Emisores de factura electrónica deben garantizar la seguridad de los datos de sus clientes

- Obligatoriedad del uso de factura electrónica cumple su primer año.
- Su aplicación no exime de responsabilidades estipuladas en la Ley 8968.
- Malas prácticas derivan en sanciones.

La Agencia de Protección de Datos de los Habitantes (PRODHAB), entidad adscrita al Ministerio de Justicia y Paz, hace un llamado a los emisores de factura electrónica, para que profundicen las medidas de seguridad y privacidad con que almacenan los datos personales que solicitan a sus clientes.

La PRODHAB ha atendido varias consultas telefónicas de ciudadanos preocupados con relación a malas prácticas que se han vuelto recurrentes y que podrían desencadenar en estafas o robos de datos sensibles.

“Algunas personas han indicado que cuando van a pagar no les pueden emitir su factura en el mismo momento, y para el posterior envío les solicitan dejar anotados sus datos en un cuaderno o libreta, donde a su vez están expuestos los datos de terceros”, expresó la Directora Nacional de PRODHAB, Ana Karen Cortés Víquez.

El mal tratamiento y/o almacenamiento de datos personales puede conllevar sanciones que oscilan entre los 2 y 15 millones de colones para los infractores; lo que podría resultar mucho más costoso para el negocio que invertir desde el inicio en un sistema apropiado y proactivo para su resguardo.

Para el envío de la factura los clientes deben proveer su nombre completo, número de cédula y correo electrónico. No obstante, hay quienes van más allá y solicitan datos como el teléfono, la dirección física o hasta el número de placa del vehículo (cuando se trata de pagos en gasolineras).

“Es importante recalcar que el comercio o el responsable de la base debe respetar el fin para el cual se brindan esos datos, y el cliente está en su derecho de limitarse a suministrar los datos que sean estrictamente necesarios”, aclaró Cortés.

La Ley 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales y su Reglamento, son enfáticos en que los datos personales pueden ser tratados solo cuando medie el consentimiento de su titular y que quien los recopila debe limitarse al fin para el cual los solicitó.

Incumplir este punto y solicitar los datos para generar una factura y luego cederlos sin permiso del titular a un tercero, o utilizarlos como medio de contacto para ofrecer algún servicio o promoción, también es motivo de sanción económica o hasta el cierre de la base.

Esta misma normativa establece los protocolos de actuación, las medidas de seguridad y privacidad que deberían adaptarse al recopilar o tratar datos personales.

Según la Directora: “cualquier persona puede exigirle al negocio que sus datos no queden registrados a la vista de terceros, y este deberá proporcionar los medios apropiados. Si el cliente se siente vulnerado, o bien si el comercio incurre en alguna de las faltas expuestas, puede presentar una denuncia ante la PRODHAB”.

Para esto, es necesario aportar la prueba, completar el formulario que se encuentra en http://www.prodhab.go.cr/procedimientosdeprote/ y presentarlo en las oficinas de la PRODHAB en Curridabat; si cuenta con firma digital puede enviarlo al correo electrónico prodhab@rnp.go.cr. En caso de dudas, puede comunicarse al teléfono 2528-3315.

ANTECEDENTES

El día de ayer, la Sección de Fraudes del OIJ, el Ministerio de Hacienda y el de Economía Industria y Comercio (MEIC), dieron alerta sobre una nueva modalidad de estafa digital ligada al uso de factura electrónica, donde a través de un acceso remoto los estafadores roban información sensible de empresarios.

El Viceministro de Ingresos del Ministerio de Hacienda, Nogui Acosta, solicitó a los contribuyentes dudar de cualquier llamada o visita de supuestos funcionarios bancarios o de ministerios, seguir las indicaciones del OIJ y por supuesto, hacer uso responsable de todas las herramientas tecnológicas a su disposición.

La PRODHAB se suma para advertir a los responsables de bases de datos sobre los cuidados que deben tener con los medios por los cuales solicitan los datos personales, realizar un almacenaje seguro y tener un adecuado procedimiento de destrucción o eliminación de datos cuando proceda.

Asimismo, recordar al usuario la importancia de no brindar sus datos si no son sitios o medios seguros, y limitar la exposición de sus datos para evitar vulnerabilidades.