# Ciberatacados en pandemia

*Por Pedro Dutour*
*Fotos: Gentileza*

La pandemia del coronavirus ha supuesto una mayor exposición a nivel cibernético, debido a una expansión del teletrabajo a nivel laboral y empresarial, lo que a su vez ha generado un incremento de los ciberataques. Hacknoid, firma fundada y dirigida por sanduceros, subraya que la mejor herramienta para hacer frente a los ciberataques es la prevención. Adelantarse a los *hackers*.

Los ataques cibernéticos y la ciberseguridad no son asuntos nuevos. El mundo lleva años lidiando contra los ciberdelitos, los que han aprovechado su filón durante esta pandemia de COVID-19 ante un aumento del trabajo a distancia desde el hogar. En este contexto también quedaron en evidencia las carencias o las faltas de previsión de las compañías a la hora de hacer frente a este problema que reporta dolores de cabeza y pérdida de dinero.

La plataforma Hacknoid (www.hacknoid.com) tiene más de 18 años en el rubro de la ciberseguridad y nació con el apoyo de la Agencia Nacional de Investigación e Innovación (ANII), Uruguay XXI y Endeavor. El crecimiento de la empresa ha llegado hasta Chile y Perú. Cuenta con más de 40.000 dispositivos escaneados y unos 30 clientes. Sus responsables y fundadores son dos sanduceros: Rosina Ordoqui y Pablo Giordano, quienes no dudan en asegurar que la irrupción del coronavirus en nuestras vidas puso al "descubierto" todas las "falencias" que se encontraban en estados de madurez, embrionarios y/o primitivos.

"Sobre todo, en cuanto a la colaboración y unificación de lineamientos que permitieran abordar la ciberseguridad de forma consolidada y en bloque tanto para el sector público como privado, y para sectores de industrias en particular, que se vieron muy afectadas como la salud y gobierno, entre otras clásicas a ser atacadas", explicó Ordoqui a QUINTO DIA.

La CEO de Hacknoid señaló que se trata de un fenómeno mundial, pero que en la región se ha detectado un incremento del 40% "solo en el segmento de *malware*". "Surgieron casos que debieron ser atendidos con las herramientas disponibles en medio de un entorno coyuntural muy complejo. El estar en general atendiendo otras prioridades en medio de la pandemia repercutió en el descuido o la toma desprevenida de grandes casos de ataques de oportunistas", enfatizó.

La implementación del *home office* en las empresas del país superaba el 70% en marzo, aunque no siempre las firmas cuentan con la capacidad para abordar esta modalidad. En un texto de difusión de Hacknoid, se asegura que solo el 38% de las empresas declaraban estar preparadas para un ciberataque y que los ataques a dispositivos IoT crecieron 600% anual. "Pero la buena noticia que tiene Hacknoid para usted es que el 90% de los ataques se pueden evitar", señala el texto. Giordano, CTO de la empresa (*chief technical officer* o director de tecnología), comentó que, como la mayoría de los ataques se dan por *Ransomware*, "la información no tiene un foco particular, sucede normalmente con archivos que tienen los usuarios en el equipo, recursos de red compartidos, discos NAS (almacenamiento conectado a la red), etc". "El otro tipo de ataque más común es la suplantación de identidad para pasar números de cuentas bancarias; esto se da mucho con proveedores de China. Ahí el foco del ataque es el mail, hacer el seguimiento de la información, y finalmente, el dinero", ahondó.


En concreto, los ataques a través de *Ransomware* (programas diseñados para ingresar a un sistema y aprovecharse de una vulnerabilidad para encriptar datos) llegan "mayormente" a través de correos electrónicos que "con algún pretexto buscan que los usuarios hagan click y descarguen algún archivo o accedan a alguna página *web*".

"También son muy comunes las estafas por suplantación de identidad y cambios de cuentas. Se interceptan mails, los aparentes proveedores avisan de un cambio de cuenta y las empresas pagan ahí para luego darse cuenta de que enviaron la plata a cualquier sitio", detalló el CTO de Hacknoid.

Los dispositivos más atacados, por la cantidad que circula entre la población, son los teléfonos y Pc. De todos modos, "es importante saber que otros cuantos dispositivos también son atacados".

"Cámaras y enchufes inteligentes también son foco de los atacantes. En un grupo mucho menor, también aparecen impresoras, teléfonos IP y dispositivos de almacenamiento tipo NAS", explicó Giordano.

## La prevención

¿Cómo se hace para detectar un ciberataque? Ordoqui responde que existen herramientas que permiten dilucidar una ofensiva al momento de ser aplicada, aquellas que se encuentran en el área de lo "detectvo" o "reactivo". "En el mundo de herramientas disponibles, se puede detectar

un ataque por un comportamiento anómalo en la red, infraestructura o *software*, o bien por las consecuencias, cuando estos ya han logrado niveles de penetración mayor y se han hecho ya efectivos", dijo.

También pueden darse cuenta de inmediato de un ataque cuando se trata de una denegación de servicio (DoS): ataques que "logran saturar los servicios de la organización provocando que afecte el funcionamiento de los dispositivos e incluso los pueda dejar inoperativos".

"Podemos detenernos horas contando diversas formas de detectar un ciberataque, una fuga, o una alteración de la información de nuestra empresa. Sin embargo, hay que destacar que más peligroso aun, es ser víctima de un ciberataque sin siquiera percibirlo, que en realidad es lo que sucede la mayoría de las veces, hasta tanto se divulga la información o se pone a disposición en un mercado negro de Internet", alertó Ordoqui.

Por este motivo, es que Hacknoid se centra en una etapa anterior al ciclo, el de la prevención, "donde la toma de control es más posible de llevar adelante adecuadamente en tiempo y forma". "Siendo una plataforma que nace en Uruguay, y con consultores con más de 18 años de experiencia en la región, consideramos desde el día uno, que esta es la etapa donde debemos centrarnos para sacar mejor provecho de la inversión en el área y donde se puede alinear más de cerca al negocio", enfatizó la CEO.

## Niveles de conciencia

A nivel empresarial existen muchos y variados niveles de conciencia en temas de ciberseguridad, dijo Ordoqui. "Algunas más maduras por trayectoria de transformación digital que otras, y por hechos que han ocurrido de notoria trascendencia que desataron leyes globales".

La experta indicó que en países más desarrollados y más regulados, en los que se establecen mecanismos más firmes, tanto por lineamientos de las casas matrices o por las legislaciones, se dan mayores pautas para manejarse ante los ciberataques. Mientras tanto en industrias donde la responsabilidad recae solo en la conciencia y cultura que tenga el oficial de seguridad, gerente de tecnología y directivos, "solo se limita a ver los controles e inversiones que se desprenden de la ética y responsabilidad de las personas miembro de estos equipos".

La visión de Ordoqui en torno a este tema no es tan optimista: "Drástica y lamentablemente si tuviera que generalizar, la ciberseguridad aún sigue siendo un tema de segundo plano y no tomado en cuenta ni siquiera con el auge de la transformación digital y la ola que todos estos cambios conllevan. Al menos no se toma en cuenta a la misma velocidad de los cambios en tecnologías o automatización de procesos de negocio, cuando deberían ir de la mano desde el inicio".

"La información en riesgo hoy día es toda la que la organización esté utilizando o pase por ella. Desde datos personales, secretos industriales, datos bancarios, información de entrada de datos a procesos industriales, y muchos etc", continuó diciendo. "Todos relevantes y muchos críticos para la continuidad del negocio y para poder evitar las disrupciones que puedan ocasionar *'blackouts'* o interrupciones menores, pero de pérdidas de gran impacto general", concluyó Ordoqui.

Pablo Giordano y Rosina Ordoqui.

### ¿Qué nivel de protección tiene el ambiente TI en Uruguay?

Según Rosina Ordoqui, CEO de Hacknoid, en lo que refiere a la región, Uruguay es uno de los países que más ha evolucionado en los últimos años, ubicándose dentro de los mejores posicionados en 2020.

Según el informe elaborado por la OEA y el BID en 2020, existen 12 países al momento que ya habían aprobado estrategias o políticas nacionales de ciberseguridad, incluidos Uruguay que data de 2018-2019. Uruguay en particular cuenta con un marco, que si bien no es estrategia "está organizado con referencia a estándares internacionales aplicables a las regulaciones nacionales para la mejora de la seguridad cibernética de infraestructura crítica y organizaciones públicas", según se cita en el informe.

Además, cuenta con un CSIRT (CertUy), bajo la órbita de Agesic (Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento) de gobierno. Es el primer país de la región en recibir apoyo técnico y financiero del BID enfocado al fortalecimiento de la ciberseguridad nacional. CERTuy a su vez, es miembro de la red CSIRT Américas, que le permite explotar la naturaleza colaborativa de la red.

Se considera en el sector privado una fuerte conciencia, que se ha visto fortalecida por los impulsos del gobierno en este sentido: capacitación y servicios de seguridad. Dentro de las dimensiones que se miden en el informe, encontramos algunas que han evolucionado notoriamente como, por ejemplo, en la dimensión de "Política y Estrategia", la respuesta a incidentes ha despegado de forma notoria, ubicándose en un nivel de madurez "estratégica" y "dinámica", lo cual implica tener indicadores específicos diseñados para la medición de este aspecto, así como la capacidad de hacer al proceso dinámico de acuerdo a las circunstancias.

Por el lado de la "cultura cibernética y sociedad", se encuentran grados muy consolidados en cuanto a la mentalidad, confianza y seguridad en Internet como la comprensión de los usuarios del uso de sus datos en Internet. En la dimensión de Formación, Capacitación y Habilidades de Seguridad Cibernética ha destacado la evolución en cuanto al marco para la capacitación profesional, sensibilización en general, y marco de formación.

Mientras que por el lado de la dimensión de Marcos Legales y Regulatorios, se encuentran los puntos más flojos en cuanto a protección infantil en línea, legislación de derechos del consumidor, propiedad intelectual, y delito cibernético, así como la legislación procesal contra el delito cibernético. En la última dimensión sobre estándares, organizaciones y tecnologías, Uruguay cuenta con niveles todos superiores al cuarto nivel que es el de "consolidado", obteniendo puntajes muy parejos y elevados en todos los segmentos (cumplimiento de estándares, resiliencia, calidad de software, controles, mercado y divulgación responsable).