener acceso a servicios y transacciones financieras a través de llamadas a los centros de atención telefónica;

h) **Canal(es) digital(es):** medio que permite la realización de transacciones, la prestación de servicios financieros y el intercambio de información, tales como cajeros automáticos, puntos de ventas (POS, por sus siglas en inglés), banca telefónica, Respuesta de Voz Interactiva (IVR, por sus siglas en inglés), banca por Internet, banca móvil, entre otros;

i) **Clave de Acceso (PIN):** número de identificación personal que se utiliza para acceder a servicios y operaciones financieras por medio de canales digitales;

j) **Claves dinámicas:** son claves criptográficas de un solo uso, formadas a través de una secuencia aleatoria;

k) **Cliente:** persona natural o jurídica que mantiene una relación contractual con la Entidad para la prestación de una o varias operaciones pasivas o activas;

l) **Contraseña o clave:** cadena de caracteres protegida que se utiliza para autenticar la identidad de un usuario para autorizar el acceso a la utilización de canales digitales;

m) **Dato sensible:** datos con carácter confidencial del cliente o usuario de la banca electrónica, tales como: número de cuenta; número de identificación personal; claves del cliente; número de la tarjeta; código de seguridad de la tarjeta;

n) **Desafiliación:** proceso mediante el cual los clientes solicitan a las entidades desincorporar los productos y servicios ofrecidos por éstas, a través de los canales digitales;

o) **Dispositivos de autoservicio:** equipos electrónicos ofrecidos a los clientes para realizar operaciones bancarias que no involucran dinero en efectivo, tales como kioskos, POS, entre otros;

p) **Entidad(es):** sujetos obligados al cumplimiento de las presentes Normas de acuerdo al artículo 2 de las mismas;

q) **Factor adicional:** es el segundo factor o grupo de factores de autenticación que se debe requerir al cliente;

r) **Factor de autenticación:** información utilizada para verificar la identidad de un servicio o una persona;

s) **Factor base:** es el factor mínimo requerido para realizar la autenticación inicial del

cliente;

t) **Identificación:** validación de la identidad del cliente para el uso de canales digitales, mediante la utilización de datos e información que conozca tanto la entidad como el cliente;

u) **Inteligencia de amenazas:** Información sobre amenazas que ha sido agregada, transformada, analizada, interpretada o enriquecida para proporcionar el contexto necesario para los procesos de toma de decisiones; (1)

v) **IVR:** (Respuesta de voz interactiva, por sus siglas en inglés) es un sistema telefónico que es capaz de recibir una llamada e interactuar con el humano a través de grabaciones de voz y el reconocimiento de respuestas simples; (1)

w) **Derogado**; (1)

x) **Medio de comunicación electrónica:** medio electrónico utilizado para la transmisión de mensajes desde la entidad hacia el cliente, o viceversa; (1)

y) **No repudio:** método de seguridad que permite probar la participación de las partes en una comunicación, contemplándose estos 2 aspectos siguientes:

   i. **No repudio en origen:** el emisor no puede negar que lo envió porque el destinatario tiene pruebas del envío; y
   ii. **No repudio en destino:** el receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción.

   El origen o recepción de un mensaje específico debe ser verificable por parte de un tercero de confianza; (1)

z) **Perfil transaccional:** conjunto de características asociadas al comportamiento transaccional de un cliente, de acuerdo a los análisis sistematizados realizados por la entidad, para proteger a sus clientes; (1)

aa) **Programaciones de pago:** es la autorización por parte del cliente para el débito automático en sus cuentas bancarias o autorización de cargos en sus tarjetas de crédito; (1)

bb) **Superintendencia:** Superintendencia del Sistema Financiero; (1)

cc) **Token:** dispositivo electrónico utilizado para facilitar el proceso de autenticación. Puede ser utilizado para la generación de contraseñas de un solo uso; así como, para almacenar contraseñas, firmas electrónicas o datos biométricos de la persona; y (1)

dd) **Transacciones:** servicios y operaciones financieras realizadas por medio de canales digitales. (1)

CAPÍTULO II
SOBRE LA CIBERSEGURIDAD EN LOS SISTEMAS INFORMÁTICOS

Medidas de ciberseguridad

Art. 4.- Las entidades deberán implementar o actualizar las herramientas y mecanismos para monitorear redes y demás infraestructura tecnológica que permita detectar

oportunamente eventos de seguridad o ciberseguridad, actividad o comportamientos inusuales, o movimientos laterales. Estas además deberán incluir, la inteligencia de amenazas para procurar mantenerse informado sobre amenazas e indicadores de compromiso de otras fuentes confiables.

Gestión de vulnerabilidades

Art. 5.- Las entidades deberán contar con procesos para la gestión de vulnerabilidades que consideren la identificación, evaluación, tratamiento y comunicación de las medidas de seguridad en la infraestructura tecnológica, mediante la ejecución de pruebas de penetración o intrusión y de escaneos de vulnerabilidades. Se deberán remediar o mitigar todas las brechas de seguridad, no solo las clasificadas como críticas y de alto riesgo.

Asimismo, deberán establecer una metodología para remediar todas las brechas de seguridad y no solo las clasificadas como críticas y de alto riesgo. Estas últimas deben ser remedidas de forma prioritaria, establecer planes de implementación, y efectuar el respectivo seguimiento para el resto de las vulnerabilidades, todo lo cual debe quedar debidamente documentado.

Gestión de parches

Art. 6.- Las entidades deberán contar con procesos ágiles para adquirir, probar e instalar parches para los componentes de la infraestructura tecnológica, de tal forma que éstos se mantengan actualizados; y evitar el uso aplicaciones, sistemas operativos y manejadores de bases de datos sin el respaldo del fabricante o proveedor de actualizaciones de seguridad.

Autenticación de múltiples factores

Art. 7.- Las entidades deberán implementar el uso de autenticación de múltiples factores en cualquier cuenta de usuario que acceda a través de Internet, y las cuentas privilegiadas, incluyendo las que poseen relación de confianza, de tal forma que se agreguen dos o más capas adicionales de seguridad a cada plataforma en línea a la que se accede.

Todo lo relacionado a la autenticación de múltiples factores de los clientes en canales digitales se regula en el Capítulo III de las presentes Normas.

Herramientas de protección ante la suplantación de identidad

Art. 8.- Las entidades deberán contar con herramientas para prevenir la suplantación de identidad ante amenazas basadas en correos electrónicos de phishing, spam, spear-phishing, entre otros y deben considerar la idoneidad de estas herramientas, de tal manera que sean consistentes con el tamaño de la entidad. Las entidades deberán contar con programas de capacitación constante sobre este tipo de amenazas para los empleados, haciendo énfasis en aquellos que realizan funciones de atención al cliente.

Art. 9.- Las entidades deberán realizar campañas de educación financiera en las que se den a conocer a los clientes las medidas de ciberseguridad que deben aplicar en los distintos canales digitales a los que accedan.

Art. 10.- Las entidades deberán notificar a sus clientes los medios oficiales a través de los cuales comunicarán los productos o servicios que ofrecen.

Herramientas Antimalware

Art. 11.- Las entidades deberán contar programas antivirus o antimalware y revisarlos con regularidad para asegurarse de que sean adecuados para su propósito, y sean capaces de detectar nuevas amenazas, así como revisar los ajustes de configuración para garantizar el nivel de protección esperado.

Gestión de dispositivos móviles

Art. 12.- Las entidades deberán implementar soluciones de administración de dispositivos móviles para garantizar que los datos de la entidad estén protegidos.

Herramientas de prevención de pérdida de datos

Art. 13.- Las entidades deberán contar con herramientas de prevención de pérdida de datos para tener una visibilidad ante dicho evento, de tal forma que se fortalezca la detección y prevención de la exfiltración de datos.

Cifrado

Art. 14.- Las entidades deberán cifrar la información crítica en reposo o en tránsito, incluso en dispositivos de almacenamiento extraíbles y móviles, debiendo asegurarse de que los protocolos utilizados son seguros.

Protocolos AAA (Authentication, Authorization and Accounting)

Art. 15.- Las entidades deberán contar en su infraestructura tecnológica con protocolos que realicen las funciones de autenticación de los usuarios; la autorización y uso de los de recursos o servicios; y el registro de la actividad de los usuarios para el respectivo seguimiento.

Gestión de activos

Art. 16.- Las entidades deberán mantener actualizado el inventario de activos de información críticos e identificar los datos y la tecnología asociada para priorizar acciones, en concordancia con lo regulado en las "Normas Técnicas para la Gestión de la Seguridad de la Información" (NRP-23).

Registro y seguimiento

Art. 17.- Las entidades deberán adecuar los sistemas y demás componentes de la

infraestructura tecnológica, para generar la capacidad de contar con un registro de información que permita detectar de forma activa e investigar incidencias, asegurándose de que los registros de actividades estén disponibles para su análisis cuando sea necesario, en concordancia con lo regulado en las "Normas Técnicas para la Gestión de la Seguridad de la Información" (NRP-23).

Respuesta ante incidentes de ciberseguridad

Art. 18.- Las entidades deberán contar con planes de respuesta para mitigar el impacto ante un incidente de ciberseguridad. Estos planes deben ser probados para comprobar la capacidad de respuesta e identificar brechas oportunamente, en concordancia con lo regulado en las "Normas Técnicas para la Gestión de la Seguridad de la Información" (NRP-23).

CAPÍTULO III
DE LA AFILIACIÓN, IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS CLIENTES POR MEDIO DE CANALES DIGITALES

Art. 19.- Las entidades que realicen operaciones y presten servicios financieros por medio de canales digitales, deberán informar a sus clientes de forma escrita o a través de medios electrónicos, al momento de activar por primera vez el uso del canal digital, como mínimo, lo siguiente:

a) Servicios ofrecidos y las responsabilidades de su uso;
b) Procedimientos para la afiliación, cancelación, suspensión y reactivación del servicio;
c) Límites de montos y transacciones a realizar en períodos determinados;
d) Comisiones y tarifas por el uso, con su respectiva descripción;
e) Riesgos inherentes por su utilización;
f) Procedimiento para informar cualquier irregularidad o actividad potencialmente no reconocida o no autorizada y que ha sido detectada, ya sea por el cliente o por la entidad;
g) Procedimiento para la atención de consultas y reclamos de los clientes;
h) Asunción de responsabilidades por parte del cliente y la entidad ante situaciones de fraude; e
i) Consejos para el adecuado uso por parte del cliente.

Art. 20.- En cuanto a la afiliación a los productos o servicios financieros por medio de canales digitales, tales como banca por internet y/o banca móvil, las entidades podrán implementar la aceptación de contratos electrónicos, utilizando factor de autenticación categoría 2 a que hace referencia el artículo 21 de las presentes Normas. Lo anterior, se considerará como la confirmación y autorización de uso de los servicios en canales digitales.

Art. 21.- Las entidades deberán utilizar múltiples factores de autenticación para verificar la identidad de sus clientes para realizar operaciones por medio de canales digitales. Dichos factores de autenticación serán, como mínimo 3, dentro de los siguientes:

Factor de Autenticación Categoría 1: Se compone de la información obtenida del contrato del cliente y del uso de productos, servicios u operaciones efectuadas por estos mediante los diversos canales. Esta información será utilizada mediante la aplicación de preguntas al cliente a través del canal de Banca Telefónica u otro medio digital que disponga la entidad. Para este tipo de factor las entidades deberán realizar lo siguiente:

a) Definir previamente los cuestionarios que serán aplicados para la identificación de los clientes y modificar las preguntas contenidas en los cuestionarios al menos una vez al año;
b) Establecer generadores aleatorios de las preguntas de los cuestionarios; y
c) Cuando intervenga el operador, este no deberá conocer anticipadamente las respuestas para la identificación del cliente, las cuales deben ser validadas con el uso de sistemas informáticos.

Factor de Autenticación Categoría 2: Se compone de contraseñas que sólo el cliente conoce e ingresa mediante un mecanismo o dispositivo de acceso, el cual debe cumplir, al menos, con las características siguientes:

a) Su longitud mínima y conformación debe ser de acuerdo a lo siguiente:
    i. Cuatro caracteres, para los servicios ofrecidos a través de cajeros automáticos, puntos de ventas, Banca Telefónica y servicio de IVR;
    ii. Ocho caracteres, para canales digitales y deberá incluir una combinación de caracteres alfabéticos en mayúsculas, minúsculas y numéricos: y
    iii. Cuando el cliente modifique su contraseña, la entidad debe validar que esta no se repita, con al menos, doce de las últimas contraseñas que utilizó para aquellas entidades que estén utilizando solo un factor de autenticación.
    Para el caso de entidades que utilicen dos factores de autenticación, deberá validar que las contraseñas no se repitan, con al menos, cinco de las últimas contraseñas que utilizó.
b) Su vencimiento no será superior a ciento ochenta días para todos los canales digitales; no obstante, las entidades están en la obligación de ofrecer a sus clientes sin cargo alguno la posibilidad de realizar el cambio de las contraseñas cuando éstos lo requieran. En cada oportunidad que el cliente modifique su contraseña deberá ser informado a través de su correo electrónico u otros medios; (1)
c) En el caso de las contraseñas asignadas por la entidad para el acceso a canales digitales, se debe requerir en forma automática que el cliente la modifique inmediatamente después de iniciar la primera sesión;

d) La entidad debe requerir que la primera sesión se efectúe como máximo veinticuatro horas después de haber generado la contraseña por parte de la entidad; en caso contrario, ésta debe ser inhabilitada automáticamente; y
e) En ningún caso se podrá utilizar como contraseña, la información siguiente:

   i. Un documento de identificación del cliente;
   ii. El nombre de la entidad;
   iii. Más de tres caracteres iguales consecutivos numéricos o alfabéticos; y
   iv. Fecha de nacimiento, nombres, apellidos y número telefónico, registrado por el cliente en la entidad.

Factor de Autenticación Categoría 3: Se compone de claves dinámicas de un único uso, generadas por dispositivos electrónicos o cualquier otro medio, las cuales deben cumplir como mínimo con las características siguientes:

a) Contar con mecanismos que impidan su duplicación o alteración;
b) Una vez generada la clave dinámica, ésta tendrá la vigencia siguiente:

   i. Hasta un minuto, en el caso de que sean generados por Tokens;
   ii. Hasta el cierre de sesión, para canales digitales; y
   iii. Hasta dos horas, para todos los servicios de cajeros automáticos.
c) No ser conocida antes de su generación ni durante su uso, por los funcionarios, empleados, representantes o por terceros de la entidad; y
d) Se podrán utilizar tablas aleatorias de contraseñas como factor de autenticación de esta categoría, siempre y cuando cumplan con las características listadas en este factor de autenticación.

Para el caso que las entidades puedan facilitar a sus clientes mecanismos, dispositivos o medios generadores de las claves dinámicas, deberán considerar lo siguiente:

a) Si la autenticación es estática, la validación de los datos deberá realizarse en tiempo real en los computadores centrales de la entidad; y
b) Si la autenticación es dinámica, la validación de los datos podrá realizarse fuera de línea.

Factor de Autenticación Categoría 4: Se compone de información del cliente, derivada de sus características biométricas.

Art. 22.- Los sistemas de canales digitales de las entidades deberán requerir a sus clientes un factor para inicio de sesión y deberán exigir un segundo factor más para la autenticación de categoría 3 a que hace referencia el artículo 21 de las presentes Normas. Estos factores serán aplicados de acuerdo con el esquema siguiente:

Tipo de operaciones	Factores a utilizar	
	Base	Adicional
Afiliación y desafiliación de productos y servicios.	2	3 o 4
Utilización de productos, servicios y programaciones de pago.	2	3 o 4
Pagos de servicios, canje de beneficios, retiros o adelantos de efectivo, desactivación de productos, generación y cambios de contraseñas, o transferencias electrónicas a terceros.	2	3 o 4
Apertura de segundas cuentas o productos financieros.	2	3 o 4
Actualización de datos de la ficha del cliente a través de Banca por Internet o Banca móvil y límites para las transacciones a efectuar	2	N/A
Consultas.	2	N/A
Transacciones ofrecidas a través de dispositivos de autoservicio.	2	N/A
Pagos o transferencias electrónicas entre el mismo titular y mismo banco.	2	N/A

El esquema de autenticación por operaciones indicado en el presente artículo podrá no ser requerido por las entidades, en el caso de que éstas, soliciten factores de autenticación categoría 3 o 4 para el inicio de la sesión en sus canales digitales, debiendo la entidad, previamente crear el identificador del cliente de acuerdo a lo establecido en el literal a) y el último inciso del artículo 25 de las presentes Normas. (1)

Art. 23.- Para las operaciones de pagos de servicios, canje de beneficios, retiros o adelantos de efectivo, desactivación de productos, generación y cambios de contraseñas, o transferencias electrónicas a terceros que no requieran la afiliación o registro de cuentas, se deberá utilizar el factor adicional a que hace referencia el artículo 22 de las presentes Normas.

Art. 24.- Para el uso del servicio de Banca Telefónica los clientes deberán autenticarse a través del IVR con un factor de autenticación como mínimo de categoría 2, a que hace referencia el artículo 21 de las presentes Normas.

Art. 25.- Para permitir el inicio de sesión a los clientes a través de los servicios ofrecidos por canales digitales, las entidades deberán solicitar y validar al menos, lo siguiente:

a) Un identificador de cliente de por lo menos seis caracteres; y
b) Un factor de autenticación de las categorías 2 o 3.

El identificador del cliente deberá ser único y permitirá a las entidades determinar todas las operaciones realizadas por el propio cliente mediante estos canales.

Art. 26.- Las entidades deberán inhabilitar inmediatamente el acceso a los servicios ofrecidos por canales digitales cuando el cliente presuma que se puede ver afectada o se ha visto afectada la seguridad de los productos financieros contratados con la entidad, debiendo contar ésta con diferentes medios, tanto presenciales como digitales para estos efectos.

Art. 27.- En los canales digitales, cuando corresponda, las entidades deberán proveer información al cliente, de acuerdo con lo siguiente:

a) Elementos que identifiquen que se encuentra en el sitio web de la entidad, antes de ingresar todos los elementos de autenticación. Para ello, deberán usar certificados digitales u otros mecanismos que permitan autenticar el sitio transaccional. Adicionalmente, podrán utilizar aquella que información que el cliente conozca y haya proporcionado a la entidad, o bien, que haya señalado para este fin, tales como nombres y apellidos, imágenes, entre otros; y
b) Una vez que el cliente verifique que se trata del sitio web, o canal digital oficial de la entidad e inicie una sesión segura, se deberá proporcionar de forma notoria y visible, al menos la información siguiente:

    i. Fecha y hora del ingreso a su última sesión; y
    ii. Nombre y apellido del cliente.

Art. 28.- Para el uso de los factores de autenticación, las entidades deberán cumplir, al menos, con lo siguiente:

a) Deberán mantener procedimientos que garanticen la seguridad de la información de sus clientes durante la generación, custodia, distribución, asignación y reposición o sustitución de dichos factores;
b) Tendrán prohibido divulgar o acceder la información protegida en relación a los factores de autenticación; en el caso de la información relacionada al factor de autenticación de categoría 1, toda consulta debe estar sustentada con la solicitud del cliente;
c) Tendrán prohibido solicitar, la información parcial o completa, establecida en los factores de autenticación de las categorías 2 o 3 a que se refiere el artículo 21 de las presentes Normas; y
d) Deberán informar a sus clientes que la entidad no le requerirá bajo ningún medio y bajo ninguna condición la información sobre sus factores de autenticación.

Art. 29.- Las entidades podrán establecer métodos adicionales de autenticación a los previstos en las presentes Normas para las transacciones realizadas en canales digitales.
Art. 30.- Con respecto a la sesión del cliente, las entidades deberán garantizar lo siguiente:

a) Finalizar la sesión en forma automática en los casos siguientes:
   i. Cuando la inactividad alcance los ciento ochenta segundos en canales digitales y hasta cinco minutos para banca de empresa;
   ii. Cuando el período de inactividad alcance como máximo, los treinta segundos en las operaciones realizadas mediante cajeros automáticos, kioskos y puntos de ventas; y
   iii. Cuando se detecten sesiones simultáneas;
b) Para los casos de inicio de sesión por medio de Banca por Internet o Banca Móvil se deberá remitir mensaje al cliente, por los medios electrónicos que disponga la entidad, notificando acerca del inicio de sesión; y
c) Las entidades que mediante su sitio web ofrezcan enlaces a páginas web de terceros, deberán comunicar a sus clientes que, al momento de ingresar a éstos, su seguridad no depende ni es responsabilidad de dicha entidad.

CAPÍTULO IV
DE LAS TRANSACCIONES, RESPONSABILIDAD Y OBLIGACIONES DE LA ENTIDAD

Del registro y liquidación de las transacciones
Art. 31.- Las transacciones realizadas por medio de canales digitales deberán ser tratadas y aplicadas bajo los criterios establecidos en los literales j) y l) del artículo 18 de Ley de Protección al Consumidor.

Confirmación de las transacciones
Art. 32.- Las entidades deberán generar una confirmación inmediata al cliente, sobre las transacciones que se realicen por medio de canales digitales, por medio de mensajes de texto a su dispositivo móvil registrado u otro medio electrónico, que le servirá para determinar que la misma se ha completado, salvo aquellos casos en que el cliente haya manifestado expresamente no querer recibirlas, lo cual deberá estar debidamente documentado por la entidad.

Asimismo, tendrán que enviar vía electrónica la notificación que deberá incluir, como mínimo la fecha, hora, tipo de producto, tipo de transacción, número de referencia y monto de la operación. En caso de que la transacción no sea exitosa deberá enviarse un mensaje al cliente notificando que la transacción solicitada no fue completada. En cada transacción que realicen, deberán implementar mecanismos de no repudio.

Monitoreo de las transacciones
Art. 33.- La entidad deberá contar con información del número y monto de las transacciones realizadas por cliente y tipo de producto, por medio de canales digitales, monitoreando además, el cumplimiento de los límites y otras medidas prudenciales que se hayan establecido, dependiendo del producto o servicio de que se trate, e

identificando en tiempo real posibles operaciones, inusuales, irregulares o sospechosas de acuerdo al perfil del cliente y los hábitos de uso de sus productos y servicios financieros, generando las alertas correspondientes sobre tales operaciones.

Asimismo, las entidades deben notificar en forma inmediata a los clientes, las alertas asociadas a las operaciones realizadas a través de los canales digitales, que se desvíen del perfil transaccional del cliente, determinado de manera oportuna y de forma automática por la entidad, a través de los medios que esta estime conveniente para el cliente. La notificación deberá realizarse siempre y cuando no exista un aviso por parte del cliente que permita relacionar razonablemente las operaciones que generaron la alerta.

La notificación o el mensaje enviado deberá describir como mínimo fecha y hora de la transacción, monto de la operación, número de referencia de la transacción, nombre y número de teléfono de la entidad, canal utilizado, tipo de producto y de operación.

El monitoreo de las transacciones al que hace referencia el presente artículo deberá ser efectuado por la entidad mediante herramientas informáticas robustas, especializadas en prevención de fraude.

Art. 34.- Las entidades deberán asegurar que los IVR, o cualquier otro medio electrónico facilitado por la entidad, permita al cliente acceder a opciones para reportar, de forma expedita, las presuntas transacciones u operaciones fraudulentas o no reconocidas y obtener asistencia inmediata a su reclamo, para lo cual deberán establecer procesos específicos con personal debidamente capacitado que brinden atención oportuna a sus clientes.

Art. 35.- Las entidades deberán establecer procesos y mecanismos automáticos para bloquear preventivamente el acceso a cualquiera de los canales digitales, en los casos siguientes:

a) Cuando se detecte ingresar al canal digital, utilizando información de autenticación incorrecta. Asegurarse que los intentos de acceso fallidos no excedan de la cantidad de tres intentos consecutivos para el bloqueo de este;
b) Cuando los sistemas de monitoreo detecten comportamiento transaccional inusual o irregular de acuerdo al perfil del cliente;
c) Cuando los sistemas de seguridad detecten un ataque informático que comprometa los datos o información de los clientes; y
d) Cuando existan situaciones que comprometan la seguridad de los sistemas de información y del cliente.

Art. 36.- Cuando la plataforma tecnológica que soporta los canales digitales no detecte operaciones fraudulentas, así como transacciones no solicitadas o no realizadas por el

cliente, y que de acuerdo al análisis realizado por la entidad, dichos casos no son atribuibles al cliente, las entidades serán las responsables de reintegrar, compensar o revertir los montos comprometidos, sin que esto incluya el cobro de comisiones o recargos adicionales para éste. Adicionalmente, deberán mantener a disposición de la Superintendencia los reportes o estadísticas que resulten por estos eventos.

Art. 37.- Las entidades deberán definir mecanismos de monitoreo y control para asegurar el adecuado funcionamiento de los canales digitales.

Atención al cliente

Art. 38.- Las entidades deberán poner a disposición del cliente un mecanismo que permita lo siguiente:

a) Obtener el historial de transacciones realizadas que como mínimo incluirá el número de referencia, monto, fecha, hora, tipo de transacción, tipo de producto; y
b) Un procedimiento para definir una nueva clave o contraseña.

Asimismo, las entidades proveerán a sus clientes de un número telefónico y otros medios alternativos de contacto, tales como correo electrónico, para una comunicación permanente con la entidad, incluyendo el debido soporte técnico.

La entidad establecerá mecanismos y procedimientos adecuados que operen las veinticuatro horas del día, todos los días del año, para atender reclamos de los clientes sobre sus transacciones, especificando el medio oficial de recepción de los mismos, debiendo resolver en un plazo que no podrá exceder al establecido para los diferentes productos y servicios en la legislación vigente. En el caso que no exista un plazo específico en la legislación vigente, éstos deberán ser resueltos en un plazo razonable, el cual deberá ser establecido en el procedimiento para atender reclamos. En todo caso, dicho procedimiento deberá incorporar controles internos sobre las consultas atendidas y respuestas brindadas.

Las entidades deberán informar a sus clientes, mediante campañas educacionales, sobre el funcionamiento de los canales digitales que pongan al alcance de éstos, a fin de prevenir actos que pudieran derivar en operaciones irregulares o ilegales que afecten a los clientes o a las propias entidades.

CAPÍTULO V
OTRAS DISPOSICIONES Y VIGENCIA

De la auditoría interna

Art. 39.- La Unidad de Auditoría Interna debe considerar en su plan anual de trabajo, la evaluación del cumplimiento de las disposiciones de las presentes Normas.

Detalles técnicos del envío de información

Art. 40.- La Superintendencia remitirá a las entidades, en un plazo máximo de treinta días posteriores a la fecha de entrada en vigencia de las presentes Normas, con copia al Banco Central, los detalles técnicos relacionados con el envío de la información requerida. Los requerimientos de información se circunscribirán a la recopilación de información conforme lo regulado en las presentes Normas.

Sanciones

Art. 41.- Los incumplimientos a las disposiciones contenidas en las presentes Normas, serán sancionados de conformidad con lo previsto en la Ley de Supervisión y Regulación del Sistema Financiero.

Transitorio

Art. 42.- Las entidades obligadas al cumplimiento de las presentes Normas, tendrán un plazo máximo de treinta días hábiles posteriores a la entrada en vigencia de las mismas, para dar cumplimiento a lo establecido en los artículos 19 y 38 de las presentes Normas.

Aspectos no previstos

Art. 43.- Los aspectos no previstos en materia de regulación en las presentes Normas, serán resueltos por el Banco Central por medio de su Comité de Normas.

Vigencia

Art. 44.- Las presentes Normas entrarán en vigencia a partir del día 8 de marzo de dos mil veintidós.

MODIFICACIONES:

(1) **Modificación a los artículos 3, 21 y 22, aprobada por el Banco Central por medio de su Comité de Normas, en Sesión No. CN-11/2022 de fecha 30 de diciembre de dos mil veintidós, con vigencia a partir del 16 de enero de dos mil veintitrés.**