BANCO CENTRAL DEL URUGUAY

Montevideo, 11 de enero de 2024

COMUNICACION N°2024/018

Ref: Comunicación de eventos vinculados a Tecnología, Sistemas y Seguridad de la Información – Actualización

Se pone en conocimiento de las instituciones reguladas y supervisadas por la Gerencia de Sistema de Pagos, la actualización en el requerimiento de información a presentar acerca de todo evento que pudiera afectar a los servicios y/o a sus clientes, que, por su impacto, implique una afectación al riesgo operacional o de reputación de la institución o del sistema de pagos en forma global.

A) Tipología de eventos

Los eventos a reportar podrán implicar, de manera no taxativa:

- Caídas de sistemas, propios o de terceros, que puedan afectar la operativa de la institución o interrumpir la prestación de servicios a los clientes.
- Afectación de un canal de atención al cliente, independientemente de su causa, ya sea por problemas en el propio canal o de un sistema que lo atienda.
- Dificultades para cumplir con las obligaciones inherentes al giro autorizado.
- Vulneración de sistemas, propios o de terceros, que derive en exposición o secuestro de información sensible al negocio o datos personales de los clientes u otras partes interesadas (por ejemplo: ataque de “Phishing” exitoso, encriptación de información, robo de identidad, vulneración de redes sociales institucionales, etc.).
- Todo aquel evento que, sin afectar a sistemas propios de la institución, igualmente puedan impactar en los servicios prestados y/o el reconocimiento de operaciones, exposición de datos sensibles, etc.

A su vez, cada institución deberá comunicar los eventos de esta naturaleza que afecten a sus proveedores de servicios tercerizados u ocurran en instalaciones de estos.

BANCO CENTRAL DEL URUGUAY

En todos los casos, deberán reportarse eventos que alcancen alguno de los siguientes umbrales:

1. Ameriten efectuar una comunicación a:
    a. Los clientes de la institución
    b. La Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC)
    c. La Unidad Reguladora y de Control de Datos Personales
    d. El Centro Nacional de Respuesta a Incidentes de Seguridad Informática
    e. Cualquier otra entidad o autoridad nacional.
2. Deriven en denuncia policial o judicial por parte de la institución.
3. Impliquen aplicación total o parcial del Plan de Continuidad del Negocio (BCP) o Plan de Recuperación de Desastres (DRP).
4. Implique la interrupción o afectación de servicios en algún canal de atención al cliente por un lapso igual o superior a 30 minutos.
5. Afecten la operativa de los servicios al 10% o más de los clientes.
6. Impliquen la exposición de información sensible y datos personales del 5‰ o más de los clientes.

B) Contenido de los reportes

Existirán tres tipos de reporte: inicial, de seguimiento y de cierre.

1. <u>Reporte Inicial</u>

El reporte inicial deberá contar con la siguiente información:

- Fecha y hora de detección del evento.
- Fecha y hora de ocurrencia de este.
- Descripción detallada tal cual se conoce al momento.
- Sistemas informáticos y áreas de negocio involucrados.
- Canales de atención al cliente afectados.
- Plan de acción para mitigar el evento.
- Nombre y teléfono del responsable de la institución asignado al caso.

2. <u>Reporte de Seguimiento</u>

Los reportes de seguimiento deberán contar con la siguiente información:

- Contenido del reporte inicial que no haya podido ser informado previamente o que haya sufrido modificaciones
- Ampliación de la descripción

BANCO CENTRAL DEL URUGUAY

- Estado de situación
- Avances, problemas o modificaciones en el plan de mitigación

3. Reporte de cierre

   El reporte de cierre deberá contar con la siguiente información:

   - Estado de situación al cierre
   - Análisis de causa del evento
   - Análisis de impacto del evento
   - Problemas o dificultades encontrados durante la ejecución del plan de mitigación
   - Planes de acción o medidas adoptadas para la prevención de la repetición del evento o justificación de su no adopción.

En todos los casos el Departamento de Normativa y Vigilancia de la Gerencia de Sistema de Pagos podrá requerir información adicional a la detallada.

C) Plazos de reporte

1. Reporte inicial:

Los eventos emergentes deberán comunicarse en un plazo máximo de 4 horas desde su detección. En los casos en que aún no se tenga toda la información disponible, la misma deberá ser completada en reportes posteriores.

Los eventos programados deberán comunicarse al menos 24 horas antes de su inicio.

En los casos previstos en los numerales 1 y 2 del punto A), el reporte a la Gerencia de Sistema de Pagos deberá realizarse al menos concomitantemente a las demás comunicaciones.

2. Reportes de seguimiento:

Los reportes de Seguimiento deberán realizarse cada 48 horas desde el reporte inicial hasta la resolución definitiva del evento.

3. Reporte de Cierre

El reporte de cierre deberá emitirse en un plazo máximo de 15 días corridos desde la resolución del evento.

En los casos en que aplique, podrán emitirse el reporte inicial y de cierre de forma conjunta.

BANCO CENTRAL DEL URUGUAY

El Departamento de Normativa y Vigilancia de la Gerencia de Sistema de Pagos podrá establecer plazos y periodicidad distinta para casos puntuales.

D) Modalidad de reporte

Se deberá informar al Departamento de Normativa y Vigilancia de la Gerencia de Sistema de Pagos mediante nota a través del **Portal IDI** (**tipo de dato 454** "eventos operativos y de ciber seguridad", por Trámites en Línea, opción disponible en la web del Banco - https://www.bcu.gub.uy/Acerca-de-BCU/Paginas/Tramites_Publico.aspx, o en caso excepcional, al correo electrónico de normativayvigilancia@bcu.gub.uy.

No se aceptarán como válidas las comunicaciones vía telefónica o las realizadas otras unidades organizativas del Banco Central.

E) Vigencia

Esta comunicación entra en vigor el 01/02/2024, fecha a partir de la cual queda sin efecto la comunicación 2023/147.

DE LOS HEROS MENDEZ, ANA CLAUDIA
GERENCIA DE SISTEMA DE PAGOS