

Consejos para protegerte de una filtración de datos personales

Las consecuencias de una filtración de datos personas pueden ser muy graves ya que ponen en riesgo el patrimonio e información de las personas. ¿Cómo protegerte ante situaciones como esta?

“La filtración de datos, por el tipo y cantidad de datos a los que podría accederse, implica un riesgo potencial muy alto tanto para el patrimonio como para información sensible de las personas expuestas”, señaló José Antonio Casas, presidente del Gremio de las Tecnologías de la Información y de las Comunicaciones de la Cámara de Comercio de Lima (CCL).

Explicó que en el caso de la filtración de datos personales reportada por la Asociación de Bancos (Asbanc), el riesgo está en que se hace uso indebido de datos que son públicos pero que no son provistos por instituciones del Estado y, por lo tanto, se entregan por dinero, fuera de los entornos de seguridad y de autenticación de las instituciones formales.

Entre otras limitaciones importantes, no se puede identificar plenamente quién solicita esos datos y con qué intenciones, agregó José Antonio Casas.

Políticas de seguridad

Afirmó que una filtración de datos como la ocurrida es grave porque muestra fisuras tanto en los mecanismos como en las políticas de seguridad del aparato público. Primero, porque para obtener los datos mencionados se ha tenido que aprovechar debilidades tecnológicas y/o institucionales.

Y segundo, porque toda estrategia de seguridad debe contemplar tres momentos relacionados a incidentes que aprovechan o generan fisuras en su estructura: la ocurrencia del incidente, la detección y la respuesta o remediación. “Está claro que la estrategia ha fallado desde el primer y segundo momento y eso le aumenta la criticidad al incidente”, puntualizó.

Recomendaciones

Pero, ¿qué medidas se pueden tomar para proteger a los usuarios de una filtración de datos personales?. José Antonio Casas, dio algunos consejos:

1. Utilizar métodos de autenticación robustos, es decir claves largas y complejas, difíciles de «adivinar» y que no contengan información del usuario que fácilmente se pueda inferir, como nombres de familiares, lugares y fechas personales y familiares, etc.

2. Usar métodos de doble autenticación o doble clave, lo que significa un «doble candado», para decirlo de una forma que la gente no técnica entienda.

3. No compartir sus claves ni datos personales por medios no seguros a personas que no están plenamente identificadas. Si hay una mínima duda, abstenerse de hacerlo.

4. Tener claramente determinados los procesos de suspensión/anulación de cuentas, tarjetas o de sus números celulares, si es que fuera el caso. Dichos procesos son realizados por las instituciones bancarias donde tenemos nuestras cuentas y tarjetas, y por las compañías de telecomunicaciones donde tenemos los planes de servicio pre o pos pago.

“Estos consejos son particularmente útiles para las personas naturales y para las pequeñas empresas que no tienen personal especializado en ciberseguridad”, expresó el presidente del Gremio de las Tecnologías de la Información y de las Comunicaciones de la CCL.

Fortalecer prevención

Respecto a la decisión del Gobierno de crear una unidad funcional de confianza digital para fortalecer la estrategia de prevención y mitigación de riesgos ante amenazas de vulneración de datos personales, Casas comentó que se requiere más detalles y la participación del sector privado.

“Esperamos que, tal como lo ha ofrecido el gobierno a través de los titulares de la Presidencia del Consejo de Ministros (PCM) y de la SeGTDi, involucren al sector privado lo más pronto posible para ayudar en su diseño, objetivos y metas. Se debe seguir fomentando y fortaleciendo todos los espacios de trabajo conjunto entre los stakeholders del ecosistema digital”, concluyó.