Especialista en ciberseguridad advierte que empresas deben prestar especial atención a la protección de la información.

¿Cómo cuidar su seguridad y la de sus clientes?

Según un estudio de ESET en América Latina , Perú es el tercer país más afectado por ciberataques. Por otro lado, de acuerdo al Reporte Anual de Ciberseguridad 2018 de Cisco, el robo de datos personales fue el común denominador de los ataques en el último año. Los ciberdelincuentes han encontrado en la comercialización de nombres, apellidos, perfiles de usuarios y datos financieros un nicho de mercado que incentiva la vulneración de las entidades para lucrar con dicha información.

Esta situación obliga a que las empresas mantengan un especial interés por el cuidado y protección de su información y la de sus clientes. La situación cobra mayor relevancia si consideramos que según un estudio de GFK, el 39 % de los peruanos que compran *online* teme que los productos no se entreguen adecuadamente, en tanto, un 55 % duda en dejar sus datos personales y de tarjeta de crédito. La desconfianza está presente.

Gianncarlo Gómez.
Profesor del Diploma Internacional en Gestión de la Ciberseguridad y Privacidad de ESAN. Actualmente se desempeña como gerente adjunto de Arquitectura de Seguridad en el Banco de Crédito del Perú - BCP.

Cumplimiento normativo

El Perú cuenta con la Ley 29733 (Ley de Protección de Datos Personales) que obliga a que todas las entidades públicas, entidades privadas y personas naturales tengan cuidado con el tratamiento de datos de sus clientes y de la población en general. Quienes no hayan implementado esta ley hasta el 08 de mayo del 2015, se encuentran en falta y están sujetos a algún tipo de sanción por parte de la Autoridad Nacional de Protección de Datos Personales.

Otro avance a resaltar es que el Perú formalizó su adhesión al Convenio contra la Ciberdelincuencia o Convenio de Budapest, junto a otros 55 países. El acuerdo busca la aplicación de mecanismos rápidos de cooperación internacional relacionados con la ciberdelincuencia, así como establecer una política

EMISIÓN DE CERTIFICADOS DE ORIGEN

CÁMARA de COMERCIO de LA LIBERTAD

Celeridad garantizada por un proceso certificado con la norma ISO 9001:2015

La primera Cámara del Perú certificada en ISO 9001

Contacto:
Tel.: 044 - 484210 | Anexo 39
E - mail: exportacion@camaratru.org.pe

NEGOCIOS DE COMERCIO EXTERIOR

CÁMARA de COMERCIO de LA LIBERTAD

CENTRO DE DESARROLLO EMPRESARIAL LA LIBERTAD

PERÚ Ministerio de la Producción

¡Formaliza tu empresa en el **CDE La Libertad!**

- **REALIZAMOS:** Reserva de nombre de la empresa y acto constitutivo de la misma, de manera gratuita.
- **ANÁLISIS:** De las empresas con la finalidad de mejorar sus operaciones.
- **ASESORÍA:** En temas tributarios, contables, de tecnologías de la información, marketing y financieros.
- **CAPACITACIONES:** Talleres presenciales y virtuales.

¡SERVICIO GRATUITO!

Jr. Junín 454 - Trujillo, Perú
www.camaratru.org.pe
044-484210 anexo 52

cdeconsultas@camaratru.org.pe

Horario de atención:

Lunes a Viernes:
8:30 a.m. - 1:00 p.m.
3:40 p.m. - 8:00 p.m.

Sábado:
9:00 a.m. - 12:50 p.m.

penal común, con la finalidad de proteger a la sociedad frente a los ciberdelincuentes.

Finalmente, en el país también se cuenta con una Ley de Delitos informáticos que previene y sanciona las conductas ilícitas que afectan sistemas, datos informáticos u otros bienes jurídicos de relevancia penal, mediante el uso de tecnologías de la información y comunicaciones (TIC). Sin embargo, ese marco legal es insuficiente para combatir los delitos informáticos, ya que se requieren implementar sanciones más rígidas y considerar nuevas conductas ilícitas.

¿Qué podemos hacer?

Para que una empresa pueda proteger su información y la de sus clientes, principalmente en lo vinculado a compras *online*, debemos considerar los siguientes puntos:

- La implantación de algunos *frameworks* o buenas prácticas de seguridad de la información y/o ciberseguridad. El ISO 27001:2013 o el Cybersecurity Framework del NIST son algunos ejemplos.
- Realizar un inventario y clasificación de nuestra información, así como un análisis de riesgos e implementación de controles.
- Realizar un monitoreo constante de nuestra plataforma tecnológica y un análisis de vulnerabilidades en intervalos planificados.

Todas estas recomendaciones nos permitirán adoptar una adecuada postura de ciberseguridad ante las inminentes y crecientes amenazas en el ciberespacio.

ESET (2018). ESET Security Report 2018: el estado de la seguridad de la información en las empresas de la región. Recuperado de: https://www.welivesecurity.com/la-es/2018/06/19/eset-security-report-2018-el-estado-de-la-seguridad-de-la-informacion-en-las-empresas-de-la-region/