Se refuerza la responsabilidad de los bancos por los créditos que otorgan a través de canales electrónicos

Las entidades financieras tendrán que verificar fehacientemente la identidad de las personas que solicitan la acreditación de créditos preaprobados a través de los canales electrónicos, por una medida resuelta por el Banco Central de la República Argentina para reforzar las normas de seguridad. Además, tendrán que hacer un monitoreo y control, como mínimo, de los puntos de contacto indicados por el usuario y comprobar que no hayan sido modificados recientemente.

La verificación deberá hacerse mediante técnicas de identificación positiva, lo que refuerza la obligación que ya tiene la entidad financiera de la responsabilidad de detectar la posibilidad de engaños de ingeniería social.

Recién después de la verificación, la entidad deberá comunicarle –a través de todos los puntos de contacto disponibles– que el crédito se encuentra aprobado y que, de no mediar objeciones, el monto será acreditado en su cuenta a partir de las 48 horas hábiles siguientes. El citado plazo de acreditación podrá ser reducido en el caso de recibirse la conformidad del usuario de servicios financieros de manera fehaciente.

El control deberá ser sobre todas las operaciones de créditos preaprobados realizadas a través de todos los canales electrónicos disponibles: ATMs, TAS, banca de internet (BI) y banca móvil (BM).

En diciembre del 2020, la penetración de cuentas bancarias alcanzó el 91% de la población adulta, lo cual equivale a que más de 31 millones de personas poseen al menos una cuenta de este tipo, cumpliendo con el objetivo de llegar a la mayor cantidad de usuarios posibles y permitirles utilizar servicios financieros durante el distanciamiento social.

Este nuevo control se suma a los “Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras” que deben cumplir en forma obligatoria.

En este texto, se definen prácticas y requerimientos de implementación obligatoria para las entidades financieras relacionados al control de los riesgos de tecnología y seguridad informática. En particular, para la gestión de la seguridad en canales electrónicos, las entidades financieras deben cumplimentar los requisitos mínimos regulatorios en cada uno de los siguientes procesos, entre ellos:

• Concientización y Capacitación: Es un proceso relacionado con la adquisición y entrega de conocimiento en prácticas de seguridad, su difusión, entrenamiento y educación, para clientes internos y externos, con el fin de desarrollar tareas preventivas, detectivas y correctivas respecto de los incidentes de seguridad en los canales electrónicos.

• Control de Acceso: Es un proceso relacionado con la evaluación, desarrollo e implementación de medidas de seguridad para la protección de la identidad, mecanismos de autenticación, segregación de roles y funciones y demás características del acceso de los usuarios internos y externos a los canales electrónicos.

• Integridad y Registro: Es un proceso destinado a la utilización de técnicas de control de la integridad y registro de los datos y las transacciones, así como el manejo de información sensible de los canales electrónicos y las técnicas que brinden trazabilidad y permitan su verificación. Incluye, pero no se limita a transacciones, registros de auditoría y esquemas de validación.

• Monitoreo y Control: Es un proceso relacionado con la recolección, análisis y control de eventos ante fallas, indisponibilidad, intrusiones y otras situaciones que afecten los servicios ofrecidos por los canales electrónicos, y que puedan generar un daño eventual sobre la infraestructura y la información.

• Gestión de Incidentes: es un proceso relacionado con el tratamiento de los eventos e incidentes de seguridad en canales electrónicos, su detección, evaluación, contención y respuesta, así como las actividades de escalamiento y corrección del entorno técnico y operativo.

Jueves 1 de julio de 2021.