


**CREEN QUE CHILE HA AVANZADO EN ESTA MATERIA**

# Expertos apuestan por mayor educación para responder a los ciberataques

Uno de ellos, Gabriel Bergel, comentó que una de las razones por las cuales la gente cae en engaños es la excesiva confianza que tiene. A modo de ejemplo, dijo que aún cree en el "Pepito paga doble".

**POR JAVIER MARTÍNEZ GUTIÉRREZ**  
 JAVIER.MARTINEZ@DIARIOELSUR.CL

Hoy el uso intensivo de internet y de la disposición masiva de equipos móviles hace que cada día se tome más conciencia sobre la ciberseguridad, un concepto que en los últimos tiempos ha tomado más relevancia, dados casos de filtraciones de datos o de phishing, que son mensajes falsos que buscan captar a algún iluso para robarle información importante, como los de una cuenta corriente o de tarjetas de crédito.

Uno de los expertos sobre la materia en Chile es Gabriel Bergel, el único chileno que actualmente integra el Consorcio Internacional de Certificación de Seguridad de Sistemas de Información. Es, además, organizador de "8.8 Computer Security Conference", una cita que nació en el 2011 debido a que querían crear una comunidad técnica en torno a la ciberseguridad en Chile que no existía en ese momento y había otras en Argentina y en Estados Unidos, pero que este miércoles 26 de junio tendrá su primer encuentro en Concepción, en la sede de Inacap.

El experto, además de otros que conocen sobre el tema, entregaron su parecer a cómo está la ciberseguridad en Chile.

A juicio de Bergel, existen muchas amenazas en torno a las cuales hay que estar preparados, so-

bre todo por la facilidad de acceso que tiene la gente con el uso de redes sociales y de estar en constante nexo con internet.

A su juicio, las personas están cada vez más expuestas a ser afectadas por algún ataque, como por ejemplo ocurrió con la filtración de datos de miles de tarjetas de crédito. "Esto porque hoy tenemos en un celular un computador más rápido que el que tenía la Nasa en los años 90 y en donde facilitamos toda nuestra información privada y por lo tanto las amenazas principales vienen por ese foco principal", apuntó.

## ATENCIÓN MAYOR

Por lo mismo, cree que es necesario que haya mucha educación sobre ciberseguridad, aunque se ha avanzado un poco, en

**Es necesario que haya mucha educación sobre ciberseguridad, aunque se ha avanzado un poco, en especial por lo ocurrido con los bancos.**

especial por lo ocurrido con los bancos, lo que llevó a que las autoridades pusieran atención y tomaran medidas, junto a que los usuarios estén más pendientes. Cree que hay más seguridad, pero falta en comparación a países más desarrollados.

El experto adelantó que el gobierno está preocupado y, por lo mismo, firmará un convenio con 8.8, pues está claro que es un tema importante, y en la medida que la gente no entienda que esto es relevante le seguirán robando información.

Gabriel Bergel, en todo caso, destaca que Chile tiene como fortaleza el contar con muy buenos profesionales en la materia e incluso como país debemos estar entre los tres primeros en seguridad, en especial por las leyes que se están llevando adelante. Y en cuanto a debilidades, dijo que son muy comunes en general, porque como el foco son las personas, muchas veces se trata de cosas culturales. "Las personas somos muy confiadas y hoy la principal amenaza es el phishing, que son correos falsos para robar credenciales. Y en general los chilenos son muy confiados. Es cosa de ver que el "Pepito paga doble" aún existe y la gente sigue cayendo en ese juego", hizo ver.

## SIN FRONTERAS

En tanto, Bernardo Campos, docente de Ingeniería en Informática de Duoc UC sede Concep-

ción, agregó que hablar de Chile como un escenario general es complicado, ya que internet es un medio que no conoce fronteras. "El nivel de preparación o de susceptibilidad ante un ataque de este tipo dependerá directamente del organismo o institución que resulte víctima de dichas acciones. En nuestro país existen organismos que utilizan los más altos estándares de seguridad informática, así como también existen otros que trabajan con medidas de seguridad al mínimo o lo hacen de la misma manera que hace dos décadas atrás", remarcó.

Sumó que el uso de tecnologías obsoletas es un factor influyente en cuanto a la protección de información digital. Últimamente es cada vez más frecuente enterarse sobre casos de filtraciones masivas de información de tarjetas de crédito o de cajeros automáticos que han sido intervenidos de manera maliciosa para clonar tarjetas bancarias. Esto, sostuvo, deja en evidencia que las tarjetas no solo son un medio de pago inseguro, sino que además están quedando obsoletas.

Mientras que Tania Gallardo, directora de la Escuela de Tecnologías de la Información de Universidad de Las Américas, sostuvo que cuando hablamos de ataques cibernéticos, cabe diferenciar aquellos que pueden afectar las redes, sistemas, comunicaciones y continuidad del funcionamiento de organizaciones en sectores público y privado, por ejemplo, sabotaje y espionaje informático y, por otra parte, acciones que van desde fraudes hasta delitos asociados a la explotación sexual

Las personas somos muy confiadas y hoy la principal amenaza son los phishing, que son correos falsos para robar credenciales. Y en general los chilenos son muy confiados. Es cosa de ver que el Pepito paga doble aún existe y la gente sigue cayendo en ese juego".

Gabriel Bergel, experto en ciberseguridad

de menores a través de internet, que según la PDI, son los delitos más denunciados en Chile.

La profesional señaló que existen sectores como la banca o Defensa, donde la seguridad ante posibles ataques cibernéticos es un tema ampliamente abordado, tanto desde la perspectiva tecnológica, como de normativas, protocolos y procedimientos.

"No obstante, en el ámbito de los negocios y las organizaciones en general, se observa una asimetría. Por un lado, se cuenta con un buen nivel de acceso a infraestructura tecnológica, sistemas de información y redes de comunicaciones, pero por otro, el nivel de seguridad ante ataques cibernéticos no es el adecuado para garantizar los tres pilares básicos: integridad, confidencialidad y disponibilidad de los sistemas y

la información que en ellos se maneja", apuntó.

Por otra parte, el sector público, si bien avanza hacia la digitalización, se rige bajo las mismas reglas tanto de infraestructura, acceso y políticas con relación al uso de las tecnologías y tratamiento de datos e información, por lo que la preparación para enfrentar ataques cibernéticos debería ser una prioridad.

## UN PAR DE PASOS ADELANTE

Finalmente, Jacob Donoso, director de Carreras Informática de IP CFT Santo Tomás, afirmó que Chile, si se compara con el resto de Latinoamérica, está un par de pasos más adelantado en el ámbito de infraestructura, pero la mayor carencia que existe actualmente en el mercado son profesionales idóneos para prevenir un "ataque cibernético".

"Vivimos en tiempos que los avances tecnológicos cada vez son más vertiginosos, la tecnología es desarrollada por seres humanos y esta es factible de ser alterada malintencionadamente, siempre existirán personas inescrupulosas que crearán un virus, malware o tratarán de ganar dinero con extorsiones a través de la red", estimó.

Piensa, por ello, que lo más importante en estos tiempos es la protección, pues existen innumerables bases de datos que almacenan información de alta importancia (por ejemplo, de tarjetas de crédito) sin el consentimiento de los usuarios finales, más allá de "preocuparnos por un ataque, debemos preocuparnos por quien tiene guardada nuestra información sensible".