Año 1. Número 2.

Bridge

cisco SECURE

Ciberseguridad

Contrapunto
Medicina y Ciberseguridad

Educación Remota

Conversatorio
con **Adrián Acosta**, Interpol

Contenido audiovisual

Braycom

Construimos Soluciones

Argentina
Av. Independencia 1330 – Piso 14 - Of. B – CABA
Teléfono: +54.11.5273.4470

Colombia: +57.1.580.1333
Chile: +56.2.2938.1332 - **USA:** +1.786.358.6100

Editorial

En los últimos meses mucho se ha dicho sobre la aceleración hacia la digitalización, la remotización del trabajo y el aumento de la actividad cibercriminal tomando provecho del contexto de la pandemia.

Sin embargo creo que aún hace falta una mayor reflexividad sobre cómo deben adaptarse los individuos y las organizaciones para lograr resiliencia. Resiliencia es una palabra maravillosa porque resuena en prácticamente cualquier disciplina, ya sea que hablemos de psicología, sociología, medicina, economía, infraestructuras tecnológicas y ciberseguridad, entre otras.

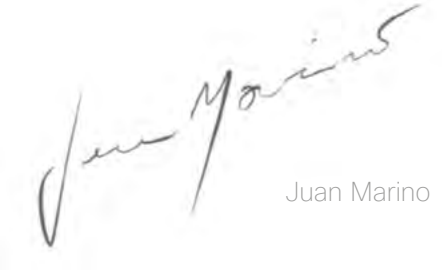
No es casual que en el diálogo entre la Dra. Melissa Palmieri y nuestro Director de Ciberseguridad para Latinoamérica Ghassan Dreibi encontraron rápidamente en el concepto de resiliencia un punto de encuentro. La prevención es fundamental, sin embargo las crisis son inevitables y la cuestión es estar preparados para superarlas, trátese de la salud de un individuo o de la supervivencia de una empresa.

El comportamiento de la sociedad ante el coronavirus y la ciberseguridad ofrecen varias similitudes. En ambos casos luchamos contra un "intangible"; así como Wannacry en Mayo de 2017, nos hizo tomar conciencia de que no estábamos preparados para enfrentar la propagación "epidémica" de un malware, lo mismo nos sucede ahora en el ámbito biológico. Si hablamos de "sentido común", que como suelen decir "es el menos común de los sentidos", encontraremos desde gente que duerme con barbijo, cubreboca o mascarilla hasta aquellos que se reúnen a celebrar la amistad compartiendo la pipa de la paz, mientras que en la cibernética tendremos a quien hace click desaprensivamente en el correo electrónico del príncipe que le dona su fortuna y en el otro extremo aquellos que adoptan medidas de seguridad tan complejas que obstaculizan el desarrollo del negocio y son sufridas o eludidas por los usuarios.

Ya hemos visto cómo algunas organizaciones han demostrado resiliencia ante la irrupción de COVID-19, pero esto ha sido en gran parte el resultado de una construcción que comenzó tiempo antes, con decisiones, que se anticiparon a las transiciones del mercado, buscando cultivar una cultura de trabajo que abrazara la flexibilidad del "workstyle", "workplace" y los "workflows".

Por otra parte, para tantos otros que han reaccionado como pudieron, soportando un tremendo estrés para garantizar la continuidad operativa, muchas veces llevándose por delante la ciberseguridad, cabe un mensaje alentador. Es que tomando las decisiones correctas y rompiendo antiguos paradigmas, es posible reconfigurar el modelo y la operación del negocio para asentarse en una "nueva normalidad" que permita el despertar de nuevas posibilidades de prosperidad que en la realidad pre-pandemia no se habrían explorado. De eso da cuenta el artículo del Ing. Pablo Marrone, líder de tecnologías de colaboración de Cisco para Latinoamérica.

Esta nueva forma de vida nos trae grandes oportunidades y también nuevos desafíos. Nuestros entrevistados y colaboradores concluyen en la necesidad de actualizar la legislación para dar respuesta a la expansión digital, en modificar la pedagogía para adaptarla al estilo de enseñanza remota, en concientizar a las personas para apuntalar su participación digital segura. Será acaso esa toma de conciencia la que permita adoptar soluciones de telemedicina, educación, trabajo remoto; y aunar esfuerzos para garantizar el funcionamiento seguro y resiliente de las infraestructuras críticas de un país.



Juan Marino

Staff

Producción Integral
Basanta Contenidos

Directora Editorial
Karina Basanta

Director de Arte
Nicolás Cuadros

Coordinadora
Andrea Lecler

Colaboran en este número
Salpufilms, Silvia Montenegro,
Pablo Lázaro, Jorge Prinzo, Freepik

Agradecimientos:
Nicolás Cacciabue, Coly Escobar

Foto de Tapa:
Drajt, Pixabay

Directora Editorial
Karina Basanta

Director de Arte
Nicolás Cuadros

Basanta contenidos

basantacontenidos.com
basanta@basantacontenidos.com
@basantacontenidos
+54 911 5014-4510 / 5260-8723

Cisco Latinoamérica

Ghassan Dreibi
Director de Operaciones de Ciberseguridad, Latam

Líderes Regionales de Ciberseguridad

Juan Marino
Fernando Zamai
Juan Orozco
Yair Lelis
Marcelo Bezerra
Darío Flores
Leticia Gammill

Editor General
Juan Marino

Agradecimientos
Pablo Marrone
Emanuel Almeida
Walter Montenegro
Daniel Peña

Marketing

Taiane Belotti
Gerente de Marketing, Seguridad Latam
Jimena Reyna Briseño
Gerente de Marketing de Contenidos, Seguridad, Latam

Bridge Nº 2

Sumario

Lo nuevo

VU Security

Durante el mes de julio, VU Security llevó a cabo la primera Conferencia Iberoamericana, "Ciberseguridad, elemento clave para inclusión social y financiera", que contó con la visión de expertos de Microsoft, Grupo BID, Telefónica y Falabella. Durante el evento se presentó el Reporte de Ciberseguridad 2020, elaborado por VU Labs con datos reveladores sobre el estado de la ciberseguridad en la región. Además, la compañía anunció una inversión de aproximadamente 30 millones de dólares en capacitación y generación de puestos de trabajo para contribuir a la alta demanda de profesionales especializados en el mercado laboral que existe hoy en todo el mundo. El evento puede volver a verse en el canal on demand de la empresa, promocionado en sus redes sociales. Ver aquí: https://bit.ly/2QmYLel

"Ciberseguridad: Riesgos, Avances y el Camino a seguir en América Latina y el Caribe", 2020.

El reporte es la segunda edición de una publicación exclusiva desarrollada a partir de un modelo del Centro de Seguridad del Universidad de Oxford. El informe contiene datos relevantes sobre las diferentes dimensiones del estado de ciberseguridad de 32 Estados Miembros de la OEA, y muestra los avances logrados por la región en materia de ciberseguridad. Asimismo, la publicación está acompañada por una página web en la que los usuarios podrán acceder a información comparativa por tema, países y los respectivos indicadores de iniciativas de ciberseguridad por año.
Descargar reporte completo

BID Mejorando vidas

OEA Más derechos para más gente

Braycom

La empresa presenta Virtual Expert su solución de acceso remoto que permite a los especialistas operar los equipos como si estuvieran en su mismo lugar físico. Habilita servicios tales como:

Virtual Expert

- Acceso remoto a consolas seriales
- Acceso remoto por SSH, Web, etc.
- Túnel VPN Punto a Punto
- Troubleshooting
- Medición de performance
- Captura de trafico y sniffing
- Análisis de tráfico mediante netflow
- Discovery de red
- Medición de calidad
- Voip, entre otros servicios.

Identidad Digital

Vinculados a la vida online, la identidad digital y el cibercrimen cobran gran relevancia y son temas fuertes que reclaman ser atendidos con urgencia. En relación a ellos, conversamos con Daniel Monastersky, abogado especialista en delitos informáticos y reputación digital.

Daniel en Twitter: @identidadrobada

El camino se presentaba largo cuando Daniel decidió que su foco estaría puesto en leyes de corte digital: "En ese momento en Argentina había una reciente ley de Protección de Datos Personales, todavía no estaba el Registro de Bases de Datos vigente, no había una ley de Delitos Informáticos, no había nada", nos cuenta. Inaugurar el camino fue su tarea.

Highlights de la conversación

A nivel internacional se está hablando mucho sobre la necesidad de colaboración entre los sectores público y privado para la investigación de los delitos informáticos y de la armonización de las normativas y la legislación, ya que se trata de delitos transnacionales, por ejemplo si el grooming se considera delito en Argentina también lo sea en Chile, Paraguay, Uruguay, y Brasil.

En relación al concepto de identidad digital, podemos hacer una diferenciación entre las personas grandes y los jóvenes: los jóvenes en general no tienen una expectativa de la privacidad, sino justamente todo lo contrario, buscan tener más seguidores, más likes. Las personas grandes tenemos otro tipo de expectativa, incluso tenemos miedo.

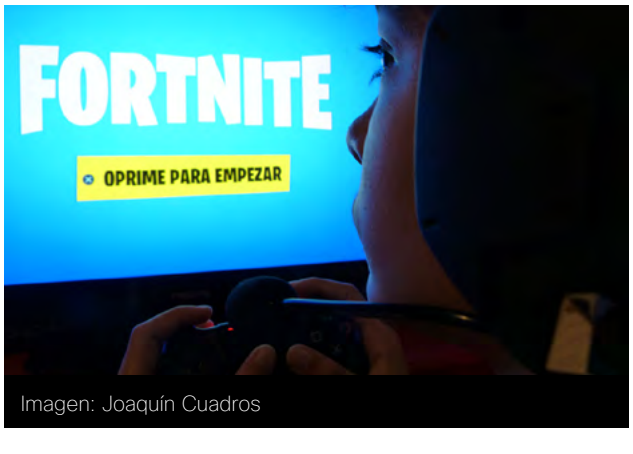


Imagen: Joaquín Cuadros

Que los chicos manejen la PlayStation, juegos en línea y participen en redes sociales, no significa que tengan conocimientos profundos acerca del mal uso de esos elementos.

Este confinamiento nos afectó a todos, y también a los delincuentes que son parte de la sociedad, en este caso, los que no estaban cometiendo delitos a través de medios digitales migraron y se sumaron a ellos.

Es fundamental hoy en día que las empresas, organizaciones y el gobierno cuenten con una figura de concientizador digital. Así como existe la posición de Data Privacy Officer, que también exista el Digital Awareness Officer, una persona cuya responsabilidad sea generar los programas de concientización digital.

Deberían existir campañas de concientización digital que sean impartidas desde el Estado, las empresas, las escuelas, que haya un cambio y se incluya en la nómina una materia de Introducción a la seguridad digital. Es algo fundamental

Video podcast

Ciberseguridad que mejora la experiencia de usuario

Resguardamos la identidad digital de tus clientes para que tu negocio crezca.

- Prevención de Fraude
- Protección de la Identidad
- Biometría
- Gestión de Riesgo

vusecurity.com | @vusecurity | corporate@vusecurity.com

Toda la verdad sobre las noticias falsas

por **Jorge Prinzo**

¿Es este cartel verdadero o falso?
Una invitación a agudizar los sentidos.

La noticia falsa es una información que se publica con forma de noticia, pero diseñada para engañar a quienes la reciben. Se crea para desprestigiar, desinformar, manipular la opinión pública y generar visitas en sitios de internet.
¿Quiénes crean noticias falsas? Hay quienes tienen interés en dañar la reputación de otras personas, instituciones o países, otros buscan generan contenidos y desinformación como forma de ganar dinero. Puede ser que administren sitios web y quieran aumentar el número de visitas, y también hay periodistas que omiten verificar fuentes.
Una vez creada y difundida, las noticias falsas multiplican su alcance al replicarse en redes sociales, servicios de mensajería instantánea y medios de comunicación masiva.

¿Qué podemos hacer si dudamos de una noticia? Investigar la fuente de donde viene, verificar quién es su autor, leer la noticia completa antes de compartirla, revisar la fecha de publicación, y buscar en internet si está en otros medios de comunicación.

Todo se complica

La creación humana y artesanal de noticias falsas no es el único origen posible, ni el más difícil de reconocer, ni tampoco el de mayor alcance. El uso de inteligencia artificial para producir y expandir el radio de acción de las noticias falsas es ya una realidad para considerar en el mundo virtualmente interconectado de hoy.
Dora Kaufman, especialista en inteligencia artificial, escribió una nota para el diario brasileño O Globo en la que señalaba que "la producción de noticias falsas no sólo está proliferando, sino que también se está volviendo más sofisticada: al agregar inteligencia artificial, surgen falsificaciones más profundas". Y planteó una situación que es necesario identificar: "vivimos en un período de crisis generalizada de confianza, que extrapola eventos en Internet. Por encima de las normas morales y éticas, del marco regulatorio y de los sistemas de castigo, y para funcionar de manera saludable, la sociedad necesita un

Imagen: Arek Socha

mínimo de confianza entre sus agentes: instituciones, gobiernos y ciudadanos. Las herramientas de la tecnología y de los medios digitales exacerban el escenario actual".

Y por si esto fuera poco

¿Es posible reconocer una noticia falsa creada mediante inteligencia artificial y difundida a escala mundial en un instante? Nadie diría que sea fácil.
Tan cierto como eso es que la inteligencia artificial es a la vez parte del problema y de su solución. Así como hay personas que crean herramientas virtuales que fabrican noticias falsas, otros se dedican a producir programas de detección y control de esos mensajes.
En una nota para el portal de tecnología Canaltech, Felipe Demartini informaba que la red social Twitter decidió incorporar una empresa que desarrolla productos de inteligencia artificial para combatir la difusión de noticias falsas. Así lo explicó: "Twitter está trabajando activamente para detener la propagación de cuentas falsas y desinformación. Aquí es donde entran los sistemas de la empresa Fabula AI, que ha desarrollado una tecnología que compara el flujo compartido de noticias falsas con noticias reales de fuentes certificadas, como una forma de identificar enlaces y perfiles involucrados en esta difusión".
No está de más recordar que detrás de las noticias falsas, y también detrás de los programas que las persiguen, hay personas.

La única verdad es la realidad amenazada

La realidad es que vivimos rodeados de noticias falsas, una verdad con la que debemos convivir sin que eso implique aceptarlas como algo natural, sino como un problema permanente que requiere atención, ya sea para evitar considerarlas como para advertir a quienes podamos para que no las den por ciertas, y también para que no las repliquen.
En una nota de la agencia británica BBC, leemos: "'Si una historia es demasiado emocional o dramática, es probable que no sea real. La verdad suele ser aburrida', afirmó la periodista ucraniana Olga Yurkova. La activista contra las noticias falsas –cofundadora del sitio StopFake– dijo que las informaciones fraudulentas son 'una amenaza para la democracia y la sociedad'".

Una obra de bien

Chequeado es el nombre de un medio digital preparado por integrantes de la Fundación La Voz Pública. No es partidario ni tiene fines de lucro. Se dedican a verificar los discursos públicos, combatir la desinformación y promover el acceso a la información y la apertura de datos.
En una nota reciente explicaban que las noticias falsas son más virales que las verdaderas, y también se viralizan más rápido. En esto, las emociones juegan un rol clave. Consideran que debe haber responsabilidad en las plataformas y redes sociales sobre los contenidos que se difunden, y que a la vez cada persona tiene el desafío de leer críticamente los contenidos que recibe, pensar antes de compartir, y verificar que sea información precisa y basada en evidencias.
Quienes producen noticias falsas incluyen contenidos engañosos y diseñan estrategias de difusión imitando formatos confiables. También desacreditan información verdadera porque no les gusta o no les conviene.
Lo que buscan es un beneficio económico o político, y a veces la intención de provocar.
A propósito de las fuentes, en Chequeado señalan los bots: algoritmos que controlan miles de cuentas en redes, que producen y difunden contenidos; también hay trolls: usuarios humanos organizados en redes; luego periodistas que no confirman el origen de los datos; e influencers: personalidades cuyas opiniones son consideradas por un público amplio.
Usualmente, el enojo es una causa frecuente para difundir un mensaje de forma casi automática. A veces es por el atractivo del dato. Y otras veces, simplemente, es la necesidad de contactar a otras personas el motivo para enviar información.
La principal recomendación de Chequeado es ser responsables de lo que elegimos difundir y consultar otras fuentes antes de hacerlo.

En tono de comedia

Las noticias falsas inspiraron a Jean-Paul Sartre para escribir una comedia. Se titula "Nekrasov" y sigue vigente (y así seguirá siendo).
Hace unos años fue interpretada durante un festival de teatro en Buenos Aires. El sitio Alternativa Teatral comentó entonces:
"Las ventas del diario gubernamental 'La Tarde de París' bajaron considerablemente y sus directivos están desesperados buscando una noticia "explosiva" para poner en primera plana. Jorge de Valera, un estafador acorralado por la policía, se presentará en la redacción del diario haciéndose pasar por Nekrasov, un alto funcionario soviético desaparecido y se introducirá, casi sin saberlo, en un territorio de negocios y conveniencias políticas basadas en el manejo inescrupuloso de la información.
A partir de ésta, su única comedia (inspirada en el famoso caso de Víctor Kravchenko, desertor del ejército rojo y crítico de la Unión Soviética), Jean-Paul Sartre satiriza el rol de los grandes medios de comunicación, la influencia de estos sobre los lectores y el provecho que de ellos pueden sacar los gobiernos".
Ante la multiplicación de este fenómeno, es de esperar que haya autoras y autores que contarán en comedias y tragedias lo que es vivir rodeados de noticias falsas.

Con toda intención

Así como las noticias falsas existen desde el origen de nuestra humanidad, también hay respuestas nacidas desde la exageración o el disparate. A falso, falso y medio es lo que proponen revistas en papel y digitales que crean sus propias noticias, falsísimas, con la sana intención de hacer reír.
Un ejemplo de nuestro país es la revista "Barcelona", que se presenta como "una salida europea a los problemas de los argentinos". La política nacional es la principal fuente de ideas para sus notas, aunque en verdad no hay tema que escape a sus observaciones.
Para la alegría brasileña existe "Sensacionalista", autodefinido como "un diario exento de verdad". Se destacan sus chistes referidos al gobierno, lo que nos lleva a pensar si podrá haber humor oficialista. Puede existir, pero seguramente no puede compararse con el humor opositor.
Hay infinidad de ejemplos de medios similares, tanto en la historia como en el ancho mundo. Si las noticias falsas son un problema que nos exige cuidados para convivir con ellas, siempre habrá quienes nos hagan reír con un remedio mejor que la enfermedad.

Hágalo usted mismo

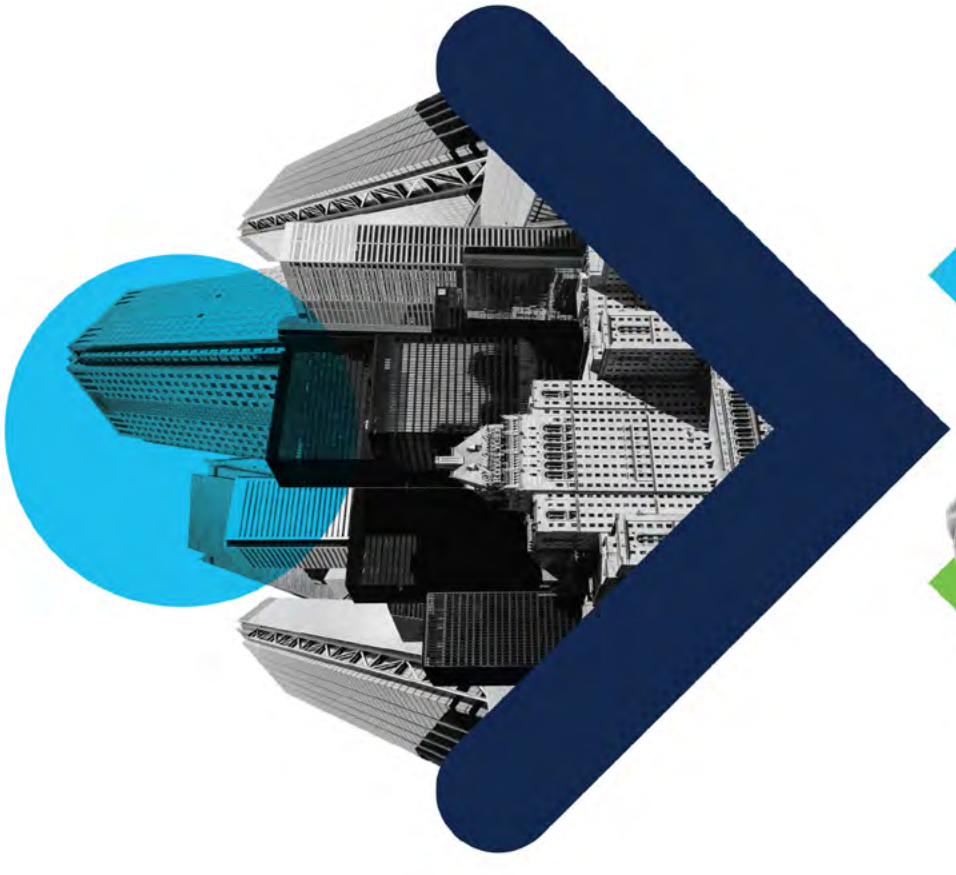
La tecnología actual ha puesto al alcance de muchos (no de todos) la posibilidad de crear y emitir los propios mensajes. También podemos replicar los mensajes de otros, cosa más habitual, y de ahí surge la extraordinaria difusión de las noticias falsas.
Tal vez sea oportuno dar un salto cualitativo: en lugar de reenviar a amigas y amigos lo que a nuestra vez recibimos, proponerles como un juego crear y compartir las propias noticias falsas. No esas torpes y reiteradas que nos llueven a diario, sino unas nuevas, originales, frescas y renovadoras. Así, cuando todo esto pase y vuelvan las reuniones, podrán recordar, evaluar y premiar a las mejores de sus propias obras.
Una regla ineludible para este juego es que todos los participantes estén al tanto de qué se trata y no pretendan divulgar esos contenidos fuera del grupo.
Mientras tanto, les sugerimos no creer todo lo que lean

CISCO
SECURE X

Experiencia simplificada

La plataforma Cisco SecureX es una experiencia integrada dentro de nuestra cartera de seguridad que se conecta con toda su infraestructura de seguridad.

Conozca más



CISCO The bridge to possible

Cibercrimen y Ciberseguridad

Juan Marino, gerente regional de Ciberseguridad de Cisco, entrevista a **Adrián Acosta**.

Pensar que podía conversar con un experto de la Organización International de Policía Criminal, es decir, Interpol, siempre fue algo que estuvo en mi imaginario. La experiencia, que les relato a continuación, fue muy interesante. Con predisposición y mostrando gran compromiso por su trabajo, Adrián Acosta nos cuenta qué significa pertenecer a una red intergubernamental integrada por casi 200 países, que buscan hacer del mundo un lugar más seguro. Y no solo del mundo real sino también del virtual.

Muchas gracias por participar en este espacio. Un poco para clarificar al lector y a la gente en general, ¿qué es Interpol? Y ¿cuál es tu labor?

Interpol es una organización internacional, dedicada principalmente a la cooperación policial internacional. Lo que hacemos es cooperar entre policías en casos criminales. Una de las tareas principales está relacionada a las capturas internacionales, es decir, cuando hay prófugos internacionales. Interpol tiene una base de datos importantes a nivel mundial que le permite a las policías saber si una persona tiene o no captura a nivel internacional. Básicamente es ese el trabajo de Interpol. Eso que aparece en las películas sobre agentes internacionales buscando gente por el mundo, bueno, eso... no sucede. Nosotros colaboramos con las policías de los 194 países miembros de Interpol.

Con tu expertise, ¿cómo ves el tema del cibercrimen? En este caso, ya no están buscando a una persona que comete un delito de algo físico, sino a criminales que se mueven en un ámbito mucho más intangible y, tal vez, potencialmente más impune. ¿Es así? Y ¿cómo evoluciona la investigación del cibercrimen?

Está la fantasía que la tecnología le da cierto anonimato a las personas en su camino criminal, y que los ciberdelincuentes cometen crímenes en distintos países sin tener que pasar por una frontera física, sin embargo, hoy hemos avanzado muchísimo en las tareas de investigación y la realidad no refleja esto que la gente se puede imaginar. El anonimato termina siendo descubierto.

Conversatorio

texto: Silvia Montenegro
video: Juan Marino

Adrián Acosta,
Digital Crime Officer de Interpol.

Es muy alentador, y me lleva a uno de los puntos que quería preguntarte. ¿Crees que hay una ventaja ofensiva o una ventaja defensiva? ¿Qué podemos hacer para inclinar más la balanza para la ventaja defensiva desde el punto de vista tecnológico? Desde el punto de vista de organizaciones, ¿se puede colaborar? ¿Es posible librar una lucha contra el cibercrimen y ganar una cierta ventaja defensiva?

Seguramente que sí, estamos trabajando en eso. En la medida en que los Estados, las empresas y las personas tomen más conciencia se preparan más. Es algo que está ocurriendo, pero no a la velocidad que quisiéramos. Ya las empresas grandes toman mucha conciencia y se están preparando continuamente para no recibir ataques, para no ser víctimas de cibercriminales, para asegurar su información, que hoy por hoy es uno de los activos más importantes que tienen. Sin embargo, a las pequeñas y medianas empresas les cuesta trabajo tomar conciencia y son los blancos principales de los cibercriminales. Las personas individuales también confían mucho en la tecnología y les complica estar preparados ante los ataques. Hoy hay que estar consciente desde el punto de vista tecnológico y tener el mejor antivirus o dispositivos, y también es preciso estar alertas como personas y no hacer click en algún mensaje o en alguna página no confiable. Hay un trabajo integral que se tiene que hacer, debe haber un contexto tecnológico que asegure el ambiente, el trabajo y la información. Pero también tiene que haber capacitación y concientización a las personas, para poder ser proactivos y no ser víctima de los cibercriminales.

En tiempos de COVID-19, ¿hay un efecto en cuanto a la actividad del cibercrimen? ¿Hay un aumento del riesgo o realmente en este mundo ciber no cambian mucho las cosas? ¿Cuál es tu visión?

Mi visión fue cambiando. Nadie estaba preparado para esta pandemia. No llegamos a prepararnos para lo que se venía, no tuvimos tiempo. Tanto los Estados y las organizaciones internacionales como las empresas y las personas fuimos sorprendidos

por esta crisis sanitaria que ocurrió tan rápido. Fue algo que nos pasó por encima sin darnos cuenta, y de un día para el otro estábamos encerrados en casa. Al principio, el cibercrimen se mantuvo en una línea constante porque los cibercriminales siguieron trabajando, se conectaban y continuaron. La gente pasó a trabajar desde sus casas y se empezó a conectar más a Internet, no solo para cumplir con sus trabajos sino también para su vida personal, para su desarrollo diario habitual. Entonces, sí, empezó a haber un crecimiento. En muchos países hubo un crecimiento exponencial bastante grande de muchos crímenes cibernéticos, como el phishing, uno de los más se pudo detectar, o el ransomware, ambos crecieron exponencialmente gracias a que la gente está más tiempo en Internet y aprovecharon esa situación. En muchos países, como en Argentina, disminuyeron los crímenes ordinarios, el de la calle, entre un 60 y un 80%. Y crecieron otros crímenes, como la violencia intrafamiliar, la violencia de género y el cibercrimen. Este es uno de los grandes cambios que hubo en este tiempo. Hoy el cibercrimen es uno de los crímenes que estamos viendo como prioridad a nivel mundial.

Me gustaría saber tu punto de vista sobre el nivel de madurez en la Región. En los países latinoamericanos, ¿hay una adopción razonable de las tecnologías? Y ¿cuál es el alcance a nivel cultural y a nivel personal? En un mapa de calor, ¿dónde estamos? ¿Estamos bien? ¿Muy desfasados? Sabiendo que el tema tecnológico se mueve a una velocidad muy grande...

En principios puedo decir que no hay una homogeneidad, no es parejo, no todos los países están en las mismas condiciones. El análisis que podemos hacer depende mucho de cada país. Sí hay Estados y países que han tomado más conciencia que otros en temas de cibercrimen, y tomar conciencia significa considerar si el cibercrimen puede afectar la economía del país, de las empresas, y entonces esa conciencia hace que algunos países tengan estrategias en ciberseguridad o firmaron la adhesión a la Convención de Budapest. Algunos países están en proceso y otros ni lo están considerando. Esos temas son importantes para ver el nivel de madurez. Rubricar la Convención de Budapest obliga a tener legislación, a estar preparado, a poseer una estrategia de ciberseguridad. Es una declaración de buenas intenciones, pero obliga al Estado a invertir más y al sector privado a tomar conciencia. En Latinoamérica y el Caribe tenemos distintas realidades, hay mucha diferencia en el desarrollo de las capacidad para contrarrestar el cibercrimen. Ya vamos dejando la parte proactiva, de la defensa, y pasamos a la instancia de ver cuándo el Estado, la empresa o la persona son víctimas de algún incidente. En general, en relación con el desarrollo de las capacidades, la investigación y la legislación, estamos bastante bien a nivel mundial y en igualdad de condiciones con muchos países de la Región. Algunos están al mismo nivel que en Europa, con capacidad para investigar y resolver los casos. Debemos seguir trabajando en armonizar la legislación, en desarrollar nueva legislación para que los crímenes nuevos que aparecen día a día no queden sin poder ser encuadrados como delito. La falta de legislación a veces dificulta plantear qué delito es, cómo se tipifica. Debemos seguir trabajando para, a través de la ley, darles a los policías las herramientas para investigar, como es la figura del agente encubierto o agente revelador y otras figuras que aparecen hoy debido a la ciberseguridad. Necesitamos legislar herramientas que den mayores capacidades de investigación. Por otro lado, algo muy importante, son las leyes de protección de datos de los países. Es imprescindible que estén tipificadas, que se desarrollen. A veces cuando uno habla de la ley de protección de datos dice vamos a poner límites a la policía, a los organismos de aplicación de la ley, y eso está ya subsanado porque nadie va a pedir una información sin la orden de un juez o de un fiscal, sin embargo, las empresas pueden llegar a publicar información de sus usuarios y esto en algunos países no está contemplado. La ley de protección de datos es muy importante para dar un contexto de previsibilidad en el orden de Internet. Estamos trabajando en ese camino. Hay países que tienen leyes bastante

buenas, y otros que están trabajando en eso. Argentina debe trabajar en actualizar su protección de datos que estaba desfasada.

En Argentina, hay un término que fue un poco polémico y politizado, que es el ciberpatrullaje. ¿Cuál es tu visión del tema?

En el ciberpatrullaje, en una visión personal, hay dos temas a considerar. Tenemos que preguntarnos para qué se hace. ¿Se hace para recabar información de inteligencia sobre lo que hacen las personas o las empresas? En este caso, para mí está mal. Ahora si se hace para buscar en fuentes abiertas la comisión de delito, el crimen en sí, sin afectar la privacidad de las personas, de ninguna manera entrar a lugares que no son fuentes abiertas sin una orden judicial, entonces está bien. Es decir, se puede hacer ciberpatrullaje sobre fuentes abiertas y buscando prevención de crimen. Porque si no el ciberpatrullaje lo puede hacer también la sociedad en general. Cuando ven que están vendiendo armas o material de abuso sexual infantil en la red hacen la denuncia en la policía. ¿Por qué no ser más proactivos y hacer ese ciberpatrullaje y ver lo que está pasando en las fuentes abiertas? Sin embargo, no se debe hacer violación de algo que no sea fuente abierta o de incurrir en violar la privacidad de las personas, eso sí está mal. Se puede hacer como se hace el patrullaje, que se recorren las calles y se ve si alguien está cometiendo algún delito, sin esperar a que la gente haga la denuncia en la unidad policial.

Claro en el patrullaje común nadie se mete en tu casa, es sobre el espacio público...

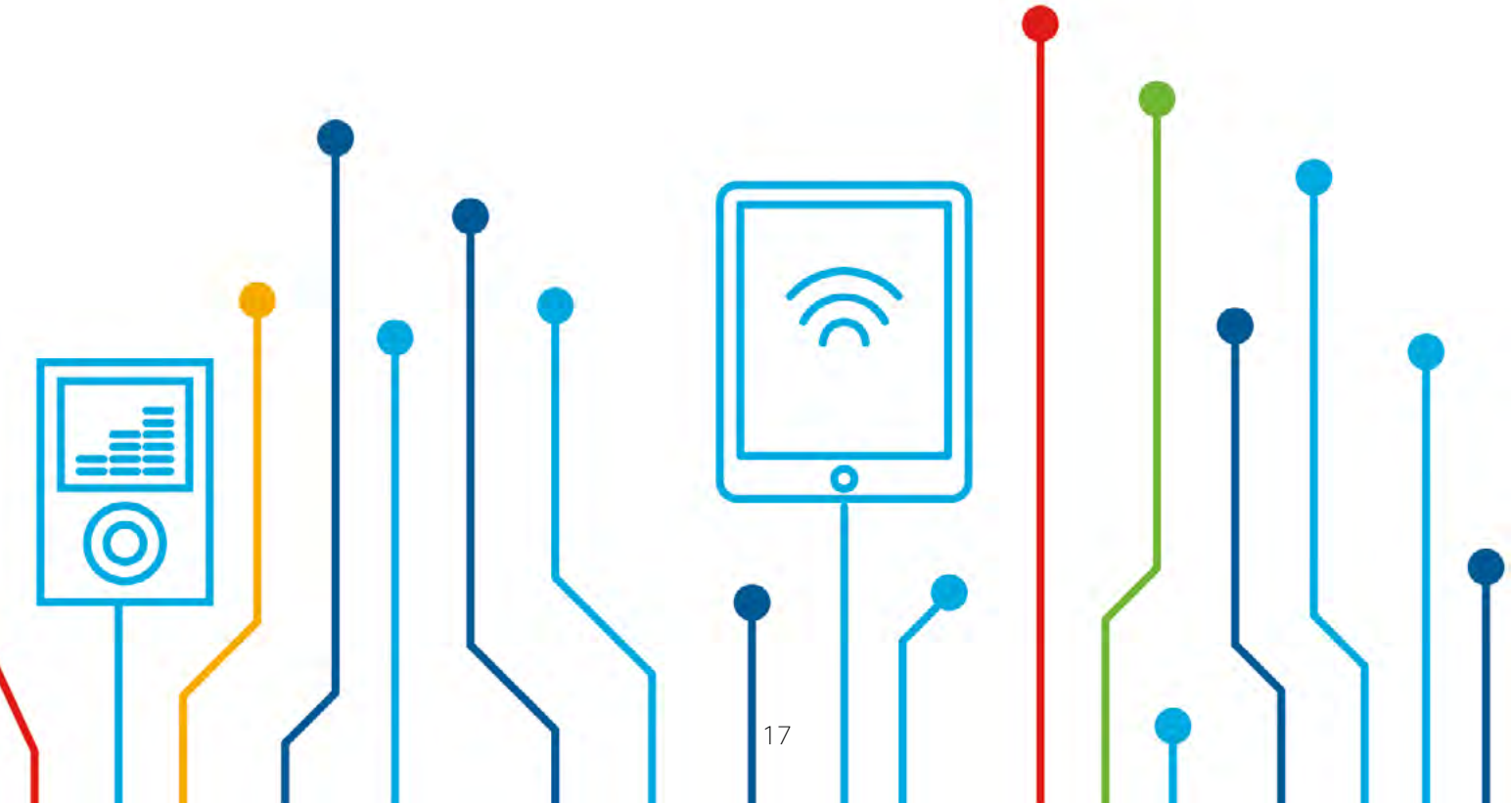
Exacto, para entrar en una casa se necesita una orden de allanamiento, una orden de un juez. Entonces el patrullaje es andar por la vía pública donde todo el mundo puede circular y haciendo un trabajo de prevención también. El ciberpatrullaje es igual, no hay que meterse en un ámbito privado.

Y, por último, ¿cuál sería la recomendación para una familia? En cuarentena pasamos mucho tiempo en casa, con teletrabajo, en familia, con chicos, ¿qué recomendación hay que darle? ¿cuáles son los riesgos a los que nos estamos exponiendo?

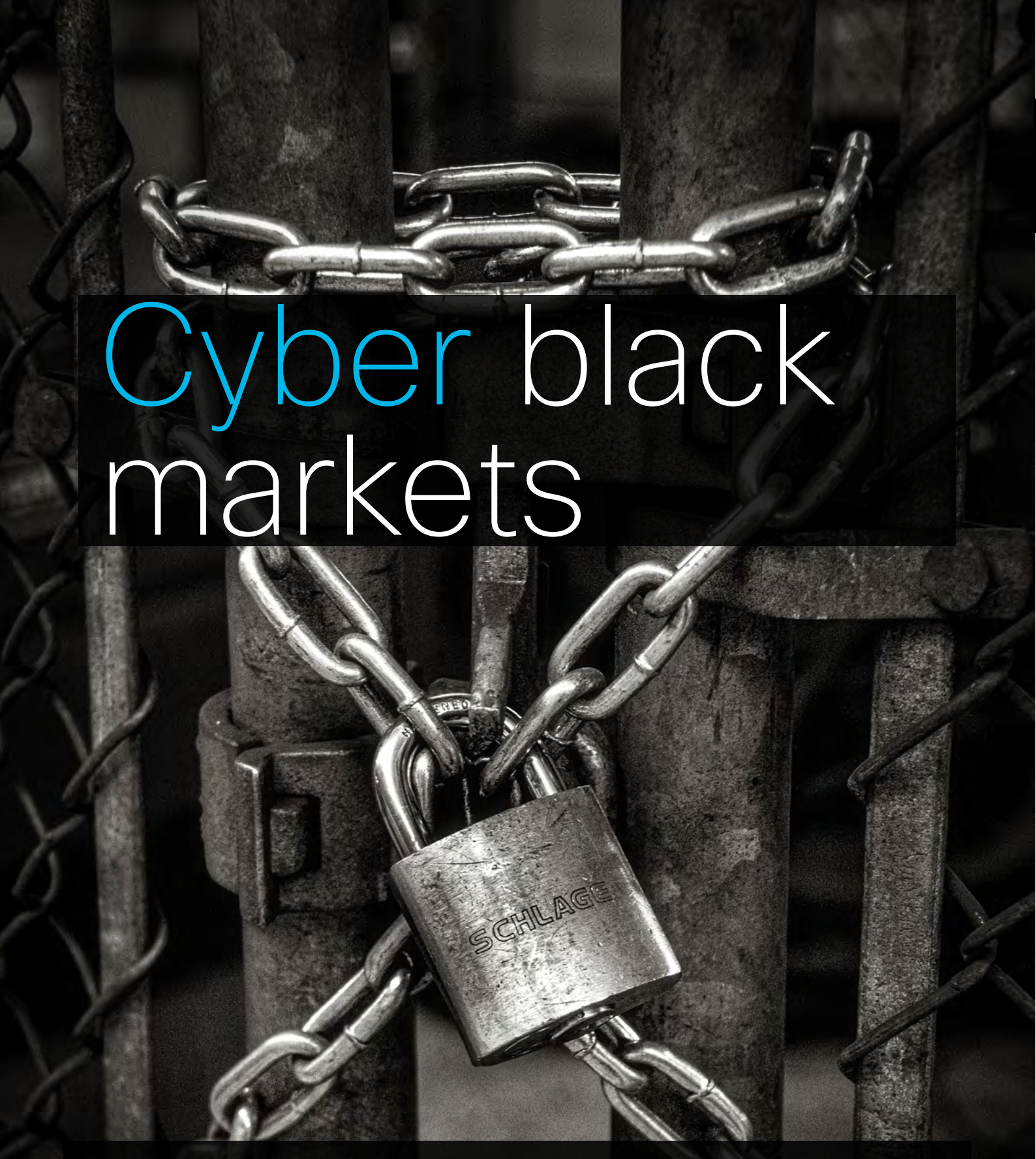
Se necesita un trabajo más proactivo de los países en temas de prevención y concientización. Los Estados tienen que abordar estos temas. En un gran porcentaje, en el cibercrimen uno no sabe lo que le puede pasar y los criminales se aprovechan de este desconocimiento de la gente, o que es falso lo que le están diciendo. Con prevención, se bajaría mucho el índice de víctimas y por ende el criminal. Pero también las empresas pueden entrenar y concientizar a la gente, sería muy útil. Y las personas deberían informarse sobre lo que está pasando en la red, siempre hay delitos nuevos.

Hemos hablado de una multiplicidad de temas muy interesantes. Te agradecemos el espacio, el tiempo. Muy enriquecedora la conversación y espero que podamos seguir colaborando desde el rol de ciudadanos y también desde el profesional. En nuestro caso desde una empresa de tecnología, desde el tuyo desde Interpol, me parece que tenemos que colaborar entre organismos públicos y privados para dar lucha al cibercrimen. Gracias y un placer haber tenido esta oportunidad de conversar contigo.

Muchas gracias, Juan, y una de las cosas que la ciberseguridad ha cambiado es que los organismos públicos y privados se unen en esta lucha y en este trabajo de prevención contra la criminalidad en la red. El policía no estaba acostumbrado a trabajar con el sector privado, y esto ha cambiado gracias a la ciberseguridad. Gracias por la invitación



Cyber black markets



Los cibercriminales no descansan, y es de público conocimiento que se han aprovechado de la pandemia, y en particular, de la cuarentena para robar información, generar estafas, acceder a cuentas corporativas. También, nuestros más jóvenes, los niños, al encontrarse en casa para estudiar y conectados prácticamente todo el tiempo, se convirtieron en uno de los sectores más afectados por los criminales: en este caso los groomers. Según la fiscal especializada en ciberdelitos de Buenos Aires, la Dra. Daniela Dupuy, se han incrementado un 80% las denuncias por grooming en los primeros dos meses de la cuarentena: es decir, el acoso de índole sexual de un mayor hacia un menor a través de la tecnología. Además del enorme indicador que esto presupone, el nivel de alerta que nos genera como investigadores es aún mayor: es bien sabido que no todo se denuncia, y si vemos un 80% de lo

Imagen: John Salvino

por **Ing. Pablo Lázaro**
Especialista en ciberseguridad y ciberdelitos
Director de proyectos de CyberOprac.

denunciado las cifras aun no contabilizadas deben ser mucho mayores.

América Latina es una región atractiva para los ciberdelincuentes: en lo referente a ataques recibidos en la región, los países más afectados por su tamaño de mercado son claramente Brasil y México, seguidos por Colombia, Argentina, Perú y Ecuador.

Pero, ¿cuáles son los motivos que justifican el aumento de este tipo de crímenes en América Latina? Los expertos apuntan a tres causas: la falta de reportes, el desarrollo económico e industrial y la dificultad de seguir la huella a los criminales.

Por este último punto es que quiero referirme a otro aspecto poco tratado del "distanciamiento social". Algo más emparentado a los delitos tecnológicos, es decir, a los delitos tradicionales cometidos a través de la tecnología. En esta oportunidad me refiero a la venta de ilícitos a través de internet. Los criminales como los narcotraficantes, los que venden productos robados o documentación adulterada, también han visto "afectado su negocio" por la cuarentena. Por la consecuencia lógica de la falta de gente en las calles, los criminales también fueron migrando su modelo de negocios y han reconvertido sus "canales de venta" a través de internet.

Si bien, esto no es en si algo nuevo, ya que hace varios años se ve: venta de armas a través de internet o venta de drogas a través de internet, se pudo vislumbrar en esta oportunidad que no se trata solo de los famosos "dark markets" de la darkweb, sino que las herramientas cotidianas que utiliza el ciudadano no necesariamente tecnológico, que se ha visto en la necesidad de instalar aplicaciones como las de delivery de comida o homebanking, también se han convertido en un peligroso canal de distribución de ilícitos como las drogas.

La mayoría de las aplicaciones de "delivery" (Glovo, Rappi, PedidosYa, UberEats, Cabify, etc.) tienen una opción para poder llevar "lo que sea" de un lado a otro. Basta con indicar la dirección de donde retirar un paquete, y hacia dónde será llevado que allí estará un mensajero, lo retirará y sin mediar preguntas lo entregará en el destino previsto.

En Argentina, el gremio que representa a este rubro de trabajadores ha denunciado desde el mes de abril de 2020 un incremento exponencial en el delivery de droga. Es decir, hubo casos, y muchos, donde ellos mismos se han dado cuenta que eran utilizados para realizar estas acciones. ¿Qué herramientas poseen para negarse? ¿Cómo hacen para denunciarlo?

Se han incrementado también, los casos donde la policía detecta este tipo de redes, pero quien termina allanado es el repartidor de comida, su bicicleta o moto. Entonces, ¿cuenta la justicia con los medios tecnológicos para detectar, rápidamente, el origen o destino de estos envíos?, ¿existen en nuestra región los instrumentos necesarios de cooperación público-privada en términos de investigación policial para proteger al empleado y perseguir al verdadero delincuente? Lamentablemente la respuesta es no. Los códigos penales de la región siguen muy enfocados en lo que es la evidencia física. En casos como estos quien realmente comanda la red puede estar fuera del país o, al menos, del distrito y utilizar terceros de una manera muy sencilla. Estas plataformas, normalmente, no tienen representación legal en la región, muchas de ellas tampoco cuentan con una plataforma de acceso a requerimientos de información por vía judicial (como si lo tienen Uber, o Facebook, por ejemplo), sino que piden un exhorto judicial para obtener la información requerida como por ejemplo la dirección IP o teléfono de quien realizó originalmente el pedido.

En otros puntos de la región este fenómeno se ve de igual manera, e incluso, con otro tipo de apps desde antes de la pandemia: es conocido el caso de la red en distintos lugares de Latinoamérica como Chile, Perú y Brasil, que utiliza una conocida app de citas para pautar encuentros que, en lugar de ser de índole sexual, se utilizan para compra/venta de droga al menudeo. Incluso a través de "emojis" el comprador puede entender que el virtual vendedor ofrece marihuana (la hoja de arce de los Emoji), LSD (el dibujo del alien) y otros.

Los números son alarmantes, crecen día a día en todo el mundo. Es necesario generar un amplio consenso en la región para lograr ámbitos de cooperación público-privada, requerir a las plataformas medios de acceso a la justicia de manera ágil y eficiente. Sin dudas, hay cosas que la pandemia logró que llegaran para quedarse, pero nuestro trabajo como especialistas en seguridad es darles visibilidad y generar espacios de trabajo que protejan a nuestra sociedad

Imagen: Laura Rivera

Educación Remota en tiempo de COVID-19

Conversamos con la Licenciada **Florencia Salvarezza,** experta en aspectos neurocognitivos del aprendizaje.

Más de 1370 millones de alumnos interrumpieron sus clases a finales de marzo cuando el mundo se puso en modo cuarentena por la pandemia de COVID-19, según datos de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO). En este contexto, la educación remota apareció como una solución para mitigar el efecto de las clases presenciales suspendidas, y dar continuidad a la educación, un derecho fundamental para todos los ciudadanos y que tiene un rol decisivo en el desarrollo de los países.

La estrategia presentó un gran reto para educadores, alumnos y familias, que debieron adaptarse inmediatamente, con mayor o menor facilidad, según los casos, ya que para hacer efectivo el aprendizaje el estudiante debe tener computadora y acceso a internet, situación que excluye a los alumnos de los estratos más vulnerables. En general, los especialistas observaron que ningún país posee hoy un sistema educativo preparado para este tipo de emergencias.

Y la Escuela desapareció...

La licenciada Florencia Salvarezza, lingüista, profesora de Psicología evolutiva y educacional, directora del Instituto de Neurociencias y Educación, INE, de la Fundación INECO, y consultora para el BID en temas de alfabetización, dice que se trata de una experiencia inédita: "De repente, la escuela, un sistema que tiene cientos de años, desapareció, y fue reemplazada por la virtualidad. Se abrió la caja de la computadora y se metió la escuela ahí. No estábamos preparados. No hubo un plan, se hizo como se pudo". Agrega que, además, la situación trajo aparejada un tema ético: "Antes de esta crisis era impensado encerrar a un niño o joven durante 100 días", así que no solo se pasó del aula a la computadora, sino que se sumaron los problemas emocionales que implica el encierro. Después de repasar sobre las cuestiones técnicas, relacionadas a los problemas de conectividad o falta de dispositivos para los integrantes de las familias, pone su mirada en aspectos pedagógicos: "¿Cuánto tiempo puede estar un niño atento a la pantalla? Poco tiempo, por eso, muchas escuelas redujeron sus clases virtuales a pocos minutos por día. Por otra parte, falta el intercambio con el docente, y con sus pares, es decir, la interacción social, el trabajo colaborativo, la inclusión, la conversación, el debate, la práctica, la corrección por parte del docente. Desde este punto, transportar lo presencial a lo virtual no es posible".

El rol de la tecnología

En la post cuarentena, ¿la educación puede volver aggiornada, mejorando el proceso a partir de la práctica que está dejando esta experiencia? La especialista, quien es profesora universitaria y conferencista internacional, rescata la herramienta poderosísima que representa la tecnología, y dice que es necesario incluirla en el aula con mejores resultados: "El desafío es volver a pensar el aporte de la tecnología como una herramienta fundamental, y ya no desde el reemplazo de la presencialidad por la virtualidad". Opina que, en esta coyuntura, no enriqueció demasiado a la educación, ya que solo se utilizaron las aulas virtuales y algunas plataformas para hacer ejercicios: "No entraron a la escuela los grandes recursos tecnológicos, que ya existen. Llegó solo una parte. Los chicos tienen que sacar fotos a sus trabajos y volverlo a subir, es casi prehistórico con respecto a lo que se puede hacer digitalmente".

Agrega que, en el próximo escenario, para empezar, se debería aprovechar sus posibilidades en lo cotidiano, por ejemplo, cuando el docente tenga que enseñar sobre la Primera Guerra Mundial, puede elegir los videos maravillosos que hay en la web sobre el tema.

Su diagnóstico incluye el rol de la industria tecnológica: "Debería involucrarse de un modo distinto para poder pensar en estas herramientas que la escuela necesita. Tecnología pensada para acompañar y complementar al aprendizaje". No es muy optimista en cuanto a mejorar la vivencia educacional aprovechando lo aprendido en estos meses: "Creo que los seres humanos tenemos mucho menos capacidad de cambio de lo que pensamos. Las costumbres pesan. Es muy difícil que los docentes, con tantos años de práctica, cambien sus métodos. Se está viendo en los países europeos, vuelven a la normalidad de antes. Por eso, creo que esos cambios los pueden motorizar las empresas de tecnología, y hacer un gran aporte a la educación"

La seguridad y la educación

Florencia Salvarezza opina que la ciberseguridad preocupa a los padres. Indica que, en estos días, además de observar cómo se manejaba la escuela en el área contenidos, los adultos de las familias sumaron la preocupación por el tema de la seguridad informática en relación con sus hijos.

"Para los más chicos, el tema no existe. Los adolescentes, por su parte, saben que puede ser peligroso, pero a esa edad les cuesta medir los riesgos. Con respecto a los universitarios es un asunto conocido, pero se divide bastante la población, aún solo para algunos la seguridad es una preocupación".

Basanta
contenidos

La distancia siempre es relativa,
depende de la percepción. Somos los dueños de
cada una de nuestras distancias: el espacio físico que nos
separa puede ser el terreno que nos une si la emoción que nos
conecta es la esperanza. El tiempo eterno que transcurre durante
la separación del ser amado puede convertirse en el instante que
apela a la cercanía entre dos personas que se piensan. Un libro
puede alejarnos kilómetros de nuestro entorno inmediato, una
palabra puede prometernos la cercanía del porvenir. Elegimos.
Somos los dueños de todas nuestras distancias.

Contenidos Multiplataforma

basantacontenidos.com

Medicina y Ciberseguridad

Contrapunto

texto: Karina Basanta
video: Ghassan Dreibi

Melissa Palmieri, doctora en Medicina, especializada en prevención y vacunas conversa con **Ghassan Dreibi**, especialista en ciberseguridad, para encontrar los puntos en común entre ambas áreas. ¿Qué tienen para aprender una de otra?, lo contamos en este artículo.

Las agendas de Melissa y Ghassan coincidieron en Webex. Luego de un intercambio fluido sobre las ideas a desarrollar iniciamos la grabación. Medicina y Ciberseguridad tienen más que palabras en común, comparten ideas, planteos, protocolos y urgencias que atender. En ambas áreas es mejor "prevenir que curar" para facilitar la resiliencia.

Melissa

En medicina lo importante es la prevención y muchas veces relacionado con ella, es necesario hacer detección. En el momento que detectamos una anormalidad iniciamos un tratamiento para perseguir la curación. Cuando los daños están causados, muchas veces pueden ser reparables, por ejemplo cuando podemos hacer una cirugía, o medicar insulina en el caso de un paciente diabético; o infelizmente, irreparables, incluso llevar a la muerte. Entonces puedo asegurar que en el área de la medicina, cuando hablamos de un relacionamiento en prevención, transitamos por esos pasos.

Ghassan

Es muy interesante este intercambio. Durante muchos años, en tecnología, cuando hablamos de virus imaginamos que era posible prevenir todas las amenazas. En los últimos años, esta percepción sobre la prevención cambió, ahora sabemos que de cualquier manera, vamos a ser atacados. Tal como sucede en medicina, aunque contemos con elementos que nos permiten prevenir, como vacunas por ejemplo, sabemos que algo nos puede suceder. Cuando algo malo sucede en tecnología, nos preguntamos cuánto tiempo hace que sucedió. Igual que en medicina se busca el paciente cero, el origen de la infección. En tecnología como en medicina debemos descubrir ese origen lo más rápido posible.

En nuestra área se tardan a aproximadamente 100 días en detectar una nueva amenaza cibernética, es decir que durante este tiempo esa amenaza está robando datos e infectando computadoras, por ejemplo, y nadie lo sabe. Entonces no solo es importante la rápida detección sino también la reacción.

Melissa

Quedé impactada con lo que dices, Ghassan. En mi área existe la vigilancia, tanto ambiental como epidemiológica, porque muchos de los virus que producen amenazas pandémicas sufren mutaciones. ¿Qué sucede? Un virus que circulaba solamente en animales, acaba migrando y entrando en círculos humanos debido a que el ser humano ha irrumpido en ambientes que no debía. Globalmente existen técnicos en salud y principalmente veterinarios que trabajan recolectando sangre de los animales, viendo la disposición de esos virus y mapeando. Esa es una forma preventiva. Mas cuando aparece esa mutación que citaba antes se vuelve una amenaza muy urgente de atender por toda la comunidad científica ¡y debe hacerlo en menos de cien días! Un poco como sucedió con el coronavirus: en el momento que se detectó había casos de neumonía muy extraños con mortalidad alta, entonces toda la comunidad científica empezó a correr contra el tiempo para mapear ese virus y hacer todo el secuenciamiento para entender y confeccionar una acción preventiva y curativa.

Ghassan

Encuentro otro punto interesante de comparación. Cada virus, cada malware puede sufrir mutaciones, los llamamos virus polimorfos. Operan de la siguiente manera: se instalan de una forma transparente en la máquina sin generar ningún síntoma, son asintomáticos, para usar un término médico, y después se actualizan, se preparan para hacer lo que venían a hacer. Para nosotros es importante comenzar a conocer los síntomas que generan los virus cuando empiezan a actuar. En Cisco creamos un centro de inteligencia global llamado Threat Intelligence que se encarga de recolectar cientos de accesos a internet y comienza a proveer anomalías nuevas que disponibiliza a través de un mapa de calor. Aquello que detecta lo comparte rápidamente para darlo a conocer. No sé si eso pasa también en tu área.

Melissa

Sí, puede suceder, todo depende del sistema de vigilancia de cada país. Al final, actuar preventivamente, depende de personas. Ahí hay otro punto en común: por más que se detecte y mapee muy bien ese agente infeccioso, si las personas que deben actuar con esa información no lo hacen, de poco sirve.

Otro punto que tiene relación con esto es que en salud vale mucho más invertir en prevención que en curación, la curación ya sería un gasto, pensemos por ejemplo en una hospitalización, una rehabilitación y hasta infelizmente la muerte. ¿Cómo lo ves en tecnología?

Ghassan

Tanto en seguridad cibernética como en medicina debemos hacer una inversión para estar preparados para algo que, sabemos, va a suceder. En ciberseguridad los virus son tan agresivos, las máquinas están tan interconectadas que debemos estar listos para actuar tanto frente a un virus que conocemos como frente a uno nuevo. En nuestra área una forma de estar preparados sería con la creación de un proceso, de un framework de prevención, que permita mantener un ambiente controlado incluso en circunstancias difíciles. Lo más importante es tomar buenas decisiones. Lo que yo siento en el escenario actual de pandemia es la dificultad de contar con buenas informaciones.

Melissa

Entiendo y estamos de acuerdo. Existe algo que es esencial y de lo que has hablado y que preocupa mucho en el área de salud, especialmente a la prevención y las vacunas: las fake news. Recientemente circuló una noticia muy preocupante para nosotros y que tiene que ver con que las próximas vacunas contra el coronavirus son creadas por grupos poderosos para introducir un chip de control de las personas. Esa noticia falsa es sumamente dañina porque puede disminuir la cobertura de la vacuna en el país y expone a la población a riesgos inconmensurables para la sociedad brasileña. Tanto tu área como la mía se enfrentan a desafíos interesantes en relación a las fake news.

Ghassan

Exacto. La falta de información afecta la toma de decisiones. Las personas buscamos la verdad. Debemos aprender a confiar más en los gobiernos, en los científicos, en los médicos, parar de buscar todo en internet. Y por otro lado, los gobiernos, los científicos y los médicos deben poder explicarnos bien por ejemplo, si implementan una aplicación para seguimiento de salud, cómo usarla, para qué sirve y cuáles son sus fines, así podremos creer y utilizarla. Debemos tener en cuenta que buenas informaciones traen buenas decisiones.

Melissa

¿Sabes? El miedo que tú podrías tener en relación a los profesionales de la salud es el mismo miedo que yo tengo al utilizar un medio digital. Y yo que trabajo con prevención y tengo leídos tantos estudios y trabajos médicos, creo que necesitamos crear información más “digerible” para una utilización digital segura. Tal vez esto refleje aquello que decías sobre que los aplicaciones de salud no están siendo tan bien utilizadas como podrían.

Ghassan

Se me ocurre otro punto de contacto con medicina y en relación a las medidas que se han tomado durante la pandemia ¿Qué hacer luego de una infección tecnológica?

Mi recomendación es implementar una segmentación. Sé que voy a ser atacado. Es evidente que no podré proteger a todo el mundo de todo el mundo porque están todos conectados. Debo hacer seguimiento, tener visibilidad y segmentar; algunas áreas podrán seguir operando y otras estarán en “cuarentena”.
En salud sucede lo mismo. Nosotros somos responsables de nuestra salud, no podemos dejar todas las decisiones de parte del gobierno, si uso una máscara es mejor para otros pero también es mejor para mí.

Melissa

Estas nuevas amenazas continuarán en nuestra vida, como bien decías. Pero tenemos algunas recetas interesantes. Recién hablabas de la utilización de máscaras. Tal como aprendimos que con la máscara podemos evitar contagiar a otros si estamos resfriados, en el área digital tenemos que aprender a depurar las informaciones y tomarlas de bases idóneas. La Organización Mundial de la Salud, Unicef y otras organizaciones ya hablan de infodemia, en relación al exceso de información que no aporta buenos datos. Tú estás aquí para ayudar a las empresas y yo a las personas, luego ellos podrán elegir qué camino seguir. Estamos aquí para orientarlos en la prevención. Como sociedad, es importante que caminemos juntos y actuemos preventivamente.

Producción de fotos remota a Melissa Palmieri, doctora en Medicina, especializada en prevención y vacunas.

Ghassan

Solemos hablar de Inteligencia Artificial. Al estar conectados hay cada vez más datos para analizar, pensemos en vehículos autónomos y en casas, por ejemplo. Para integrar todos esos elementos, la figura de seguridad tecnológica es la orquestación. Si fuese tan fácil orquestar o poner a las personas a aprender, frente al COVID-19 podríamos hacer andar una máquina con la instrucción "eliminar COVID" y ya tendríamos la solución. Con las personas pasa lo mismo, necesitamos tener flexibilidad y aprender, tener capacidad de resiliencia para recuperarnos de malas experiencias y seguir. También es importante contar con buenos profesionales. Algo que vemos en el mercado de ciberseguridad es que faltan personas idóneas. ¿Sucede lo mismo en salud?

Melissa

Lo que dices es muy importante. También sucede en salud. Ahora se está viviendo una situación muy particular en Brasil, no hay mucha paciencia ni mucha conciencia colectiva.

Ahí tú has traído la palabra resiliencia, del latín *resilire*, que significa saltar hacia atrás, rebotar. La resiliencia está asociada a la capacidad de sobreponerse a los problemas, de superar los momentos difíciles y reponerse. Algo muy interesante que se estudió es que es muy importante que exista el desorden y el caos para que haya sobrevivencia y crecimiento. Las personas que viven situaciones y experiencias de estrés y que las atraviesan con resiliencia son seres humanos que luego van a actuar de una forma mejor. Por ejemplo, en la situación actual de pandemia que puede ocasionar a algunas personas depresión, angustia, ataques de pánico mientras no tengan claridad sobre la llegada de las vacunas o los tratamientos, si las personas fueron resilientes durante ese período, seguramente cuando esto pase podrán vivir relaciones más armónicas consigo mismas, con su familia y en su trabajo. En medicina, para mí ser resiliente es mantener una forma de vida saludable: alimentarse bien, hacer actividad física, dormir muy bien y acceder a las vacunas disponibles.

> Es crucial la importancia de una educación continuada y razonada para saber qué creer y en quién confiar, tanto en salud como en el uso de tecnologías de la información y comunicación.
> La prevención primero: la frase "mejor prevenir que curar" acierta en todos los aspectos.

Producción de fotos remota vía Webex a Ghassan Dreibi, Director de Operaciones de Ciberseguridad, Latam, Cisco.

Ghassan

Estoy de acuerdo contigo en todos los puntos en relación a la resiliencia. Y pienso además en la urgencia de algunas personas para volver a la normalidad, para volver a viajar, por ejemplo. Así como para eso será necesario seguir un protocolo, corroborar la salud, las vacunas, también en ciberseguridad si no tenemos un control mínimo nos exponemos a acciones criminales. Así como los virus son complejos y no los podemos controlar, aquí sucede lo mismo. Si no tenemos un ambiente tecnológico controlado y estable, no sabremos quién accede a él. En salud, sabemos a quién buscar cuando algo pasa, al pediatra si se trata de nuestros hijos. En tecnología también es necesario tener un canal de comunicación abierto, un socio tecnológico, esa es mi recomendación, Melissa. Si tenemos un ambiente estable, controlado, actualizado y mantenido, si sabemos a quién buscar cuando sucede alguna cosa facilitamos la resiliencia.

Melissa

Muy interesante y necesario el intercambio, Ghassan, gracias a tí.

Ghassan

Muy linda conversación, Melissa, muchas gracias

> En relación a la confianza en ciberseguridad tenemos una frase que dice “zero trust to be trusted”, es decir no confiar en nada hasta tener la prueba que se puede confiar.

> La falta de información afecta la toma de decisiones. Debemos tener en cuenta que buenas informaciones traen buenas decisiones.

Ciberseguridad: trabajo del presente y del futuro

El trabajo es una de las mayores preocupaciones del ser humano. Constantemente nos cuestionamos acerca de cómo incentivar el mercado laboral de acuerdo a las condiciones de cada país o región, con qué disciplinas, cuáles serán las mejores prácticas para hacerlo crecer, cómo proteger a los trabajadores frente a los cambios que traen las distintas eras.

Cada "revolución" trajo nuevas perspectivas, nuevas formas de desarrollo, nuevos temas para pensar, entender y desarrollar. Se renovaron algunas prácticas, eliminaron otras y se crearon oportunidades al incorporar nuevas.

Una de las funciones de los Estados es la adelantarse a los cambios a través de una planificación anticipada que ordene e interprete información proveniente de los distintos sectores de la sociedad. Esta información privilegiada, le permitirá tomar decisiones en cuanto a políticas públicas que conecten educación y salida laboral.

De acuerdo a sus características, desarrollo y cultura, habrá países que preferirán centrarse en la vocación del ciudadano y otros que elegirán hacer foco en las necesidades económicas que debe afrontar el país, y así incentivar la educación con un enfoque más funcional.

Informes internacionales se valen en la actualidad de nuevas y ricas fuentes de datos a través de las cuales se obtiene información privilegiada y sin precedentes sobre las oportunidades emergentes para el empleo en la economía global así como una comprensión precisa de las distintas habilidades que necesitan incorporar los profesionales.

Con la mirada en el futuro y los pies en la tierra.

En su informe "Jobs of tomorrow", de enero de 2020 el World Economic Forum revela que "96 empleos en siete grupos profesionales están emergiendo rápidamente en tándem, lo que refleja factores "digitales" y "humanos" que impulsan el crecimiento en las profesiones del mañana. Se prevé que los trabajos del futuro crecerán un 51% en 2020 y proyecta que se presentarán 6,1 millones de oportunidades de trabajo a nivel mundial. Éstos reflejan la adopción de nuevas tecnologías, dando lugar a una mayor demanda de empleos de Economía Verde, roles a la vanguardia de la Economía de Datos e Inteligencia Artificial, así como nuevos roles en Ingeniería, Computación en la nube y Desarrollo de productos. Por otro lado, las profesiones emergentes también reflejan la importancia continua de la interacción humana en la nueva economía, dando lugar a una mayor demanda de empleos en la Economía del cuidado; roles en Marketing, Ventas y Producción de contenido; así como roles a la vanguardia de Gente y Cultura".

La cuarta revolución industrial está creando millones de nuevas oportunidades laborales para las cuales gobiernos, organizaciones comerciales y personas deben prepararse, procurando capacitación técnica y fortaleciendo recursos internos como la empatía, creatividad, liderazgo, capacidad para negociar y resolver problemas.

Una disciplina transversal que crea empleo

Conjuntamente con la aceleración en transformación digital, surgen temas a los que hay que atender con especial dedicación, el más importante es, acaso, la seguridad de los sistemas y la protección de la información. En este sentido, la ciberseguridad se vuelve en sí misma un trabajo del presente y del futuro, con incontables oportunidades de empleo y desarrollo.

Atendiendo a esta necesidad, y a la urgencia de colaboración entre los sectores públicos y privados, OEA (Organización de los Estados Americanos) y Cisco firmaron un acuerdo en agosto de 2019 que dio origen a los Consejos de Innovación en Ciberseguridad. Esta iniciativa incluye cursos gratuitos de ciberseguridad para al menos 100.000 estudiantes a través del programa Cisco Networking Academy.

Los cursos están dirigidos por expertos en ciberseguridad, y pueden realizarse al ritmo de cada estudiante, de manera online y gratuita. Además, los estudiantes que tomen parte del programa recibirán

Imagen: Fanjianhua

una certificación avalada por Cisco y la OEA y una distinción que podrán compartir en sus perfiles profesionales.

Tal como concluye el informe del WEF que citáramos más arriba "tenemos a nuestro alcance herramientas que ofrecen una visión granular sin precedentes de la naturaleza y las oportunidades en el mercado laboral. El imperativo emergente es utilizar dichas herramientas con prudencia y al servicio de los trabajadores en su búsqueda de empleo productivo y satisfactorio", el progreso individual y colectivo de una nación no es fruto de la casualidad, más bien se construye en la unión entre el sector público y el privado, asumiendo los desafíos y oportunidades con responsabilidad

En mayo de 2020 el acuerdo OEA-Cisco extendió su alcance al anunciar un fondo de US$150.000 dólares para financiar proyectos de innovación en ciberseguridad para Latinoamérica.

Con el foco en la **estrategia**

por **Martín Marino**
Director de Braycom

5 key points para armar una estrategia de ciberseguridad

Hace unos días mi hijo me preguntó cuál es mi superpoder. Como por un túnel mi mente viajó a mis cinco años. Contornos borrosos y muy iluminados resaltaban mi traje azul y rojo, mi máscara y el brazo derecho extendido hacia arriba con una potencia sobre humana. Para ampliar mi base de apoyo, las piernas estaban ligeramente separadas y adheridas al piso como dos estacas. Mi cuerpo era una barrera de acero frente a cualquier ataque, estaba plenamente enfocado en una defensa. Sin embargo, mi hermano se acercó por atrás, me sacó la máscara y empezó a hacerme tantas cosquillas que el acero se volvió cera y me derretí de risa por unos cuantos minutos. ¿Cuál era mi verdadero super poder? ¿Cuál es hoy?

Analogías aparte, y con los pies en la tierra, muchas veces cuando las organizaciones plantean sus necesidades de ciberseguridad hablan de una serie de productos poderosos en sí mismos que crean la ilusión de proteger a la entidad frente a cualquier amenaza. Sin embargo, los tiempos que corren reclaman otra cosa, algo más elaborado, que esté respaldado por una estrategia y que en ella estén incluidos productos, procesos y personas.

En Braycom elaboramos cinco puntos esenciales para desarrollar una estrategia de ciberseguridad adaptada a las necesidades de hoy. Los compartimos aquí contigo:

1. Integrar la ciberseguridad a la estrategia de negocio.

Negocio y ciberseguridad tienen una dependencia mutua, no pueden transitar por separado. Las juntas directivas deben involucrarse con la forma de hacer seguras las operaciones e incluirla en sus planes de negocio. Una administración desprevenida puede dejar de ser un buen negocio.

2. Ciberseguridad transversal a todas las áreas.

Pensar y actuar cada área imbuida de procesos de ciberseguridad. Los puntos de entrada de una amenaza son tantos como personas y dispositivos conectados a la red propia y de toda la cadena de valor.

3. Resiliencia es más que prevención.

Los expertos aseguran que a partir de la alta exposición debido a la aceleración en la transformación digital, es seguro que nuestra organización será atacada en algún momento. Por ello, además de una fuerte acción preventiva, debemos aprender a ser resilientes, es decir a sobreponernos y seguir operando. Una vía posible es trabajar en la recuperación del área dañada mientras las otras continúan sus procesos y así evitar la detención del negocio.

4. Capacitar a todos los integrantes de la organización.

El factor humano suele ser el principal punto de acceso de un ataque. Dar herramientas de capacitación contra amenazas a todos los integrantes de la organización se vuelve un elemento imprescindible en la era digital. La urgencia también reclama nuevas posiciones que generen y promuevan procesos de ciberseguridad.

5. Procesos en lugar de productos.

Una organización cibersegura es aquella que además de asesorase y conformar una arquitectura robusta de seguridad digital, promueve acciones y procesos que incluyen todos los factores que la integran: perímetros, endpoints, redes, cloud, aplicaciones, sistemas, trabajadores, y la lista sigue.

Vuelvo al inicio, a la pregunta de mi hijo, y la reformulo: ¿cuál es el superpoder de nuestras organizaciones? Acaso sea nuestra capacidad para trabajar en equipo, los procesos y las estrategias que nos lleven a cumplir los objetivos que nos planteamos

Crear mi estrategia de ciberseguridad con Braycom

Argentina
Av. Independencia 1330 – Piso 14 – Of B – CABA
Teléfono: +54.11.5273.4470

Colombia: +57.1.580.1333
Chile: +56.2.2938.1332 – **USA:** +1.786.358.6100

Imagen: Ximena Nahmias

Infraestructuras Críticas

Colaboración

Interoperatibilidad

Estándares

Conciencia

Un denominador común en los discursos de todas las fuentes consultadas para este artículo.

por **Walter Montenegro**

Walter Montenegro
Gerente de Ciberseguridad de Chile.

Valentín Soulages
Cyber Partner, Risk Advisory, Deloitte.

El dato como centro La información como valor.

La cuarta revolución industrial, denominación de un proceso de cambio producido por la transformación digital, ubica las miradas de los estados, organizaciones e individuos en la protección y cuidado de los datos. Con la información como centro del funcionamiento óptimo de distintos procesos que abarcan tanto gestiones y prácticas personales como sociales, los líderes del sector público y privado del mundo en general, y Chile en particular, acercan su accionar en busca de trabajo conjunto y participativo.

"Hablar de infraestructuras críticas en procesos de transformación digital es hablar, indefectiblemente, de grandes volúmenes de datos que contienen información de extrema importancia para el funcionamiento equilibrado de industrias, cadenas de suministro, cadenas de valor y su última milla, el usuario final", indica Valentin Soulages, Cyber Partner, Risk Advisory, Deloitte.

Sin embargo, ¿qué son las infraestructuras críticas? Podemos decir que son todos aquellos sistemas físicos o virtuales que hacen posible las funciones y servicios considerados esenciales y que contribuyen al buen desempeño de los sistemas más básicos a nivel social, económico, medioambiental y político. Cualquier alteración o interrupción en su suministro, debido a causas naturales (una catástrofe climática, por ejemplo) o provocada por el factor humano (como un ataque cibernético a una central de energía eléctrica) podría acarrear graves consecuencias. Por ello, los principales activos a proteger son el dato y la información que aporta.

"Lo más importante a entender es que esta transformación digital en las industrias entregará la capacidad para generar nuevos modelos de negocio, basados en los datos y en la conectividad de sus productos a través de IoT (Internet of Things) como son: plantas altamente especializadas y optimizadas, con un control avanzado de procesos utilizando miles de sensores que proporcionarán datos en línea, como podría suceder en una planta de energía eléctrica, por ejemplo; transporte autónomo, medidores inteligentes, sensores que monitoreen fugas en la red de agua, movilidad inteligente (semáforos inteligentes, sistemas de análisis de flujos de tráfico), generación y transporte inteligente de energía, entre otros muchos usos. También va a contribuir la llegada del 5G, con sus posibilidades de conectividad a una velocidad superior y una menor latencia", comenta Carolina Pizarro, Strategy Senior Manager, Risk Advisory, Deloitte.

Ciudades, empresas, organizaciones y personas habían iniciado este camino, en algunos sectores de forma leve. La pandemia de COVID-19, empujó a todos a hacer frente a la continuidad de sus operaciones de forma digital. El "cisne negro", máximo imprevisto, aceleró el proceso adentrándonos de lleno en el cambio hacia la digitalización. Sin embargo, acompañado de los grandes beneficios a los que lleva este trayecto, surgen nuevas situaciones que reclaman ser atendidas, la más relevante es la seguridad de la información. Si bien en esta materia y en ciberseguridad Chile se ha manifestado activo, estos temas aún requieren observación, reflexión y acciones concretas.

Un estudio reciente realizado entre Deloitte y la Subsecretaría de Comunicaciones demuestra que el 50% de los chilenos consideran que el robo de información y la privacidad de las personas son dos de los principales riesgos al exponerse a las nuevas tecnologías que trae la transformación digital. En palabras de Víctor Toscanini, Country Manager interino de Cisco Chile, "uno de los ejes que debemos atender conjuntamente entre el sector público y el sector privado, es establecer políticas y procesos de ciberseguridad para proteger los datos y lograr su implementación en colaboración". Sector público,

Imagen: Matthew Henry

privado, instituciones y tercer sector irán entonces tras un uso eficiente de recursos y el desarrollo de nuevos beneficios para los ciudadanos. "El dato debe ser protegido en toda su cadena de valor: desde su generación hasta su destrucción", agrega Soulages.

"La aceleración en el cambio de los hábitos cotidianos que produjo la pandemia de COVID-19 obligó a desafiar paradigmas instituidos en forma de trabajo, educación, salud, formas de encuentro", comenta Pizarro. La presencia física tuvo que ser reemplazada urgentemente por la virtual, que arrancó a los trabajadores de las oficinas para dotarlos de teletrabajo, a los alumnos de las aulas para subirlos, en los mejores casos, a plataformas de videoconferencia para continuar el proceso educativo vía e-learning. "Hubo también la necesidad de contar con información conectada y confiable para la toma de decisiones sanitarias, e incluso la telemedicina, producto del distanciamiento físico impulsado por las normas sanitarias de Chile. La confianza en los datos será uno de los conceptos más relevantes a futuro, y que va de la mano con la seguridad tanto de la información privada como de la información confidencial", concluye.

Infraestructuras críticas: sus necesidades en términos de transformación digital segura

Un ataque masivo y coordinado a alguno o varios de estos sectores, establece una condición de importancia crítica para un país, pues pone en juego la estabilidad del mismo y la confianza de la ciudadanía en el Estado para enfrentarse a estas amenazas. En este sentido, el concepto de seguridad tradicional se transforma para dar paso a una nueva función del Estado sobre la defensa de su soberanía en el espacio digital y la protección de los derechos de sus ciudadanos frente a las amenazas emergentes en el escenario de una vida más digital y gobernada por la información.

Las infraestructuras críticas necesitan incrementar sus niveles de seguridad, monitoreo, respuesta ante incidentes, resiliencia y comunicación en tiempo y forma de los incidentes, integrando la seguridad en los procesos de negocio y creando un entorno de trabajo más seguro para todos. Para lograr estos objetivos, las organizaciones necesitarán una estrategia de ciberseguridad innovadora basada en principios de buena gestión de riesgos, considerando sus activos más críticos y los escenarios que plantea un evento de riesgo de estas características. "La ciberseguridad tiene que ser parte integrante de todo el proceso de transformación digital, de ninguna manera debe ser pensada como adicional o paralela sino como transversal a toda la organización. Pensemos, por ejemplo, en las comunidades conectadas y sus grandes volúmenes de datos provenientes de distintos actores, un ataque a cualquiera de ellos podría causar daños irreparables en muchos casos", apunta Walter Montenegro, Gerente de Ciberseguridad, Cisco Chile.

"Un programa de protección para la IC (Información Crítica) establecerá, en primer lugar, la base para facilitar el intercambio de información entre los opera-

dores de infraestructura crítica a través de políticas y directrices. En segundo lugar, permitirá una focalización sistemática, mejoras a través de mediciones más claras de gobernanza, madurez y ciberseguridad de las redes. Tercero, requerirá operadores para fomentar una cultura de alfabetización en riesgos cibernéticos en todos los niveles de las organizaciones. El objetivo es que todos los sectores críticos establezcan un sistema robusto y efectivo contra las ciber amenazas en evolución", puntualiza Carolina Pizarro.

Hacia dónde debemos mirar. Lo que debemos atender.

Imaginemos por un momento la fortaleza que podrían tener los distintos sectores considerados críticos en Chile si sus soluciones de ciberseguridad fueran interoperables, cada entidad contara con un centro de respuestas ante amenazas interconectados e intercambiando información actualizada en forma constante sobre sitios maliciosos, alertas de ataques, nuevos virus o hackers. Imaginemos empresas grandes, medianas y pequeñas con políticas y procesos implementados de protección cibernética. Imaginemos acuerdos de cooperación entre sector público y privado donde la excepción sea la empresa que no está en ellos.

"Los que tienen éxito son los países que logran establecer la cooperación, intercambian información y desarrollan proyectos comunes. La ciberseguridad no debe ser tratada como un tema político partidista, la ciberseguridad es transversal. Todas las personas pueden ser potenciales víctimas de fraudes y todas las instituciones y empresas pueden ser blanco de ataques. Se debe ir en busca de alcanzar el mismo objetivo", indica Carlos Landeros, Director CSIRT y Jefe de División de Redes de Seguridad Informática del Ministerio del Interior, en el marco del ciclo de webinars Tecnología y COVID-19, organizado por ACTI.

Sin embargo, si bien Chile está en muy buena posición y con importantes avances dentro de Latinoamérica, aún hay camino por recorrer. Algunos de los puntos que requieren impulso son:

- Igualar las posibilidades de acceso digital, aún dispar entre las distintas regiones, es uno de ellos. El informe de *"Digital Readiness Chile"* estudio local desarrollado por profesionales de la Fundación País Digital, bajo la solicitud de Cisco, realiza un diagnóstico que busca certezas para encauzar el desarrollo digital del país, y concluye que las regiones de Antofagasta, Metropolitana y de Magallanes son las únicas que se encuentran en etapa de amplificación. Es decir, estas regiones alcanzaron los mayores puntajes en las siguientes dimensiones: infraestructura y adopción tecnológica, capital humano, necesidades básicas, facilidad para el comercio, inversión privada y gubernamental, y clima emprendedor.
Adicionalmente y en términos generales, Chile ha sido evaluado en la etapa de *aceleración* en el estudio *Cisco Digital Readiness Index de 2019*, el Índice de preparación digital que Cisco desarrolló para medir de manera integral el nivel de preparación digital de un país. El estudio tomó como base 141 países y con él se buscó proporcionar orientación sobre cómo cada uno de ellos puede mejorar su preparación general para fomentar una economía digital inclusiva. Aquí, Chile obtuvo la ubicación número 34 del ranking a nivel mundial, ocupando la primera posición de América Latina. Sin embargo, esta "aceleración" se encuentra fragmentada, concentrada y con crecimientos dispares. Para que Chile mejore sus niveles de preparación digital, se recomienda generar políticas públicas basadas en evidencias técnicas a fin de incentivar la preparación digital de acuerdo a las condiciones contextuales de cada región del país.
- Implementar políticas y procesos. Las grandes empresas ya llevan aprendido sobre esto y son las más proclives a adoptarlos, sin embargo, las pequeñas y medianas aún tienen mucho por hacer. La pandemia las ha arrojado a continuar sus operaciones en la vía digital, deben ahora aprovechar ese impulso imprevisto para profesionalizar sus modelos de negocio bajo estos parámetros, siempre teniendo en cuenta la ciberseguridad para resguardarse ellas mismas y toda la cadena de valor asociada.
- Lograr el caudal máximo de interoperatividad de soluciones. Crear estándares y trabajar sobre plataformas que permitan reconocerse y aceptarse entre sí.
- Profundizar en temas de legislación y definir una ley marco de ciberseguridad.

Legislación en ciberseguridad

"En el caso de Chile, ya existen algunas iniciativas legislativas, por ejemplo, la modificación del Decreto (DS N°533, 2015) que creó el Comité Interministerial de Ciberseguridad y que tiene por objetivo dotar de herramientas para una efectiva ejecución y seguimiento de la Política Nacional de Ciberseguridad, en vías a una Institucionalidad en esta materia. Esto ya ha permitido importantes avances, por ejemplo, la creación del CSIRT de Gobierno, cuyo rol es coordinar las acciones de respuesta ante incidentes de ciberseguridad, la colaboración y compartición de información entre organizaciones del sector público y privado", apunta Carolina Pizarro.

Con respecto a los proyectos de ley, existen dos que tienen mayor avance; el primero es el proyecto sobre delitos informáticos que, en términos generales, actualiza la legislación a los nuevos tipos de criminalidad informática que han surgido en las últimas décadas; y, por otra, implementa algunas de las obligaciones específicas del Convenio de Budapest sobre Cibercrimen que Chile suscribió el año 2017.

"El otro proyecto que está en el Congreso, es la ley de datos personales, que contempla una serie de normas para el manejo de datos personales, datos sensibles, los derechos que tienen las personas sobre sus datos, las responsabilidades de quienes los manejan tanto en el sector privado como en el público y las multas a las que se arriesgan por el mal uso de la información" agrega Soulages.

"Hoy queda pendiente y es de gran importancia, la ley marco de ciberseguridad que vendría a crear la institucionalidad en esta materia y que permitiría definir las políticas y estándares de ciberseguridad al sector


Imagen: Skeeze

público y también al sector que se denomine como parte de infraestructura critica (transporte, energía, salud, entre otros)", coinciden Pizarro y Soulages.

"Aprobar una ley marco que defina qué áreas de la economía se consideran en Chile infraestructuras críticas, una vez definidos estos sectores será fundamental que cada uno de ellos cuente con su propio CSIRT (Equipo de Respuestas ante incidentes de Seguridad Informática)", aconseja Carlos Landeros, Director CSIRT y Jefe de División de Redes de Seguridad Informática del Ministerio del Interior, por ejemplo en el sector eléctrico, el bancario, incluso en la minería, que es clave para la economía chilena. Todos los Equipos de Respuesta ante Incidentes de Seguridad Informática podrían trabajar coordinados bajo una estrategia que contemple los siguientes puntos como medidas de protección: monitoreo 24/7, herramientas y estrategias de apoyo, compartir y publicar información, aplicar estándares e implementar planes, educar y concientizar.

A modo de cierre

Los procesos industriales de hoy exigen una alta conectividad entre sus componentes, sin renunciar a los requerimientos básicos de continuidad de negocio y alta disponibilidad. Por ello, es necesario crear nuevos procesos de fabricación inteligente capaces de una mayor adaptabilidad a las necesidades y a los procesos de producción, así como a una asignación más eficaz de los recursos.
"Las operaciones tradicionales y su soporte en tecnologías de la información comienzan a traspasar los límites entre el mundo real y el mundo virtual, en lo que se conoce como los nuevos sistemas de producción ciber-físicos", agrega Valentín Soulages. "Es extremadamente importante que las organizaciones comprendan que la ciberseguridad se constata como un elemento habilitador para que las nuevas tecnologías sean operativas, no sólo abarcando los elementos tecnológicos ya mencionados, sino también los procesos en la cadena de valor", puntualiza Pizarro.
En el mismo sentido, siempre que hablemos de ciberseguridad estaremos evocando tres conceptos que llevados a la acción nos permitirán lograr buenas prácticas: integración, acompañamiento y colaboración. "Integrar las distintas soluciones como en una orquesta disminuye la probabilidad del riesgo. El acompañamiento por parte del proveedor de las soluciones es imprescindible como guía, pues en el modelo digital todo cambia constantemente. Por último, y como elemento clave, estamos llamados a colaborar entre todos los actores: disponibilizar las experiencias ayuda a prevenir", afirma Montenegro. "La plataforma de ciberseguridad del futuro estará basada en estos tres pilares", concluye Soulages

Las infraestructuras críticas necesitan incrementar sus niveles de seguridad, integrándola a su proceso de negocio: monitoreo, comunicaciones en tiempo y forma, respuestas eficientes ante incidentes y resiliencia. Deberán crear una estrategia de seguridad innovadora basada en una buena gestión de riesgos que considere sus activos más críticos, me gusta hablar de crear un "Programa de Protección de Infraestructuras Críticas" que incluya el desarrollo de una cultura de alfabetización en ciber riesgos. En este contexto será imprescindible el intercambio de información entre las distintas infraestructuras para crear una colaboración preventiva y resiliente", dice Soulages.

Transformación Digital

Chile

Estado: aceleración

Digital Readiness Chile, el estudio desarrollado porprofesionales de la Fundación País Digital, bajo la solicitud de CISCO Estados Unidos, realiza un diagnóstico que busca certezas para encauzar el desarrollo digital en este país.

El informe se constituye como un insumo técnico que pretende medir la preparación digital de Chile, prestando especial atención a cada una de las zonas que componen el territorio nacional.

En este artículo presentamos una síntesis de sus observaciones y conclusiones más relevantes.

En las últimas décadas, la innovación y el incremento del desarrollo tecnológico han producido cambios sustanciales en las distintas esferas que componen la sociedad. La transformación digital constituye un factor clave en el desarrollo de los países y los ciudadanos que lo habitan. En este sentido, la llamada cuarta revolución industrial se posiciona como uno de los cambios más profundos en el último tiempo.

Para entender la preparación digital en Chile, el estudio siguió los criterios metodológicos de Country Digital Readiness: Reserch to Determine a Country´s Digital Readiness and Key Intervenciones (CISCO, 2018), que reconoce la existencia de 3 etapas de preparación digital: activación (nivel básico), aceleración (nivel intermedio) y amplificación (estadio superior). A su vez, en el documento se definen 7 áreas con las que la preparación digital es posible de ser cuantificada. En razón de ello, para el caso de Chile, las dimensiones e indicadores analizados se configuraron de la siguiente manera:

1. Infraestructura tecnológica
2. Adopción tecnológica
3. Capital humano
4. Necesidades básicas
5. Facilidad para el comercio
6. Inversiones privadas y gubernamentales
7. Clima emprendedor

A partir de allí, se realizó el análisis de participación de estas variables en las 16 regiones o unidades político-administrativas territoriales de Chile (Ñuble y la nueva división de Biobío como anexos).

Resultados

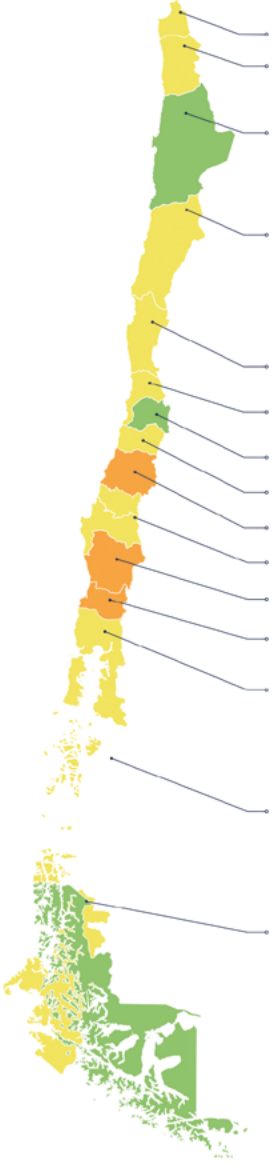
El nivel de preparación digital, en las regiones de Chile, se definió de acuerdo al resultado que ellas presentaron en cada una de las 7 dimensiones antes mencionadas. Se estableció como máximo teórico, un total de 25 pts., lo que representa que el territorio está completamente preparado para la transformación digital.

En el caso de Chile, el máximo puntaje lo obtuvo Región Metropolitana, con 15,52 pts., y el más bajo, Región de La Araucanía, con solo 6,17 pts. En la página siguiente, se detalla el resultado ponderado de cada una de las regiones, indicando la fase de preparación digital que representa cada resultado.

El informe concluye que Chile ha sido evaluado en la etapa de aceleración. Sin embargo, esta “aceleración” se encuentra fragmentada, concentrada y con crecimientos dispares. Para que Chile mejore sus niveles de preparación digital, se deben generar políticas públicas basadas en evidencias técnicas a fin de incentivar la preparación digital de acuerdo a las condiciones contextuales de cada zona del país.

Las condiciones actuales permiten que Chile se ubique en una posición ventajosa, con el potencial para encabezar la cuarta revolución Industrial, en aras de una mayor equidad social para todo el territorio nacional.

Adicionalmente y en términos generales, Chile ha sido evaluado en la etapa de aceleración en el estudio Cisco Digital Readiness Index de 2019, el Índice de preparación digital que Cisco desarrolló para medir de manera integral el nivel de preparación digital de un país. El estudio tomó como base 141 países y con él se buscó proporcionar orientación sobre cómo cada uno de ellos puede mejorar su preparación general para fomentar una economía digital inclusiva. Aquí, Chile obtuvo la ubicación número 34 del ranking a nivel mundial, ocupando la primera posición de América Latina

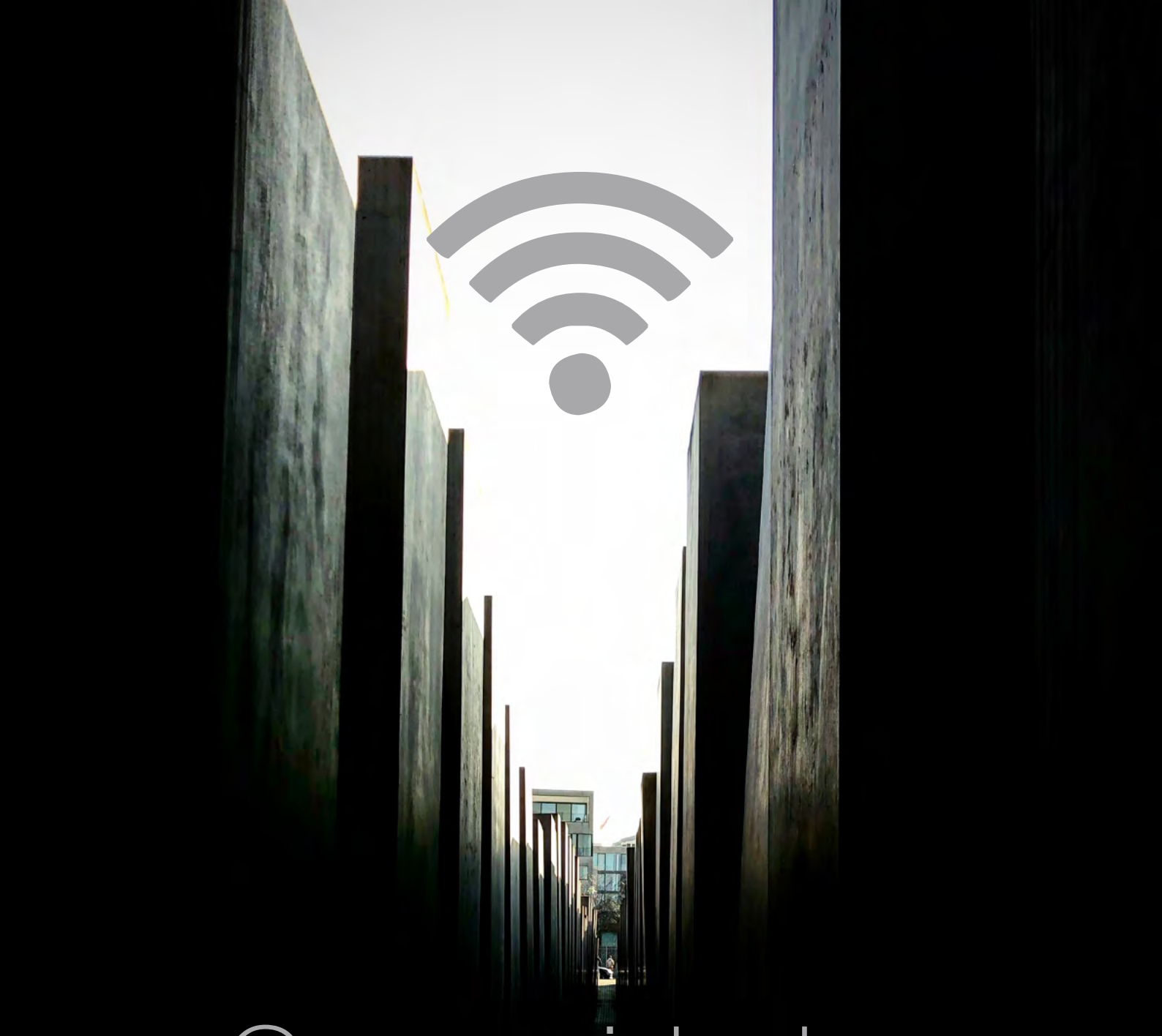


Región »	Puntaje	Fase de preparación digital
Región de Arica y Parinacota	12,75	*Aceleración*
Región de Tarapacá	9,98	*Aceleración*
Región de Antofagasta	14,31	*Amplificación*
Región de Atacama	7,95	*Aceleración*
Región de Coquimbo	8,63	*Aceleración*
Región de Valparaíso	11,6	*Aceleración*
Región Metropolitana	15,52	*Amplificación*
Región de O'Higgins	7,77	*Aceleración*
Región del Maule	6,99	*Activación*
Región de Biobío	8,95	*Aceleración*
Región de La Araucanía	6,17	*Activación*
Región de Los Ríos	6,99	*Activación*
Región de Los Lagos	8,89	*Aceleración*
Región de Aysén	13,15	*Aceleración*
Región de Magallanes	13,6	*Amplificación*

Con los puntajes obtenidos, se generó un **ranking de 1 a 15**, donde 1 es la región más preparada para la transformación digital y 15, la con menor capacidades instaladas.

1. Región Metropolitana
2. Región de Antofagasta
3. Región de Magallanes
4. Región de Aysén
5. Región de Arica y Parinacota
6. Región de Valparaíso
7. Región de Tarapacá
8. Región de Biobío
9. Región de Los Lagos
10. Región de Coquimbo
11. Región de Atacama
12. Región de O'Higgins
13. Región del Maule
14. Región de Los Ríos
15. Región de La Araucanía

Digital Readiness Chile,
nivel de preparación digital por región



Comunidades conectadas

por **Juan Marino**

Estimada lectora, estimado lector, cierre sus ojos por un momento y vuelva en su imaginación a su vida de hace algunos meses atrás, digamos seis. Independientemente de si usted vivía en un medio rural o en un espacio urbano, seguramente su entorno estaba atravesado por algún tipo novedoso de tecnología. Ahora por favor, abra sus ojos. El tiempo parece haberse adelantado rápidamente en términos de uso tecnológico, ¿verdad? Incluso más allá del presente.

Según proyecciones de la ONU (2018), la población residente en áreas urbanas alcanzará el 68% de la población mundial, ya que habrá sumado 2.500 millones de personas en todo el mundo en 2050.

Para ir más profundo en el tema de la transformación digital y su impacto en las comunidades conectadas o ciudades inteligentes, conversé con Pelayo Covarrubias, Presidente del Directorio de la Fundación

Imagen: Carlos Jonay Suarez

País Digital y Director de Relaciones Institucionales de la Universidad del Desarrollo de Chile.

La pandemia de COVID-19 nos ha impulsado a la adopción tecnológica de forma exponencial. En Palabras de Covarrubias, "Este laboratorio COVID_19 nos ha enseñado a todos a usar y valorar la tecnología: desde la primera infancia hasta los adultos mayores asumimos la continuidad de nuestras actividades de forma digital. La tecnología ha tenido relevancia en la administración de esta pandemia y luego en la administración social y económica. Sin duda las telecomunicaciones juegan un rol fundamental y ha sido sumamente importante que hayamos podido mantener, a través de ellas, el teletrabajo, la asistencia médica, la educación y sobre todo, las relaciones con nuestros afectos, imposibilitadas de encuentro físico cercano".

Hoy día la transformación digital no solamente habla del negocio sino también de la sociedad y cómo la llevamos. Esto incluye a las ciudades, impulsadas a actualizarse en relación a la nueva revolución industrial donde el dato y la información que él contiene, son el centro y comportan el mayor valor a proteger.

Detengámonos un momento, y con los datos como centro, repensemos la ciudad a partir de ellos, proyectemos que su uso esté basado en un principio fundamental y diferenciador.

Recientemente, País Digital y Cisco realizaron un estudio que indica el estado de madurez tecnológica en las distintas regiones de Chile ¿Cuáles son algunas de las conclusiones más relevantes que se extrajeron del estudio?

El estudio Digital Readiness Chile, 2019, nos trajo tremendas informaciones para entender cómo estamos en el interior de Chile y cómo estamos en relación a Latinoamérica. Probablemente, si miramos la región, en general somos un continente de followers, no hemos sido líderes en relación al desarrollo digital, más bien hemos ido a buscar tecnología en los países desarrollados y la hemos adoptado, no hemos sido grandes desarrolladores. Eso nos dejó como latinoamericanos, naturalmente, bastante atrás en la primera, segunda y tercera revolución industrial. Entonces, una de las cosas que hemos empujado desde País Digital es que no pase lo mismo en la cuarta. El estudio hace mucho sentido porque nos ayuda a entender qué tenemos que hacer al interior de Chile para poder llegar al nivel superior o nivel amplificado, además nos trajo muy interesantes noticias: la primera es entender que no solo se trata de infraestructura tecnológica, sino de otras variables incluidas en el análisis, como por ejemplo, la adopción tecnológica, es decir cómo adoptamos cada uno la tecnología y cómo la usamos de manera correcta.

En Chile, por ejemplo, el 95% de la gente ocupa el teléfono celular para uso de las redes sociales. Lo que sería muy bueno que suceda es que también lo utilice para hacer e-commerce, banca electrónica o para tener trámites digitales con el Estado. Es decir, que se ocupe no solamente bajo una lógica de consumo social sino también bajo una lógica productiva, eso nos generaría un salto cualitativo. Luego también el índice se adentra en el análisis del capital humano; no es lo mismo residir en una ciudad como Santiago que en una región rural, eso influye muchísimo en el capital humano, la adopción tecnológica y su uso. Lo mismo con las necesidades básicas, el índice las toma y las analiza: redes de agua potable, energía, alcantarillado, y me pregunto ¿y la internet?, en esta época de pandemia, ¿no debería considerarse una necesidad básica? Una persona que está conectada versus aquel que no lo está, produce una brecha digital infinita. Esos son elementos que el estudio nos trajo y que nos permite orientar el trabajo de las políticas públicas para producir el acercamiento.

Saber dónde estamos parados y también observar que no estamos quietos, que nos estamos moviendo hacia el progreso. Tengo la sensación de que eres un convencido que se puede generar una adopción correcta de las tecnologías y se puede posicionar a Chile mucho más adelante a fuerza de una buena concientización y un trabajo sistémico.

Sin dudas, pero tenemos que darle urgencia no solo en Chile sino también en Latinoamérica. Esto se trata de transformación cultural, no solo de tecnología. La sensación de urgencia es un tema que estoy viendo con preocupación. Creo que en la medida en que nosotros vayamos teniendo una forma de pensar distinta es que tenemos la posibilidad de saltar ciertas etapas y llegar a ser países desarrollados. Tenemos que darle mucha importancia a empujar con mayor urgencia la necesidad de esta cultura digital como una forma de producir la transformación, en foros particulares como este y, sobre todo, en foros nacionales.

¿Podemos considerar a la ciudad conectada como una infraestructura crítica? ¿Qué particularidades tiene Chile en relación a la región?

España cuenta con movilidad y redes fijas ambas a 100%. La matriz de conectividad es totalmente distinta a la nuestra. En el caso chileno, estamos muy bien en lo que es movilidad, casi el 100% de los chilenos tienen smartphones y conectividad e internet inalambrica mayormente 4G. Sin embargo, esta respuesta no es todo lo que necesita el país para dar el salto productivo. Hoy el 54% de los hogares tienen conectividad fija, por lo tanto, necesitamos pasar del 54% al 100% como lo hizo España o Japón. A esta situación hay que sumarle las características geográficas del país con sus distintas regiones y la densidad geográfica de cada zona. Las personas mayoritariamente conectadas están en la ciudad, aquí se nos presenta una brecha entre lo rural y lo urbano, eternamente mal distribuido. Otro punto relevante es que, a mayor edad, menor uso de internet. También tenemos problemas educacionales: hemos visto que a menor nivel educacional, es menor el uso de internet, eso es preocupante porque hace que la brecha se extienda. No he nombrado aún la variable económica porque creo que aún más importantes que ella son la educacional, la geográfica y la etaria, luego viene para mí la económica porque hoy en día Chile es un país muy competitivo, tiene uno de los costos de infraestructura más baratos del mundo en banda ancha y banda móvil. Por lo tanto, más que el tema socio económico, son importantes los temas culturales y sobre todo educacionales. Y te lo reflejo en lo siguiente. Con respecto a Internet, el 100% usa redes sociales, el 30% lo utiliza para educación, solamente el 26% hace trámites digitales con el Estado, y el 25% realiza trámites digitales con la banca. Por lo tanto, estamos obligando a los adultos mayores, a los más pobres y menos educados a hacer las actividades presenciales, y esto está produciendo las brechas que estamos conversando. Por eso, en la lógica de las infraestructuras críticas, empujamos con tanta fuerza la mirada de ir conectando con capacidades de red fija de forma que les permita trabajar a las PyMEs, desarrollarse a los adultos mayores, y educarse a los niños.

No solo es cuestión de más tecnología sino también de cómo la adoptamos y la usamos. Te he escuchado hablar sobre la importancia de la institucionalidad. Creo que en ese sentido hay mucho camino por recorrer. Es necesaria más interconexión, sobre todo en cuestiones de infraestructuras críticas. Es importante y necesaria la coordinación a nivel país y a nivel internacional. La intención está y el tema está planteado pero hay mucho por trabajar conjuntamente entre el sector público y privado.

Yo creo algo muy parecido. La sensación de urgencia vuelve. Debiésemos estar mucho más avanzados de lo que estamos. No me cabe duda de que en el mundo de la ciberseguridad la institucionalidad debería estar creando proyectos para empujar y no solo para defender. Debemos fomentar, a partir de la institucionalidad, proyectos que hoy día no estamos realizando. Fuimos avanzando, sí. Desde País Digital, para darte un ejemplo, estamos empujando desde 2015 y hasta 2020 un proyecto que se llama 100% Trámites Digitalizados. Pues bien, estamos solamente en el 54%, por lo tanto, no cumplimos nuestra meta. Eso a mí naturalmente no me gusta, porque es ver el vaso medio vacío. Si lo veo medio lleno, destaco que avanzamos sobre lo que no había, un 54%, alguien podría decir, vamos bien, y hemos sacado leyes de tramitación digital muy importantes. Hoy día el Estado chileno es digital por defecto, lo que me parece muy interesante en el mecanismo, pero tenemos que empujarlo con mucha más fuerza. Porque la cultura de los países que están liderando en la materia es una cultura digital, entonces avanzan mucho más rápido, ellos ya están en la Inteligencia Artificial, están en la frontera de los datos. Estamos en discusiones muy distintas entre naciones, y eso es un tema que me preocupa.

Me pregunto si en términos de educación estamos haciendo las cosas que hay que hacer, o las que podemos hacer. A nivel personal, siento que el modelo educativo en general es arcaico, y más ahora, con esta situación de pandemia quedó claro que cuando queremos hacer remoto el sistema de educación es algo así como querer meter un círculo dentro de un cuadrado. ¿Cómo lo ves? ¿Crees que la pandemia nos va a llevar a cambios drásticos por ejemplo en educación?

Creo que hay que diferenciar ciertos temas. En el ámbito educativo, durante la pandemia todos tuvimos que subirnos a las plataformas por un tema de motivación de vida, para continuar nuestras actividades. Las plataformas de colaboración como Webex y otras tuvieron un crecimiento de uso exponencial. Sin embargo, las clases a distancia no son iguales que las presenciales, por lo tanto, la pedagogía se quedó atrás. La pedagogía digital nos presenta un desafío. Qué vimos: que el nivel de aprendizaje que nuestros alumnos tienen a distancia es menor que el nivel de aprendizaje que tienen de manera presencial. Aquí debemos diferenciar por tipo de materias, si pensamos en materias "duras", como las matemáticas, por ejemplo, veremos que perfectamente pueden ser enseñadas a distancia y seguramente van a tener un cierto nivel de cumplimiento de los principios básicos que están detrás de ellas. En cambio, si miramos aquellas disciplinas que buscan enseñar a trabajar en equipo, a fortalecer los recursos de comunicación, a lograr un pensamiento crítico, que son habilidades más blandas, el trabajo a distancia se hace muy complejo. El ser humano nace y comienza a aprender, la tecnología entrega más herramientas para que pueda aprender aún más y mejor. Tenemos que aprender en primer lugar sobre pedagogía digital, es decir, lo que implica enseñar a distancia y cómo hacerlo, luego, que naturalmente hay habilidades que son distintas desde el mundo presencial al mundo digital. Nunca habíamos tenido un laboratorio a nivel mundial como el que nos trajo la pandemia de COVID-19, que está dejando grandes aprendizajes. Seguramente uno de ellos será determinar qué actividades estarán destinadas a cubrirse a distancia y cuáles de forma presencial.

Ciudades inteligentes: optimizan procesos de forma digital para el bienestar de las personas.

Vamos a ir a un modelo híbrido.

Sin dudas, *blended* total. Se va redefinir la forma de enseñanza que hemos vivido hasta hoy.

Me gustaría saber si estás viendo que las instituciones están prestando atención al tema de la ciberseguridad, si se están dando los pasos suficientes para proteger a los Estados de la región y sus infraestructuras críticas.

Producto del coronavirus, las empresas comenzaron a repensar sus negocios. Hace diez años venimos empujando a las empresas a reimaginar sus operaciones de cara a la transformación digital. Veamos el e-commerce: en EE.UU. se esperaba que alcanzara un 25% en 2025, sin embargo, producto de la pandemia creció al 40%. La motivación del uso no vino de la tecnología ni de la cultura, sino de la urgencia, porque no se podía hacer de otra manera. Mi sensación es que no ha habido preocupación por el tema de la ciberseguridad, ni a nivel público ni privado hasta ahora. Lo que le ha pasado al mundo es que ha tenido que sentir la amenaza para reaccionar. Hoy día sí, ya que estamos conviviendo con la amenaza, las empresas se están reimaginando su lógica empresarial a partir de un mundo digital, están reimaginando sus organizaciones a partir del teletrabajo y sus modelos de negocio a partir de lo que están viviendo. Desde aquí es que están incluyendo la ciberseguridad como un elemento, pero es preciso que lo vean de manera transversal. Queda mucho trabajo por hacer porque hay que ir cambiando la cultura hacia una civilización digital.

Para terminar: ¿cuál es tu anhelo en los próximos años?

Me encantaría que en Latinoamérica nos apeguemos más al mundo de la ciencia. Que creamos en nuestras capacidades, producir tecnología y transferirla al mundo

> Pelayo Covarrubias en "Ciclos Digitales para la Sociedad", organizados por Fundación País Digital de Chile:

"Tenemos el desafío de llevar adelante la transformación cultural que necesitamos para construir esta nueva revolución digital. Debemos llevar este aprendizaje a las ciudades, a cada uno de los hitos que la ciudad nos permite: personas, empresas, gobierno".

"Hoy día no nos podemos quedar en pensar una ciudad solamente de forma analógica, ya la tenemos que pensar digital".

"Hoy estamos avanzando todos en la misma dirección para construir una mejor ciudad, cada vez vemos más participación tanto del sector público como privado".

Entrevista a Antonio Godoy, Jefe de Infraestructura, Gerencia TICA, Minera Candelaria.

La industria minera es, sin dudas, uno de los pilares económicos de Chile. Para profundizar acerca de la situación actual de la minería en términos de transformación digital y cómo este proceso se realiza teniendo en cuenta la seguridad de los trabajadores y la ciberseguridad de los sistemas, conversé con Antonio Godoy, Jefe de Infraestructura, Gerencia TICA, en Minera Candelaria. Nuestro encuentro se realizó vía Webex, la plataforma de colaboración de Cisco. Aún en la distancia física, sentí el encuentro con Antonio muy cercano y alentador: cercano por las experiencias laborales compartidas y futuras, alentador por la proyección positiva a la que se encamina Minera Candelaria.

por **Daniel Peña**

Imagen: Burghard Mohren

Minería

La minería es un fuerte motor económico para Chile, en este sentido y a tu juicio ¿puede considerarse una infraestructura crítica?

La minería para el país tiene una gran importancia y es crítica para su desarrollo, como ejemplo, te comento algunas cifras interesantes:
• El PIB minero es un 9% del PIB nacional, según lo indica el Consejo Minero de Chile.
• Las exportaciones mineras representan el 51% del total de exportaciones del país.
• El empleo en minería entrega 227.000 puestos de trabajo directos, 578.000 indirectos y representa un 9.5% del total país (2019, Consejo Minero con datos del INE y Cochilco), por lo tanto, como ya te lo indicaba, su importancia en la economía y el desarrollo del país es fundamental.
Ahora bien, acá lo importante también es cómo nosotros, desde la tecnología, logramos apoyar y empujar, para que se puedan seguir manteniendo y mejorando los índices actuales. En las últimas décadas, las nuevas tecnologías se han hecho parte de prácticamente todos y cada uno de los procesos.

¿Cuáles son las principales necesidades de la industria minera hoy?

Desarrollar una minería segura, innovadora, con altos índices de productividad y eficiencia, y por supuesto, con un adecuado manejo de la información, son aspectos clave para ser competitivos y sustentables en la industria minera de hoy. El dinamismo de este sector económico nos desafía a lograr que la información esté disponible más rápido para mejorar la eficiencia y controlar de mejor forma los riesgos propios de este negocio y su productividad.

¿Cómo crees tú que puede contribuir la tecnología digital al desarrollo de la industria minera?

Hoy la digitalización es imprescindible para la industria minera y no se concibe su desarrollo sin tecnología. En la actualidad todos los procesos mineros requieren automatización, Inteligencia Artificial, Internet de las cosas, entre otras. Todo con el objetivo de mejorar la eficiencia, apoyar en la toma de decisiones y permitir a los trabajadores una labor más segura, minimizando los riesgos y maximizando su bienestar.

Exacto, la seguridad de las personas siempre está en los primeros lugares, ¿verdad?

Sin dudas. Es uno de los valores empresariales centrales de nuestro modelo de negocios, sumado al respeto, integridad y excelencia.

Y hoy día, más que antes, dependemos de la tecnología y hemos visto cómo gracias a ella hemos podido seguir operando.

Efectivamente ha sido clave, porque hoy hay mucha tecnología disponible en el mercado y hemos comenzado a adoptarla para continuar operando y desarrollando nuestros procesos. Por ejemplo, tenemos varios casos en que no podemos trasladar personas entre ciudades, menos aún entre países y dado que el negocio requiere continuidad, la tecnología actual nos ha permitido seguir las operaciones al estar conectados con los equipos de veedores y con los trabajadores todo el tiempo. La tecnología ha sido clave en estos tiempos.

Ahí es donde empieza a jugar un rol fundamental la ciberseguridad, entonces, ¿cómo crees tú que pueden la Seguridad y la Ciberseguridad ser facilitadores de la Transformación Digital en la industria minera?

Estimo que en eso la palabra clave es confidencialidad. La confiabilidad que le podamos dar a los sistemas y a los procesos, asegurarnos de que siempre sean ciberseguros y no dejar ninguna brecha abierta. Hoy las redes OT, enfocadas en todos los procesos productivos, tienen que ser seguras. En este ámbito no se puede dar la licencia de no cumplir con altos estándares en ciberseguridad, de hacerlo, se puede ver comprometido el centro de nuestro negocio. Por eso, insisto, el desarrollo y la implementación de tecnología deben ir de la mano de la ciberseguridad.

¿Cuáles son las necesidades de la industria minera en términos de transformación digital segura?

Podemos plantearlo desde tres miradas fundamentales: Personas, que incluye seguridad, bienestar, capacitación y adaptación a los cambios; Productividad, costos y eficiencia del negocio, es decir cómo aportamos; y por último, cómo formamos parte de todo el proceso, cómo intervenimos en cada una de las actividades que se desarrollan al interior o alrededor de este negocio.

Teniendo en cuenta que hoy las redes IT y OT, ambas, están conectadas, ¿cuáles crees que son los activos que debe proteger la transformación digital en esta industria?

Creo que la información se transformó en un activo clave. La data es fundamental para las decisiones que se toman hoy y para las que se tomarán en el futuro. Otro punto relevante tiene que ver con habilitar las operaciones remotas, permitir operar un equipo desde cualquier lugar es clave mirando al futuro, esto nos permite apostar aún más por una mayor seguridad para las personas.

¿Consideras alguna especificidad de la industria y el contexto del país que determine prioridades o necesidades diferentes a las de la región o el mundo?

Estimo que las necesidades de esta industria son similares en diferentes partes del mundo. En general las compañías están en la búsqueda de cubrir las mismas necesidades, algunas con un mayor grado de avance que otras, pero todas persiguen un mismo fin.

Siendo Candelaria parte de Lundin Mining, una empresa multinacional, ¿cómo ves tú la minería chilena respecto al resto del mundo en cuanto al grado de avance en ciberseguridad?

Lo veo muy similar. Hoy tenemos la suerte de trabajar

Imagen: Khusen Rustamov

con otras operaciones del grupo en distintos lugares del mundo y en esta dinámica notamos que todos estamos viendo los mismos problemas y enfrentándonos a las mismas condiciones. Estamos enfocados en los mismos tópicos, trabajando en ciberseguridad prácticamente al mismo nivel y desarrollando niveles de redes muy parecidas.

Y respecto del marco legal, ¿cómo ves el apoyo del gobierno en cuanto a políticas de ciberseguridad para la industria?

Creo que es un tema que está creciendo en nuestro país, que cada día está avanzando más. Hay más regulaciones e incluso más tecnología de seguimiento. Creo que en el sector público tenemos un aliado.

Respecto a todos los sistemas de ciberseguridad que están disponibles, ves tú que haya algún gap, algún vacío que haya que llenar? ¿Estamos cerca o lejos de una situación ideal?

Pienso que no es un tema exclusivo de la ciberseguridad. Hoy existen muchas tecnologías disponibles, algunas imposibles de implementar por los costos asociados, incompatibilidades, etc. Ahí los referentes tecnológicos deben seguir buscando formas de entrar en las agendas de esta industria y evaluar cómo seguir transformándose en aliados.

En los planes de crecimiento que tiene Candelaria para ir hacia una operación remota o autónoma, ¿ves que hay camino por recorrer en lo que tiene que ver con adopción de tecnología de ciberseguridad?

Sí, yo creo que nos queda mucho por recorrer, hay grandes oportunidades para avanzar y profundizar en estos temas tan relevantes. Es importante conocer qué están haciendo en el mundo, seguir buscando alternativas y aprender de las experiencias ajenas.

Cuando se planifica el crecimiento y la disrupción, ¿qué podrían esperar ellos de una plataforma de ciberseguridad?

Esperarían, ante todo, que cubra sus necesidades, que les permita seguir siendo competitivos en el mercado actual. La disrupción digital ha permitido a muchas empresas diferenciarse de otras y triunfar. Por lo tanto, la plataforma de ciberseguridad tiene que ir en ese mismo camino, permitirnos marcar diferencias y seguir creciendo.

Te gustaría agregar algo que no hayamos preguntado en relación a la transformación digital segura?

Sólo agregar que en Minera Candelaria, el objetivo es ser una empresa minera de clase mundial, que está permanentemente buscando tecnologías que permitan una producción segura para las personas, para proteger el medio ambiente, colaborar con las comunidades y mantener la continuidad operacional. Con Cisco llevamos una larga relación y es importante seguir fortaleciéndola. Así que muchas gracias Daniel por esta invitación a conversar.

Muchas gracias a ti nuevamente, Antonio

> “En la industria minera protegemos tanto a las personas como a la información. Cuando hablamos de transformación digital segura, la palabra clave es **confidencialidad** por eso el desarrollo y la implementación de tecnología deben ir de la mano de la ciberseguridad.”

Hoy puede ser un gran día, y mañana también

por **Pablo Marrone**
Collaboration Sales Manager, Latam, Cisco.

La pandemia traerá la crisis. Una frase que resuena, ¿verdad? Me pregunto: ¿te inmoviliza el miedo, o te energiza el desafío? No hay lugar para "business as usual". El mundo en general y Latinoamérica en particular, están en un estado más volátil, incierto, complejo y ambiguo que nunca. Lo que decidamos en estos días, y experimentemos en las siguientes semanas, puede definir nuestra existencia como organización, empresa o gobierno.

Por ello, en esta nota detallamos algunos puntos que pueden ayudar a afrontar el futuro inmediato y orientar a transitar el cambio.

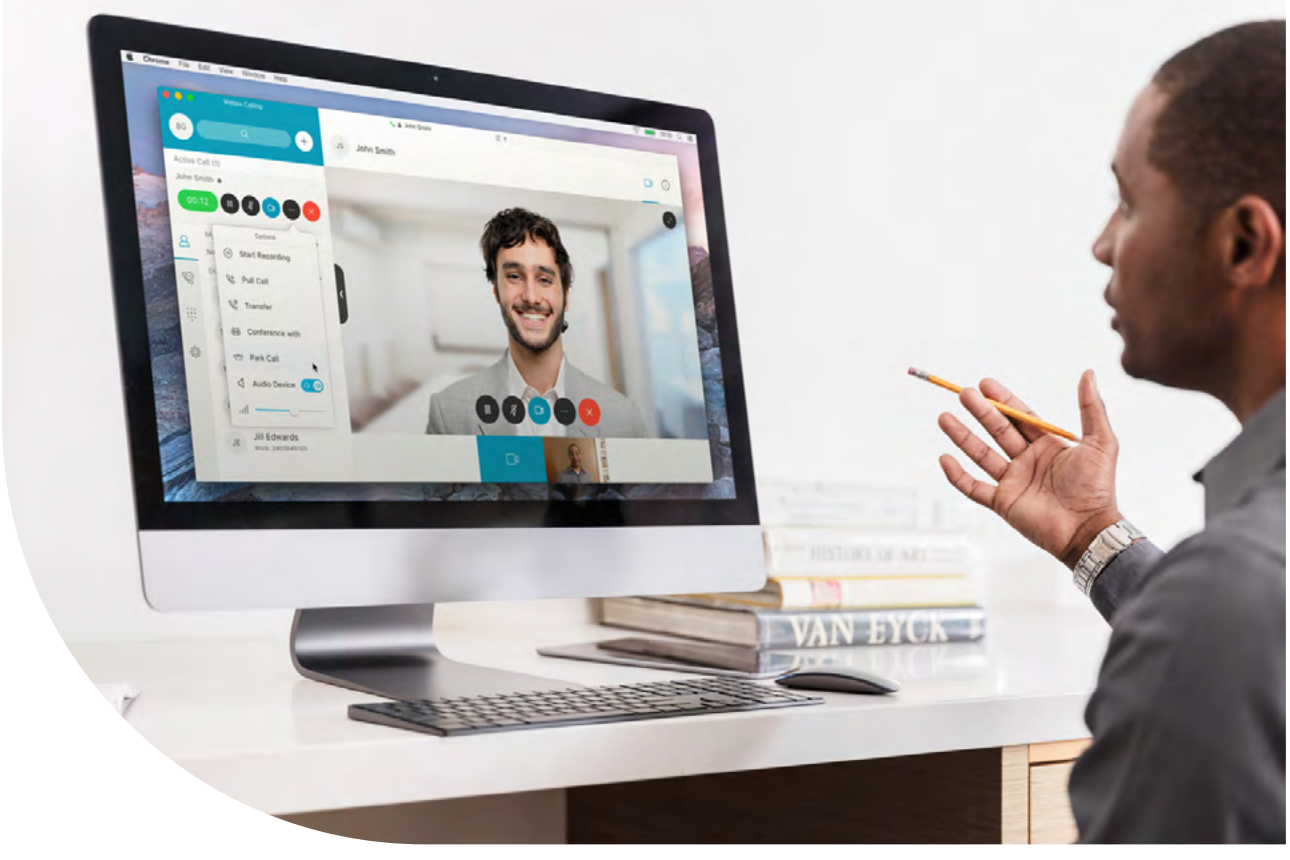
El nuevo "presencial". El trabajo, la salud, la educación, el entretenimiento, nunca volverán a ser los mismos, se dice. Lo "remoto" es, al día de escribir este artículo, el nuevo "presencial" para cualquier actividad. Sin ir más lejos, los servicios WEBEX han multiplicado 10 veces su uso en número de reuniones y casi 40 veces en número de participantes en el período que va de febrero a mayo de 2020. Las conexiones remotas entre equipos reemplazan a las reuniones presenciales, se redefine el co-working, se rediseñan oficinas y se adoptan nuevas dinámicas y formas de trabajo.

Nuevas pautas culturales. Las pautas fosilizadas del siglo XX crujen y reclaman ser reemplazadas. La tecnología puede ayudar en el proceso de cambio, sin embargo, hoy más que nunca será necesario que los responsables de TI trabajen junto a los líderes de negocio para que haya una verdadera sinergia enriquecedora. Juntos, luego, elegirán las soluciones integradas de sus proveedores/partners para hacer frente a la demanda y el desafío crecientes.

A no quedarse quietos. No hay lugar para "congelarse". Como dijo Winston Churchill: "nunca desperdicies una buena crisis". Es el momento de actuar y tomar las decisiones organizativas y tecnológicas que nos proyecten. Ya lo ha cantado Serrat: "aprovecharlo o que pase de largo, depende en parte de ti".

El post-pico de pandemia. Como dice la letra de una conocida canción de Serrat, "no hago otra cosa que pensar en ti", normalidad. Esta situación de post pandemia se plantea a menudo como el escenario deseado en algunas salas directivas y en la sociedad en general. Sin embargo, el mejor escenario posible al día de hoy es lo que podríamos denominar el "post-pico de pandemia", con muchos meses de descenso lento de las curvas de contagio, y convivencia con la enfermedad.
Es un excelente momento para dejar de añorar la "normalidad". Nuestros equipos de trabajo se desenvolverán por un tiempo prolongado en un escenario de dispersión de sitios. Nuestros clientes nos siguen necesitando del otro lado de "la red". Nuestros gerentes aún quieren saber qué pasa y qué hacemos, y buscan las herramientas para gestionar e inspirar.
Para aquellos que no hacen otra cosa que pensar en la "vieja normalidad" es un buen momento para sacarse la venda de los ojos y acelerar. Las herramientas necesarias están disponibles y han mos-

Cultura y tecnología imprescindibles en las organizaciones para el post achatamiento de la curva.



trado tener la escalabilidad, resiliencia y seguridad requeridas por la "nueva normalidad".

Ambientes laborales híbridos. Entre los pensamientos nostálgicos, destacan las ideas de volver a la oficina. Pero lo que antes era la excepción ahora es lo natural. La tecnología que desordenadamente adoptamos para trabajar desde casa es el nuevo default. Y una de las ventajas que trajo su implementación es evidente: la idea de la oficina como único centro indispensable cedió su lugar a que el trabajo pueda realizarse de manera óptima con equipos y personas de talento operando desde cualquier lugar. Los responsables de recursos humanos cuentan ahora con una paleta de posibilidades de elección geográfica como nunca antes había ocurrido. El mejor talento está a distancia de un click. La distancia física puede capitalizarse como oportunidad en lugar de ser un obstáculo.
De cara a las próximas semanas, se erigen además dos verdades inapelables. En primer lugar hay "grupos de riesgo" (por edad o condiciones de salud preexistente) que no pueden volver a la oficina, tal vez ni siquiera salir a la calle hasta tanto la pandemia se repliegue, o esté disponible una vacuna. En segundo lugar, es altamente probable que se presenten rebrotes de contagio, o aparezcan otros "cisnes negros" como el COVID-19. Por ello la ductilidad de ubicación de los colaboradores es clave para la continuidad operativa.
En resumen, ya ha comenzado el tránsito a los ambientes laborales híbridos. Las organizaciones, gobiernos y empresas han comenzado la mudanza en relación a su disposición y disponibilidad geográfica.

Bienaventurados. Vamos subiendo la cuesta hacia la nueva normalidad. Puede pensarse como un nuevo amanecer para las organizaciones, empresas y gobiernos. Queda en cada uno de nosotros congelarnos en el miedo a lo que viene o reconocer la multiplicidad de posibilidades delante nuestro, que no solo nos permitirán transitar el presente, sino también ser resilientes en el futuro. Tenemos la buenaventura de poder decidir: "aprovecharlo o que pase de largo depende, en parte, de ti"

Asesoramiento personal, aquí

Protección con el amparo de los dioses. Talos

por **Emanuel Melo Galvao de Almeida**
Cisco Advanced Threat Solutions, Brazil

Las dos preguntas más frecuentes que escucho mientras trabajo en los eventos de Cisco en todo el mundo son: ¿qué es Talos y qué significa este nombre?

Talos es uno de los equipos de investigación y desarrollo de seguridad más grandes y confiables del mundo. Este equipo de Cisco es responsable de implementar protecciones, crear nuevos mecanismos de detección, encontrar nuevas vulnerabilidades, proporcionar informaciones de inteligencia a la comunidad y ayudar a nuestros clientes y asociados con sus incidentes de seguridad.

Teniendo en cuenta que es esencial anticipar posibles ataques, la investigación de vulnerabilidades y el análisis de nuevas amenazas son actividades esenciales para mantener la Internet más segura. Hoy, Talos encuentra en promedio una nueva vulnerabilidad por día e implementa protecciones contra estas amenazas antes del lanzamiento de sus parches.

Talos existe desde hace 7 años y surgió de un equipo de investigación de seguridad llamado VRT, creado por la compañía Sourcefire y absorbido por Cisco después de su adquisición en 2013. En ese momento, Cisco delegó a VRT la tarea de crear una nueva unidad con el objetivo de unificar todas las otras áreas de investigación de seguridad de la compañía en todo el mundo.

En la mitología griega, Talos era un autómata gigante forjado en bronce y creado por Hephaestus, dios del fuego y de la tecnología, para proteger la isla de Creta contra piratas e invasores. Como en la leyenda, esta es nuestra misión. Proteger incansablemente la Internet contra nuevas amenazas. Para eso, Talos cuenta con más de 350 especialistas, incluidos investigadores, ingenieros, lingüistas, desarrolladores y otros operadores. Con esto, garantizamos una Internet más segura para nuestros clientes y para toda la comunidad

Ping Pong de preguntas y respuestas a Ghassan Dreibi

Cybersecurity Operations Director, Latin America, Cisco.

¿Por qué ciberseguridad? Puedes responder desde cualquier punto de vista.

Hoy está muy presente el tema de seguridad de datos. La gente pregunta por qué es seguridad de datos y no ciberseguridad. Para mí ciberseguridad es cuando sumamos inteligencia, capacidad de trabajar con un scope mucho mayor que nuestra organización. Cuando empiezo a mirar lo que ocurre alrededor del mundo o lo que pasa en una organización en EE.UU. o en China, donde sea, y cómo eso se torna un conocimiento para mí, eso es ciberseguridad. Es tener un conocimiento mucho mayor de lo que está pasando.

¿Qué cualidades debe tener un CISO (Chief Information Security Officer) para destacarse hoy?

Para ser un buen CISO se debe tener capacidad de previsión, intuir qué va a pasar en el futuro. Justamente, como gestores o proveedores de ciberseguridad, lo que hacemos es proteger de desconocidos. No sabemos qué va a surgir mañana, no sabemos a quién va a afectar. Y el ambiente en que estamos hoy cambia mucho. No solamente el ambiente externo, sino también el nuestro propio. Y la pandemia de COVID-19 es una muestra de esto. Entonces, ¿por qué la ciberseguridad?, ¿por qué tener mayor capacidad de escuchar al externo, escuchar al otro, escuchar qué pasó con alguna experiencia?, porque es casi imposible controlar los cambios, controlar las mudanzas que hay de ambiente, de personal, de condiciones. La ciberseguridad, y justo en el momento que vivimos, puede ayudar a ser resiliente. Ciberseguridad es resiliencia, es ser flexible, es ser capaz de tomar decisiones, pero con mucha inteligencia, con mucho conocimiento.

¿Dónde queda el infierno de un CISO?

El infierno sería estar solo, mirar el problema, mirar la situación en la que se está ahora y no saber para dónde ir, qué hacer, en quién buscar apoyo.

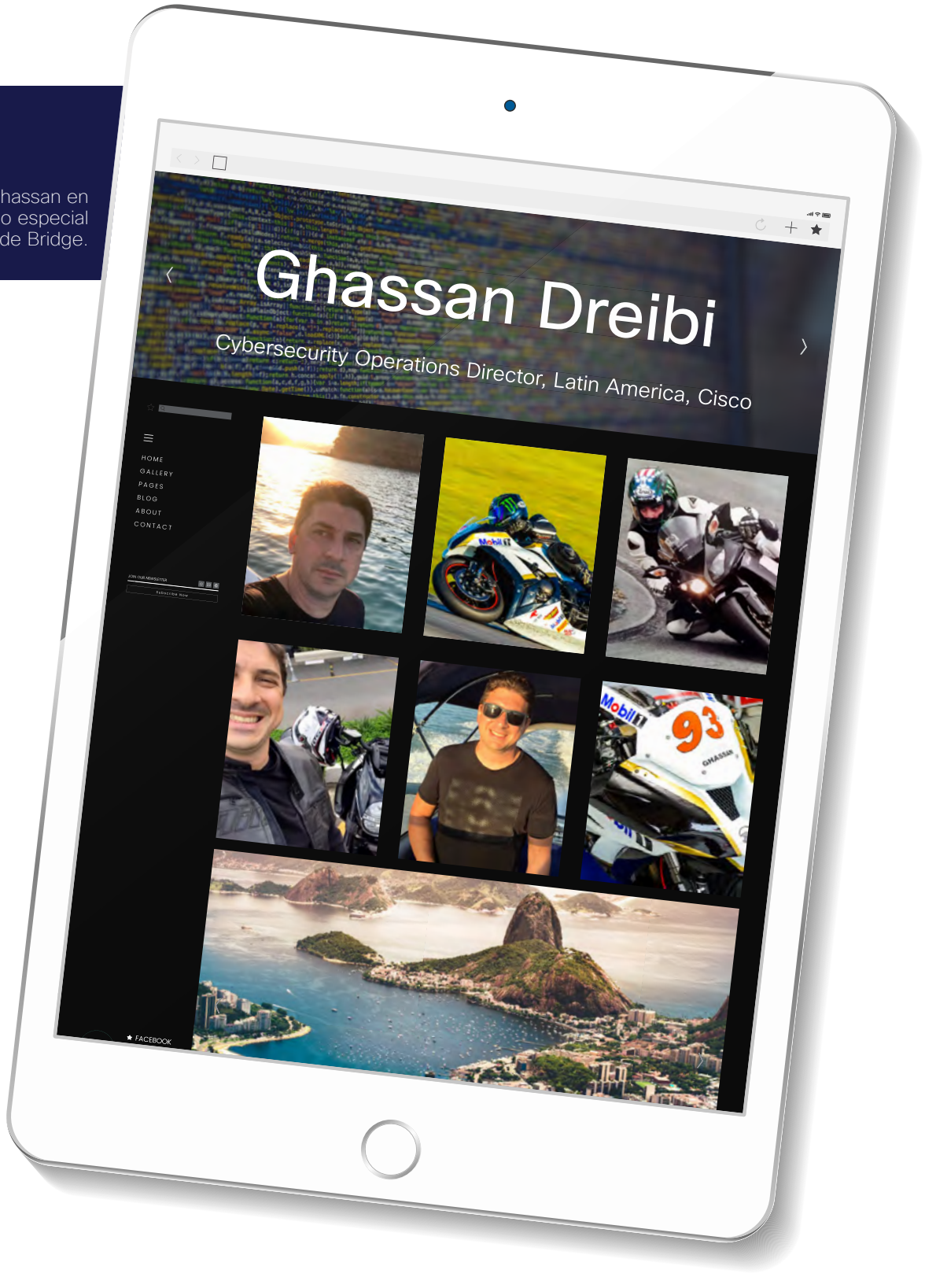
¿Y el cielo?

Creo que nunca va a haber un cielo para un CISO, sino que siempre va a estar entre el infierno y la vida. Lo más cerca que se puede llegar es tener el mínimo de conocimiento, el mínimo de proceso para tomar buenas decisiones, aunque sean decisiones con varios puntos poco claros. El CISO siempre va a tener muchos desafíos, mucha presión, porque las cosas cambian y él se torna responsable por algo nuevo. Durante la pandemia se expandió nuestra vulnerabilidad. Antes de ella estábamos en un ambiente controlado, cerrado, protegido, la potencialidad de una nueva amenaza era estricta. Ahora la potencialidad de amenaza es mucho mayor. Nuestros hijos están conectados todo el tiempo, nosotros también. Estamos haciendo lo que siempre pedimos no hacer, por ejemplo, no dejar a la familia todo el tiempo con el iPad, no dejar a las personas todo el tiempo mirando la computadora. En términos prácticos, la intención ahora desde esa resiliencia del CISO y de esta coyuntura es cómo hacemos que esto sea posible de forma más amigable, más transparente para el usuario, pero manteniendo el nivel de seguridad adecuado a una corporación. Realmente es bastante difícil para un CISO llegar a lo que podría ser un cielo.

¿Qué es imprescindible para armar una estrategia robusta de ciberseguridad?

Mucha gente me pregunta si es posible la ciber-

Lado B de Ghassan en un diseño especial de Bridge.



seguridad, porque es una lucha contra lo desconocido. Es un escenario de muchos cambios, flexibilidad e innovación, pero sí es posible si mantenemos una disputa con eso que cambia. Debemos tener algo básico, un proceso más estructurado, saber quién hace qué, quién habla con quién, en este momento, en este escenario, quién es responsable, cuáles son los socios de negocios que nos apoyan. En 2020, me cuesta creer que las personas reciban amenazas y aún no sepan a quién pedir ayuda. Por ejemplo, si te clonaron una tarjeta de crédito, ¿quién te ayuda? Recién cuando sucede el incidente se busca información. El CISO tiene que armar un proceso de ciberseguridad que involucre a las personas y al proceso corporativo y con todo eso traducir a una buena inversión tecnológica. Cuando desde Cisco hablamos con ejecutivos, intentamos salir un poco de la inversión en tecnología, aunque el mundo se convierta simplemente en tecnología hoy en día. Hace falta un proceso de personas, de educación, de colaboración entre ejecutivos y trabajadores de la misma empresa, y una línea clara de diálogo, y ahí, sí, la adopción de tecnología va a estar bien hecha. ¿Por qué es importante este tipo de proceso? Porque de lo que estamos hablando hoy es del futuro, de una plataforma, de una arquitectura de ciberseguridad que sea traducción de este

proceso, de este framework que incluye sistemas, aplicaciones y personas.

Y ¿cómo se logra en términos prácticos?

Hay que leer bien a los usuarios, a las aplicaciones, casi todo. Luego de reunir toda esa masa de datos, tenemos que saber procesarlas y ahí está el gran desafío de la estrategia de ciberseguridad: cómo mirar tanta información, tantos datos. Ese es otro infierno para el CISO. Es mucha información, todos los días, a cada segundo, y es necesario saber qué es importante y qué no, en general ahí está la gran falla donde el hacker entra. Hoy es muy raro que las personas estén desprotegidas, pero tampoco están completamente protegidas, incluso el poner más herramientas de protección no significa que estén más protegidos. Un ejemplo práctico, quizás soy tan agresivo con soluciones y productos de ciberseguridad, que no tengo la capacidad de manejarlos y por ahí ingresa una amenaza, un hacker. Hay una falla de visibilidad, tengo un sensor, pero nadie lo miró, no estuvo alerta.

¿Qué tiene para aprender una organización de un hacker?

El hacker cambió, es una organización criminal, están bien organizados, muy enfocados, colaboran muy bien entre sí. Distinto de nosotros, que muchas veces no hablamos con el compañero de al lado, con el gobierno o la policía. Estamos aislados contra todas esas organizaciones, contra nosotros mismos. El hacker es una organización y tiene un objetivo de lucro, no puede perder tiempo, no es un romántico, su gran desafío es la entrega de la amenaza, es lo único que discute. Y es lo único que el CISO no discute, que es la forma en cómo recibe la amenaza. En 2020 la mayor forma de entregar amenazas es por e-mail, debido a la fragilidad del ser humano, hacer que se interese por algo y haga un click, así de simple. Quizá con una gran inversión en confianza, en educación, en transparencia, este gran potencial de amenaza podría ser arreglado, pero hemos mirado para otro lado. Y esto me trae otro concepto. Si solucionamos el tema de la entrega de amenazas por e-mail, por phishing, la organización criminal va a buscar otra forma de entregarla. Por eso, la vida de un CISO no es simplemente contestar a un punto, sino contestar y seguir mirando al próximo, y siempre estar en esta posición. Ya no es más la responsabilidad del CISO, es la responsabilidad corporativa de toda la organización. Y no todas las empresas están listas para esto.

¿Cuál es el primer paso para un futuro mejor en materia de ciberseguridad?

En mi opinión, hay que generar confianza. Hay que aclarar por qué y quién es. Y eso en seguridad es muy antiguo, porque el primer principio es tener un certificado digital que valide la confianza. Es lo que hablamos del zero trust. Hay una frase en inglés: The zero trust to be trusted. No confío en nada para tener confianza, es un poco el nuevo mundo. La educación es clave para saber en qué y en quién confiar.

¿Por qué crees que algunas organizaciones no invierten lo suficiente en ciberseguridad?

Cuando decimos que los hackers son más sofisticados, más estratégicos, y que nosotros somos más lentos, no estamos diciendo que haya menos inversión en ciberseguridad, siempre hay mucha. El top of mind es hacer inversión en ciberseguridad. En mi opinión la inversión está hecha en forma equivocada. En el mundo que vivimos, el COVID es un buen ejemplo, metafóricamente hablando: se propaga lateralmente, no se ve, mucha gente tiene el virus y no lo sabe, cuando llega a sistemas críticos es realmente grave, y además cambia, no hay una forma de proteger a menos que se sepa cuál es el “paciente cero”; y así es en ciberseguridad. La amenaza llega silenciosa y muchas veces no hay información. El ejemplo más conocido es el WannaCry, un malware que encriptaba las máquinas e impactó en todo el mundo. Imaginen que ingresaba a las máquinas, preguntaba si estaban vivas y después las encriptaba. Nadie vio cuando ingresó. Se supo que existía la amenaza cuando la amenaza empezó a mostrar que existía. Si no se mostraba, nadie iba a saber que estaba ahí. Y pasó por todo el mundo en horas. Las empresas tienen que protegerse de mejor manera, sacar los datos y limpiar la nube, esas decisiones son las que tiene que tomar la organización en temas de inversión. Comprar un producto y pensar que es seguro, es una forma de defensa que ya no existe. Como metáfora, creo que la pandemia que vivimos en ciberseguridad es igual a la pandemia de COVID-19. En mi opinión están manejando muy mal el tema, deberíamos proteger a quien necesita ser protegido y no aislar a toda la gente y esperar. En ciberseguridad es igual, hay que proteger el servidor o los procesos que tienen que ser protegidos y aceptar que un grupo de personas o de máquinas van a ser impactados, pero no impactarán el negocio. Así debería ser en ciberseguridad y no lo es.

¿Las leyes garantizan de alguna manera la seguridad?

Nadie sabe mucho sobre las amenazas, las empresas no son iguales. Cada una debe saber sobre qué se tiene que proteger. Y si no se sabe, lo primero es reconocer y analizar este tema. ¿Las leyes garantizan seguridad? Cuando me preguntan esto digo que estar en regla, estar en conformidad con la ley, no garantiza la ciberseguridad, pero si estás bien enfocado en la plataforma de ciberseguridad, vas a estar en regla naturalmente. Va por ahí.

¿Cómo prepararse para el futuro?

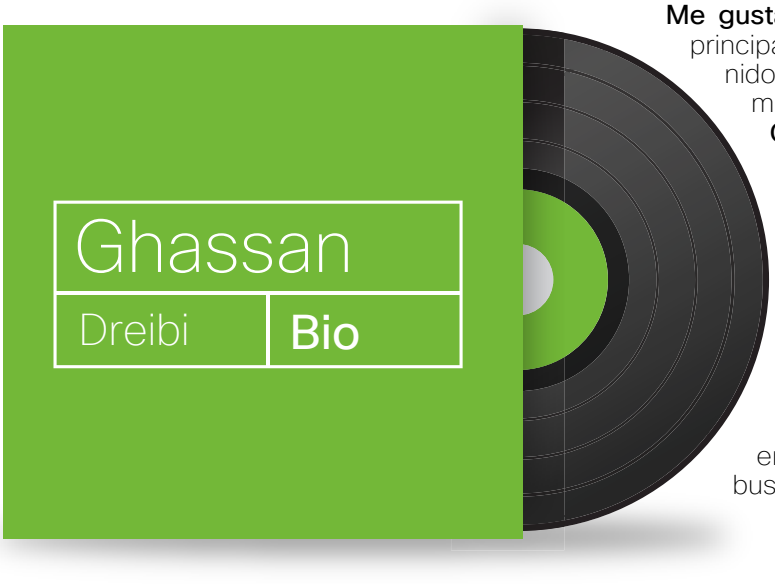
Me parece que están muy bien las discusiones o el análisis relacionado con el problema y la situa-

Ghassan en Interlagos, San Pablo, 2016. Foto gentileza G. Dreibi.

ción que vivimos y quién pone las reglas. Agregaría que la primera pregunta de esta nota debería ser el principio, hay que preguntarse ¿qué es la ciberseguridad para la empresa?, ¿quién es el responsable de eso?, ¿qué lugar ocupa esa responsabilidad dentro del board corporativo o proceso de prioridades? Esto tiene que estar en la mesa ahora. En estos momentos de pandemia, estamos hablando en videoconferencias sobre las soluciones de la nueva normalidad, y la verdad es que yo no creo en esto, creo que lo normal va a venir y estamos preparándonos para algo que tenemos ahora y que no es el futuro. Porque el futuro es otra cosa y ese es el gran trabajo del CISO y de las empresas, prepararse para lo que va a venir

Lado A

Nombre: Ghassan Dreibi Junior.
Profesión: Cientista de la Computación (formación).
Nacionalidad: Brasilero.
Cargo: Director de Ciberseguridad, Latam.
Empresa: Cisco.



Lado B

Me gusta: disfrutar mucho tiempo con la familia, principalmente en viajes no programados y definidos a último momento, donde no tengamos mucho control de lo que va pasar.

Otros títulos: Dive Master con más de 2000 buceos registrados, piloto de Superbike, Licenciado para navegación en vela y motor.

En mi tiempo libre: me encanta la velocidad, amo los autos, motos, barcos y todo que tenga algo de motor. Por muchos años fui piloto de Superbike y me encanta el desafío de mejorar performance en todo lo que hago.

Hubiera sido: maestro o profesor, me encanta enseñar y estar con personas que buscar crecer.

El complejo mundo de las Fake News

Entrevista al licenciado en Ciencias de la Comunicación **Julio Alonso,** profesor universitario y consultor en Tecnologías Educativas.

Desinforman, engañan, desorientan, manipulan, distraen, dañan reputaciones, tienen siempre una intención expresa. Suelen colarse con éxito en temas políticos, y a veces solo adquieren la forma de una broma de mal gusto. En tiempos de pandemia, con los individuos hiperconectados, las *fake news* están más vivas que nunca. En todo caso, no son un fenómeno nuevo. Con otro nombre, las mentiras estuvieron presentes en la historia de la humanidad. La manipulación de la información, junto con la traición y los celos, le dio pulso al relato de una de las obras maestras de Shakespeare, "Otelo"; escribió la leyenda del "Diario de Yrigoyen", para muchos historiadores una falsedad inventada por los golpista que derrotaron en 1930 al presidente de Argentina; fueron funcionales a las técnicas de la comunicación de masas de gobiernos totalitarios del siglo XX; y estuvieron haciendo de las suyas en la elección presidencial que coronó a Donald Trump como el presidente de EE.UU., por mencionar algunos ejemplos.

En este informe, el licenciado en Ciencias de la Comunicación Julio Alonso, jefe de Trabajos Prácticos de la Cátedra de Datos en la Universidad de Buenos Aires (UBA), ofrece su perspectiva para desentrañar el tema de las noticias falsas que provocan este peligroso círculo de desinformación, y que hoy se replican miles de veces en cuestión de segundos. Explica que, desde 2017, trabaja coordinando a un grupo de estudiantes de la UBA en relación con la desinformación, las *fake news* y la posverdad -distorsión deliberada de la realidad, que manipula creencias y emociones para influir en la opinión pública-, a partir de lo que sucede con las plataformas sociales.

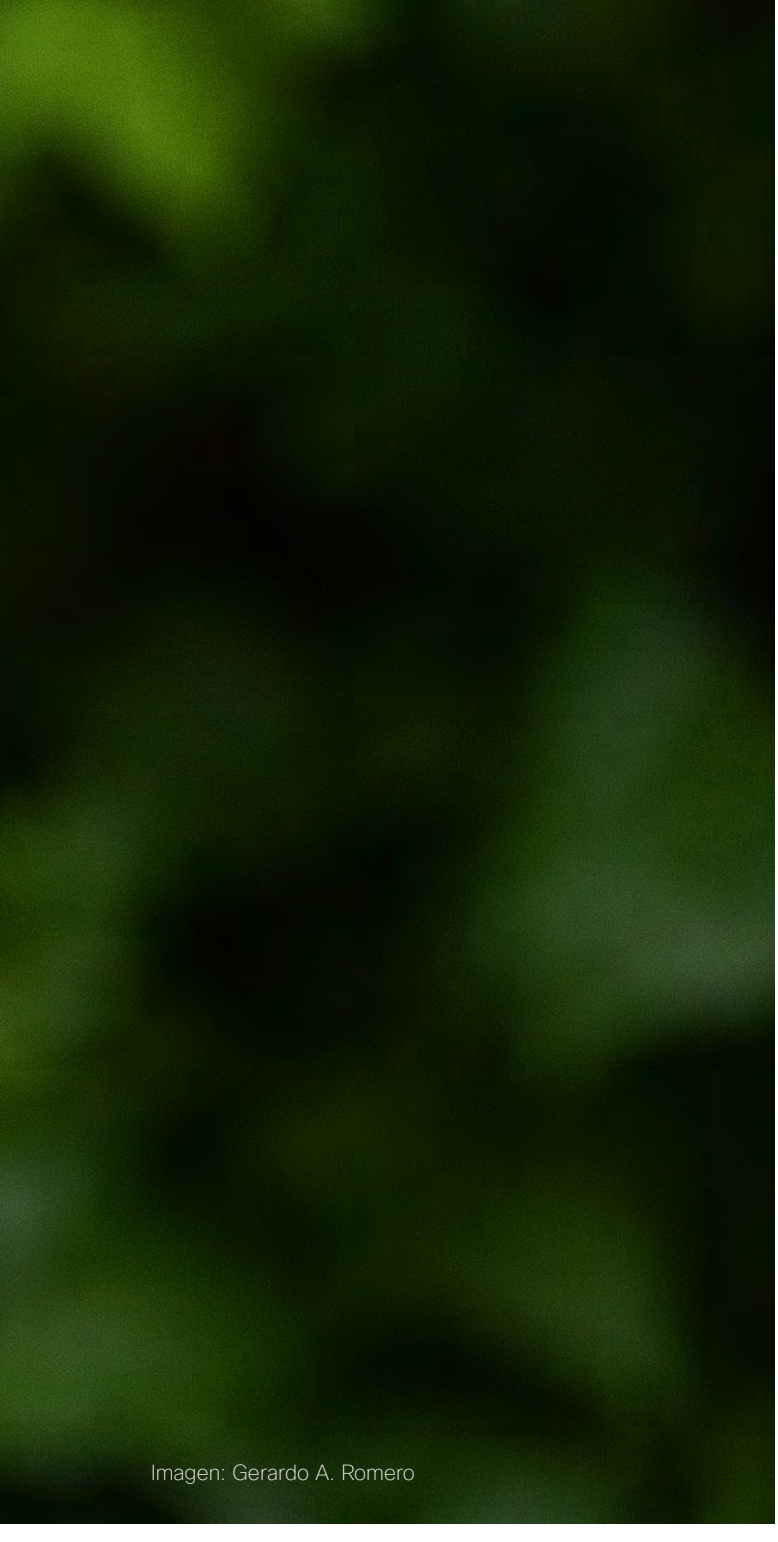


Imagen: Gerardo A. Romero

El trabajo elaborado, que fue presentado el año pasado en el XVII Encuentro Latinoamericano de Facultades de Comunicación Social que se llevó a cabo en Sucre (Bolivia), expone que en definitiva la realidad planteada por una determinada agenda, ya sea política, mediática, pública o personal, funciona como una base para estudiar las relaciones de poder en el plano del discurso. Agrega que para combatir la desinformación hace falta más que una herramienta valiosa como lo es el *fact-checking*, es decir, la verificación de los datos. En el informe indican que "mientras siga imperando el modelo *pay per click* -publicidad digital donde el anunciante paga cada vez que el internauta hace click en su anuncio-, la discusión sobre la verdad continuará estando subordinada al interés comercial", e indica que la comprensión del contexto de cada caso crea las condiciones necesarias para un análisis que no caiga en la tentadora dicotomía de realidad/falsedad, sino en uno que muestre la complejidad intrínseca del fenómeno de la posverdad.

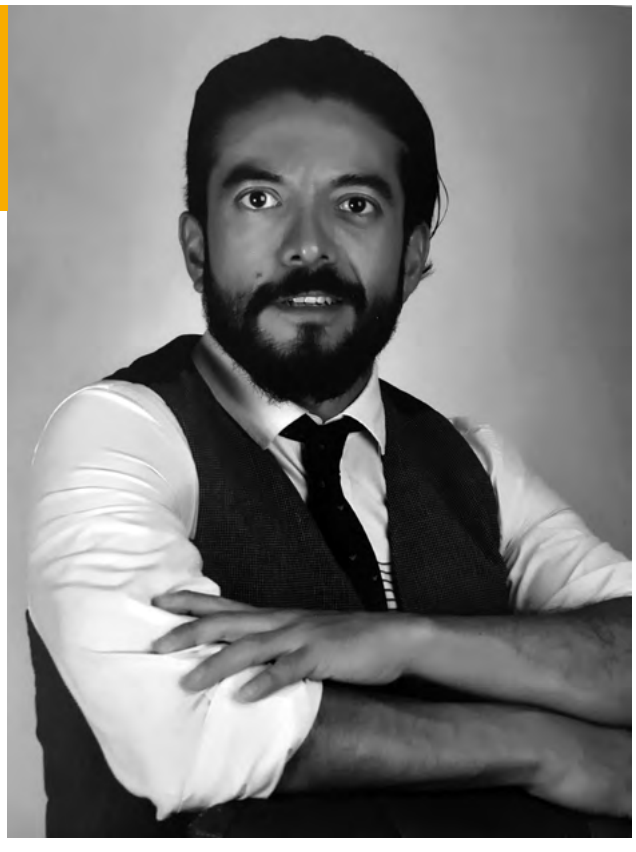
Julio Alonso explica la diferencia que existe entre redes sociales y plataformas digitales. La red social es una "comunicación punto a punto", la unión de varias personas que se conectan para compartir información. Pero ¿qué son Facebook, Instagram, Twitter, YouTube? "Son plataformas digitales, empresas tecnológicas que buscan la comunicación entre usuarios, y que terminan siendo empresas multimillonarias y multiplataformas". Solo Facebook tiene un universo de 2.000 millones de usuarios, que le dan más de 800 millones de "Me gusta" a algún contenido cada día.
El escenario se hace más complejo cuando entran en escena otros factores. Uno de ellos es el nuevo consumidor que no solo consume, sino que también produce, el "prosumidor": "Los usuarios son capaces de generar sus propias instancia de comunicación, y producir movimiento". Agrega otro condimento: "Los troll center parecen ser un invento de algún político, y la verdad es que el mundo está lleno de granjas de troll que genera tendencias. Son herramientas para sostener y generar conversaciones. Entonces la desinformación tiene que ver con qué sucede cuando uno genera una narrativa en estas plataformas digitales".

Recomienda revisar distintos espacios, como el sitio "Chequeado", que se especializa en desenmascarar las noticias falsas, y destaca: "Twitter hizo una jugada importante. Ahora antes de dar un retweet, pregunta si se leyó la información, animando al individuo a leer hasta el final. Muchas veces se ve el titular y se retuitea".

Pero además de verificar datos, hay que entender el contexto de las plataformas. Para definir la problemática, también introduce el concepto de la "cámara de eco", es decir, la comunidad compuesta por individuos que comparten un ideario, y que están impactados por el "filtro burbuja", algoritmo que segmenta y jerarquiza la información que cada uno ve en sintonía con los filtros y los likes. "El algoritmo organiza y pone el factor de relevancia a lo que veo. Le doy información y me devuelve, no me deja ver otra cosa".

También se refiere a cómo se moldean los formatos de comprensión de lo que uno ve en estas plataformas: "En Google revisamos las imágenes asociadas al acto de ´llorar´, y en la mayoría aparecieron mujeres, esto es un sesgo, no estamos hablando de desinformación, sino que se moldean los formatos de comprensión de lo que uno ve en esas plataformas".

Podría decirse que la sofisticación en este medio muchas veces está al servicio de nuevas formas de manipulación y desinformación. Lo que no pierde vigencia, seguramente, es el concepto de Marshall McLuhan, el visionario de la aldea global, quien dijo que el medio es el mensaje, es decir, lo que organiza la manera de pensar



Democratizar la

Entrevista a **Yair Lelis,** CyberSecurity Regional Sales Manager, Cisco Latin America.

La conversación con Yair nos ayudó a entender cómo está México en relación a los demás países de la región en términos de adopción de tecnología de ciberseguridad y cuáles serán los próximos pasos a seguir.

Hay un meme que ha circulado activamente durante los meses de pandemia y que sirve a Yair Lelis para ilustrar la rápida digitalización de los últimos meses: es aquel que se pregunta ¿quién ha hecho que se acelerara la adopción tecnológica en tu empresa?
Opción A: CIO
Opción B: la tecnología misma
Opción C: el COVID-19

La respuesta obvia es C, el COVID-19.
"No sólo ha hecho madurar más rápido a los early adopters sino que nos ha aventado a hacer algo diferente con la tecnología para comunicarnos", comenta.

La sensación existencialista de haber sigo arrojados a la vida digital, posiciona a empresas como Cisco en un lugar fundamental pues el alcance de su operación abarca los distintos vectores que facilitan la colaboración segura. "Cisco estimula la colaboración en forma segura, hace posible que trabajar de forma remota tenga resguardo. Los servicios de VPN (Virtual Private Network, por su sigla en inglés) tuvieron un crecimiento exponencial, de alrededor de 170%. Sin embargo, no sólo se trata de conectarse remotamente y en forma segura, sino también de asegurar el contexto de esa información, por ejemplo, la navegación", nos cuenta Yair.
México, como otros lugares del mundo, vislumbra que posiblemente muchos inmuebles ocupados por oficinas queden en desuso en los próximos meses ya que la remotización del trabajo demostró ser efectiva para la gestión empresarial. "Creo que la palabra clave es conciencia. Se está tomando conciencia de esto y de que la ciberseguridad es un pilar para hacerlo posible", dice.

¿Quién toma las decisiones cuando se trata de incorporar tecnología de ciberseguridad o adoptar conductas que la promuevan?

Por un lado, hemos visto que la decisión tiende a ser más del negocio y menos de la tecnología. Y eso es fantástico porque si el negocio es consciente de que la ciberseguridad es algo que se asocia a todos los procesos, entonces vamos un paso adelante. El negocio es el que habilita esas conversaciones nuevas sobre qué procesos queremos adoptar, qué tipo de tecnologías es deseable tener con base en las inversiones que hemos hecho y sobre todo, qué tipo de políticas deberían seguir los usuarios finales. Cuando esas conversaciones suceden quiere decir que alguien está cuidando el negocio en lugar de sólo mirar la tecnología. Es un proceso paulatino, no todas las organizaciones lo llevan adelante aún, pero está sucediendo cada vez más.
Por otro lado, esas decisiones las tomamos todos haciendo lo que hacemos cada día: cuidando en donde hacemos click.

Imagino que con este cambio repentino las organizaciones deben estar atentas a encontrar especialistas de ciberseguridad. ¿Hay talento disponible?

Para nosotros es una alerta roja porque en todo el mundo y sobre todo en esta región falta talento desarrollado en ciberseguridad, y eso es un mea culpa que tenemos que hacer tanto la industria como la academia y los gobiernos. Afortunadamente, cada vez estamos viendo más programas de ciberseguridad que son promovidos por estos sectores. En México estamos llevando a cabo dos iniciativas: los councils con la OEA donde tenemos a los tres actores, industria, privados/públicos y academia tratando de llevar la democratización de la ciberseguridad a cabo. Adicionalmente, hacemos tracking de educación para que cualquier cliente o cualquier persona pueda acceder a esa capacitación de for-

ma gratuita y que eso nos lleve a incrementar el awareness de ciberseguridad, ya sea con Cisco Network Academy o con cualquier otro partner de educación.

¿Por qué es importante contar con una estrategia de ciberseguridad y una plataforma integrada?

Porque la estrategia fija los objetivos y el camino a seguir, indica los procesos y permite que todos los actores implicados estén en línea. La estrategia es el faro. Con respecto a una plataforma integrada, ella permite contar con la visibilidad necesaria para una óptima gestión, como es el caso de Secure X. Clientes de Cisco para la región nos solicitan ayuda para tener visibilidad sobre el tráfico completo (trabajo, sitios de compras, etc.), ya que con ella pueden defenderse de mejor forma si algún empleado hace click en algún lugar que lo complique en términos de ciberseguridad.

¿Qué piensas de la siguiente frase: "la ciberseguridad debe ser un fluir continuo, se parece más a un proceso que involucra soluciones y personas que a una serie de productos"?

¡Qué buen punto! Partamos desde aquí: internet nació de forma segura ya que para acceder era necesario tener cierto nivel de autorización. Luego se hizo pública, se buscó democratizarla, hacerla accesible a todos. Ahora toca democratizar la ciberseguridad porque entonces, a ese cúmulo de conexiones en internet le empezamos a atornillar soluciones de seguridad por todos lados, que no conviven ni se integran entre sí y eso es lo que ha fallado. De ahí que sí, es un proceso llegar a esa democratización y también un anhelo. Claramente la tecnología juega un papel fundamental en ese proceso pero también las personas, que son las que hacen click en ese enlace prometedor y falso.

Imagino que debe ser difícil cambiar el paradigma de trabajo en empresas u organismos que no tienen en su ADN el trabajo remoto. Pienso en los mercados de educación y salud por ejemplo.

La demanda por conectividad remota ha sido bárbara en este tiempo para esos dos mercados cruciales, y es challeging para el año que sigue.
La ciberseguridad tiene como objetivo garantizar que el negocio y la operación continúen, no busca vender más clases ni tener más pacientes, incorporarla se trata de un camino constante, que irá madurando. Los mercados de salud y educación deberán enfocarse en garantizar que la experiencia de usuario final se vea lo menos afectada posible en caso de algún problema.

Hemos visto que en general el mercado ha crecido en términos de ataques. A todos nos llegan mensajes del tipo "¿quieres ver las últimas estadísticas del COVID?, haz click aquí". El cibercrimen se ha ido especializando y capitaliza toda novedad. Por eso, de nuestro lado, debemos garantizar que la colaboración suceda de forma segura y tenga detrás de ella una estrategia de recuperación ante cualquier tipo de incidente, es lo que llamamos Incident Response, es decir que la respuesta ante el incidente sea rápida, facilite la recuperación y se evite la interrupción del servicio.

¿Hay algo que quieras agregar que no te haya preguntado?

Cuán importante tiene que ser la ciberseguridad en adelante. Debemos mejorar nuestra ciber higiene día a día y además contar con mejor tecnología. Empezar a ser nosotros mismos los motores del cambio hacia una nueva cultura de ciberseguridad. Además, es preciso que seamos muy conscientes del uso de nuestros datos y nuestra información. En México está pasando algo muy importante que es el robo de identidad, que crece a ritmo espectacular.
Esta forma de exposición a la que nos estamos acostumbrando, de mostrar en cada foto que sacamos y publicamos dónde estamos, qué nos gusta, nuestras preferencias, hace que se amplifique la información a la que pueden acceder los cibercriminales y que el TAM (Total Addressable Market) sea increíblemente más grande para ellos. Al ser conscientes de qué y cuánto publicamos y economizar esas publicaciones, cuidamos de nosotros y también de nuestras familias. En este sentido, es importante preguntarnos ¿dónde está nuestra información?, ¿qué tanta información tenemos en la nube?, ¿qué tanta información es vulnerable?

En tu conocimiento, ¿qué medidas deberían tomarse en México en particular y la región en general para lograr una mayor concientización en términos de seguridad digital?

Cuando doy charlas o seminarios relativos a ciberseguridad me gusta poner a prueba a la audiencia, llevarla a la acción. Generalmente, invito a las personas a entrar en una página web que, a través de integración de distintas bases de datos, permite saber si su información fue vulnerada alguna vez a través del correo electrónico. Invito a los lectores a hacerlo ahora desde aquí, con sólo el ingreso de su e-mail: https://haveibeenpwned.com/

A veces es necesario ver para creer

Principios de liderazgo en ciberseguridad:

lecciones aprendidas durante la pandemia COVID-19 para prepararse para la nueva normalidad

En su informe emitido en Mayo 2020, el World Economic Forum establece 5 principios que prometen ser una guía para ayudar a los líderes de hoy a configurar un curso de acción responsable que equilibre los objetivos a corto plazo con los imperativos a mediano y largo plazo. El siguiente artículo es una síntesis reproducida de sus postulados.

Cinco principios

1- Fomentar una cultura de resiliencia cibernética

La resiliencia es ante todo un problema de liderazgo y es más una cuestión de estrategia y cultura que de táctica. Ser resiliente requiere que aquellos que están en los niveles más altos de liderazgo reconozcan la importancia de la gestión proactiva del riesgo y se centren más en la capacidad de la organización para absorber y recuperarse de un ataque cibernético que interrumpiría los servicios esenciales.

2- Concéntrese en proteger sus activos y servicios críticos

Las empresas deberán priorizar los recursos y las inversiones en las áreas más esenciales para mantener la continuidad operativa, proteger los activos digitales críticos y garantizar el cumplimiento.

3- Equilibre las decisiones informadas sobre el riesgo durante la crisis y más allá

Las empresas están haciendo cambios en su modelo operativo y panorama tecnológico a una escala y ritmo sin precedentes, lo que requerirá algunas compensaciones de riesgo a medida que se adaptan y responden con urgencia a la crisis. Sin embargo, a medida que entren en la nueva normalidad, deberán reevaluar las dependencias digitales y los riesgos acumulados para restaurar su perfil de riesgo a un nivel aceptable.

4- Actualice y practique sus planes de respuesta y continuidad comercial a medida que su negocio pasa a la nueva normalidad

Esta crisis ha recordado a los líderes empresariales la importancia de adaptar y probar regularmente sus planes de respuesta y resistencia frente a diferentes escenarios de desastre (incluidas las pandemias) con sus proveedores y socios comerciales clave. Esto incluye el uso de estas pruebas para desafiar las suposiciones (como los tiempos de recuperación) y desarrollar medios para medir la capacidad de resiliencia, la respuesta, la recuperación y otras capacidades clave necesarias para anticipar, resistir y recuperarse y adaptarse a condiciones adversas, ataques o compromisos en los sistemas que están habilitados por recursos cibernéticos.

5- Fortalecer la colaboración en todo el ecosistema

Las alianzas y colaboraciones en ciber-resiliencia entre pares del sector público y privado en todo el ecosistema son esenciales para facilitar el intercambio transparente de información e ir más allá de la suscripción hacia un compromiso más activo.

Los principios en este documento son una respuesta preliminar a la crisis que se desarrolla. Su objetivo es guiar a los líderes específicamente responsables de la ciber-resiliencia y a otros líderes empresariales. Si bien las empresas pueden tener que regular las medidas de acuerdo con diferentes entornos políticos, estos conceptos pueden proporcionar un marco para un curso de acción responsable en este período crucial.

Informe completo

El nuevo normal

La crisis de COVID-19 ha generado desafíos sin precedentes para las organizaciones, forzando a todos a hacer malabarismos con las responsabilidades profesionales y personales. Es probable que los próximos meses traigan aún más incertidumbre.

Al adherirse a las prácticas propuestas, los líderes empresariales pueden cumplir mejor sus responsabilidades para mantener la postura de seguridad de su organización y mantener la continuidad del negocio durante esta pandemia y más allá. Con prácticas efectivas de gestión del riesgo cibernético y resiliencia cibernética, las empresas pueden lograr futuros más inteligentes, más rápidos y más conectados, impulsando el crecimiento y la eficiencia del negocio.

A medida que las amenazas cibernéticas para las empresas continúan evolucionando, los líderes de los sectores público y privado tendrán que abordarlas en los mundos digital y físico para mitigar cualquier daño potencial a las personas y evitar la interrupción de los servicios críticos. Las empresas que entienden y actúan de acuerdo con las señales y advertencias pueden adaptarse y convertir en ventaja un mundo cada vez más ambiguo y veloz

CISCO Partner

OCP TECH

OCP.TECH

US
333 S.E. 2nd Avenue,
Suite 2810, Miami, Fl 33131
United States of America

T +1.305.537.0800
F +1.305.537.0704

info@ocp.tech

Panamá
Oceania Business Plaza Torre 2000
Piso 33 a 1, Boulevard Pacífica
Punta Pacífica
Panamá City
República de Panamá

T +507.387.7300

Taiwan
No, No. 97, Songren Road, Xinyi District,
Taipei City, Taiwán 110

T +886.953.656.967