Estrategia de Reducción de Fraudes para puntos Finales del SIPAP

Departamento de Ciberseguridad

Versión 1.1

INFORMACIÓN DEL DOCUMENTO

Nombre:	**Estrategia de Reducción de Fraudes para puntos Finales del SIPAP**
Código:	BCP-EST-FRA-END
Descripción:	Documento que establece el compromiso de los Participantes del SIPAP en la colaboración para la detección, prevención y denuncia de casos de fraude
Versión Actual:	1.1
Fecha Finalización:	17/06/2025

VERSIONES DEL DOCUMENTO

Versión	Fecha	Autor	Comentarios
1.0	24/03/2025	Departamento de Ciberseguridad	Versión inicial
1.1	28/05/2025	Departamento de Ciberseguridad	Revisión de documentos del Banco Mundial

DOCUMENTOS BASE

Documento	Fecha de Publicación
LEY N° 7.503.- SISTEMA NACIONAL DE PAGOS.	Junio 2025
BIS - Reducing the risk of wholesale payments fraud related to endpoint security.	Mayo 2018
BIS - Digital fraud and banking: supervisory and financial stability implications.	Noviembre 2023

DOCUMENTOS RELACIONADOS

Documento	Fecha de Publicación
Banco Mundial - Fraud risks in fast payments.	Octubre 2023

CONTENIDO

1. INTRODUCCIÓN 4
2. OBJETIVO GENERAL 5
3. OBJETIVOS ESPECÍFICOS 5
4. ALCANCE 5
5. DEFINICIONES Y ACRÓNIMOS 6
6. FRAUDE EN EL CONTEXTO DEL SIPAP 7
7. SIPAP: PARTICIPANTES Y ECOSISTEMA 8
8. ESTRATEGIA DE REDUCCIÓN DE FRAUDES 10
9. ROLES Y RESPONSABILIDADES 10
10. ELEMENTOS Y PRÁCTICAS DE LA ESTRATEGIA 12
10.1. Elemento 1: Identificar y comprender el alcance del riesgo 12
10.2. Elemento 2: Establecer requisitos de seguridad de puntos finales 13
10.3. Elemento 3: Promover el cumplimiento 14
10.4. Elemento 4: Proveer y utilizar información y herramientas para mejorar la prevención y detección 15
10.5. Elemento 5: Responder de manera oportuna a un potencial fraude 15
10.6. Elemento 6: Apoyar la capacitación continua, la concienciación y el intercambio de información 16
10.7. Elemento 7: Mejora continua de los controles de seguridad 17
11. APRENDIZAJE Y EVOLUCIÓN 19

1. INTRODUCCIÓN

En el contexto de una creciente sofisticación de los fraudes en los sistemas de pagos, el Comité de Pagos e Infraestructuras de Mercado (CPMI) ha impulsado una iniciativa internacional orientada a reforzar la seguridad de dichos sistemas. Esta iniciativa involucra a bancos centrales, infraestructuras de mercados financieros y demás instituciones del sector, con un enfoque particular en los puntos finales como eslabones críticos en la cadena de transacciones.

En línea con esta iniciativa, el Banco Central del Paraguay (BCP) ha desarrollado la presente Estrategia de Reducción de Fraudes para los Puntos Finales del SIPAP, con el propósito de guiar y fortalecer los esfuerzos de prevención, detección y respuesta frente a posibles fraudes en el Sistema de Pagos del Paraguay (SIPAP).

Esta estrategia busca fomentar la cooperación entre todos los Participantes del ecosistema (incluyendo Participantes directos, indirectos, subparticipantes, patrocinadores, reguladores y supervisores) promoviendo un enfoque coordinado y proactivo en la protección de las infraestructuras críticas del sistema de pagos. Al reducir los riesgos de fraude, se contribuye directamente a la estabilidad y confianza en el sistema financiero nacional.

El documento establece un conjunto de lineamientos estratégicos que deberán ser adoptados por todos los Participantes del SIPAP, con foco específico en las operaciones realizadas a través del Sistema de Pagos Instantáneos (SPI) y el Sistema de Liquidación Bruta en Tiempo Real (LBTR). El objetivo central es minimizar la probabilidad de fraudes en las órdenes de transferencia de fondos, promoviendo al mismo tiempo una cultura de seguridad, cooperación y mejora continua.

2. OBJETIVO GENERAL

Establecer una estrategia integral para la mitigación de fraudes en las órdenes de transferencia de fondos procesadas a través del Sistema de Pagos del Paraguay (SIPAP), con énfasis en la seguridad de los puntos finales, a fin de fortalecer la confianza, eficiencia y estabilidad del sistema financiero nacional.

3. OBJETIVOS ESPECÍFICOS

- Definir los lineamientos estratégicos que orienten a los Participantes del SIPAP en la prevención, detección y respuesta frente a eventos de fraude en los puntos finales.
- Establecer los componentes esenciales de la estrategia aplicables de manera uniforme a todas las entidades Participantes del sistema.
- Determinar los mecanismos de seguimiento y verificación del cumplimiento, adopción e implementación de la estrategia por parte de los Participantes.
- Fomentar una cultura de seguridad, colaboración e intercambio de información entre los actores del ecosistema de pagos.

4. ALCANCE

Los lineamientos establecidos en este documento deben ser aplicados por todas las entidades Participantes del SIPAP, incluyendo a los Participantes directos, indirectos, patrocinadores y subparticipantes que operen a través del Sistema de Pagos Instantáneos (SPI) y el Sistema de Liquidación Bruta en Tiempo Real (LBTR) y otros sistemas que procesen órdenes de transferencias de fondos hacia estos.

En particular, los Participantes patrocinadores serán responsables de asegurar que sus patrocinados o subparticipantes cumplan con los requisitos y controles establecidos en la presente estrategia. Para ello, deberán implementar mecanismos de evaluación, monitoreo y verificación periódica que garanticen el adecuado nivel de seguridad en los puntos finales utilizados por sus asociados.

Esta estrategia se aplica exclusivamente a las operaciones canalizadas a través del SPI y del LBTR, quedando fuera de su alcance otros tipos de transacciones o sistemas no contemplados expresamente en este documento.

5. DEFINICIONES Y ACRÓNIMOS

BCP: Banco Central del Paraguay.

SIPAP: Sistemas de Pagos del Paraguay, administrado por el BCP, que incluye las siguientes Soluciones Tecnológicas: i) LBTR – Liquidación Bruta en Tiempo Real; ii) ACH - Cámara Compensadora Automatizada; iii) SPI - Sistema de Pagos Instantáneos; iv) DEPO - Depositaria de Valores; v) SML - Sistema de Pagos en Moneda Local, interconexión con otros Bancos Centrales con los cuales se tiene convenio firmado, y su correspondiente conexión con los sistemas expuestos más arriba; iv) Otros sistemas autorizados por el BCP.

Liquidación Bruta en Tiempo Real (LBTR): Es un sistema de liquidación bruta de pagos, procesados en tiempo real, que permite las transferencias electrónicas de fondos propios de los Participantes o por orden de sus clientes, en forma individual y continua, es decir, de una en una, sin neteo, donde la liquidación es definitiva e irrevocable, incluyendo operaciones propias del BCP. Además, incluye la liquidación definitiva de posiciones netas de otros Sistemas de Pagos. De igual forma, las entidades que participen de algún sistema de pagos administrado por el BCP deberán liquidar sus operaciones en la moneda y transacciones autorizadas al momento de su participación.

Sistema de Pagos Instantáneos (SPI): Es un sistema que procesa pagos, en el que la transmisión del mensaje de pago y la disponibilidad de los fondos finales al beneficiario se produce en tiempo real, durante las 24 horas del día, los 7 días de la semana. La liquidación final en la cuenta de los Participantes se realiza a través de un proceso de compensación en el LBTR de conformidad a las reglas operativas emitidas sobre dicho servicio.

Red de mensajería: Se refiere a la infraestructura y los protocolos que permiten la transmisión de información entre los diferentes Participantes involucrados en el proceso de pago.

Fraude: Cualquier acto deliberado de engaño o manipulación en las órdenes de transferencia de fondos dentro del ecosistema SIPAP, específicamente en el LBTR y SPI, con la intención de causar una pérdida financiera a una o varias partes involucradas, o comprometer la integridad y estabilidad del SIPAP.

Punto final: un punto en el lugar y el momento en el que se intercambia información de instrucciones de pago entre dos partes en el ecosistema SIPAP, como entre:

- Una red de mensajería y un Participante en la red;
- Un sistema de pago y un Participante en el sistema;

- Un sistema de pago y una red de mensajería;
- Un Participante y otro Participante.

Un punto final no se relaciona únicamente con las partes en cualquiera de los extremos de una cadena de transacciones de órdenes de transferencias de fondos, sino con cada eslabón de la cadena a medida que transmite o recibe instrucciones en nombre de ellos mismos o de otros. La seguridad del punto final se basa en medidas tomadas con respecto al hardware, software, acceso físico y acceso lógico, junto con la organización y los procesos que los rodean.

En el contexto de la presente estrategia, puntos finales (endpoints) se refiere a los dispositivos y sistemas tecnológicos que se conectan directamente a una infraestructura crítica de pagos o liquidación, como el LBTR y el SPI.

Específicamente, los puntos finales comprenden, entre otros, los siguientes:

- Servidores de los Participantes (bancos, financieras, cámaras, casas de bolsa, etc.) que se conectan a la infraestructura.
- Estaciones de trabajo (computadoras) utilizadas para operar sistemas que interactúen con el LBTR y/o el SPI.
- Puntos de conexión (redes de comunicación, servicios web y otras formas de conexión) al LBTR y/o SPI que ofrecen los Participantes a sus clientes finales para procesar órdenes de transferencias de fondos.
- Cualquier otro dispositivo o sistema que permita enviar, recibir o procesar órdenes de transferencias de fondos al LBTR y/o SPI.

CPMI (*Committee on Payments and Market Infrastructures)*: es un organismo internacional que establece normas, promueve, supervisa y formula recomendaciones sobre la seguridad y la eficiencia de los pagos, la compensación, la liquidación y otros mecanismos relacionados, apoyando así la estabilidad financiera y la economía en general.

IOSCO (*International Organization of Securities Commissions*): es un organismo internacional que reúne a los reguladores de valores del mundo y es reconocida como la entidad que establece los estándares globales para la regulación de los mercados financieros.

6. FRAUDE EN EL CONTEXTO DEL SIPAP

El fraude representa una de las amenazas más críticas y dinámicas para el SIPAP. Su creciente sofisticación, exige que los Participantes adopten medidas proactivas para protegerse no solo de pérdidas económicas directas, sino también del riesgo sistémico que surge de la pérdida de confianza en el ecosistema.

El fraude se manifiesta de diversas formas que pueden impactar directamente al ecosistema del SIPAP. Algunas de estas formas pueden ser:

1. **Fraudes sobre la Orden de Transferencia:** Esta es la forma más directa de fraude, donde el objetivo es la transacción en sí. Puede ocurrir mediante:

   Transacciones no autorizadas: Los atacantes roban las credenciales de los clientes para ejecutar transferencias sin su consentimiento, usualmente a través de software malicioso (malware) o phishing.

   Manipulación del ordenante: Se engaña al cliente legítimo para que, actuando de buena fe, autorice un pago a una cuenta fraudulenta, a menudo suplantando la identidad del Participante (spoofing).

2. **Fraude de Productos o Servicios Financieros:** El engaño se extiende más allá de las transferencias, involucrando la promoción de productos falsos (fondos de inversión, préstamos, u otros) para que los clientes entreguen su dinero voluntariamente bajo falsas promesas.

3. **Ataques directos al Participante:** En esta modalidad, el Participante es el objetivo principal. Los defraudadores pueden usar datos de clientes robados para abrir cuentas intermediarias (cuentas mula) destinadas al blanqueo de capitales o, en ataques más complejos, comprometer directamente los sistemas del Participante para manipular datos y ejecutar fraudes a gran escala.

Entender que las tácticas antes descriptas representan el panorama actual, que no son de ninguna manera exhaustivas ni permanentes nos ayudaran a ver al fraude como lo que realmente es, una amenaza dinámica que evoluciona tanto como la tecnología. El fraude, especialmente en sus formas digitales, es un riesgo que se vuelve cada vez más sofisticado y se espera que evolucione aún más.

7. SIPAP: PARTICIPANTES Y ECOSISTEMA

Un sistema de pagos seguro, confiable y eficiente constituye un componente esencial para el funcionamiento estable del sistema financiero. En Paraguay, el Sistema de Pagos del Paraguay (SIPAP) está respaldado por una infraestructura tecnológica y una red de mensajería que interconecta a sus Participantes, conformando un ecosistema complejo y dinámico.

El Banco Central del Paraguay (BCP), en su rol de administrador, operador y propietario del SIPAP, asume la responsabilidad de velar por la integridad, disponibilidad y seguridad del sistema. Esto resulta especialmente relevante considerando que el SIPAP también es utilizado como herramienta clave para la implementación de la política monetaria y la provisión de liquidez al sistema financiero.

En este ecosistema, la evolución constante de los riesgos, en particular aquellos asociados al fraude, exige una vigilancia continua. Las vulnerabilidades en los puntos finales (conexiones a través de las cuales se transmiten instrucciones de órdenes de transferencias de fondos) pueden ser explotadas por actores maliciosos, afectando no solo a entidades individuales, sino comprometiendo la confianza en el sistema en su conjunto.

Por tanto, garantizar la seguridad de los puntos finales requiere la participación coordinada de todos los actores involucrados: Participantes directos, indirectos, patrocinadores, subparticipantes o patrocinados, así como los órganos reguladores y supervisores. La colaboración efectiva entre estos actores es fundamental para anticipar, mitigar y responder de manera oportuna a los riesgos emergentes, contribuyendo así a la solidez y resiliencia del SIPAP.

La potencial falta de confianza en la integridad del sistema en su conjunto podría provocar que precauciones individuales, tomadas por los Participantes ante posibles preocupaciones sobre la seguridad de la red que forma parte del ecosistema, su propia protección o la de otros miembros, originen un obstáculo significativo en el procesamiento de pagos, disminuyan la liquidez en los mercados financieros y generen una acumulación de transacciones pendientes de liquidación, así como exposiciones crediticias bilaterales entre las instituciones financieras. En este escenario, los Participantes podrían verse motivados a implementar medidas de control adicionales antes de ejecutar pagos, o incluso optar por limitar o cesar el procesamiento de las órdenes de pago. En el peor de los casos, tales medidas podrían eventualmente restringir la actividad económica y afectar la estabilidad financiera. Al abordar el riesgo potencial de fraude en sistemas de pagos para el sistema financiero y la economía en general, se identifican los diferentes desafíos:

- Los fraudes en los sistemas de pagos están volviéndose más complejos y se espera que sigan aumentando.

- Los sistemas de pagos, en especial el LBTR y el SPI, ofrecen procesamientos inmediatos y definitivos de las transacciones, lo que los hace particularmente atractivos para actividades fraudulentas. Esta inmediatez y finalidad no solo los convierten en blancos preferentes de fraude, sino que también complican la gestión y mitigación del riesgo asociado.

Para que la seguridad sea efectiva en los puntos finales, es crucial el apoyo conjunto de los Participantes del SIPAP y de aquellos encargados de controlar o supervisar cada punto final, garantizando así que los controles apropiados estén implementados y funcionando de manera eficaz.

El Banco Central del Paraguay, en su calidad de administrador del SIPAP, y los organismos reguladores y supervisores, tienen un rol clave en fomentar esta

coordinación, estableciendo lineamientos, monitoreando el cumplimiento e impulsando el desarrollo de capacidades conjuntas. Solo a través de una actuación articulada y continua será posible mitigar los riesgos de fraude, preservar la confianza de los usuarios y asegurar la estabilidad del sistema de pagos en su conjunto.

8. ESTRATEGIA DE REDUCCIÓN DE FRAUDES

La presente estrategia está dirigida a todos los actores involucrados en el Sistema de Pagos del Paraguay (SIPAP), incluyendo al Banco Central del Paraguay (BCP), entidades Participantes, así como a sus reguladores y supervisores. Su propósito es establecer un marco de referencia común para la prevención, detección, respuesta y comunicación frente a incidentes de fraude que pudieran afectar la integridad del sistema de pagos, con énfasis en los puntos finales.

La estrategia se compone de siete elementos clave, diseñados para funcionar de manera integral, abordando la prevención, detección, respuesta y comunicación frente al fraude. Los elementos ofrecen lineamientos generales que permiten flexibilidad en su aplicación, facilitando así la adaptación y su ejecución operativa, considerando los cambios en el entorno de riesgos y la evolución de tecnologías y herramientas de gestión de riesgo.

Si bien esta estrategia se alinea con los estándares internacionales, en particular el documento *Reducción del riesgo de fraude en pagos mayoristas relacionado con la seguridad de los puntos finales* (Reducing the risk of wholesale payments fraud related to endpoint security), no pretende reemplazar las normativas vigentes, sino complementarlas, reforzando especialmente la protección de los puntos finales del SIPAP.

Cada elemento de la estrategia contribuye a fortalecer la seguridad en los sistemas SPI y LBTR, promoviendo una gestión integral del riesgo de fraude.

9. ROLES Y RESPONSABILIDADES

Banco Central del Paraguay (BCP): Su rol como administrador, operador y supervisor del SIPAP asume las siguientes responsabilidades específicas dentro de esta estrategia:

- Establecer los requisitos de seguridad en los puntos finales para los Participantes del SIPAP como parte de los requisitos de participación.
- Emitir lineamientos generales para orientar la implementación de controles relacionados con la seguridad en los puntos finales.
- Poner a disposición los mecanismos pertinentes para llevar a cabo las autoevaluaciones obligatorias de cumplimiento de los requisitos de seguridad.

- Supervisar que los Participantes aborden las debilidades de seguridad identificadas mediante la implementación de planes de remediación.

Participantes y Proveedores de Redes de Mensajería: Sus responsabilidades en la implementación de los siete elementos de la estrategia son:

- Identificar y comprender el alcance de los riesgos asociados con la seguridad de los puntos finales, incluyendo los riesgos de pérdida de confianza en la integridad del SIPAP.
- Establecer sus propias medidas de seguridad en los puntos finales, basadas en riesgos, según sea necesario, además de cumplir con los requisitos del BCP.
- Contar con procesos para promover el cumplimiento de sus respectivos requisitos de seguridad en los puntos finales.
- Adoptar y utilizar, en la medida de lo posible, información y herramientas que mejoren sus capacidades para prevenir y detectar intentos de fraude.
- Contar con procedimientos y prácticas que les permitan responder de manera oportuna y eficaz ante eventos de fraude, reales o sospechados.
- Establecer procedimientos y prácticas, así como destinar los recursos necesarios, que favorezcan la capacitación continua y la concienciación sobre los riesgos de seguridad en los puntos finales.
- Monitorear de forma continua la evolución de los fraudes y los riesgos de seguridad en los puntos finales, así como la efectividad de los controles implementados, revisando y actualizando sus medidas de seguridad.

Participantes Patrocinadores: Deben asegurar que sus patrocinados o subparticipantes cumplan con los siguientes puntos:

- Asegurar que sus patrocinados o subparticipantes cumplan con los requisitos y controles establecidos en la presente estrategia.
- Implementar mecanismos de evaluación, monitoreo y verificación periódica que garanticen el adecuado nivel de seguridad en los puntos finales utilizados por sus asociados.
- Informar al BCP el estado de cada patrocinado en lo que respecta al cumplimiento de esta estrategia.

Participantes y Subparticipantes: Deben adherirse a los requisitos establecidos por los Participantes patrocinadores e implementar medidas de seguridad en sus propios puntos finales.

10. ELEMENTOS Y PRÁCTICAS DE LA ESTRATEGIA

10.1. Elemento 1: Identificar y comprender el alcance del riesgo

Los Participantes identificarán y comprenderán el alcance de los riesgos asociados con la seguridad de los puntos finales, incluyendo los riesgos de potenciales pérdidas de confianza en la integridad del SIPAP.

Para hacer operativo este elemento, se deberán implementar las siguientes prácticas:

Evaluación de riesgo anual formal: cada Participante deberá llevar a cabo una evaluación de riesgo anual formal para identificar los riesgos de seguridad de los puntos finales. Esta evaluación deberá considerar explícitamente el riesgo de que los Participantes y otras partes interesadas pierdan la confianza en la integridad del SIPAP como resultado de casos de fraude.

Colaboración con proveedores externos: los Participantes podrán utilizar proveedores externos para realizar pruebas de intrusión, simulaciones de crisis u otros mecanismos que les permitan identificar vulnerabilidades y mejorar sus controles internos. Cuando estas actividades afecten al SIPAP, se requerirá aviso y autorización previa del BCP.

Consultas con Organismos Regionales: se recomienda que los Participantes mantengan contacto con organismos regionales o foros especializados, a fin de identificar riesgos transversales y nuevas amenazas relevantes.

Desarrollo de procedimientos de reporte: cada Participante deberá establecer procedimientos internos para la detección, documentación y comunicación oportuna de incidentes o sospechas de fraude, estas deben estar alineadas a las normas vigentes.

Proceso continuo de concienciación de clientes: los Participantes deberán desarrollar un proceso continuo de concienciación de los clientes sobre la importancia de la seguridad a través de canales de comunicaciones adecuados.

Evaluación del entorno tecnológico: cada Participante deberá realizar una evaluación periódica del entorno tecnológico actual y emergente que pueda afectar la seguridad de los puntos finales, considerando nuevas amenazas, vulnerabilidades y vectores de ataque.

Plan de acción integral: los Participantes deberán desarrollar y mantener actualizado un plan de acción integral para abordar los riesgos identificados. Este

plan deberá incluir medidas preventivas, de detección y respuesta, una asignación clara de responsabilidades y consideraciones.

10.2. Elemento 2: Establecer requisitos de seguridad de puntos finales

El BCP establecerá requisitos de seguridad en los puntos finales para sus Participantes como parte de los requisitos de participación. Dichos requisitos podrán incluir medidas para la prevención y detección de fraudes, para la respuesta inmediata ante fraudes y, cuando corresponda, para alertar sobre amenazas de fraude emergentes.

Además de los requisitos establecidos por el BCP, cada Participante del SIPAP debe identificar y establecer sus propias medidas de seguridad en los puntos finales, basadas en riesgos, según sea necesario.

Para hacer operativo este elemento, se deberán implementar las siguientes prácticas:

Establecimiento de requisitos de seguridad: cada Participante será responsable de implementar, mantener y fortalecer los requerimientos de seguridad establecidos por el BCP. Se deben establecer controles de seguridad que abarquen componentes técnicos, físicos y organizacionales. Esto incluye, entre otros, el resguardo del hardware, software, accesos físicos y lógicos, así como procedimientos operativos seguros para el tratamiento de órdenes de transferencias de fondos. Además, cada Participante podrá incluir requerimientos propios de seguridad en los puntos finales, adecuados a su contexto operativo y perfil de riesgo.

Uso de tecnologías avanzadas: los Participantes deberán evaluar la adopción de tecnologías avanzadas, como inteligencia artificial o sistemas automatizados de monitoreo, cuando estas contribuyan a mejorar la detección y prevención del fraude.

Implementación de procedimientos de respuesta rápida: los Participantes tienen la responsabilidad de desarrollar, implementar y mantener procedimientos claros y efectivos para responder de manera inmediata a las alertas de fraude.

Integración de requerimientos de seguridad en tecnologías: los Participantes deberán incorporar los requerimientos de seguridad diseñados para prevenir, detectar, responder inmediatamente al fraude, y comunicar alertas sobre amenazas de fraude, dentro de las reglas y configuraciones de sus sistemas y tecnologías operativas. Esta integración deberá incluir medidas concretas, como la configuración de sistemas de detección de intrusiones, herramientas de análisis de transacciones en tiempo real, y procedimientos de notificación de incidentes,

asegurando así que las capacidades de respuesta ante el fraude sean parte inherente y efectiva de las operaciones diarias.

10.3. Elemento 3: Promover el cumplimiento

Con base en la comprensión de los riesgos y en los requisitos de seguridad, los Participantes deben contar con procesos, según sea necesario, para promover el cumplimiento de los respectivos requisitos de seguridad en los puntos finales.

El BCP podrá emitir lineamientos generales para orientar la implementación de controles relacionados con la seguridad en los puntos finales. No obstante, corresponde a cada entidad Participante definir, implementar y mantener los mecanismos necesarios para dar cumplimiento a los requisitos de seguridad, en función de sus propios riesgos y características operativas.

Para hacer operativo este elemento, se deberán implementar las siguientes prácticas:

Autoevaluaciones Periódicas: los Participantes deberán realizar autoevaluaciones de cumplimiento de los requisitos establecidos al menos una vez al año o según lo requiera el BCP. El BCP pondrá a disposición los mecanismos pertinentes para llevar a cabo las autoevaluaciones obligatorias, como plataformas web de autoevaluación y/o modelos de evaluación independiente.

Planes de remediación: el BCP podrá solicitar que los Participantes aborden las debilidades de seguridad identificadas mediante la implementación de planes de remediación. Dichos planes deberán incluir acciones correctivas específicas, plazos para la remediación y asignación de responsabilidades.

El BCP podrá supervisar el progreso de los planes de remediación y tomar medidas adicionales si se detecta un incumplimiento persistente. Los Participantes deberán remediar todas las debilidades detectadas que puedan afectar los controles de prevención de fraude.

Revisión y supervisión: los Participantes deberán establecer mecanismos internos de revisión periódica para evaluar el cumplimiento continuo de los controles de seguridad. Cuando se considere necesario, podrán recurrir a auditorías independientes como medida adicional de validación.

Capacitación y concienciación: cada Participante deberá promover internamente una cultura de cumplimiento, a través de campañas de concienciación, talleres u otros mecanismos de sensibilización adecuados a su organización.

10.4. Elemento 4: Proveer y utilizar información y herramientas para mejorar la prevención y detección

Los Participantes deberán adoptar y utilizar, en la medida de lo posible, información y herramientas que mejoren sus capacidades para prevenir y detectar, de manera oportuna, intentos de fraude en órdenes de transferencias de fondo de bajo (SPI) y alto valor (LBTR).

Para hacer operativo este elemento, se deberán implementar las siguientes prácticas:

Colaboración y comunicación: los Participantes deberán adoptar mecanismos para recopilar, analizar y utilizar información relevante que contribuya a la detección y prevención de fraudes en sus operaciones realizadas a través del SPI y el LBTR.

Herramientas de detección y prevención: cada Participante deberá implementar sistemas de monitoreo que permitan identificar patrones inusuales o comportamientos anómalos asociados a intentos de fraude. Se alienta el uso de tecnologías avanzadas como inteligencia artificial, aprendizaje automático (machine learning) o análisis de comportamiento cuando sean técnicamente viable.

Los Participantes deberán mantener actualizadas sus herramientas y procesos de prevención y detección, incorporando nuevas metodologías, funciones o reglas en respuesta a amenazas emergentes o vulnerabilidades detectadas.

Mecanismos de colaboración: los Participantes podrán establecer mecanismos seguros de intercambio de información, alertas y buenas prácticas con otros actores del ecosistema SIPAP. Esto podrá incluir su participación en grupos sectoriales, foros técnicos o espacios colaborativos.

Evaluación y mejora continua: los Participantes deberán realizar auditorías y evaluaciones periódicas de los sistemas de detección y prevención para identificar áreas de mejora.

10.5. Elemento 5: Responder de manera oportuna a un potencial fraude

Los Participantes deberán contar con procedimientos y prácticas que les permitan responder de manera oportuna y eficaz ante eventos de fraude, reales o sospechados. Esto incluye, cuando sea posible y apropiado, apoyar la comunicación oportuna y la atención de solicitudes de acción sobre instrucciones de órdenes de transferencias de fondo potencialmente fraudulentas. Estas acciones deberán implementarse conforme a los protocolos

y mecanismos establecidos por los Participantes, sin alterar la finalidad de las órdenes de transferencia de fondos que ya hayan sido liquidadas.

Para hacer operativo este elemento, se deberán implementar las siguientes prácticas:

Procedimientos de respuesta ante incidentes: los Participantes deberán asegurar que estos procedimientos incluyan la identificación, notificación y mitigación de fraudes. Es esencial que estos procedimientos especifiquen claramente los canales y puntos de contacto para la comunicación de incidentes, incluyendo información de contacto relevante para situaciones de emergencia fuera del horario laboral habitual. Esto garantizará que se puedan tomar medidas rápidas y coordinadas en cualquier momento, maximizando la capacidad de mitigación y respuesta ante incidentes de fraude.

Canales de comunicación: el BCP establecerá canales de comunicación claros y eficientes para reportar incidentes de fraude.

Capacitación y simulacros de respuesta a incidentes: los Participantes deberán realizar capacitaciones periódicas de prevención y detección de fraude, además deberán llevar a cabo simulacros para asegurar que estén preparados para responder a incidentes de fraude. Los simulacros deberán evaluar la eficacia de los procedimientos de respuesta y proporcionar retroalimentación para mejoras.

Evaluación y mejora continua: los Participantes deberán realizar auditorías periódicas y evaluaciones de los procedimientos de respuesta a incidentes de fraude para identificar áreas de mejora. Los Participantes deberán incorporar los resultados obtenidos de estas auditorias y evaluaciones continuas sobre incidentes pasados y realizar ajustes necesarios para fortalecer la capacidad de respuesta.

10.6. Elemento 6: Apoyar la capacitación continua, la concienciación y el intercambio de información

Los Participantes deberán establecer procedimientos y prácticas, así como destinar los recursos necesarios, que favorezcan la capacitación continua y la concienciación sobre los riesgos de seguridad en los puntos finales. Asimismo, deberán promover, en la medida en que sea apropiado y legalmente permitido, el intercambio de información relevante sobre la evolución de dichos riesgos y los controles aplicables.

Para hacer operativo este elemento, se deberán implementar las siguientes prácticas:

Programas de capacitación continua: cada Participante deberá desarrollar e implementar programas de capacitación continua orientados a su personal, con el objetivo de fortalecer las competencias en prevención del fraude y protección de puntos finales. Estos programas deberán ser actualizados regularmente, incorporando nuevas amenazas y tecnologías.

Medios de concienciación: los Participantes deberán implementar campañas de concientización dirigidas a su personal y clientes sobre la importancia de la seguridad en los puntos finales. Estas campañas deberán utilizar diversos medios de comunicación, incluyendo talleres, seminarios y materiales educativos en línea.

Intercambio de información: los Participantes deberán promover el intercambio de información a través de plataformas para su difusión mediante mecanismos seguros.

Evaluación y mejora de programas de capacitación: los Participantes deberán realizar evaluaciones periódicas de los programas de capacitación para identificar áreas de mejora. Incorporar la retroalimentación de los Participantes y ajustar los programas de capacitación según sea necesario para asegurar su efectividad y relevancia.

10.7. Elemento 7: Mejora continua de los controles de seguridad

Los Participantes deberán monitorear de forma continua la evolución de los fraudes y los riesgos de seguridad en los puntos finales, así como la efectividad de los controles implementados. Con base en ese análisis, deberán revisar y actualizar sus requerimientos, procedimientos, prácticas y recursos de seguridad, a fin de fortalecer su capacidad de prevención, detección y respuesta ante amenazas emergentes.

Para hacer operativo este elemento, se deberán implementar las siguientes prácticas:

Monitoreo continuo de riesgos: los Participantes deberán monitorear de forma continua la evolución de los fraudes y los riesgos de seguridad en los puntos

finales, revisando la efectividad de sus controles y actualizándolos conforme a las amenazas emergentes.

Revisión y actualización de controles de ciberseguridad: los Participantes deberán revisar y actualizar regularmente los controles de ciberseguridad implementados. Esto incluye la evaluación de la efectividad de los controles actuales y la implementación de mejoras basadas en las últimas prácticas y tecnologías disponibles.

Coordinación y colaboración: los Participantes deberán fomentar la coordinación y colaboración entre todas las partes interesadas. Esto incluye la participación en grupos de trabajo, la asistencia a conferencias y talleres sobre ciberseguridad, así como intercambio de información y mejores prácticas con otros Participantes del SIPAP y con organismos regionales e internacionales.

Aprendizaje y adaptación: los Participantes deberán mantener una cultura de aprendizaje continuo y adaptación. Esto implica la integración de las lecciones aprendidas de incidentes de seguridad y ejercicios de simulación en las políticas y procedimientos de seguridad.

Evaluaciones de ciberseguridad: el BCP y los Participantes deberán llevar a cabo evaluaciones periódicas de los riesgos y controles de seguridad. Estas evaluaciones deberán ser sistemáticas y basarse en métricas claras y objetivas para garantizar la efectividad de las estrategias de seguridad implementadas.

Implementación de nuevas tecnologías: los Participantes deberán monitorear la evolución de las tecnologías de seguridad y considerar la implementación de nuevas soluciones que puedan mejorar la protección de los puntos finales. Esto incluye la adopción de herramientas avanzadas de inteligencia artificial, aprendizaje automático y análisis de big data para la detección y prevención de fraudes.

11. APRENDIZAJE Y EVOLUCIÓN

El panorama financiero actual, caracterizado por una rápida digitalización y una creciente sofisticación del fraude, hace imperativo que la seguridad del SIPAP sea abordada como un pilar fundamental para la estabilidad. Esta estrategia de reducción de fraudes no es solo una respuesta a los riesgos actuales, sino un marco proactivo diseñado para fortalecer la resiliencia del ecosistema frente a las amenazas futuras.

El éxito de esta iniciativa no recae únicamente en la acción del BCP, sino en el compromiso y la acción coordinada de todos los Participantes del ecosistema. La colaboración, el intercambio de información y la responsabilidad compartida son, por tanto, los ejes centrales sobre los cuales se construirá una defensa colectiva y eficaz.

Finalmente, la implementación de esta estrategia no debe ser vista como un evento único, sino como el inicio de un ciclo de mejora continua. El monitoreo constante, el aprendizaje derivado de los incidentes y la adaptación a un entorno de amenazas en permanente evolución son esenciales para mantener la relevancia y efectividad de los controles. El BCP, en su rol de administrador, acompañará este proceso, reafirmando su compromiso de velar por un sistema de pagos seguro, eficiente y, sobre todo, confiable, que sustente la estabilidad del sistema financiero nacional.

LUIS FERNANDO VERA ORTIZ

Firmado digitalmente por LUIS FERNANDO VERA ORTIZ
Fecha: 2025.07.11 09:39:36 -03'00'