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

CONSIDERANDO:

I. Que el artículo 100 de la Ley de Supervisión y Regulación del Sistema Financiero, establece que excepcionalmente, en circunstancias que hagan prever la ocurrencia de posibles desequilibrios del sistema financiero o por razones de interés social, el Comité de Normas con al menos dos de sus miembros podrá emitir, sin más trámite, normas técnicas de carácter temporal y de vigencia inmediata, sin la consulta previa a la que se refiere dicho artículo. La vigencia de las normas no podrá exceder de ciento ochenta días.

II. Que dado el contexto actual de la pandemia por Covid-19 el cual ha acelarado la transformación digital y se ha masificado el uso de los canales digitales para el desarrollo de los servicios financieros, por lo cual los sistemas informáticos de las entidades financieras han sido vulnerados tanto a nivel local como internacional, para ello es propicio implementar medidas para prevenir la materialización de eventos de fraudes financieros por parte de atacantes y ciberatacantes sobre diversos productos financieros de los clientes, a los cuales se acceden por diversos canales digitales para realizar operaciones financieras en las distintas plataformas electrónicas que se les ha facilitado a los mismos.

III. Que es imprescindible emitir Normas de carácter temporal para anticipar el cumplimiento de algunas medidas de ciberseguridad reguladas en las "Normas Técnicas para la Gestión de la Seguridad de la Información" (NRP-23), emitidas por el Banco Central de Reserva, a través de su Comité de Normas, que se deben aplicar en los sistemas informáticos mediante los cuales se recopila, procesa, transmite y se almacena la información de los productos y servicios financieros que las entidades ofrecen a sus clientes.

POR TANTO,

en virtud de las facultades normativas que le confiere los artículos 99 y 100 de la Ley de Supervisión y Regulación del Sistema Financiero,

ACUERDA, emitir las siguientes:

NORMAS TÉCNICAS TEMPORALES SOBRE MEDIDAS DE CIBERSEGURIDAD E IDENTIFICACIÓN DE LOS CLIENTES EN CANALES DIGITALES

CAPÍTULO I
OBJETO, SUJETOS Y TÉRMINOS

Objeto

Art. 1.- El objeto de las presentes Normas es reforzar las medidas de ciberseguridad en los sistemas informáticos de las entidades financieras mediante los cuales se recopila, procesa, transmite y se almacena la información de los productos y servicios financieros que las entidades financieras ofrecen a sus clientes, así como también la implementación de medidas para la correcta identificación de los clientes.

Sujetos

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

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) **Comité de Normas:** Comité de Normas del Banco Central de Reserva de El Salvador;
b) **Entidades:** Sujetos obligados al cumplimiento de las presentes Normas de acuerdo al artículo 2 de las mismas;
c) **Factor base:** Es el factor mínimo requerido para realizar la autenticación inicial del cliente;
d) **Factor adicional:** Es el segundo factor o grupo de factores de autenticación que se debe requerir al cliente;
e) **IVR:** (Robot de voz interactivo, 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; y
f) **Superintendencia:** Superintendencia del Sistema Financiero.

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 en lo posible, la inteligencia de amenazas para procurar mantenerse informado sobre amenazas e indicadores de compromiso de otras fuentes confiables.

Las medidas que se tomen deberán, brindar a corto plazo la implementación o una mejora tangible a sus herramientas o mecanismos, según el caso, debiendo adecuar el plan presentado a la Superintendencia requerido en las "Normas Técnicas para la Gestión de la Seguridad de la Información" (NRP-23), de conformidad al artículo 34 de las presentes Normas.

Gestión de vulnerabilidades
Art. 5.- Las entidades deberán contar o mejorar 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 todas las brechas de seguridad no solo las clasificadas como críticas y de alto riesgo.

Gestión de parches
Art. 6.- Las entidades deberán contar con procesos agiles para adquirir, probar e instalar parches para los componentes de la infraestructura tecnológica de tal forma que éstos se mantengan actualizados.

Autenticación de múltiples factores
Art. 7.- Las entidades deberán implementar el uso de autenticación de múltiples factores en cualquier cuenta a la que se acceda a través de Internet, incluidas entre estas las cuentas de usuarios de los clientes para acceder a las aplicaciones móviles, de tal forma que se agreguen dos o más capas adicionales de seguridad a cada plataforma en línea a la que se accede. Todas las cuentas a las que se acceda a través de Internet que no sea de confianza deben considerar autenticación de múltiples factores, de igual forma utilizar autenticación de múltiples factores para cuentas privilegiadas, tales como las cuentas de administrador.

Herramientas de protección de correo electrónico (phishing)

Art. 8.- Las entidades deberán contar con herramientas robustas para filtrar correos electrónicos de phishing, spam, spear-phishing y otras amenazas basadas en el correo electrónico 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 constantes sobre las amenazas de phishing para los empleados, haciendo énfasis para aquellos de atención al cliente.

Asimismo, las entidades deberán realizar campañas de educación financiera en la que se dé a conocer a los clientes medidas de ciberseguridad que deben aplicar en los distintos canales digitales a los que acceden.

Las entidades deberán notificar a sus clientes los medios oficiales por los cuales deberán comunicar asuntos relativos a productos o servicios que ofrecen.

Herramientas Antimalware

Art. 9.- Las entidades deberán contar y revisar con regularidad los programas antivirus o antimalware para asegurarse de que sean adecuados para su propósito y sean capaces de detectar nuevas amenazas y revisar los ajustes de configuración para garantizar el nivel de protección esperado.

Gestión de dispositivos móviles

Art. 10.- Las entidades deberán implementar soluciones de administración de dispositivos móviles para garantizar que los datos de la entidad estén adecuadamente protegidos.

Herramientas de prevención de pérdida de datos

Art. 11.- Las entidades deberán contar con herramientas robustas de prevención de pérdida de datos para tener una adecuada visibilidad ante dicho evento de tal forma que se fortalezca la detección y prevención de la exfiltración de datos.

Cifrado

Art. 12.- Las entidades deberán cifrar los datos sensibles en reposo o en tránsito, incluso en dispositivos de almacenamiento extraíbles y móviles o cuando los datos se envían a través de una red que no es de confianza.

Protocolos AAA (Authentication, Authorization and Accounting)

Art. 13.- Las entidades deberán contar con una infraestructura con protocolos que realicen las funciones de autenticación de los usuarios, autorización y utilización de recursos o servicios, y registro de la actividad de los usuarios.

Gestión de activos

Art. 14.- Las entidades deberán mantener actualizado el inventario de activos de información críticos e identificar los datos y la tecnología asociada para priorizar acciones.

Registro y seguimiento

Art. 15.- 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.

Seguridad en la cadena de suministro

Art. 16.- Las entidades deberán aplicar la seguridad en la contratación de proveedores de servicios de tecnología, con énfasis en los servicios en la nube.

Respuesta ante incidentes de ciberseguridad

Art. 17.- 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.

CAPÍTULO III
MEDIDAS DE AUTENTICACIÓN DE LOS CLIENTES POR MEDIO DE CANALES DIGITALES

Art. 18.- 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. 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 podrá consultar o 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.
b) Su vencimiento no será superior a sesenta días para todos los canales electrónicos; 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;
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. 19.- Los sistemas de canales digitates 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 18 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
Utilización de productos, servicios y programaciones de pago.	2	3
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
Apertura de segundas cuentas o productos financieros.	2	3
Actualización de datos de la ficha del cliente a través de Banca por Internet o Banca móvil	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

Art. 20.- 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 anterior.

Art. 21.- 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 18 de las presentes Normas.

Art. 22.- 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. 23.- 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. 24.- 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 la información siguiente:
    i. Aquella 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. 25.- Para el uso de los factores de autenticación, las entidades debrán 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 por los factores de

autenticación;

c) Tendrán prohibido solicitar, la información parcial o completa, establecida en los factores de autenticación de las categorías 2 ó 3 a que se refiere el artículo 18 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. 26.- Las entidades podrán establecer métodos adicionales de autenticación a los previstos en las presentes Normas para las transacciones realizadas en canales digitales.

Art. 27.- 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 veinte segundos en canales digitales y hasta cinco minutos para banca de empresa; (2)
    ii. Cuando el período de inactividad alcance los diez segundos en las operaciones realizadas mediante cajeros automáticos, kioskos y puntos de ventas;
    iii. Cuando se detecten sesiones simultáneas; y
b) 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.

Del registro y liquidación de las transacciones

Art. 28.- 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. 29.- 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.

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 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. 30.- 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 para dichos servicios y productos, 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 desvien 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 se deberá realizar siempre y cuando no exista una notificación por parte del cliente que razonablemente relacione la realización de estas 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. Para ello, las entidades deberán asegurar que los IVR permitan 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.

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

Art. 31.- 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 intente ingresar al servicio utilizando información de autenticación incorrecta. En ningún caso, los intentos de acceso fallidos podrán exceder tres intentos consecutivos.
b) Cuando los sistemas de monitoreo detecten comportamiento transaccional inusual o irregular; o los sistemas de seguridad detecten un ataque informático que comprometa los datos de los clientes.
c) Cuando existan situaciones que comprometan la seguridad de los sistemas de información y del cliente.

Art. 32.- Cuando la plataforma tecnológica que soporta los canales digitales no detecte operaciones fraudulentas, así como transacciones no solicitadas o no realizadas por el cliente, en cualquiera de los canales, las entidades serán las responsables ante el cliente 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. 33.- Las entidades deberán definir mecanismos de monitoreo y control para asegurar el adecuado funcionamiento de los canales digitales.

CAPÍTULO IV
OTRAS DISPOSICIONES Y VIGENCIA

Transitorio

Art. 34.- Los cambios al Plan de Adecuación requerido mediante las "Normas Técnicas para la Gestión de la Seguridad de la Información" (NRP-23), para incorporar las mejoras y ajustes que se deriven de lo establecido en las presentes Normas, deberá ser remitido a la Superintendencia en un plazo máximo de siete días hábiles a partir de la entrada en vigencia de las presentes Normas. (1)

En ningún caso la implementación de las acciones presentadas en dicho Plan, asociadas a garantizar la seguridad de la realización de las operaciones de los clientes, podrán superar el plazo de veinte días hábiles.

En caso de que las entidades no logren cumplir con el plazo de implementación señalado, deberán remitir las justificaciones razonadas y sustentadas a la Superintendencia para que esta pueda otorgar un plazo de prórroga máximo de treinta días hábiles contados a partir del vencimiento del plazo mencionado en el inciso anterior, para el caso de las entidades que se rigen por su Ley especial de creación y que la contratación de servicios se regulen según lo dispuesto en la Ley de Adquisiciones y Contrataciones de la Administración Pública y no logren cumplir con el plazo de implementación señalado, la Superintendencia podrá otorgar un plazo máximo de prórroga de noventa días hábiles contados a partir del vencimiento del plazo mencionado en el inciso anterior. (2)

Sanciones

Art. 35.- 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.

Aspectos no previstos

Art. 36.- 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. 37.- La vigencia de las presentes Normas será de ciento ochenta días, a partir del veintitrés de agosto de dos mil veintiuno.

MODIFICACIONES:

(1) **Modificación al artículo 34 aprobada por el Comité de Normas del Banco Central de Reserva de El Salvador, en Sesión No. CN-10/2021 de fecha 27 de agosto de dos mil veintiuno, con vigencia a partir del día 27 de agosto de dos mil veintiuno.**

(2) **Modificaciones a los artículos 27 y 34 aprobadas por el Comité de Normas del Banco Central de Reserva de El Salvador, en Sesión No. CN-13/2021 de fecha 14 de septiembre de dos mil veintiuno, con vigencia a partir del 14 de septiembre de dos mil veintiuno.**