

Ciberseguridad: lo que deben hacer las entidades financieras para evitar fraudes en compras online

Las infracciones a las obligaciones sobre seguridad de la información corresponden son graves y tienen multas que van de 20 a 100 UIT (de S/ 88,000 a S/ 440,000), señaló María del Pilar Sánchez asociada senior en Rebaza Alcázar & De Las Casas.



Cuando se realizan pagos o transferencias recurrentes se pueden obviar los procedimientos de autenticación, según la asociada senior en Rebaza Alcázar & De Las Casas. CSIC 11/11/2021

Actualizado el 05/12/2021 05:56 a.m.

Jonathan Terranova

Al tener un producto financiero, como un tarjeta de crédito, es común tener inseguridad debido a los fraudes, suplantaciones, entre otras acciones delictivas. Si bien no hay una legislación específica para la [ciberseguridad](#) en el Perú, sí hay una regulación para las empresas del sistema financiero. María del Pilar Sánchez asociada senior en [Rebaza Alcázar & De Las Casas](#) habló con [Gestión.pe](#) sobre ello.

“Las empresas financieras ya vienen implementado procedimientos de ciberseguridad que ha estipulado (mediante la Resolución SBS N° 504-2021) la Superintendencia de Banca, Seguros y AFP ([SBS](#)) en febrero del 2021, pero tienen plazo para que todas los incorporen hasta junio el 2022”, señaló Sánchez.

Autenticación general

Según Sánchez, la autenticación general es efectuada cuando se desea tomar un servicio que ofrece directamente la entidad financiera (por ejemplo, consultar estados de cuenta, transferencia entre cuentas, entre otras acciones).

La empresa financiera debe verificar la identidad del usuario y reducir la suplantación de la identidad. En ese sentido, deben incorporar procedimientos en base a los siguientes ejes:

- Algo que solo el usuario conoce: normalmente se pide crear un usuario y clave.
- Algo que el usuario posee: preguntas adicionales para, por ejemplo, recuperar contraseña.
- Algo que el usuario es: vinculado a procedimientos biométricos o reconocimiento facial.

“Estas categorías de autenticación deben ser tomarse en cuenta por las empresas financieras para autenticar a los clientes o usuarios para los servicios provistos mediante canales digitales. Además de ello, se deben generar credenciales e informarles a los usuarios”, mencionó.

Autenticación reforzada

Esta autenticación para todo lo vinculado a pagos y transferencias de dinero (compras en tiendas de forma online, pagos a cuentas de otras personas, servicios, entre otras). Esta incluye, explicó Sánchez, **la utilización de dos de los tres mencionados para la autenticación general (cualquiera de estos).**

Además de ello, la empresa financiera tiene que generar un código de autenticación mediante métodos criptográficos y, en caso de que la operación se exitosa, se debe notificar los datos de la misma al usuario.

“Ya se ha visto que, cuando se usa la tarjeta de crédito para realizar pagos, el banco le notifica al usuario luego de estos. Esto tendría que ser implementado por todas las empresas del sistema financiero. El evitar suplantación, independientemente de quien lo use (por ejemplo comprado) y hacia quien se use (vendedor) es responsabilidad totalmente de las entidades financieras”, indicó.

“Las empresas financieras han presentado a la SBS un plan de adecuación, el cual muchas ya han venido implementando. Si bien para julio del 2022 ya debería estar efectuada la implementación, y con ello las acciones fraudulentas disminuyan, estas no se van a poder eliminar, pues siempre hay espacios para que se intenten de formas no previstas”, puntualizó.

Extensión

Según Sánchez, hay una excepción para que no se tengan que seguir los procedimientos de autenticación, y es cuando se realizan pagos o transferencias recurrentes.

“Por ejemplo, en caso de tener una cuenta a la que siempre se hace transferencias, se guarda como favorito, y no se tendría que autenticar más”, mencionó.

¿Usuarios pueden denunciar?

Es complicado para el usuario detectar que no se están cumpliendo con los procedimientos, pues tienen un componente técnico que puede escapar del conocimiento común; no obstante, si el usuario cumple con las disposiciones que le otorgue la entidad financiera tiene la facultad de levantar una queja.

“Por ejemplo, si el usuario cumple con avisar al banco de que hay operaciones desconocidas en su cuenta, que se perdió la tarjeta, entre otros casos, la entidad está en la obligación de actuar según la naturaleza del fraude en caso ocurra. En el escenario de un usuario que maneje los temas técnicos y se de cuenta que la empresa financiera está en falta, puede reclamar ante la SBS e Indecopi”, manifestó Sánchez.

Mencionó, además, que las infracciones a las obligaciones sobre seguridad de la información corresponden son graves y tienen multas que van de 20 a 100 Unidades Impositivas Tributarias (UIT), equivalentes a de S/ 88,000 a S/ 440,000.



GESTIÓN

Regístrate gratis al newsletter e infórmate con lo más completo en

Regístrate

Acepto los [Términos y condiciones](#) y [Políticas de privacidad](#)

[Más newsletter](#)

NO TE PIERDAS

Contenido de [Gestión](#)

Conoce cuáles son los feriados y días no laborables que le quedan al 2021

G

Evergrande avanza hacia la reestructuración; Gobierno chino busca contener riesgos

G

Dólar abrió al alza mientras el mercado está atento a moción de vacancia presidencial

G

Vladimir Cerrón: "Perú Libre rechaza moción de vacancia presidencial"

G

Bono 210 soles: Quiénes son los beneficiarios y cómo se entregará esta ayuda económica

G

Ómicron: todo lo que se sabe de la nueva "variante de preocupación" del coronavirus

G

GESTIÓN

Director Periodístico
JULIO LIRA SEGURA

Empresa Editora Gestión
Jorge Salazar Araoz N° 171, La Victoria, Lima.

Copyright © gestion.pe
Grupo El Comercio - Todos los derechos reservados

Cargando siguiente...

**Cevallos: decisión de
algunos políticos de no...**