# Los retos de la ciberseguridad

Las palabras ciberseguridad, cibercrimen y ciberguerra han tomado relevancia en el mundo de la seguridad en general. Esto debido, en parte, a la evolución tecnológica y, en mayor medida, al incremento en las violaciones de seguridad, actos criminales y a la presencia de armas de guerra basadas en la información, así lo explica el docente de la Facultad de Ingeniería Informática de la USIL, Marco Antonio Salcedo Huarcaya.

“La ciberseguridad es la práctica de defender las computadoras, los servidores, dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos”, precisa.

**Salcedo indica que, según una investigación sobre la ciberseguridad, realizada por KIO Networks, Endeavor y PayPal, a finales del 2020, en Latinoamérica, la principal barrera de adopción de la ciberseguridad dentro de los emprendimientos es la falta de presupuesto (34%), seguida por la ausencia de integración en la estrategia (18%) y la dificultad técnica de implementación (14%).**

**“En el Perú la situación es más compleja, según un estudio de ciberseguridad realizado por Fortinet, a nivel de Latinoamérica fue el tercer país con mayor número de ataques cibernéticos durante el 2021, después de México y Brasil”, subraya.**

Entonces, ¿cuál es el reto de la ciberseguridad en el país? Para el especialista de la USIL es enfrentar desafíos como crear un marco regulatorio integrado y no fragmentado, pues lo hace más complejo y difícil de cumplir. Y por parte de las organizaciones, es importante reconocer el rol del oficial de seguridad de la información o director de seguridad de la información de una empresa (en inglés, CISO). Además, dice que es importante contar con técnicos especializados en ciberseguridad, tener un área de seguridad de la información y asignar un presupuesto suficiente.

## Sin una estrategia a la vista

**Marco Antonio Salcedo afirma que, si bien el Perú no cuenta con una estrategia de ciberseguridad, lo que tiene son diversas normas relacionadas a este tema como la Ley N° 30999 de Ciberdefensa, que tuvo como objeto establecer el marco normativo en esta materia del Estado peruano.**

También está la Ley N° 27269 de Firmas y Certificados Digitales; la Ley N° 28493 que regula el uso del correo electrónico comercial no solicitado (spam); la Ley N° 29733 de Protección de Datos Personales, entre otras. “Pero, si es importante mencionar que el Gobierno Peruano ha decidido dar el primer paso para establecer la planificación y ejecución de un conjunto de acciones que permitan el desarrollo articulado y sostenido de la sociedad de la información en el país, a través de la promulgación del Decreto Supremo N° 066-2011-PCM que aprobó el Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0”, explica.

# Ciberataques más personalizados

En opinión del gerente de la empresa de ciberseguridad, Incared, Elvis Vargas, los ciberataques no se han incrementado debido a la COVID-19, sino que han cambiado volviéndose más personalizados.

“Si antes te atacaban con DDoS, denominados ataques de fuerza bruta donde usualmente te bloqueaban las páginas web o los sistemas de las empresas, ahora, por ejemplo, utilizan el ransomware, que es un virus que accede mediante un correo electrónico o link a una determinada máquina, encriptando la información”, detalla.

**Precisa que hay dos tipos de ataques, uno a la aplicación y el otro al usuario. Explica que una mala manipulación del usuario puede tener como consecuencia que le vacíen sus cuentas en el banco.**

**Para frenar este tipo de ciberataques, Vargas asegura que se necesitan acciones de autenticación de dos factores. El primero, proteger con la huella digital; y el segundo, con un código. Refiere que a este tipo de cuidados está evolucionando el mercado para que todo acceso a una aplicación tenga una doble confirmación por parte del usuario.**

Mencionó que es necesario este tipo de autenticaciones porque el celular no es seguro y mucho menos los mensajes de texto que envían. “Estos SMS navegan a través de las redes 3G o 4G y pueden ser interceptados volviéndose vulnerables”, subraya.

Refiere que, si bien WhatsApp es de alguna manera más seguro, el problema es cuando se instala este dispositivo se tiene que validar por un SMS y este puede ser interceptado.

## País más reactivo que previsor

**Por su parte, el gerente general de ESET Perú, Jorge Zeballos, define al Perú como un país más reactivo que previsor en términos de seguridad. Precisa también que somos un país que no alcanza los estándares regionales porque no estamos acostumbrados a tomar todas las líneas de seguro que le sean atribuibles a nuestro negocio.**

“Ahora que estamos en una transformación del mundo hacia el campo absolutamente digital, donde las empresas han sido concebidas en este ámbito con activos absolutamente digitales, si no se toman las precauciones, el negocio simplemente desaparece”, puntualiza.

Para evitar dicha situación ¿cuánto puede gastar una empresa en ciberseguridad? Jorge Zeballos, sostiene que un microempresario que maneja todo su negocio en una computadora no va tener que invertir más allá de S/ 300 anuales para que tenga controlado desde la gestión de claves, contar con una red privada local, entre otros.

“Bank of America tiene, por ejemplo, un presupuesto en términos de ciberseguridad ilimitado y Microsoft de alrededor de un billón de dólares”, detalla.

**Según la Encuesta Global Digital Trust Insights de PwC 2022, la mayoría de las empresas no controlan los riesgos cibernéticos de terceros, riesgos que se oscurecen por la complejidad de sus relaciones comerciales y sus redes de proveedores.**

“Los hallazgos son una señal de alerta en un entorno en el que el 60% de los encuestados de la alta dirección anticipan un aumento de los delitos cibernéticos en 2022. También reflejan los desafíos que enfrentan las organizaciones para generar confianza en sus datos, asegurándose de que sean precisos, verificados y seguros, para que los clientes y otras partes interesadas puedan confiar en que su información estará protegida”, señala el estudio de PwC.

# Ciberataques más comunes

Según la compañía de ciberseguridad CANVIA, los ciberataques más comunes en los que caen los usuarios son:

**1.- Ransomware**

Se trata de un software malicioso que, al infectar el equipo, otorga al ciberdelincuente la capacidad de bloquear un dispositivo desde una ubicación remota, encriptando y secuestrando los archivos. ¿Cómo ingresa? Normalmente un ransomware se transmite como un troyano o gusano, infectando el sistema operativo, al descargar un archivo no seguro o explotando una vulnerabilidad de un software en uso.

**2.- Zoom-bombing**

Es la posibilidad de irrumpir en una videoconferencia en Zoom

sin el permiso de la persona que creó la reunión. Puede resultar sencillo interrumpir en este tipo de videoconferencias porque muchas veces las URL para acceder a los encuentros se rastrean haciendo una búsqueda digital o bien si alguien, por error, la comparte o deja publicada en algún sitio.

**3.- Phishing**

Se relaciona con el envío de correos electrónicos que tienen la apariencia de proceder de fuentes confiables (bancos, tiendas, entre otras), pero que en realidad buscan manipular a la persona que lo recibe para robar información confidencial.

**4.- Spyware**

Este software sigue las actividades del colaborador en línea, tanto en equipos como en dispositivos móviles. Puede supervisar y copiar todo lo que se escribe, carga, descarga y almacena, en forma de troyano, virus, gusano, entre otros.