

1. Introducción

El objetivo de este Protocolo, elaborado por la Asociación Bancaria Costarricense (ABC), es establecer, como medida de autorregulación, un procedimiento estandarizado para la atención de incidentes por fraudes o posibles fraudes electrónicos que sean reportados por los Clientes o que sean detectados por las entidades bancarias.

El presente Protocolo está dirigido para las distintas entidades agremiadas a la Asociación Bancaria Costarricense.

Por lo anterior, se establece lo siguiente:

2. Definiciones

- **Fraude informático (fraude electrónico):** Es la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, donde se influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema. (referencia Código Penal, Ley N° 4573)
- **Phishing:** Fraude tradicionalmente cometido a través de internet, que pretende conseguir datos confidenciales de usuarios, tales como identificación o claves de acceso a cuentas de diversos sistemas. Para lograr este objetivo, generalmente se realizan envíos masivos de correos electrónicos (email), que simulan provenir de entidades de confianza, advirtiéndole a la víctima que, por "motivos de seguridad" o con el fin de "confirmar su cuenta", entre otros, debe suministrar sus datos



personales, claves u otra información confidencial, para lo cual se utiliza un sitio web fraudulento y se requiere a la víctima a que haga “click” en un enlace (link) incluido en el mensaje. Posteriormente, con esta información confidencial, los delincuentes realizan transferencias a cuentas de terceros y retiran el dinero.

- **Pharming:** Modalidad de estafa online (en línea) mediante la manipulación de los servidores DNS (Domine Name Server) para re-direccionar el nombre de un dominio, visitado habitualmente por el usuario, a una página web idéntica a la original, que ha sido creada para obtener datos confidenciales de usuarios como identificación o claves de acceso a cuentas de diversos sistemas.
- **OTP:** One time password, tecnología que permite generar una clave para uso en una única oportunidad, como por ejemplo token (virtuales o físicos), tarjetas de claves dinámicas, entre otros.
- **Phreaking:** Hacking orientado a la telefonía y estrechamente vinculado con la electrónica aplicada a los sistemas telefónicos.
- **Vishing:** Es una variante del phishing, pero por teléfono. Consiste en el envío de un correo electrónico en el cual los delincuentes consiguen detalles de datos bancarios mediante un número telefónico gratuito, en la cual una voz computadorizada de aspecto profesional requiere de las víctimas la confirmación de su cuenta bancaria, solicitándoles el número de cuenta, tarjeta, PIN y otros datos confidenciales.
- **Fuente de información:** La entidad bancaria podrá recibir la información sobre la sospecha de un posible delito informático mediante los siguientes medios:
 - El cliente
 - Departamento de Seguridad del Banco
 - Sucursal o Centro de Contactos

- Informantes
- Organismo de Investigación Judicial

3. Criterios de seguridad y calidad de la información

- Criterios de seguridad de la información

- *Confidencialidad:* Hace referencia a la protección de información cuya divulgación no está autorizada.
- *Integridad:* La información debe ser precisa, coherente y completa desde su creación hasta su destrucción.
- *Disponibilidad:* La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.

- Criterios de calidad de la información

- *Efectividad:* La información relevante debe ser pertinente y su entrega oportuna, correcta y consistente.
- *Eficiencia:* El procesamiento y suministro de información debe hacerse utilizando de la mejor manera posible los recursos.
- *Confiabilidad:* La información debe ser apropiada para la administración de la entidad y el cumplimiento de sus obligaciones.

4. Seguridad y calidad

En el desarrollo de los criterios de seguridad y calidad, las entidades deberán tomar en cuenta todas las herramientas necesarias desde el punto de vista de hardware, software y



equipos de telecomunicaciones, que permitan prevenir, detectar y corregir situaciones de riesgo que comprometan directamente los diferentes servicios, la información bancaria y la información de los clientes.

Complementariamente a las herramientas, que en la actualidad posean las entidades, se deberán hacer análisis y retroalimentaciones constantes de frente a las modalidades delictivas y su permanente evolución y nuevas formas de materialización, que permitan en consecuencia generar aplicaciones que aumenten, en primera instancia, el nivel de seguridad de los diferentes servicios; y adicionalmente, forzar a los grupos delincuenciales a exponerse más en el plano físico y material para que se puedan detectar sus movimientos durante la prestación de esos servicios, como por ejemplo:

- Estrategias de apersonamiento a las oficinas por parte de los clientes para la autorización de cuentas favoritas para la realización de transferencias.
- Equipamiento al personal de cajas y plataforma de instrumentos de detección de documentos de identidad alterados o falsificados.
- Capacitación permanente del personal bancario.

Otras medidas de seguridad que podrán implementar las entidades bancarias son las siguientes:

- a. Proteger las claves de acceso a los sistemas de información. En desarrollo de esta obligación, las entidades deberán evitar el uso de claves compartidas, genéricas o para grupos. La identificación y autenticación en los dispositivos y sistemas de cómputo de las entidades deberá ser única y personalizada.
- b. Dotar a sus terminales o equipos de cómputo de los elementos necesarios que eviten la instalación de programas o dispositivos que capturen la información de sus clientes y de sus operaciones.

- c. Definir los procedimientos y medidas que se deberán ejecutar cuando se encuentre evidencia de la alteración de los dispositivos usados en los canales de distribución de servicios financieros.

Cada entidad bancaria debe garantizar que dentro de los registros de bitácora de sus sistemas se pueda individualizar el acceso hecho por el usuario del cliente, de manera que no exista duda de éste y que pueda ser utilizado como prueba.

5. Aspectos preventivos-de la entidad bancaria hacia los clientes

Las entidades bancarias brindarán al usuario financiero toda la información necesaria para la prevención de un delito informático mediante folletos informativos donde conste las medidas de precaución sobre delitos informáticos ya conocidos y las nuevas modalidades, así como, las acciones que deben realizar cuando haya sido víctima de un fraude electrónico.

Adicionalmente, los bancos podrán:

- a. Generar regularmente publicidad informativa mediante los canales que institucionalmente tenga previstos.
- b. Crear aplicaciones de información y capacitación para el usuario financiera a través de la página web.
- c. Crear un canal de comunicación interno para los funcionarios de la institución, con el fin de recopilar posibles denuncias relacionadas a fraudes. Estas denuncias deberán ser valoradas por un equipo interdisciplinario y especializado.
- d. Entre otros.

6. Disposiciones Generales en caso de una sospecha de Fraude Electrónico



- a. Si existe una sospecha de un delito informático en algunos de los canales de servicio, se deberá inhabilitar, inmediatamente, el canal al usuario del cliente que realizó la transacción, además de inhabilitar, por prevención, la cuenta financiera destino, tarjetas y dispositivos de doble autenticación. También deberán remitir una alerta a los funcionarios del Departamento de Seguridad, quienes analizarán el caso en concreto.
- b. En caso de delito informático, el usuario financiero debe interponer su denuncia ante el Departamento de Seguridad del Banco y ante el Organismo de Investigación Judicial.
- c. Los Departamentos de Seguridad de las entidades financieras deberán crear un expediente por cada reporte de un delito informático que se genere, este debe contener toda la información relevante.
- d. Las entidades bancarias deberán recolectar toda aquella información que se requiere en una Orden de Levantamiento del Secreto Bancario (ANEXO A), para garantizar el resguardo de la evidencia.

7. Procedimiento en caso de Fraude Electrónico detectado por la Entidad Financiera

Son entes que pueden recibir alertas de fraude electrónico, los siguientes:

- i. Canales de Gerencia
- ii. Departamento de Seguridad
- iii. Departamento de Seguridad en los Sistemas
- iv. Las diferentes áreas del negocio bancario

Independientemente, del ente que reciba la respectiva alerta, a nivel institucional se deberán realizar las directrices necesarias que permitan una comunicación ágil y pronta al

Departamento de Seguridad o Seguridad de Sistema. Una vez realizado esto, se recomienda la realización de las siguientes acciones:

- a. Notificar al Departamento de Seguridad y de Seguridad en Sistemas.
- b. Comunicar a los grupos de alerta de páginas fraudulentas, en caso de que lo amerite. (aplicable cuando dichos grupos existan a nivel institucional de los bancos)
- c. Se procede a bloquear el usuario en línea del cliente y se modifica el status temporal de la cuenta objeto de defraudación para que únicamente pueda recibir depósitos.
- d. Se deberá comunicar al cliente:
 - i. Sobre el caso y las medidas adoptadas
 - ii. Solicitarle que se presente a alguna de las sucursales de la entidad financiera para verificar las transacciones hechas por su persona, y aquellas que no reconoce como propias.
 - iii. Llenar los formularios correspondientes. Se recomienda que dicho formulario sea lo más detallado posible para poder detectar todos los hechos relevantes.
- e. Cuando el cliente se presente en una sucursal de la entidad deberá identificarse mediante su cédula de identidad. El personal que lo atienda deberá también verificar las firmas registradas. En dicha visita, se le otorgará una nueva clave de seguridad para realizar sus transacciones en línea, además de los dispositivos de seguridad que utilicen tecnologías OTP. Adicionalmente, y para mayor seguridad, el banco podrá decidir proceder al cierre de la cuenta y la apertura de una nueva.
- f. Se le debe consultar al usuario financiero si ha proporcionado su información personal y bancaria a una tercera persona, en cuyo caso se deberán realizar las siguientes gestiones:
 - i. Revisar los movimientos de las cuentas bancarias del usuario y verificar si se han realizado transacciones fraudulentas.
 - ii. En caso de que exista fraude, bloquear las cuentas bancarias.

- g. En caso de ser necesario la entidad financiera podrá comunicarle a los Departamentos de Seguridad de otros bancos sobre la ejecución de fraudes electrónicos. Cuando se realicen transacciones entre entidades bancarias mediante SINPE, siempre se deberá comunicar al banco receptor. Adicionalmente, se le comunicará a la Comisión Anti-Fraudes de la Asociación Bancaria Costarricense, en las sesiones que se convoquen para analizar la efectividad del presente protocolo.
- h. Periódicamente, se debe actualizar la información del sitio web para que contenga sugerencias de seguridad en relación a los delitos informáticos.
- i. Se recomienda que una vez que haya sido mitigada la situación en concreto se proceda a una reunión del equipo que participa en la prevención de casos de delitos informáticos, para analizar la efectividad del procedimiento realizado y la posibilidad de realizar mejoras para el siguiente evento.
- j. Para brindarle mayor seguridad al cliente, las entidades financieras podrán recomendar al usuario financiero la utilización de medidas de seguridad como: tarjeta dinámica, token, complejidad en las claves electrónicas, smart card del Banco Central, entre otras.

8. Procedimiento en caso de un reclamo por Fraude Electrónico presentado por un Usuario Financiero

- a. El usuario financiero podrá interponer un reclamo ante la entidad financiera. El reclamo podrá realizarse por las siguientes formas: vía telefónica, correo electrónico o fax, o en la sucursal del banco. Independientemente de la vía utilizada por el usuario, éste siempre deberá presentarse en la sucursal bancaria para formalizar la gestión.
- b. El usuario financiero debe interponer una denuncia judicial ante el Organismo de Investigación Judicial por el monto del perjuicio. Posteriormente, presentarse a la entidad financiera con el fin de confirmar el reclamo firmando toda la documentación relacionada, para lo cual se debe identificarse, adecuadamente, con el personal

respectivo presentando su cédula de identidad, y respondiendo a aquellas interrogantes necesarias para corroborar su identidad. Asimismo deberá verificar las firmas autorizadas en las cuentas bancarias. Todo lo anterior, de acuerdo con el procedimiento establecido a lo interno de cada banco

- c. Se le debe consultar al usuario financiero si ha proporcionado su información personal y bancaria a una tercera persona, en cuyo caso se deberá realizar las siguientes gestiones:
 - Revisar los movimientos de las cuentas bancarias del usuario y verificar si se han realizado transacciones fraudulentas.
 - En caso de que exista fraude bloquear las cuentas bancarias.
- d. El funcionario que recibe el reclamo deberá informar al Departamento de Seguridad sobre la existencia de una alerta de un delito informático para que proceda a realizar la restricción de las cuentas del usuario para que solo reciban depósitos, brindar una nueva clave de seguridad para realizar sus transacciones en línea. Adicionalmente, y para mayor seguridad, el banco podrá decidir proceder al cierre de la cuenta y la apertura de una nueva.
- e. El Departamento de Seguridad realizará el análisis del reclamo presentado por el usuario financiero y genera un informe del mismo y debe comunicar al cliente y al área de investigaciones del banco sobre la resolución del caso.
- f. La comunicación al cliente referente al avance de la investigación y al manejo de su reclamo, se llevará a cabo de acuerdo a los protocolos internos con los que cada institución cuente.
- g. La recopilación, mantenimiento y resguardo de toda la información documental, electrónica y demás que sea necesaria para la atención, esclarecimiento y seguimiento institucional y policial, será responsabilidad del área de seguridad que cada institución tenga determinada para ese fin.

ANEXO A

INFORMACIÓN A RECOPIRAR POR LAS ENTIDADES BANCARIAS

Cuenta Afectada

1. Detalle de los reportes de extravío y robo de las tarjetas del usuario financiero y número de cédula de identidad. Especificar la fecha y hora de reporte, número de tarjeta, tipo de tarjeta.
2. Detalle de los movimientos y eventos registrados en la bitácora del servicio web Internet Banking del número de identificación (código de usuario) del usuario financiero.
3. Detalle de los funcionarios del banco que efectuaron consultas, reimpresión de tarjetas o el número de identificación personal (PIN) u otra acción en torno a la cuenta del usuario financiero, así como a la identificación de la persona titular de dicha cuenta y sus autorizados. Identificar: código de usuario, número de identificación, nombre del funcionario, fecha, hora, dirección IP, nombre del sistema involucrado, descripción del evento.



4. Indicar si el usuario financiero tenía activo algún mecanismo adicional de validación de su número de identificación (código de usuario) en el servicio web Internet Banking, a saber: tarjeta de clave dinámica, token, entre otros, para lo que se debe identificar el detalle de la asignación y activación del dispositivo, así como el número de identificación de éste, la oficina y el nombre del funcionario que realizó el trámite.
5. Histórico de movimientos de la cuenta del usuario financiero.

Cuenta Destino

1. Documentación original de la apertura de la cuenta (contrato, recibos de servicios públicos, autorizados, etc.).
2. Históricos de movimientos recientes en ventanilla y cajeros automáticos, compras ligadas a las cuentas, acreditaciones de fondos, comprobantes originales de las transacciones. Resguardar la secuencia fotográfica y los videos de seguridad en donde se hizo cada uno de los retiros.
3. Detalle de los movimientos y eventos registrados en la bitácora del servicio web Internet Banking del usuario financiero (código de usuario) titular de la cuenta.
4. Detalle de reportes de extravío de las tarjetas asociadas a la cuenta destino.
5. En el caso de existir transferencias de fondos de la cuenta destinataria hacia otras cuentas, que se presume son parte o la totalidad de los dineros provenientes de la cuenta afectada en el Banco de donde proviene la sospecha; debe suministrarse la información detallada en los apartados anteriores.