

# Bridge



Ciberseguridad



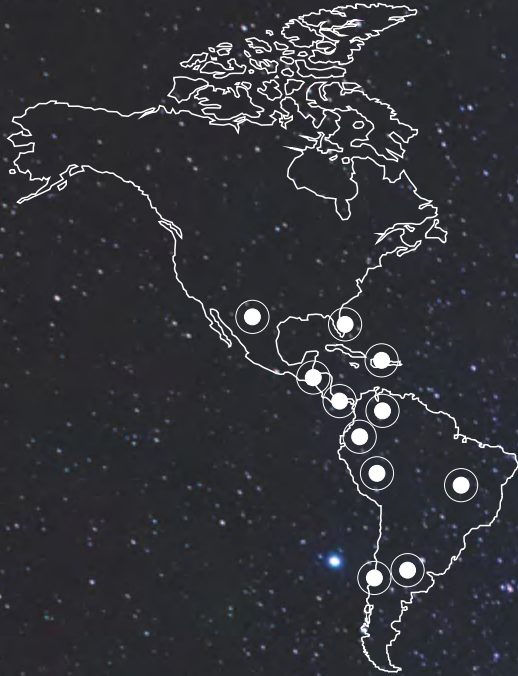
Especial  
Mujeres en Ciberseguridad

Contrapunto  
Taekwon-Do y Ciberseguridad

Colombia  
Transformación digital segura en Salud

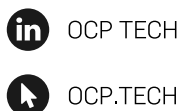


Contenido  
audiovisual



# OCP TECH

INGENIERÍA CONVERGENTE  
PARA SOLUCIONES PRÁCTICAS  
*Expertos en soluciones de ciberseguridad*



**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 Pacifica  
Punta Pacifica  
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



# Editorial

Desde hace años merodea por mi cabeza una idea muy simple, pero de un tremendo poder transformacional: “cada persona está en una posición única, privilegiada, irreplicable, para tener su mejor idea”. La clave está en el pronombre posesivo “su”. El cúmulo de experiencias, conocimientos y deseos que nos diferencian como individuos configuran la llave de acceso a esa idea, que es como la fruta madura a la que alguien puede alcanzar antes que cualquier otra persona.

Sobre este fundamento, creo que el verdadero sentido de honrar la diversidad está en reconocer el valor extraordinario de la singularidad y potenciarlo de forma colaborativa para innovar y solucionar cualquier desafío que debamos enfrentar como comunidad. La expulsión de lo distinto nos condena no solo a una pobreza social y espiritual sino también, desde una lógica productiva, a limitar nuestras posibilidades de innovación.

En esta tercera edición de Bridge seguimos enriqueciéndonos a través de la pluralidad de voces y de la búsqueda de sabiduría trazando puentes entre disciplinas que pueden parecer tan divergentes como las artes marciales o la labor de los Bomberos Voluntarios, pero que sin embargo convergen, más de lo que uno puede sospechar, en los principios que gobiernan la ciberseguridad.

Deseo que esta lectura te nutra y te acerque aún más a *tu* mejor idea, y que al voltear la última página sientas la urgencia de reunir tu voz con las voces de las mujeres y hombres que comparten sus perspectivas en esta publicación.

Juan Marino

# Staff

## Producción Integral Basanta Contenidos

Directora Editorial  
Karina Basanta

Director de Arte  
Nicolás Cuadros

Coordinadora  
Andrea Lecler

Producción audiovisual  
Salpufilms

Colaboran en este número  
Silvia Montenegro,  
Marta Pizzini, Jorge Prinzo

Fotografía e ilustración  
Basanta Contenidos  
Freepik  
Pixabay

Agradecimientos  
Marta Assandri  
Isabella Cacciabue  
Joaquín Cuadros  
Coly Escobar  
Nicolás Cacciabue  
Santino Cuadros

Foto de Tapa  
Alexandr Ivanov, Pixabay



Directora Editorial  
Karina Basanta



Director de Arte  
Nicolás Cuadros



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

Impresión: FP Impresora  
Antonio Beruti 1560, Florida Oeste,  
Provincia de Buenos Aires  
Tel: 11-4760-2300  
www.fpimpresora.com.ar

## Cisco Latinoamérica

Director de Operaciones  
de Ciberseguridad  
Ghassan Dreibi

Líderes Regionales  
de Ciberseguridad

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



**Editor General**  
Juan Marino

### Agradecimientos

Walter Montenegro  
Fernando Zamai  
Marcelo Bezerra  
Leticia Gammill  
Juan Pablo Mongini  
Paola Sarmiento  
Javier Castro  
Jackeline Carvalho

## Marketing

Taiane Belotti

Gerente de Marketing, Seguridad Latam

**Jimena Reyna Briseño**

Gerente de Marketing de Contenidos, Seguridad, Latam

---

El contenido de los avisos publicitarios y de las notas no es responsabilidad del editor sino de las empresas y/o firmantes. La Editorial se reserva el derecho de publicación de las solicitudes de publicidad. La reproducción total o parcial de cualquiera de los artículos, secciones o material gráfico de esta revista no está permitida.

Bridge N° 3

# Sumario

Editorial	3	
	4	Staff
	6	Sumario
Cisco Engage	8	
	10	<b>Conversatorio</b> Banco Supervielle y Bomberos Voluntarios de San Miguel por Silvia Montenegro
El desafío de la armonía por Walter Montenegro	16	
	18	<b>SASE</b> Todo lo que necesitas saber sobre Secure Access Service Edge
Experiencia de Edesa Ad Content Braycom por Diego Máspero	20	
	22	<b>Taekwon-Do y Ciberseguridad</b> Contrapunto por Silvia Montenegro
Nota de Tapa Especial Mujeres en Ciberseguridad Producción integral conjunta WOMCY / Bridge	26	
	42	<b>El secuestro y extorsión en la era Digital</b> Ad Content OCP Tech por Fabio Sánchez
Transformación digital segura en Salud Entrevista al Dr. Jairo Pérez Cely por Javier Castro	44	
	50	<b>El rol de la Identidad Digital en el Proceso de Vacunación COVID-19</b> Ad Content VU Security por Néstor Serravalle
Protección de Datos: LGPD por Fernando Zamai	52	
	54	<b>Resiliencia de la fuerza laboral</b> por Juan Pablo Mongini
Guerra Cibernética por Marcelo Bezerra	58	
	61	<b>Spoiler Bridge 4</b> Lo que viene



# 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

# Brasil

Nuevas oportunidades: La democratización de los servicios financieros en la era de la experiencia.

Más datos. Más usuarios móviles. Más aplicaciones. Más complejidad. Cisco nos ayuda a prepararnos para el banco digital del futuro. Estamos viviendo un momento inédito: nunca fue tan fácil el acceso a los servicios financieros. Millones de brasileras y brasileros hoy forman parte de la bancarización digital.

Pensando en esa realidad, Cisco realizó recientemente un evento virtual donde algunos de los especialistas más destacados en tecnología y finanzas de Brasil, utilizaron casos prácticos para presentar soluciones inéditas que garantizan experiencias personalizadas y seguras al nuevo consumidor digital.

## Temario

### PIX y OpenBanking

Panel sobre Tecnología y Finanzas con **João Bezerra**, **Ricardo Guerra (Itaú)**, **Marino Aguiar (Santander)**, **Jean Sigrist (Neon)**, e **Carlos Alves (Riachuelo)**.

### Colaboración y trabajo remoto

La complejidad pos pandemia en entornos híbridos, con **Thiago Santanna (Cisco)** y **Estevam Carvalho (BTG Pactual)**.

### Transformación digital

La experiencia de usuario en el crecimiento exponencial de XP, con **João Valentin (AppDynamics)**, **Eduardo Berti** y **Marcelo Vidu (XP Inc.)**.

### Madurez en seguridad

Cómo la tecnología nos puede ayudar en esta era económica, con **Ghassan Dreibi (Cisco Secure)** y **Renato Augusto (Bradesco)**.



click aquí

Asista  
ahora



### Resiliencia en los negocios

Experiencias conectadas integrando protección y automatización, con **Carlos Pereira, Cisco**.



### Cómo la Caixa Econômica Federal conectó a Brasil

Antes de la inclusión financiera, es necesaria la inclusión digital, declara la sesión con **João Bezerra Leite y Claudio Salituro, de CEF**.

En una amena charla, Esteban Lus Bietti, CTO del Banco Supervielle, y los responsables del Cuartel de Bomberos Voluntarios General Sarmiento, Comandante Mayor Carlos Ramírez y Comandante Salvador Capano, encuentran puntos en común en sus trabajos. Distintas tareas, pero llevadas a cabo con idéntica responsabilidad, celeridad y pasión.



# Conversatorio



texto: Silvia Montenegro

video: Lus Bietti  
Ramírez  
Capano

## con los Bomberos Voluntarios de San Miguel

Hoy, en general, las organizaciones y las empresas dependen de sus capacidades tecnológicas y de los planes de contingencia y servicios de protección que garanticen seguridad para neutralizar riesgos y ofrezcan confianza para resistir un posible ataque cibernético. Además de diseñar robustos planes de acción, con estándares, reglas, protocolos, métodos y el conocimiento de la legislación vigente, los expertos en tecnología y ciberseguridad deben estar preparados para “apagar incendios” digitales, reportar actividad sospechosa en línea, implementar estrategias para sostener o retomar un entorno online seguro, mantener e impulsar una cultura de seguridad digital.

En esta línea y salvando las grandes diferencias, se puede decir que el trabajo de los responsables de tecnología y ciberseguridad está emparentado con la crítica labor del Bombero, profesional que lleva adelante programas de seguridad contra incendios o siniestros, con el fin de salvar vidas y bienes materiales.

Por eso, cuando se reunieron Esteban Lus Bietti, Chief Technology Officer (CTO) del Banco Supervielle, el Comandante Mayor Carlos Ramírez, jefe del Cuartel de Bomberos Voluntarios General Sarmiento, y el Comandante Salvador Capano, 2do jefe del Cuartel, la conversación se tornó fluida y destacaron muchos puntos en común. El encuentro se llevó a cabo en las instalaciones del Cuartel de Bomberos Voluntarios General Sarmiento, de San Miguel, Provincia de Buenos Aires.



### **Esteban Lus Bietti**

Les quiero agradecer por este encuentro. Es la primera vez que entro en un Cuartel de Bomberos. Creo que tenemos muchas cosas para intercambiar, compartir y aprender unos de otros.



### **Carlos Ramírez**

Es un placer reunirnos acá, charlar y compartir las experiencias vividas en los servicios e intercambiar ideas.

### **Salvador Capano**

El Cuartel es nuestra segunda casa. La comunidad se identifica mucho con nosotros, con los Bomberos. La gente se acerca, ve cómo estamos equipados. Les explicamos que los recursos son muy importantes y que tenemos lo justo y necesario para enfrentar las emergencias, siempre recalamos eso.

### **Esteban Lus Bietti**

Sí, los recursos son muy importantes, aunque a veces pueden ser limitados, mientras que las tareas que debemos hacer no son limitadas, al contrario, son muchísimas y de distintas índole. Tenemos que poner mucha cabeza y corazón. Me imagino que ustedes de eso pueden hablar largo y tendido, porque son Bomberos Voluntarios...

### **Carlos Ramírez**

Sí, nuestro trabajo es especial. Para nosotros nada es grato, sabemos del dolor de la gente, de su sacrificio, vemos las pérdidas que se ocasionan. También tenemos la oportunidad de difundir, de capaci-

tar. Es muy importante la parte humana. Entrenamos mucho al Bombero para que los elementos rindan al máximo, para optimizar el material que tenemos, para que el equipo esté operativo por mucho tiempo. Le informamos nuestras necesidades a las autoridades del Partido de San Miguel. Nos escuchan, estamos en contacto directo con el equipo técnico, que conoce la importancia de la prevención. Ahora, antes de aceptar un proyecto, nos consultan a nosotros sobre qué habría que agregar para la seguridad. Si hubiese un incendio, cuáles serían los elementos que deberían tener o lo que no debería haber. Sé que más o menos eso es lo que vos aplicás también en tu empresa...

### **Esteban Lus Bietti**

Me siento totalmente identificado, porque muchas veces tenemos que conseguir presupuesto para hacer algo que termina derivándose para otra cosa que, en principio, es más importante hasta que sucede algo, como vos contás. Para nosotros también es muy importante trabajar en la prevención del hecho. Primero porque es menos costoso, es más fácil remediarlo, y nos ayuda a nosotros como empresa, al cliente final, y en el caso de ustedes a la sociedad entera, que no tiene que salir corriendo y gastar recursos. Para nosotros es importante tratar de generar valor, y participar desde el principio del proceso, cuando se toman las decisiones. En esta etapa, podemos diseñar cómo se construyen o qué medidas hay que tener en cuenta. Y nos permite prevenir más que actuar o reaccionar cuando sucede un incidente. También debemos ver cómo seguimos los procedimientos, qué es lo que hay que hacer ante cada caso. No solo es importante prevenir, sino que, una vez que el evento se materializa o sucede, debemos saber qué es lo primero que tengo que hacer, a quién debo llamar o avisar para tratar de no tapar el impacto de lo que sucedió, sino darle visibilidad para que se puedan tomar acciones y resolver el incidente con el menor impacto posible. Deben tener un montón de experiencias.

### **Salvador Capano**

Sí, el recurso es importante, y también se tiene que modernizar. Hoy hay tecnología, avance, confort. Y los Bomberos, mediante el recurso y el protocolo, tenemos que estar actualizados y modernizados, con la última tecnología. En el ámbito bomberil, debemos estar muy bien equipados, pero además hay que considerar que el equipo tiene vencimiento. Hoy los fuegos son de muy alta velocidad o propagación, por eso, no podemos tener un equipo que tiene una norma de hace cinco años atrás. Debemos acceder al equipo más moderno para poder hacerle frente a ese fuego. Antes sabíamos que se quemaban maderas y papel. Hoy se quema madera, papel, ácido, plástico, corcho, sintético, y todo eso hace un efecto cinético, por eso no nos sirve el equipamiento de hace cinco años atrás. Lo mismo sucede con una escalera mecánica. Antes había edificios de hasta 10 pisos, hoy tenemos construcciones de 25 pisos. Entonces, poseemos un recurso muy caro, importante, costoso de mantener, pero en algunos casos obsoleto. La gente dice qué buena escalera que tienen, pero si supieran que estamos limitados... Llegamos a un piso 8 y hay edificios de 20 pisos.



Imagen: Ulrike Leone, Pixabay

### Esteban Lus Bietti

En el ámbito de seguridad una de las frases más conocidas es que el eslabón más débil es el usuario, por eso, lo que nosotros podemos hacer es concientizar a la gente. Puedo poner un montón de medidas de seguridad, pero si el usuario después hace click o ingresa en los sitios que no tiene que entrar, la seguridad se termina vulnerando y se produce algún tipo de ataque. ¿Cómo hacen ustedes para convencer al usuario? ¿Cómo hacen para capacitar?

### Carlos Ramírez

Dijiste una palabra importante. Capacitar. En el momento en que pasó algo debemos transmitir el motivo para impulsar que no suceda otra vez. Y que la gente lo capitalice. Cuando sucede, saber cómo puedo atacarlo y, a la vez, divulgar para que no se repita. La prevención es capacitar y a eso estamos apuntando ahora. La Municipalidad entendió que la única manera es difundir. ¿Cómo lo hicimos? A través de un informe, fotos, datos sobre los puntos débiles de una construcción y por dónde el fuego avanza más fuerte. Eso mismo estamos haciendo con la población. Nuestro cuartel cuenta con gente que capacita en Reanimación Cardiopulmonar (RCP), ya han pasado 5000 personas. Y les decimos que hoy cualquier persona es útil para colaborar con nuestra labor en una primera instancia del suceso, en una primera escena. Si hay un incendio, lo primero que hay que hacer es llamar a los Bomberos o a Emergencias, inmediatamente, porque el tiempo vale oro. Hay una cadena que hay que seguir y no se puede cortar. El primero que ve el incendio tiene que llamar. Ni bien llega el sistema de emergencia la cadena está cerrada.



Salvador Capano (izq.) Carlos Ramírez (Der.).

### Salvador Capano

Para la comunidad es importante la información que damos. Nosotros informamos al vecino. Aquí hay zonas que son más precarias y sabemos que tal vez la casa no tiene matafuego, pero le decimos al vecino que tenga un balde con arena, un balde con agua, que abra las ventanas, que no tire colillas en los tachos de basura. Estadísticamente, esta acción da buenos resultados. Internamente le prestamos mucha atención a la capacitación, que es obligatoria y constante. El Bombero que no se capacita, no puede cumplir la función. Si nosotros tenemos equipos de última tecnología y no lo sabemos usar... Primeramente está la seguridad del bombero y la prestación del servicio, que es la finalidad nuestra, salvar vidas y bienes.



Imagen: Shutterstock, Pixabay

### Carlos Ramírez

Por eso, es importante el capital humano. Después de cada servicio, tenemos que trabajar con la gente. Es nuestra mayor tarea. Los Bomberos están capacitados, y seguimos protocolos para cada clase de servicios. Para lo que no estamos preparados es para las pérdidas humanas. Cuando hay tragedias con pérdidas de vida, tenemos que trabajar con los bomberos para que vuelvan a rendir. Tienen que estar muy preparados para no ponerse en riesgo a ellos mismos y a sus compañeros.

### Esteban Lus Bietti

El trabajo de ustedes, donde hay vidas en juego, tiene un gran nivel de complejidad. Nuestra labor es parecida en muchos aspectos, como veníamos charlando, pero por supuesto tiene que ver con trabajar con máquinas y con las personas que forman parte del equipo. En este sentido, es fundamental tener al equipo concientizado, capacitado, motivado.

### Salvador Capano

Dijiste otra palabra fundamental. Equipo. Nosotros somos seis que salimos a la calle, falla uno, fallamos todos. Algunos podemos saber más de algún tema, pero todos son fundamentales. Y además una persona sola no apaga un incendio. Uno corta la luz, otro rescata a la víctima, hay alguien que maneja el autobomba y otro que tira la manga. Somos un equipo. Si se cae uno, tenemos que reemplazarlo por alguien capacitado y preparado. Nosotros no queremos héroes en una placa de bronce. Nosotros queremos un equipo en el que cada uno rinda. Todas las tareas son importantes y, además, todos sabemos todo el trabajo, porque nos rotamos. Hoy puedo tirar de la manga, y mañana me toca estar colgado en una cuerda rescatando a la persona o



La escucha atenta fue una de las características más sobresalientes de esta conversación.

manejar la autobomba. Con las pérdidas humanas, la situación se complica. Aunque el bombero haya dado todo, a veces se complica. Y es inevitable que el Bombero se bajonee.

### Carlos Ramírez

Nuestro lema es salen seis, vuelven seis.

### Esteban Lus Bietti

Muy interesante todo lo que nos compartieron. Les agradezco por el trabajo que hacen, por charlar este rato. Me llevo muchas cosas para pensar y reflexionar y ver qué puedo aplicar en mi equipo. Si logramos trabajar como los Bomberos, seguro vamos a estar mejor que antes **!**



# 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





“ Buscar la coherencia y la integración puede ser un camino posible para acercarnos a la armonía en ciberseguridad ”





# El desafío de la armonía

por **Walter Montenegro**

Armonía es un término que se utiliza comúnmente para describir o definir una situación equilibrada, de confort, agradable, en donde los elementos que la componen están perfectamente alineados en ese preciso instante, y que muchas veces se quiere, por bienestar, mantener en el tiempo. La palabra deriva del griego y significa acuerdo, concordancia. Desde una perspectiva general, la armonía es el equilibrio de las proporciones entre las distintas partes de un todo, y su resultado siempre connota belleza.

En música, la armonía es el estudio de la técnica para construir y enlazar acordes (notas simultáneas), así como las progresiones y principios de conexión que los rigen. También abarca conceptos tales como el ritmo armónico. Es decir que, con la música, también tenemos la posibilidad de generar armonía, de producir estos espacios placenteros y de bienestar, ya sea con un solo instrumento o varios.

Pensemos por un momento en una pieza musical compleja como podría ser un concierto, con varios instrumentos ejecutados a la vez. Posiblemente escuchemos algunos timbres de forma clara y otros tal vez pasen desapercibidos, sin embargo todos unidos aportarán belleza a la obra. Las emociones comenzarán a fluir en comunión a la percepción de los sonidos. Imaginemos que, de pronto, uno de los instrumentos comienza a interpretar otra pieza musical, en otro ritmo, en otro tono. Por más mínimo o

insignificante que parezca ese instrumento, se romperá la armonía, las emociones cambiarán de algo agradable, a algo totalmente molesto y seguramente ya no querremos seguir escuchando.

En ciberseguridad, al igual que en la música, necesitamos contar con armonía. Si nuestro objetivo es disminuir los riesgos, se requiere que cada “instrumento” esté en sintonía con su par, con el cual se comunica y comparte información para generar la colaboración necesaria entre ellos.

Bastante se ha hablado en la industria este último tiempo de la increíble cantidad de soluciones de ciberseguridad existentes en el mercado. Si nos remitimos al último CISO Benchmark Survey, 86% de las empresas encuestadas declararon tener entre 1 y 20 marcas de proveedores para este segmento. Es decir, claramente es más complejo generar la armonía que buscamos entre 20 “instrumentos” que solo algunos.

Tal como en la música, en donde entre más instrumentos interactúan se hace más necesario un director de orquesta para liderarlos, en ciberseguridad ocurre lo mismo. La cantidad creciente de soluciones requiere que exista un “director de orquesta” que las organice, ordene sus reportes y permita finalmente generar la armonía necesaria para investigar algún incidente en tiempo acotado y responder rápidamente a las amenazas detectadas por alguna de las soluciones.

El desafío no es simple, pero debemos trabajar en esa dirección, en buscar la coherencia, el *fiato*, la integración, con el único fin de acercarnos a tener la tan ansiada “armonía” en ciberseguridad ■



# SASE

Todo lo que necesitas  
saber sobre SASE  
(Secure Access  
Service Edge)

## ¿Qué es SASE?

Secure Access Service Edge (SASE) es una arquitectura de red que combina capacidades de VPN y SD-WAN con funciones de seguridad nativas en la nube, como puertas de enlace web seguras, agentes de seguridad de acceso a la nube, firewall y acceso a la red de confianza cero. Estas funciones se entregan desde la nube y el proveedor de SASE las proporciona como un servicio.

## ¿Por qué SASE?

Con la transformación digital de las empresas, la seguridad se traslada a la nube. Esto está impulsando la necesidad de servicios convergentes para reducir la complejidad, mejorar la velocidad y la agilidad, habilitar las redes multinube y proteger la nueva arquitectura habilitada para SD-WAN.

## ¿Para qué SASE?

El modelo SASE consolida numerosas funciones de red y seguridad, que tradicionalmente se entregan en soluciones puntuales en silos, en un único servicio integrado en la nube. Al consolidarse con SASE, las empresas pueden:

- Reducir costos y complejidad.
- Proporcionar orquestación centralizada y optimización de aplicaciones en tiempo real.

- Ayudar a asegurar el acceso perfecto para los usuarios.
- Habilitar un acceso móvil y remoto más seguro.
- Restringir el acceso según la identidad del usuario, el dispositivo y la aplicación.
- Mejorar la seguridad aplicando una política coherente.
- Aumentar la eficacia del personal de seguridad y de la red con una gestión centralizada.

## ¿Cómo adoptar SASE?

Gartner considera que SASE es una visión de un futuro modelo de redes seguras para las empresas. Actualmente no es una realidad de ningún proveedor. Hoy en día, SASE está mejor representado por la convergencia de SD-WAN administrada en la nube y la seguridad entregada en la nube. Pasar a un modelo SASE será un proceso gradual a medida que TI reconsidere cómo conectar una fuerza de trabajo remota a los recursos de información distribuida que necesitan. También es probable que haya una demanda creciente de modelos de adquisición “como servicio” que ofrezcan más flexibilidad |

# ¿Por qué elegir a Cisco para adoptar SASE?



“SASE se trata de la unión entre networking y seguridad, juntas de la mano. Esto me recuerda cuando hace algunos años Cisco reunió red de datos (data networking) y red de voz (voice networking), las cuales se encuentran completamente integradas para nuestros clientes en la actualidad. Hemos visto este tipo de fusiones antes y la experiencia de tantos años nos permite ser más efectivos, tener mayor control y visibilidad, manteniendo una arquitectura flexible de cara al futuro. SASE es el mismo viaje, la misma trayectoria en la cual Cisco ha ayudado a sus clientes por 30 años”.

**Yann Walters**, VP, Americas Security Sales, Cisco.



“Porque adoptar SASE significa recorrer un camino, y en Cisco realizamos ese viaje desde hace años, cada día, junto a nuestros clientes. Cisco siempre se ha enfocado en la experiencia del cliente y en proveer servicios de calidad y excelencia. En términos de nube, lo que hicimos en Latinoamérica, con el apoyo de nuestra organización en todo el mundo, fue crear una infraestructura local. Contamos con una extensión de los servicios globales en la nube, y somos parte de este gran proveedor para ofrecer este tipo de soluciones. Estamos entregando a nuestros clientes una mejor latencia, una mejor experiencia. Si algo sucediera, contamos con un acuerdo de nivel de servicios (SLA - service level agreement), un proceso diferente de entrega de servicios, totalmente transparente para nuestros clientes, muy diferente de otras ofertas en la nube que tan solo ofrecen servidores muy básicos sin una alineación adecuada, sin un proceso de resiliencia en los negocios”.

**Ghassan Dreibi**, Cybersecurity Operations Director, Latin America, Cisco.



“Nuestro enfoque de SASE ayuda a las organizaciones a asegurar el acceso sin importar dónde residan los usuarios y las aplicaciones, combinando funciones de redes y seguridad nativas en la nube y entregadas en modelos flexibles de consumo “as-a-Service”. Con foco en la experiencia de usuario, la protección de los datos y la simplificación de las operaciones, somos un verdadero socio para nuestros clientes en su camino de implementar aplicaciones en ambientes multinube”.

**Juan Pablo Mongini**, Head of Enterprise Networks Sales in Latin America, Cisco.



“Para lograr la promesa de SASE hay una infraestructura y arquitectura tecnológica ‘detrás de escena’ que difiere profundamente entre fabricantes. Las empresas que transicionan a SASE deben adentrarse en ella, especialmente para reconocer que la eficacia en seguridad trasciende la prevención y depende de la detección y respuesta a tiempo frente a amenazas que van a ocurrir. Por otra parte, si SASE habla de una convergencia de la red y la seguridad y Gartner recomienda ‘idealmente un solo vendor que pueda ofrecer la mayoría de los componentes de SASE’ surge que mucho antes de la propia gesta del concepto, Cisco venía construyendo las bases de lo que ahora se nombra de este cierto modo”.

**Juan Marino**, Regional Manager Latin America, Cisco.

Ad content



# Experiencia de Edesa con Braycom

# En primera persona

por: **Diego Máspero**

Ingeniero en Sistemas y CIO de Edesa, Salta, Argentina.



Corría el año 2016 cuando en Edesa tomamos la decisión, y el riesgo, de hacer lo que debíamos hacer: adaptar y optimizar nuestros sistemas de TI. Estaba claro desde el inicio el desafío de mejorar la performance, bajar los costos de la operación, lograr mayor fiabilidad de la infraestructura y facilitar el uso. Ese objetivo volvía inminente migrar toda la infraestructura de nuestro Data Center, y las tareas a realizar implicaban muchos y grandes cambios:

- ⚙️ Servidores a tecnología Intel.
- ⚙️ Storage a nueva tecnología SDS (Software Defined Storage).
- ⚙️ Unificación de hipervisores en VMware.
- ⚙️ HW de respaldo a disco (facilidad para realizar futuras migraciones) y SW de respaldo a Veeam (tecnología sencilla de utilizar y amigable que ya conocíamos).
- ⚙️ Networking de alta capacidad.
- ⚙️ Sistemas operativos de servidores a Linux y Windows Server.
- ⚙️ Motor de BD Oracle a 12g.

Fue en ese contexto que analizamos el know-how de tecnologías que disponía Braycom y nos contactamos con ellos. Descubrimos gratamente que tenían amplios conocimientos de VMware, Networ-

king y Seguridad, una combinación poco habitual en el mercado en un mismo proveedor.

Con el correr de las reuniones, nos dimos cuenta que Braycom tenía algo diferente a los otros proveedores que conocíamos, notamos que se sentaban a nuestro lado y analizaban las propuestas a ofrecer desde un punto de vista similar al nuestro, no tan interesados en vender un producto sino en resolver el problema de la mejor manera y lo más económicamente posible.

Juntos planteamos tanto expectativas económicas como de performance, funcionalidad, facilidad de upgrade, facilidad de uso y acompañamiento post entrada en producción, y en todos los casos todas fueron cumplidas y superadas.

Hoy disponemos de una solución completamente redundante y en un esquema activo-activo que nos permite tener un business continuity plan (BCP), ímpensado con la anterior tecnología de que disponíamos.

Contar con un socio tecnológico estratégico como Braycom, que está enfocado en cómo ayudarnos a resolver nuestros problemas con un presupuesto acotado como el que estamos acostumbrados en nuestro país, nos permite encarar nuevos proyectos como por ejemplo, transitar el recorrido a SASE en términos de ciberseguridad, o el armado de un sitio remoto que nos permita tener todo el data center 100% operativo en menos de 24 hs., en caso de desastre mayúsculo de destrucción de ambos data centers.

En ese camino estamos |

# Taekwon-Do y Ciberseguridad



## Contrapunto

texto: **Silvia Montenegro**

video: **Juan Marino**

### ¿Qué es el Taekwon-Do?

Un contundente método de combate sin armas. Un arte marcial moderno con raigambre en una milenaria tradición guerrera. Un estilo de vida. En esta nota, Juan Marino entrevista al Gran Maestro Néstor Galarraga.

Con el objetivo de profundizar en la esencia del Taekwon-Do, que desde sus lineamientos propone recorrer un camino interior hacia la “sabiduría en la mente, la fortaleza en el cuerpo y la pureza en el corazón”, Juan Marino, gerente regional de Ciberseguridad de Cisco, visitó al Gran Maestro Néstor Galarraga, quien dirige una organización con más de 200 mil practicantes y es referente no solo en el propio deporte sino en su enseñanza y difusión. Sus trabajos en diferentes áreas concernientes al Taekwon-Do son reconocidos en el campo internacional y valorados por su seriedad y originalidad.

Al inicio del encuentro, Juan Marino expresó el gran honor de disfrutar de ese momento y de conversar

con el autor del libro “El Poder del Guerrero”, publicado por la editorial Tequisté en plena cuarentena por COVID-19, y que incluye las reflexiones, anécdotas y conceptos del deportista argentino luego de una gran trayectoria: “Leí detenidamente su libro, pero no puedo dejar de preguntarle justamente ¿dónde reside el poder del guerrero?”.

Para Néstor Galarraga, se trata de una construcción interna, que fortalece el exterior y alumbró un potente descubrimiento personal: “El verdadero poder está adentro. Aprender a defenderse es un camino a través del cual, irreversiblemente, uno termina en lo introspectivo”.

### Táctica y Estrategia

El paralelismo entre el deporte y la ciberseguridad, que fue la hipótesis que acercó al representante de Cisco al Dojang -espacio físico para el entrenamiento del Taekwon-Do-, se reveló desde el comienzo del encuentro: “En ciberseguridad nos defendemos no solo de un atacante sino de toda una organización criminal, y en ese camino de la defensa hay muchas cosas para hacer. En nuestro ámbito decimos que el atacante tiene tácticas, técnicas y procedimientos, ¿cómo se juega eso en el Taekwon-Do?”.



Federico Teissandier y Gonzalo Hauri durante una práctica para ilustrar la entrevista.



Contenido audiovisual con demostración práctica.

# Integridad Perseverancia Autocontrol **Cortesía** Espíritu Indomable

El Gran Maestro explicó que el enfoque es parecido: “Hay una estrategia general, luego está la táctica, que interviene para aplicar diferentes partes de esa estrategia, que es, te diría, universal. Hay 2000 combinaciones de técnicas de mano, y 1800 combinaciones de técnicas de pie. Entonces, es muy amplio hablar de la estrategia, porque hay que tener en cuenta el contexto. No es lo mismo defenderse adentro de un transporte público o en una casa, no es lo mismo estar solo o acompañado por tus hijos. Si sufrís un asalto y estás acompañado por tu familia, la reacción defensiva está limitada. Y si estás solo tal vez pueda darse la oportunidad de crear una situación en la que puedas reaccionar y defenderte, sobre todo cuando se percibe que está en riesgo la integridad”.

## Percepción y Disciplina

Juan Marino consultó sobre la “fantasía” que suele rodear a las artes marciales que postula al experto como alguien capaz de afrontar con éxito cualquier situación de peligro: “¿Cómo lo ve usted? ¿Cómo es prepararse para lo que no se conoce? En ciberseguridad, de alguna manera, nos sucede lo mismo, no sabemos cómo nos van a atacar...”, consultó.

“Es cierto. Cuando empecé a practicar tenía la ilusión de poder defenderme frente a diez personas armadas. Sin embargo, el arte marcial realmente forma en cómo no entrar en una situación de desventaja, es decir, te va preparando el ojo, te va volviendo mucho más sensible, y desde allí se revela un estado de percepción respecto a la violencia fundamentalmente. Al percibir, podés decidir con mucha claridad dónde pararte”.

“Me imagino que esa percepción impide que uno entre en pánico y sepa cómo responder”, completó Juan Marino, y agregó que los expertos tecnológicos no pueden quedarse solo en la teoría: “Las organizaciones más maduras simulan escenarios de ataque y defensa. ¿Cuál es el rol de la simulación y del juego en un arte marcial?”.

Néstor Galarraga explicó que en Taekwon-Do todo es práctica: “Su desarrollo no se da a través de un libro desde el cual aprender, se da desde la práctica. Es entrar en una comunidad donde todo se aprende a través del trabajo. Nosotros estamos íntimamente relacionados con el juego, hay alguien que ataca y otro que juega a defenderse, y eso se lleva a estados muy cercanos a la realidad, porque, digamos, el concepto de marcialidad es indispensable para poder ponerle control a la pelea.



Marino y Galarraga durante la conversación.

Si tomamos esa base, yo preparo a dos personas para que peleen prácticamente hasta en un estado natural, tengo el control, sé que cuando genero el stop puedo detenerlos, y eso es porque hay obediencia y respeto hacia el instructor, bajo el amparo de la disciplina”.

### La técnica

Juan Marino puso en relieve tres ejes sobre los que nace el Taekwon-Do, el ataque, el contraataque y la anticipación; y reconoció que, en su ámbito, la ciberseguridad, el contraataque es poco común: “Puede darse entre Gobiernos bajo la forma de ataque cibernético como futuro de la guerra. En cambio, podemos entender cómo ataca el otro y cómo anticiparnos. ¿Se puede ver un ejemplo de lo que significa esto en Taekwon-Do?”

Y entonces entró al salón Federico Teyssandier, vestido con su dobok -pantalón, chaqueta, cinturón-. Y se armó un sofisticado “juego” entre él y el Gran Maestro, quienes pusieron en escena la filosofía del deporte, la práctica, el pensamiento, la acción. A través de la potencia de los dos contrincantes, sus movimientos estratégicos, la precisión de las patadas o los contraataques, la agilidad y la coordinación, el dominio del cuerpo se fue armando como una especie de ajedrez corporal, muy armonioso y a la vez potente.

El maestro Galarraga, cinturón negro y IX Dan, mostró con gran generosidad y predisposición su destreza,

reflejos y equilibrio. A medida que luchaba, fue diciendo: “Lo ataco con un golpe de puño, para lograr una respuesta favorable en esta situación. Ahora estoy en desventaja. Él me ataca y yo estoy vulnerable. Ante ese ataque, tengo que elegir una posición mejor para mí. Podría correrme, es una posición mejor, pero temporal, porque me va a alcanzar con el otro puño. Pero voy a tener una herramienta preparada para esa acción que va a generar mi oponente. Es una situación de anticipación, lo detengo cuando la técnica no terminó de ser ejecutada. Si logro conectarlo en esa posición, voy a utilizar algo que es fantástico en todo arte marcial, que es que la fuerza de él se suma a la fuerza de mi puño...”

Una cosa es ponerlo en palabras, otra muy distinta, verlo. En ese juego con su contrincante, marcó movimientos de contraataque, técnicas lineales, formas de control: “Debo tener en cuenta cuáles son las acciones que él puede generar y qué tengo que hacer para controlarlas. Esa es una situación de contraataque”.

### Superarse a uno mismo

A fuerza de patadas, golpes, bloqueos, saltos, equilibrio y reflejo, el Taekwon-Do se convierte en una herramienta para la mejora física, psíquica y social. Néstor Galarraga agregó: “Uno sabe cuándo anticipar y cuándo contragolpear. Si te ganaron en la acción, la única posibilidad es tratar de minimizar los daños. Y ver que respuestas dar, ya los daños no pueden evitarse”.





Federico Teyssandier y Néstor Galarraga durante la demostración. Puedes ver el contenido audiovisual completo a través del código QR en el inicio de la nota.

Juan Marino habló del concepto de resiliencia: “En ciberseguridad pensamos que el ataque va a suceder y en muchos casos no se va a poder evitar. ¿Cómo entiende el Taekwon-Do la resiliencia?”

“El Taekwon-Do es resiliencia. Entendemos que la pelea real es con uno mismo y una de las primeras cosas que aprendemos es a cambiar la limitación por el desafío”, explicó el Gran Maestro, y agregó: “Podemos aprender a acomodarnos con la limitación, si no fuera superable. Siempre vamos a tener una visión positiva”. Habló de las limitaciones que cada uno puede tener y, especialmente, de aquellas que están basadas en el miedo: “El miedo inmoviliza y nosotros enseñamos a superarlo a través de la acción inteligente”.

### Un Mundo Mejor

El esfuerzo, la perseverancia, el trabajo comprometido transforman a las personas en luchadores de la vida. Y el arte marcial se basa en un programa técnico que exige el respeto de códigos de conducta, como la cortesía, la integridad, el autocontrol, la valoración de la cultura y la tradición. Los maestros orientales dicen que quien haya practicado Taekwon-Do sabe que es belleza y crudeza, soltura y rigor, tradición e innovación, fortaleza y sensibilidad, obediencia y creatividad, arrojo y prudencia, humildad y autoridad. Un medio, nunca fin.

“Nos puede dedicar un último pensamiento desde la marcialidad, Maestro, para nosotros, que estamos fuera de la disciplina, inmersos en el mundo, en el

ámbito corporativo o en otras organizaciones”, propuso Juan Marino.

El mensaje fue: “A través del Taekwon-Do enseñamos a los alumnos a abrazar, vivir y compartir una serie de valores y principios para intentar alcanzar un mundo mejor. La ciencia, la técnica, la tecnología están dentro del ser humano y lo hacen irremplazable”.

Antes de agradecer las enseñanzas y despedirse del Gran Maestro, Juan Marino dijo: “Interpreto entonces que la técnica del Taekwon-Do se puede comparar con la tecnología, y que el secreto no está allí, sino en todo lo que las envuelve: los principios, los valores, una forma de ver la vida, un modo de ser” 🗣️



El equipo al finalizar la producción.



Imagen: Basanta Contenidos

# Especial Mujeres en Ciberseguridad

Producción integral conjunta WOMCY - Bridge

Cuando delineamos el sumario para esta edición de Bridge buscamos integrar referentes que aportaran una experiencia distinta, con otra voz y un punto de vista marcadamente diferente a las anteriores. Por eso decidimos incluir la mirada femenina y desarrollar un Especial Mujeres en Ciberseguridad conjuntamente con WOMCY (Women in Cybersecurity). Bocetamos y produjimos el proyecto junto a Leticia Gammill, Líder de Canales de Seguridad para Cisco Latam y Presidenta-Fundadora de WOMCY Latam, a quien agradecemos profundamente.



**Leticia Gammill** lidera el equipo de socios regionales de Ciberseguridad en Cisco. Es responsable de la estrategia, el posicionamiento y la habilitación de la arquitectura y las soluciones de ciberseguridad para los socios, proveedores de servicios y distribuidores de esa empresa. Supervisa la implementación, el seguimiento y el éxito de los programas de canales y las iniciativas de rentabilidad de los socios en la región.

Con 15 años de experiencia en la industria de la ciberseguridad, asesorando a clientes y socios en las Américas en todas las fases de su estrategia de ciberseguridad, la experiencia de Leticia incluye estrategias de expansión regional y ejecución en empresas de primer nivel.

Es la Fundadora y Presidenta de WOMCY, Latin America Women in Cybersecurity, una organización enfocada en la tutoría y desarrollo de programas especiales para promover carreras en ciberseguridad y aumentar la presencia de profesionales de esta disciplina en América Latina. Se graduó de EHTP en Porto, Portugal, y tiene un MBA de la Kellogg School of Management de la Northwestern University.



## Martha Liliana Sánchez Lozano

Ha desarrollado una notable carrera en Ciberseguridad en Colombia, tanto en ámbitos oficiales como privados, y organizaciones no gubernamentales. Para hablar sobre este tema, sobre el camino que recorrió y los pasos a seguir, Leticia Gammill, Líder de Canales de Ciberseguridad de Cisco, la entrevistó para Bridge. La conversación tuvo lugar mediante Webex, la plataforma de colaboración de Cisco.



Contenido  
audiovisual

texto: **Jorge Prinzo**

video: **Leticia Gammill**

**¿Qué se necesita para iniciar una carrera en ciberseguridad? ¿Es imprescindible la formación técnica, o la experiencia?**

En mi caso empecé por el interés de conocer nuevas cosas. Siempre me he alentado a actuar en temas innovadores y a veces hasta desconocidos. La ciberseguridad me interesa porque no solo afecta mi realidad, sino también al funcionamiento del mundo. Los ataques que estaban surgiendo afectaban al espacio digital, y no había personas que se ocuparan del problema. Eso me llamó la atención: actuar en campos novedosos, estudiarlos, entenderlos, luego transmitir esa información y cambiar el comportamiento alrededor, crear nuevas formas de actuación, así como un nuevo campo laboral y académico. Es un requisito fundamental para quienes trabajan en estas carreras tener esa actitud innovadora. Respecto a la experiencia y los conocimientos, yo tenía esa base técnica y tenía experiencia profesional que me ayudó a orientarme; sin embargo, en el camino, me di cuenta de que no era imprescindible, sino que se necesitaba también de otras habilidades. No es algo solo de ingenieros, o militares; me ha tocado relacionarme con administradores, abogados, sociólogos, representantes de organismos de derechos humanos... son tantos los intereses que tenemos en ciberseguridad, que cualquier persona que se interese, que quiera crear cosas nuevas y cambiar su entorno, es bienvenida.

**Es imprescindible seguir estudiando, porque son temas que evolucionan muy rápido, son muy dinámicos, y es preciso actualizarse permanentemente. ¿Cómo ves la ciberseguridad en Colombia?**

La implementación de políticas de ciberseguridad en Colombia ha sido un proceso que comenzó hacia 2007, luego del ataque cibernético contra Estonia, cuando fue evidente que un país podía ser paralizado, que podía haber muertes, o afectar al sistema financiero. Como respuesta al incremento de delitos, forjamos una política con leyes específicas y una infraestructura sobre ataques informáticos. En 2011, analizamos el panorama y notamos que no existían programas de capacitación, que no iba a haber gente que pudiera afrontar estos nuevos retos. En ese momento yo era directora de un programa de tecnología en la Escuela Superior de Guerra, entendimos que había algo nuevo que hacer, y creamos la primera Maestría en Ciberseguridad y Ciberdefen-

sa de América Latina. Fue el punto de partida para abrir nuevos caminos, y nuevos programas en universidades. Hoy estamos enfocados en crear confianza y seguridad digital, trabajando con todas las partes involucradas, porque es un tema de todos, y de responsabilidad compartida. Según el índice de ciberseguridad nacional, Colombia está ubicada por encima de la media mundial, y en América Latina en el tercer lugar, luego de Chile y Brasil. Hemos avanzado, y podemos avanzar aún más en innovación, en protección de los activos críticos, y en integración de todas las partes interesadas.

**Quiero destacar tu compromiso con la formación; hay necesidad de profesionales, tanto en Colombia como en toda América Latina. Además de responder a las amenazas cibernéticas, necesitamos pensar en la falta de profesionales en nuestra industria. En un ámbito tan dinámico, Martha, ¿cómo es un día típico, en tu rol?**

Tengo diferentes roles, porque siempre hay temas pendientes a desarrollar. Siempre estoy leyendo, estudiando, buscando desafíos. Tengo reuniones con diferentes actores, me llaman de la Academia, o de Defensa, organizaciones de Derechos Humanos, para realizar eventos, proponer nuevas líneas de trabajo... También preparo mis clases, ahora dedico más tiempo a la Academia. Trato de transmitir a la gente que no conoce estos temas, a quienes piensan que esto es solo algo técnico, que no es así. Participo también en mesas sectoriales para desarrollar y fortalecer políticas de gobierno. Y finalmente, ahora estoy enfocada en problemas sociales. Soy la presidenta de Internet Society Colombia, una organización que piensa cómo Internet va a ser seguro y confiable para el mundo, con un enfoque social, pensando cómo vamos a llevar la conectividad a la gente más vulnerable. Creé la organización en Colombia, soy la primera presidente, y me dedico a buscar recursos para generar proyectos en Colombia, para que podamos hacer los cambios necesarios, porque nadie va a venir a solucionar nuestros problemas. Intento modificar el espacio en el que estoy, tratando de crear oportunidades para nueva gente. Al crear la Maestría, conseguí becas para que sesenta personas estudiaran gratis, y eso generó nuevos empleos. No es que uno cambie la industria, pero aporta un grano de arena. Así es el día a día en mi rol.

**Lograste un espacio propio en instituciones rígidas en diversidad de género. ¿Cuál fue el impacto de ser pionera en la industria, en tu vida profesional?**



## MiniBio

**Martha Liliana Sánchez Lozano**, PhD, MBA, C|CISO, ISO 27001

Ingeniera de Sistemas, MBA de la Universidad de los Andes, Master en Ciberdefensa de la Universidad de Alcalá de España, Doctora del programa de Derecho Internacional de la Universidad Alfonso X el Sabio, de España, Con mención “Cum Laudem” en el tema de investigación: los Retos del Derecho Internacional Humanitario para Conflictos Armados en el Ciberespacio. Oficial de la reserva activa de la Fuerza Aérea Colombiana, en el grado de Coronel. En 2014 participó en la mesa de expertos nacionales con apoyo de la OEA para fortalecer la seguridad cibernética, integró el comité de ciberdefensa para las fuerzas militares de Colombia y desde 2015 ha participado en las mesas de construcción del CONPES de seguridad digital 3854 y 3995 de confianza y seguridad digital. Desde 2015 lideró el proceso de diseño e implementación del programa de ciberseguridad y ciberdefensa de la Escuela Superior de Guerra de Colombia, siendo la primera Directora de la Maestría de Ciberseguridad y Ciberdefensa en 2016. Entre 2017 y 2018 se desempeñó como Asesora Nacional de Seguridad Digital en la Presidencia de la República de Colombia. Autora del libro “Los conflictos armados en el ciberespacio: Retos del Derecho Internacional Humanitario” (2017, Colombia). Actualmente es docente Internacional de postgrado en ciberseguridad y ciberdefensa y miembro ejecutivo de Internet Society Colombia Chapter, de la que fue fundadora. Top WOMCY 2020.

Me gusta innovar, salirme del modelo que se espera que cumpla como mujer en la sociedad. Estudié Ingeniería de Sistemas, una carrera que cuando comencé era “de hombres”. Fue complicado, pero con esfuerzo pude destacarme. Ya siendo ingeniera decidí entrar a la Fuerza Aérea, y en aquel momento, por ejemplo, las mujeres no podían ser pilotos, algo que hace diez años fue permitido. Comencé a trabajar con radares, en un ámbito aún más complicado que cuando estudiaba, por los porcentajes de hombres y de mujeres, la posición de poder que tienen los hombres, y la inequidad de género que existe. Lo hice con dedicación, esfuerzo y paciencia; no desistí, aunque en muchos momentos pensé en hacerlo; me decía: “basta, no tengo por qué soportar esto”, pero seguí y logré hacer mi carrera. También cuando comenzamos con la ciberseguridad había un sesgo machista.

Venían a dar charlas hombres de otros países, y me convocaban para las conferencias porque querían que participe una mujer por compromiso, como para cubrir una cuota. Yo les decía que había muchas mujeres en este tema. Esas prácticas tratan de desestimar nuestros conocimientos, nuestra experiencia, porque somos mujeres, o porque soy madre y tengo hijos y me ocupo de cuidarlos. Pero por otro lado, también hay personas que me han ayudado. Es un problema difícil, en todas las áreas, pero he encontrado esas personas con visión amplia, que dijeron “yo confío en usted, y vamos para adelante”. Eso permitió avances en esta cuestión, pero sobre todo ser pionera en el tema me ayudó a lograr entrar en roles casi inalcanzables para mujeres, y a través de los cuales he logrado ayudar a fortalecer la ciberseguridad en Colombia.

**¿Podrías definir con una palabra tu amor por la ciberseguridad?**

No una, sino dos palabras: satisfacciones y retos. Me ha permitido sentir que esto es para lo que yo nací, y pude evolucionar, tal vez porque me atrae la novedad.

**¿Cuáles son tus proyectos para 2021?**

Me gusta escribir, y he escrito un libro, Los conflictos armados en el ciberespacio, sobre los desafíos del derecho internacional en el área cibernética, y es parte del doctorado que hice en España. Es el primer libro de América Latina sobre estos temas.

Ahora estoy trabajando en mi segundo libro, sobre ciberdiplomacia en América Latina, un tema que solo se ha desarrollado en Europa. Estoy manteniendo contactos con la Comunidad Europea y con universidades de Colombia, para que tenga relevancia y se empiece a desarrollar esta área. Espero dedicarme a escribir en el próximo año, y también a generar nuevas capacitaciones en las universidades. Me han llamado para ser docente en ciberseguridad y ciberdefensa en universidades de México. Además, seguiré buscando recursos para los proyectos de la organización que presido en Colombia. Esos son los planes que tengo en el corto plazo ■



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](http://basantacontenidos.com)



Andréa  
Thomé



Sucede que a fin de año, entrevistar a líderes empresarias puede volverse tarea difícil. Sucede que a fin de año, las tareas enloquecen, las personas se agitan y lograr una entrada nueva en la agenda puede ser un desafío imposible de lograr. Sin embargo, en la entrevista con Andréa Thomé, esos supuestos solo formaron parte de un imaginario, de la experiencia de otros. Si algo demuestra la fortaleza en el liderazgo, es la capacidad de promover, distribuir, alentar y llevar a la acción con perspectiva de éxito, todas características sobresalientes en nuestra entrevistada. Y además un plus inolvidable: su calidez, respeto y profesionalismo implacables en todo momento.

por: **Karina Basanta**



**Tu recorrido profesional da cuenta de una gran fortaleza y perseverancia ¿Qué significa para ti empoderarse?**

Significa ser autosuficiente para motivar, movilizar, proporcionar fuerza y velocidad para lograr resultados. Este proceso nos permite descubrir que independientemente de cualquier adversidad, cuando queremos, podemos y logramos lo que queremos.

**Y al revés, ¿qué es la fragilidad para Andréa Thomé?**

La fragilidad nos advierte que se necesita más fuerza y una dosis más alta de empoderamiento para mantener el equilibrio. Nos lleva a sentir peso en las dificultades, pero nos permite reflexionar. En momentos de fragilidad nos desafiamos a nosotros mismos y crecemos, para volver más fuerte a la zona cero.

**Recientemente he leído una entrevista realizada a Tarja Halonen, ex presidenta de Finlandia, donde sostiene que la cuestión de género resultó ser un factor clave para explicar la calidad de las respuestas de los gobiernos frente a la pandemia. A tu entender, ¿a qué nos referimos las mujeres cuando decimos que hacemos mejor las cosas?**

Características como la sensibilidad, el enfoque, la asertividad y la capacidad analítica nos ponen en ventaja cuando nos enfrentamos a crisis como experimentamos en esta pandemia. Otro aspecto que admiro en las mujeres es la capacidad de diseñar escenarios basados en el análisis crítico y en la intuición que ya nace con ellas.

**¿Por qué WOMCY (Women in Cybersecurity)?**

WOMCY nació de una necesidad que hoy impacta positivamente a cientos de mujeres en más de 18 países de América Latina y Centroamérica. Al buscar una ONG en LATAM en 2019 para unirse y poder contribuir, Leticia Gammill, nuestra Fundadora

y CEO, simplemente no encontró y luego decidió fundar su propia ONG.

Desde entonces, hemos reclutado líderes, definido programas, acciones, creamos equipos, llegamos a personas especiales e incluso hemos ganado la simpatía de hombres que nos ayudan como parte de nuestro equipo WOMCY He for She.

Hace poco más de un año, cuando recibí la invitación de la CEO, por nombramiento de un ex líder que tuve en una etapa de mi carrera, no pude evitar admirar el alcance de la propuesta que es el resultado de 9 programas y el trabajo de 6 equipos en Brasil liderados por un grupo de más de 50 talentos.

Pasamos por el mundo corporativo, asociaciones, universidades y escuelas, con conferencias, información, tutoría, programas de formación, difusión de vacantes y mucha recepción a ejecutivos, gerentes, especialistas, jóvenes, principiantes, estudiantes y profesionales en transición profesional a ciberseguridad.

Puedo decir que nunca he aprendido tanto y nunca me he sentido tan útil al poder ayudar a los necesitados en un sector tan prometedor.

**A tu entender, ¿cuáles son las habilidades que se necesitan para destacarse en ciberseguridad?**

Curiosidad, habilidad de investigación, búsqueda continua de conocimiento, visión crítica, pensamiento innovador, equilibrio y visión predictiva para minimizar los incidentes.

**¿Cómo ves la ciberseguridad en Brasil y cómo es el posicionamiento del país en relación a Latinoamérica?**

Tenemos mucha experiencia en la prevención y respuesta a incidentes de seguridad, sobre todo porque hemos experimentado muchos ataques. Al mismo tiempo que se experimenta el sabor amargo de los incidentes, se obtiene la capacidad de conocer sus características, aprender a evitar su incidencia y responder con agilidad y eficacia a sus impactos adversos.

El sector en Brasil ha alcanzado una posición prominente si lo comparamos con el escenario de la última década. Hoy en día la ciberseguridad forma parte de la agenda estratégica de cualquier industria, aunque no necesariamente recibe la prioridad que merece. Pero el IBGC - Instituto Brasileño de

Gobierno Corporativo, por ejemplo, definió en una publicación el papel del Consejo de Administración en relación con los riesgos cibernéticos.

Y creo que el tema también ha adquirido relevancia en otros países de América Latina, donde percibo una plena colaboración entre ellos, ya sea en el intercambio de conocimientos, recursos e información.

Creo que en el post-pandemia mucho debe ser revisado de acuerdo con los resultados que experimentamos. La cultura de la ciberseguridad debe recibir un mantenimiento intenso, las herramientas de seguridad deben ser desafiadas y complementadas y los procesos deben ser mejorados y transformados para ofrecer el mejor costo-beneficio a las empresas.

Una palabra para describir tu amor por la ciberseguridad.

Desafío.

¿Cuáles son los próximos pasos en 2021 en términos de ciberseguridad?

La pandemia nos enseñó y al mismo tiempo nos expuso mucho. Hemos notado en algunos escenarios que las medidas básicas de seguridad no eran eficaces o eran inexistentes durante las crisis.

Por favor, comparte con nosotros un breve mensaje final acerca de tu anhelo en cuestiones de ciberseguridad.

Quiero ver más mujeres en este sector que es tan prometedor, que aporta tantos beneficios a las empresas, los individuos y el mundo. También deseo que no haya brecha salarial, conocimiento u oportunidades para los diversos géneros en nuestro mercado.

Por último, quiero sobre todo poder ver crecer la industria con más reconocimiento, diversidad y que las defensas corporativas se fortalezcan cada vez más contra el fraude y los incidentes de ciberseguridad.

## MiniBio

Graduada en Ciencias de la Computación y MBA en Gestión Empresarial, Andréa se desempeña actualmente como directora para soluciones de Ciberseguridad en everis. Además, es líder de la operación de WOMCY Brasil (Mujeres en ciberseguridad) y mentora de negocios, CISM, Harvard Manager Mentor, CobITF, PMBM, ORM Admin. Reside en la ciudad de San Pablo, Brasil.



# ÚNETE A WOMCY

**Somos una organización sin fines de lucro,  
conformada por mujeres, con foco en el  
desarrollo de la Ciberseguridad  
en América Latina.**

**WOMCY**

LATAM Women in Cybersecurity

[www.womcy.org](http://www.womcy.org)



## Milena Realpe Díaz

Entrevista a la Teniente Coronel Milena Realpe Díaz, Jefe de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra de Colombia.



Contenido  
audiovisual

texto: **Jorge Prinzo**  
video: **Leticia Gammill**

**¿Qué se necesita para comenzar una carrera en ciberseguridad? ¿Es imprescindible contar con experiencia y conocimientos técnicos?**

Sí, hay que tener una formación, y lo más recomendable es iniciar con Ingeniería en sistemas, Ingeniería electrónica, cualquier ingeniería afín a estos programas. Este tema es muy apasionante y cambia todos los días, lo que nos obliga a estar en constante capacitación. Ese sería el inicio: una carrera basada en ingeniería que le dé el contexto general, y luego el estudiante puede elegir la especialidad en ciberseguridad, o ciberdefensa, en el caso militar. Necesariamente debemos tener una formación.

**¿Cómo ves la ciberseguridad en Colombia y cómo es el posicionamiento del país en relación a Latinoamérica?**

Colombia ha hecho un trabajo bien importante. Empezamos en 2011 con el primer documento de ciberseguridad y ciberdefensa, y hemos tratado de darle continuidad. De hecho llevamos ya cuatro políticas, actualizaciones, y planes de acción. Y ha surtido efecto porque hemos podido alcanzar esos planes de acción. Quisiéramos avanzar con más velocidad, pero eso depende de muchos factores, económicos, de recursos humanos... El año pasado la OEA publicó un estudio a nivel de Latinoamérica, que ya había hecho en 2016, comparando cómo habían crecido los países de la región en diferentes aspectos, por ejemplo en política, en concientización, en cultura informática, en normativa y leyes..., y en Colombia, para nuestra alegría, hemos crecido en todos esos aspectos. Ahora somos miembros del Convenio de Budapest, lo que también fue un avance para nuestro país. Nuestra primera política se llamó Lineamientos en ciberseguridad y ciberdefensa; luego pasamos a otro tema donde dábamos fortalecimiento a la economía digital, y ahora pasamos a la confianza de las personas en ese nuevo dominio donde estamos viviendo, compartiendo, trabajando... Este nuevo dominio, el ciberespacio, no solamente nos cambió la forma de hacer las cosas sino también de fondo nos cambió la vida a todos. Estamos avanzando como país; tenemos que seguir trabajando, pero creo que vamos en un buen camino.

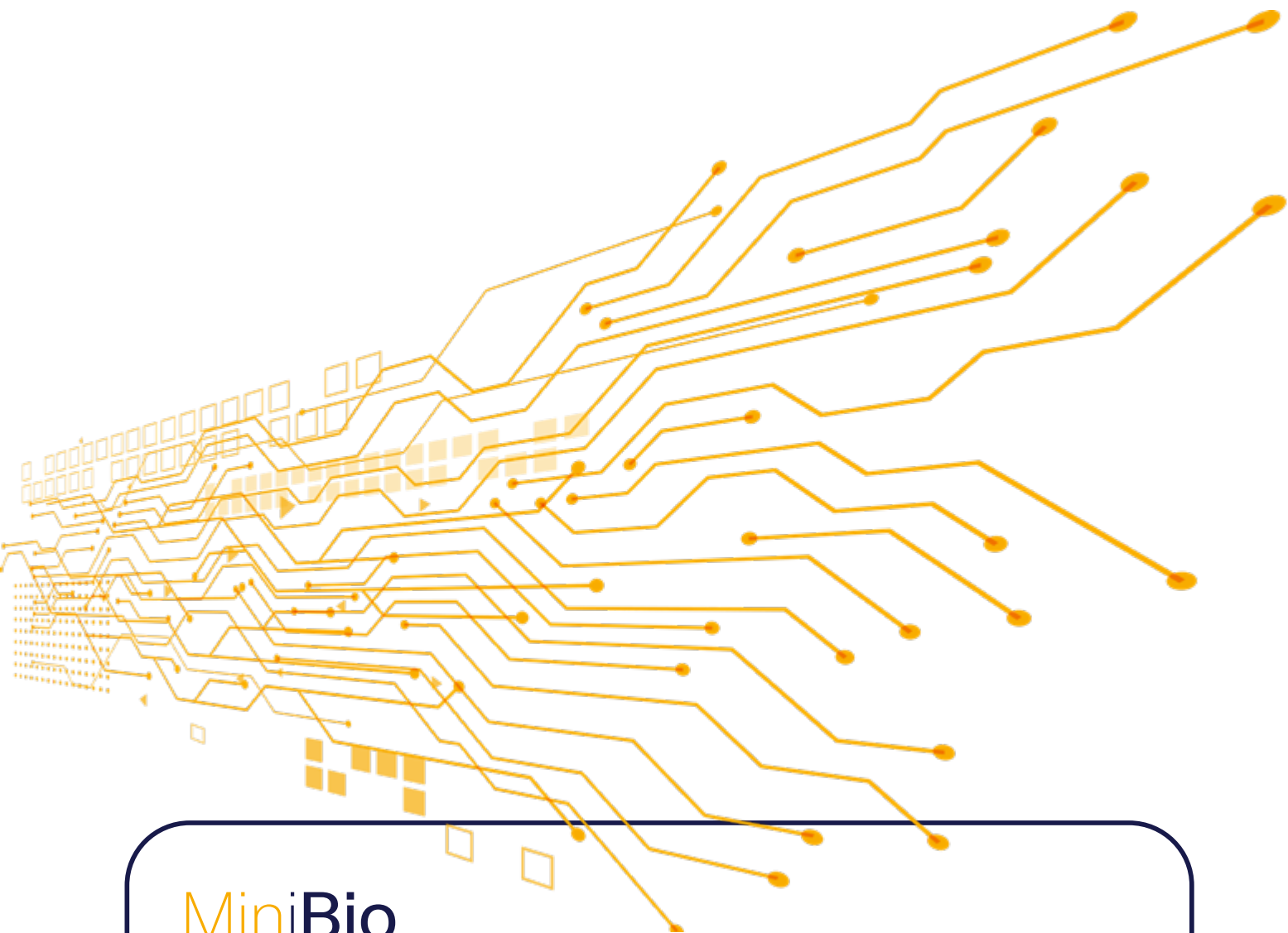
**Por favor describe un día típico en tu rol.**

Es un día que inicia muy temprano, a las cinco de la mañana. Me gusta hacer deportes, es lo primero que hago en las mañanas. Atiendo también a mis hijos, en mi rol de mamá, antes de salir a la jornada laboral. Y ya entrando en el área de ciberseguridad, atiendo los requerimientos de mis estudiantes en la Maestría. También leo y me actualizo en el día a día en tecnología. Este momento que nos ha tocado vivir a la humanidad a consecuencia de la pandemia ha obligado a que la mayoría de las empresas tengan que incorporar procesos digitales; entonces los usuarios, los clientes, la información, las bases de datos... todos los requerimientos de esos usuarios se conectan a internet, incluso los que antes no estaban. Estamos haciendo uso de muchos sistemas que requieren seguridad. Entonces nos toca capacitarnos, nos toca leer, ser autodidactas. Hay muchos documentos importantes que se generan, autores que publican en internet sus estudios, y están a la mano de todos. Es simplemente querer hacerlo, tener pasión por hacerlo, y lo demás fluye. Ése es el día a día de mis tareas en la Escuela Superior de Guerra. Cuando podemos hacerlo físicamente es físicamente, y de lo contrario trabajando desde la casa, resolviendo y asesorando en temas de ciberseguridad para los diferentes sistemas, apoyando a los estudiantes en temas de investigación, y escribiendo también. Me gusta escribir, generar nuevos conocimientos y compartirlos. Y además se complementa con mis roles de mamá, de esposa, de hija, de hermana, todos los roles que como mujeres nos toca también atender y nunca dejar atrás, sino que por el contrario ya que son ese soporte que nos lleva adelante, los que nos dan la fortaleza, esa familia que está ahí apoyándonos en nuestro rol profesional.

**A tu entender, ¿cuáles son las habilidades que se necesitan para destacarse en ciberseguridad?**

Ser persistentes. A veces las cosas no salen a la primera vez como quisiéramos. Entonces: insistir, insistir e insistir en lo que queremos, porque al final lo podemos lograr. Y la pasión: ser apasionados por lo que hacemos, que nos guste lo que hacemos es un factor indispensable para progresar y ser feliz. Al final del ejercicio eso es lo que nos hace ser felices: trabajar en lo que nos gusta, estudiar lo que nos gusta, investigar lo que queremos.

**Parece que has logrado encontrar un espacio en distintas instituciones algo rígidas en cuanto a diversidad de género y profesión. ¿Qué significa esto para ti y qué impacto tuvo en tu vida personal?**



## MiniBio

Ingeniera de Sistemas con 18 años de experiencia profesional en seguridad de la información, gestión de tecnologías de información y comunicaciones, análisis de vulnerabilidades, Ciberseguridad, Ciberdefensa, gobierno de la seguridad de la información, análisis de vulnerabilidades, gestión de incidentes, creación de CSIRT, CERT y SOC. Asesora y docente militar y universitaria. Ponente Nacional e Internacional. Participó en la formulación del documento CONPES 3701 “Lineamientos de Política de Ciberseguridad y Ciberdefensa para Colombia” y en el CONPES 3858 “Política de Seguridad Digital”; cofundadora del Comando Conjunto Cibernético de las Fuerzas Militares de Colombia. Directora de varios proyectos de seguridad informática y telecomunicaciones, con altas condiciones humanas y éticas. Magister en Seguridad de la Información (Universidad de los Andes), Magister en Ciberseguridad y Ciberdefensa (Escuela Superior de Guerra), Especialista en Seguridad de redes, Seguridad Física y Seguridad de la Información. En la actualidad se desempeña como Jefe de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra de Colombia y Asesora en Ciberseguridad y Ciberdefensa del Ministerio de Defensa Nacional de Colombia.

Las fuerzas militares se han ido transformando. Hemos dado participación desde hace varios años a la mujer, se ha trabajado en temas de inclusión. Entonces a mí ya no me tocó tan difícil. Creo que para destacarse en el área de ciberseguridad, y en cualquier área, lo que se debe hacer es mostrar resultados en los proyectos que presentamos

ante la institución, eso es lo que nos guía. Es lo que evidencia que alcanzamos esa meta que nos propusimos. Eso traté de hacer: mostrarles cómo las fuerzas militares requerían asumir la responsabilidad en ciberseguridad y ciberdefensa. Es lo que me ha permitido destacarme un poquito en este tema: mostrar resultados, innovar, pensar en prospectiva

hacia dónde va la ciberseguridad y la ciberdefensa, y adelantarnos a lo que pueda pasar.

**¿Qué es la fragilidad para la Mayor Milena Realpe? Puedes responder desde cualquier punto de vista.**

Creo que hay que enfocarlo en nuestro tema. La fragilidad en nuestros sistemas permite que seamos vulnerados, que tengamos riesgos en ciberseguridad. Si tenemos equipos frágiles, que no fueron configurados de tal manera que tengan buenos controles de seguridad, somos frágiles ante cualquier ataque, y nuestra información puede ser afectada: la confidencialidad, la integridad, la disponibilidad... Si no queremos ser frágiles, si queremos ser fuertes ante posibles atacantes que quieren acceder a nuestros sistemas, tenemos que proteger nuestros equipos, hacer una configuración fuerte.

**Una palabra para describir tu amor por la ciberseguridad.**

La pasión: la pasión de hacer estas cosas. Para mí es apasionante trabajar en ciberseguridad, y en mi caso particular en ciberdefensa. Innovar, proponer, plantear en prospectiva cuestiones militares de mi país, Colombia, no tiene comparación. Mirar cómo podemos crecer, cómo avanzar basándonos en experiencias de otros países, proponer algo nuevo para nuestro país, es espectacular para mí, es una pasión.

**¿Cuáles son los próximos pasos para 2021 en términos de ciberseguridad?**

La mayoría de las empresas han migrado al dominio digital, obligatoriamente tocó reinventarnos y hacerlo. En términos de oportunidades laborales, para los expertos en ciberseguridad, el campo es grandísimo. Los profesionales, y los que quieran empezar, tienen mucha oportunidad laboral, y además muy buena remuneración. Todos los sistemas necesitan garantizar su seguridad, que esa información esté resguardada bajo buenos controles, y eso nos lo da la ciberseguridad. La tecnología va a seguir creciendo, cada día vamos a tener nuevas tecnologías disruptivas que habrá que estudiar. La educación es fundamental. Y buscar nuevos proyectos que nos permitan seguir creciendo. Eso nos va a llevar a que pueda progresar nuestro país y nuestra región, y que nuestro campo de acción pueda ampliarse ■



Imagen: Kobby Mendez-Unsplash



# Macrina Pérez Bermúdez

Entrevista a la Presidenta del grupo de ciberseguridad del sector asegurador en México y colaboradora en la creación de conciencia sobre esta materia desde WOMCY México.



por: **Marta Pizzini**

## ¿Qué significa “seguridad” para Macrina Pérez Bermúdez?

Trabajar en línea con la confianza de que la información es confidencial, íntegra y está siempre disponible.

**Tu recorrido da cuenta de una vasta experiencia en términos de ciberseguridad. La actualización y la búsqueda de soluciones a nuevas problemáticas requieren estar alerta dispuesta a nuevos conocimientos todo el tiempo, ¿cómo se juega en ti el balance entre continuidad en tu carrera y actualización constante?**

El aprendizaje continuo es un proceso de toda la vida. El desarrollo tecnológico, las nuevas metodologías, los procesos de trabajo, nuevas amenazas, ataques, etc., generan brechas de habilidades y conocimientos que solo pueden ser superadas mediante la permanente actualización de conocimientos, de lo contrario te pierdes la oportunidad de combinar tu experiencia con las nuevas formas de hacer/ver las cosas y limitas el valor que puedes entregar.

## A juzgar por la acelerada transformación digital que se desencadenó durante el 2020, la ciberseguridad se perfila como un trabajo del presente y del futuro, con una promesa amplia acerca de fuentes de trabajo. ¿Cómo se atrae fuerza laboral a este sector prominente?

Según el estudio de ISC2 del 2020, el déficit de personal de ciberseguridad mundial es de 3.1 millones: 17% corresponde a Latinoamérica. 12% a Norteamérica, 5% a Europa y el 66% a la región de Asia-Pacífico. En México, el tamaño de la brecha de la fuerza laboral es de 195.594 profesionales.

A mi entender, para atraer fuerza laboral se podrían tomar algunas decisiones como:

- El sector empresarial debería acercarse al sector académico y expresar sus requerimientos y tendencias en ciberseguridad.
- Formar especialistas en ciberseguridad a través de programas técnicos y habilidades suaves.
- Promover modelos de trabajo alternativos (local, a distancia, combinados).
- Dar oportunidad a jóvenes sin experiencia, con alto potencial.
- La ciberseguridad es principalmente para personas técnicas, pero también para no técnicas.



A tu entender, ¿cuáles son las habilidades que se necesitan para destacarse en ciberseguridad?

Yo diría que las tres "A" son clave:

- **Anticipación:** ser proactivo, estar un paso antes, prepararnos y estar listos para lo que vendrá.
- **Alineación:** adaptar nuestro rol, el que sea que juguemos, para ser un "habilitador" de valor en la transformación.
- **Adaptabilidad:** rediseñar los programas de ciberseguridad con base en las necesidades del negocio, entorno, situación específica o imprevisible, etc.

¿Cómo ves la ciberseguridad en México y cómo es el posicionamiento del país en relación a Latinoamérica?

Creo que México tiene muchas áreas de oportunidad en términos de ciberseguridad, aunque carece de una legislación de seguridad informática y de una estrategia de ciberseguridad a nivel país. Sin embargo, desde 2018 (a raíz de los ataques de SPEI, Pemex, CFE), he visto que el enfoque está cambiando, ha empezado a ser una prioridad para las empresas privadas, dispuestas a involucrarse, a invertir y a concientizar en temas de seguridad de la información. México y América Latina seguirán enfrentando *ransomware* y ataques dirigidos principalmente.

Una palabra para describir tu amor por la ciberseguridad.

Pasión.

¿Cuáles son los próximos pasos en 2021 en términos de ciberseguridad?

- Seguridad en el trabajo a distancia: es una prioridad en la "Nueva Normalidad", asegurar y proteger la información en cualquier lugar.
- Mayor confianza en servicios y seguridad en la nube.
- Mayor colaboración entre las empresas de un mismo sector, compartiendo inteligencia de ciberseguridad.
- Inteligencia artificial y ciencia de datos aplicados a tecnologías de ciberseguridad.

Por favor, comparte con nosotros un breve mensaje final acerca de tu anhelo en cuestiones de ciberseguridad.

El eslabón más débil en el mundo de la ciberseguridad sigue siendo el ser humano, por ello es importante desarrollar y fomentar habilidades digitales: sé inteligente y prudente en línea como en el mundo real |

## Roles más requeridos en ciberseguridad

**Seguridad en la operación:** se trata de la primera línea de defensa, los ingenieros especialistas en tecnología.

**Administración de la seguridad:** son quienes definen la estrategia y los lineamientos de seguridad.

**Administración de riesgos:** identifican, analizan y priorizan los riesgos de seguridad de cara al negocio.

**Cumplimiento regulatorio:** conocen e interpretan las leyes, normas a cumplir.

**Desarrolladores de software seguro:** quienes están enfocados a incluir seguridad en las aplicaciones.

**Especialistas en análisis de vulnerabilidades y pruebas de penetración:** son los encargados de evaluar, por ejemplo, la infraestructura, aplicaciones.

**Forenses informáticos,** es decir, quienes investigan y resuelven casos de violación de seguridad de la información.

## MiniBio

Macrina Pérez Bermúdez cuenta con más de 20 años de experiencia en tecnologías y seguridad de la información, administración de riesgos, compliance, administración de SOCs, implementación de DRPs, gestión de identidades, impartición de programas de concientización. Ha trabajado en empresas especializadas en Ciberseguridad, la ONU en Viena, Austria, y actualmente se desempeña en la industria de Seguros, donde contribuye a fortalecer la seguridad tecnológica. Es Presidenta del grupo de ciberseguridad del sector asegurador en México. Colabora en la creación de conciencia en ciberseguridad desde WOMCY México.

Uno de los activos más valiosos y subestimados en la era digital es la información, que reside en nuestros equipos, nuestro correo y nuestros repositorios en nube. Es esta información la que está expuesta a innumerables amenazas en la red y solo basta un click combinado con inadecuados controles de seguridad para que quede a merced de criminales inescrupulosos que podrán subastarla, extorsionarnos o mal utilizarla en territorios extranjeros, fuera de la jurisdicción legal de nuestros países.

Es con un solo click que cualquiera de nosotros puede caer en las más elaboradas trampas jamás imaginadas, exponiendo información personal o de la empresa sin darse cuenta de haber sido objeto de un ciberataque avanzado y poniendo en riesgo su prestigio y patrimonio, que demorará años en recuperarse después de mucho esfuerzo y dinero. Es por esto que hoy urge la necesidad de concientización individual y empresarial acerca del riesgo latente al que estamos expuestos, y del cual somos responsables independientemente del área de la organización y función que desempeñemos. Cada uno de nosotros es dueño y responsable de la información que maneja, envía, guarda, del buen uso que le da y las precauciones que toma.

Las cifras de los últimos años muestran un incremento en los ataques de malware y phishing debido a una digitalización acelerada apalancada directamente por la pandemia del 2020. Cifras suministradas a INTERPOL por partners privados, muestran que de febrero a marzo de 2020, hubo un crecimiento del 569% en registros maliciosos, incluidos malware y phishing, y un aumento del 788% en registros de alto riesgo.<sup>1</sup>

Este apetito voraz de los ciber delincuentes por usuarios neófitos en temas digitales se vio compensado en inicios de la pandemia cuando en febrero 2020 muchos tuvieron que aislarse en sus casas y verse obligados a participar digitalmente de diferentes actividades, acceder a servicios y transaccionar de forma remota cuando antes lo hacían de una manera presencial, y en esos inicios de navegación por el mar de la gran red, quedaron indefensos al acecho de delincuentes y vulnerables a un sinnúmero de vectores de riesgo totalmente desconocidos hasta ese momento y que aún hoy siguen ignorando.

Pero no estamos solos en esta lucha, los grandes fabricantes de software y hardware y sus aliados vienen desarrollando un portafolio de soluciones que están al alcance de todos y que desde diferentes enfoques buscan proteger, prevenir o remediar los diferentes puntos de acceso al riesgo al que están expuestos individuos y empresas en esta nueva era digital; hoy en día la seguridad de la información

puede enfocarse en controles que son transparentes para los usuarios, protegiéndolos de las amenazas más avanzadas sin que ellos se percaten de esto, o controles más persistentes y activos en los dispositivos del día a día como laptops y celulares, llegando al tradicional antivirus y antimalware que requiere una atención más asidua de la nueva población digital inexperta.

Un ejemplo de control transparente y activo para usuarios empresariales es el monitoreo de ip y dominios inseguros que constantemente son alimentados en un repositorio global. Una solución como Cisco UMBRELLA, que atiende las solicitudes DNS tradicionales, puede validar en tiempo real para determinar posibles amenazas y bloquear dichas solicitudes sin que el usuario deba intervenir: tan solo apuntar los DNS hacia Cisco UMBRELLA se puede iniciar una protección eficaz y activa de usuarios en el momento, fuera y dentro de la empresa, desde sus casas y a los dispositivos más sensibles, brindando una visibilidad a los analistas de seguridad de los posibles ataques en curso y sistemas comprometidos en un ataque.

Otro ejemplo es el análisis del comportamiento de los usuarios mediante un constante monitoreo de sus actividades usuales. Con esta actividad es posible determinar si un usuario fue objeto de un ataque y se está haciendo uso indebido de sus accesos y cuentas; se logra mediante un estudio predictivo de los patrones de comportamiento de un usuario conocido o bajo análisis de pares y permite visualizar si determinadas acciones y actividades puntuales o consistentes se salen de la media o del comportamiento común de un individuo o de un grupo. Con esta información, el analista de seguridad puede detectar y actuar de forma ágil ante un posible ataque que se este perpetuando a la organización.

**OCP TECH** ofrece a sus clientes un enfoque de consultoría avanzada que le permite brindar, de forma integral, soluciones y servicios que respondan ante los nuevos riesgos de la era digital, creando una ruta de adopción eficiente y ágil alienada a los objetivos de negocio.

**OCP TECH** es una empresa estadounidense que procesa más de 150 millones de dólares al año con operaciones en todas partes del mundo. Nuclea varias compañías y cuenta con oficinas en Latinoamérica

[1] INTERPOL report shows alarming rate of cyberattacks during COVID-19, Agosto 4 de 2020, <https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19>

Ad content

por **Fabio Sánchez**

Director práctica de Ciberseguridad  
fabio@ocp.tech

# El secuestro y extorsión en la era digital

# Transformación digital segura en Salud

Entrevista al **Dr. Jairo Pérez Cely**,  
Director del Dpto. de Cuidado Crítico  
del Hospital Universitario Nacional de  
Colombia y Profesor de la Universi-  
dad Nacional de Colombia.

texto: **Javier Castro**  
video: **Basanta Contenidos**

**En Salud, el proceso de atención y la presencialidad siempre estuvieron íntimamente ligados. ¿Cómo impactó el aislamiento producido por la pandemia en este sentido?**

Como tú lo mencionas, nosotros veníamos en un formato tradicional de la prestación del servicio, donde teníamos un contacto persona a persona durante el proceso. En el momento que aparece la pandemia, se vuelve un riesgo este tipo de contacto. Por otro lado, se entra al aislamiento social como medida preventiva. Esto nos llevó a dos escenarios donde vimos la oportunidad de generar nuevas estrategias. La primera de ellas fue tener un abordaje diferente con las personas con enfermedades crónicas que no pudieron continuar con sus tratamientos o controles en hospitales o centros de alta complejidad y también personas residentes en zonas rurales. Al no permitirse el desplazamiento pudimos realizar los controles de forma remota a través de medios tecnológicos digitales.

Contenido  
audiovisual



# Aceleración Digital Colombia



Por otro lado, también pudimos continuar con la prestación de servicios de alta complejidad en patologías relacionadas o no con el COVID. Esto hace referencia a que muchas instituciones tuvieron que empezar a prestar servicio en cuidado crítico, sin tener el talento humano con experiencia, o con formación en estas áreas. Tuvimos que buscar la forma de ayudar a estos centros y a estas regiones a prestar servicios en cuidado crítico de forma remota. Entramos como Hospital Universitario y como Universidad Nacional a dar apoyo a través de nuestro programa de teleapoyo en cuidado crítico.

### **¿Cómo ha apoyado la transformación digital al programa de Telesalud y qué nuevos desafíos presenta?**

La transformación digital se volvió nuestra principal alternativa para prestar servicios de salud. Primero, desde el punto de vista de la disponibilidad de algunos servicios a los que no se podía acceder en algunas regiones. Por ejemplo, hemos habilitado en este tiempo servicios de infectología y nefrología en regiones que no contaban con ellos.

Segundo, desde el punto de vista de asistencia. Tercero, desde el punto de vista de la capacitación. Cuarto, desde el acompañamiento, durante la pandemia y luego de ella. Este acompañamiento se da en tres sentidos: en el manejo de los pacientes, de los equipos biomédicos y de la gestión general en el espacio de cuidados intensivos. Pensemos que algunos profesionales se vieron frente a un ventilador mecánico por primera vez, pues nuestra ayuda fue capacitarlos paso a paso en la operación del sistema de forma remota a través de la plataforma y en tiempo real. Desde la gestión también ayudamos a las regiones a controlar brotes en el personal de salud, entonces tuvimos que involucrarnos en el paso a paso de todo el proceso de asistencia de pacientes de COVID.

La transformación digital también nos ha traído otras oportunidades como las que tienen que ver con programas de prevención y promoción de la salud.

### **A primera vista pareciera que la Telesalud tiene como uno de sus beneficios facilitar el acceso al sistema de Salud. A tu entender ¿qué otros beneficios tiene y cuál es su principal punto débil en Colombia?**

El principal punto débil es algo muy importante a tener en cuenta y es la conectividad. En el programa de teleapoyo de cuidados críticos, pasamos revista en varias horas del día sobre el estado de los pacientes, pues no podemos esperar al día siguiente o a la siguiente semana a ver qué estrategia implementamos para que mejoren. Cuando nos vamos a comunicar, desafortunadamente no hay conexión. A veces se cae la llamada, a veces no podemos ver

imágenes. Un reto para el Ministerio TIC (Tecnología de la Información y las Comunicaciones) del país es cómo mejorar esa conectividad.

Otra debilidad es que los programas de medicina han aumentado muchísimo en el país, entonces nos toca mirar que sean seguros.

Otra debilidad es que nosotros queremos ofertar todo lo que tenemos disponible, sin embargo tal vez eso no sea lo que la región necesita. Debemos mirar las necesidades de cada una y entonces disponibilizar lo que precisan.

Otra debilidad es la cultura a través de la transformación digital, no solo en salud sino también en otras áreas. Debemos volver esta nueva forma de trabajo y educación que hemos aprendido de forma tan urgente, algo normal para seguir implementando, ya que nos facilita la prestación del servicio. Siempre digo que la telemedicina llegó para quedarse.

### **Por lo que venimos hablando, parece que la pandemia ha traído y promete nuevos avances en Telesalud en Colombia. ¿Cómo impactó la donación de Cisco por medio del programa de Country Digital Acceleration (CDA) de Colombia?**

Voy a hablar específicamente de nuestro programa de teleapoyo en cuidado crítico. Definitivamente nosotros no hacíamos esto antes. Cuando empezamos a analizar en el mes de marzo el comportamiento de la pandemia en Europa, Asia y principalmente en España e Italia donde se desbordó la capacidad hospitalaria y, específicamente, las unidades de cuidados intensivos, desde la Universidad y desde el Hospital surgió la preocupación sobre qué iría a pasar si se lograba conseguir los ventiladores que el gobierno nacional tenía proyectado conseguir, que era llegar a más de 10.000 camas de cuidado intensivo, lo cual hoy es una realidad. Nos preguntábamos quiénes iban a manejar ese tipo de equipo biomédico cuando no se había tenido esa experiencia previa. Para ello se necesita talento humano del equipo base de cuidados intensivos, que no es solamente el médico especialista en cuidados intensivos, sino también las enfermeras y todo el personal con experiencia y especialización.

Cuando planteamos esto, decidimos entrar en contacto con las regiones para ofrecerles nuestra principal fortaleza a su principal debilidad: el talento humano. Pero se presentó el problema de cómo conectarnos. Allí es donde apareció Cisco. Uno tenía la necesidad y otro como satisfacerla, Cisco puso el canal para que nos pudiéramos comunicar. Cisco nos ayudó de dos maneras: llevando equipos a diferentes regiones como Amazonas, Tumaco, Quibdó, que son áreas con muchas limitaciones de servicios. Además nos donó los equipos y sus licencias, en estas regiones que nombraba y en 22 hospitales a los hoy estamos ayudando con teleapoyo de talento humano en cuidado crítico. Con Cisco hubiéramos querido llegar a más lugares, a otras zonas más remotas aún, sin embargo no fue posible por problemas de



conectividad en la región. Desafortunadamente, la falta de conectividad en ciertos lugares es aún una realidad y hoy muestra las consecuencias. Ese es el gran aporte que nos ha hecho Cisco: haber podido implementar ese plan y poder mantenerlo en el futuro. Como siempre lo he dicho, no es solamente la pandemia y cómo nos unimos para dar respuesta a estas necesidades urgentes que nos llevaron a acelerar muchos procesos, sino también cómo mantenemos eso, porque el problema del talento humano en las regiones va a continuar con y sin pandemia. En todo eso, Cisco nos está ayudando.

**¿Hubo avances en educación de personal especializado en Salud bajo la metodología digital remota en este tiempo que todos nos vimos arrojados a la vida digital?**

Sí, claro, muchísimo. Hoy tenemos 22 hospitales a los que estamos ayudando. No tuvimos presencialidad en ninguno y los hemos ayudado a todos. El avance en capacitación y educación alrededor del cuidado crítico ha sido muy importante. Otro tema de gran relevancia es la capacitación en tiempo real. Usted está viendo al paciente, el monitor, el ventilador, puede ayudar a interpretar las gráficas, los exámenes, puede indicar cómo realizar

“

El reto ahora es mantener lo que hemos ganado y convertir en una oportunidad la pandemia para mejorar todos los servicios de salud en el país.

”

el proceso de atención. La comunicación sincrónica permite tener esa interacción con el otro profesional, que él me pregunte y yo le plantee, como experto y también como académico. La capacitación continúa todo el tiempo.

Por otro lado, desde la academia, en la educación formal en posgrado y pregrado, también estamos llevando toda la educación gracias a la transformación digital.

### ¿De qué hablamos cuando hablamos de Ciberseguridad en Salud?

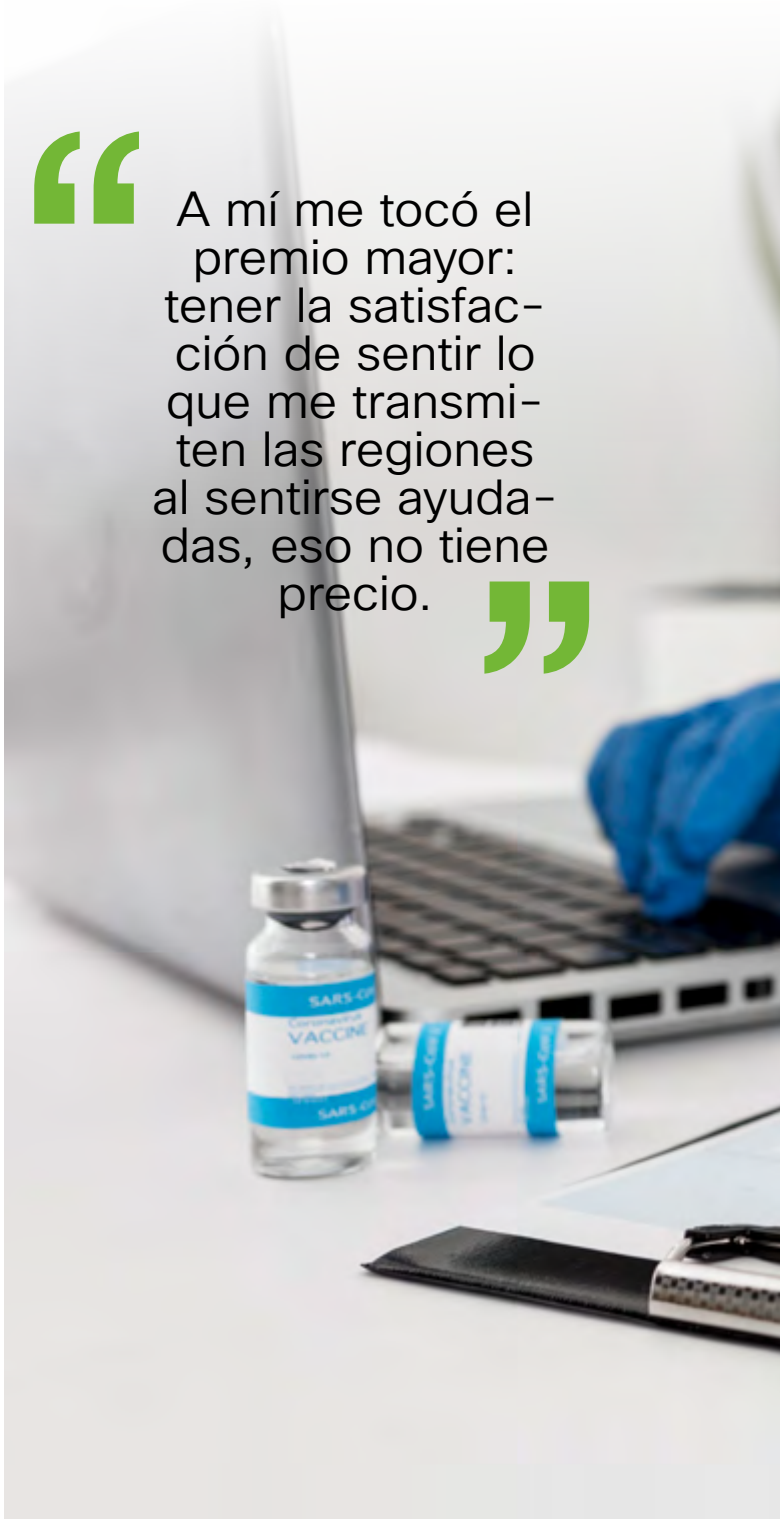
Esto para nosotros sí que es importante. Nuestro actor clave a proteger son los datos que forman luego la historia clínica de una persona. Siempre es información sobre personas y debe ser completamente confidencial. Cuando hablamos de ciberseguridad en salud, significa que los datos deben ser conocidos solamente por el profesional y el paciente, y debemos tener la seguridad de que sea así. Muchos países han sido víctimas de la ciberdelincuencia en el ámbito de la salud, eso es muy estresante para nosotros como profesionales de la salud, porque si vamos a atender a un paciente en alguna región, no podemos hacerlo desde cualquier plataforma, necesitamos garantizar, antes que nada, que esa comunicación será segura.

**Definitivamente, el principal activo a proteger durante la digitalización de los sistemas es la información. En términos médicos, tanto la información de los pacientes, como de los tratamientos y la continuidad del perfecto funcionamiento de los sistemas es crucial y altamente crítica entonces, ¿cuáles crees que son las características que debería tener una plataforma de telesalud para considerarse altamente cibersegura?**

Exactamente, el principal activo a proteger es la información. Como comentaba, lo primero que debe garantizar es que nadie más tendrá acceso a la comunicación entre el profesional y el paciente, salvo que nosotros de manera voluntaria queramos compartirla. La información debe ser netamente confidencial. Por otro lado, al menos en cuidados críticos, debe permitir la conectividad en tiempo real, ya que las decisiones que debemos tomar son inmediatas. El tercer aspecto es que nos permita guardar los datos y que podamos tener su trazabilidad para poder acceder a ellos siempre que se requiera, por supuesto, de forma altamente confidencial y bajo todas las medidas de seguridad, como sucede en toda historia clínica.

**¿De acuerdo con toda esta experiencia, cuál es el futuro a mediano y a largo plazo en Telesalud?**

Vienen retos muy importantes. Así como asumimos el reto de enfrentar la pandemia, también debemos asumir el reto de mantener estos lazos que hemos



**“ A mí me tocó el premio mayor: tener la satisfacción de sentir lo que me transmiten las regiones al sentirse ayudadas, eso no tiene precio. ”**

establecido entre muchos actores para mejorar la prestación de servicios en las regiones. Los gobiernos locales, el gobierno nacional, y los mismos hospitales han hecho importantes inversiones en infraestructura, principalmente en ampliación y prestación de nuevos servicios de cuidados críticos. Sin embargo cuando termine la pandemia seguiremos con el mismo problema que siempre hemos tenido en las regiones y es el personal altamente calificado para prestar servicios de alta complejidad. El reto es cómo mantener estos lazos y cómo seguir sumando en esto que hasta hoy vinimos haciendo. Cómo mantener estos puentes entre el hospital de la ciudad, el hospital de alta complejidad y el hospital regional, pero todo coordinado, y como mantener el puente a través de estas plataformas, como estar





Imagen: Freepik

comunicados de manera permanente para mejorar aún más la prestación de servicios. Creo que ese es el reto más importante que nos viene ahora porque el problema de no tener el personal altamente calificado va a continuar en los hospitales regionales. Entonces debe asegurarse que a través de estas tecnologías, podamos prestar ese servicio de forma remota hacia esas regiones. Creo que ahí está el reto, mantener lo que hemos ganado y convertir en una oportunidad la pandemia para mejorar todos los servicios de salud en el país.

Allí están estos lazos que hemos establecido con ustedes por ejemplo, con las regiones, con otras disciplinas o profesiones, como ingenieros, los lazos de coordinación con los ministerios. El reto es seguir sumando.

**Dr. Pérez, muchas gracias por esta conversación y por sus valiosos aportes para la salud de Colombia.**

Muchas gracias, Javier, muy amable. Gracias a ustedes también por toda la colaboración y por permitirnos llegar a las distintas regiones. A mí me tocó el premio mayor: tener la satisfacción de sentir lo que me transmiten las regiones al sentirse ayudadas, eso no tiene precio. Yo personalmente quiero agradecerles a cada uno de ustedes por haber puesto su granito de arena para que eso pueda llevarse a cabo. Muchas gracias, Javier, de verdad 🇨🇴

Ad content

# El rol de la Identidad Digital en el Proceso de Vacunación COVID-19



Entrevista a Kennedy Roman,  
Director Comercial Regional para Ca-  
ribe y Centro América de VU Security.

Contenido  
audiovisual

La irrupción en el mundo de la imprevista pandemia por COVID-19 aceleró el proceso de transformación digital en todas las áreas. En tiempos de distanciamiento social y aislamiento, la tecnología se convirtió en una aliada de Gobiernos, empresas y ciudadanos. Supo acercar soluciones, herramientas, métodos, que ofrecieron una cuota importante de seguridad a la humanidad en jaque y ayudaron a superar retos hasta hace poco difíciles de imaginar.

En este sentido, la experiencia del acuerdo sobre “Identidad Digital en el Proceso de Vacunación COVID-19”, que unió a Gobiernos de Centro América con VU Security, una compañía multinacional especializada en la prevención de fraude y la protección de la identidad, es muy interesante y motivadora, ya que muestra cómo la ciberseguridad ofrece respuestas estratégicas, seguras y sencillas

para algunas de las problemáticas medulares que enfrenta la sociedad hoy.

Kennedy Roman, Director Regional para Caribe y Centro América de VU Security, explica cómo se adoptaron soluciones del negocio más regulado, que es la banca, para acompañar al ciudadano en el proceso de vacunación, certificando la seguridad desde el momento de la identificación de las personas hasta la “farmacovigilancia”, un elemento muy significativo que las farmacéuticas ya pusieron sobre la mesa. A la vez, se logró fortalecer el nexo entre los Gobiernos y la industria tecnológica.

Desde la seguridad de su casa, el ciudadano fue invitado a cumplimentar el proceso de registrarse para la vacunación, de aceptar los términos y condiciones, entre otros pasos, accediendo a una



por Néstor Serravalle  
Global Chief Sales Officer  
VU Security

Ilustración: kotkoa/Freepik

plataforma de registro: “Nos apoyamos en nuestras aplicaciones de biométrica. El ciudadano simplemente debe digitar su número de identidad, tomarse una selfie, y completar un cuestionario de preguntas, validadas por instituciones médicas a nivel mundial. Comunica si padece alguna enfermedad crónica o alergias, dónde vive, fecha estimada para vacunarse, entre otros datos”. A partir de esta información, se establece la segmentación, orden de prioridad, grupos de interés y condiciones de salud de la ciudadanía; se genera la cita para la vacunación; y posteriormente se monitorea la evolución y posibles efectos secundarios de cada persona.

Kennedy Roman agrega: “La identidad digital es la base para la construcción de este proceso. Además de validar al ciudadano, se lo relaciona con el lote de vacuna aplicado y se desarrolla la estrate-

gia de farmacovigilancia y monitoreo de efectos secundarios. El proceso nace digital y se mantiene digital. Esto ha cambiado todo el sistema de programas de vacunación, que era manual”.

Destaca que se logró generar flujos para todos los segmentos: “Muchos Gobiernos dudaban sobre el proceso digital en lugares con brechas de tecnología y temas de conectividad. Sin embargo, a través de distintas plataformas, el ciudadano puede autenticarse y enrolarse. Con un dispositivo móvil básico, cualquier persona puede convertirse en un multiplicador de enrolamiento, ayudando a familiares, vecinos, compañeros de trabajo. La comunidad está unida en esta pandemia”.

El foco de la ciberseguridad es hacer un mundo más seguro, más sencillo y, especialmente, que los beneficios que el universo digital trae aparejado alcancen a toda la comunidad 📌



Protección de datos:  
Cómo poner la seguridad  
cibernética al servicio de

**LGPD**

por: **Fernando Zamai**



La Ley General de Protección de Datos (LGPD), una especie de versión brasileña del Reglamento General Europeo de Protección de Datos (GDPR), entró en vigor el 18/9. La Ley considera datos confidenciales cualquier información que permita la identificación, directa o indirectamente, de una persona física que se encuentre viva y considera como datos personales: nombre, DNI, CPF, sexo, fecha y lugar de nacimiento, teléfono, domicilio, ubicación vía GPS, retrato, en fotografía, registros sanitarios, ingresos de tarjetas bancarias, etc.

Esto convierte a las organizaciones que operan en suelo brasileño en guardianes de esta información confidencial y la pone en la mira de una multa que puede llegar a los 50 millones de reales. En octubre, casi dos meses después de la entrada en vigor de la ley, las primeras decisiones sobre la LGPD ya estaban ganando publicidad. La Justicia ha estado considerando, principalmente, el intercambio indebido de datos y, en consecuencia, la falta de protección de los datos personales.

LGPD alcanzó a un mercado que prácticamente no estaba preparado para esta nueva realidad. En medio de la pandemia y con la creencia de que la fecha volvería a posponerse, las empresas aún están adaptando los procesos administrativos, operativos y legales. También se ha vuelto urgente un análisis en profundidad de la infraestructura de ciberseguridad para un uso efectivo de la tecnología que busca proteger la base de datos de los clientes.

Hablando de infraestructura tecnológica, la pandemia COVID-19 obligó a las empresas a poner a buena parte de sus empleados a trabajar desde casa, es decir, con acceso remoto a servidores corporativos y sin las protecciones tradicionales entregadas a las organizaciones. Esto aumentó la tasa de vulnerabilidad, lo que hizo que 2020 supere el ré-

cord de crecimiento anual de phishing, ransomware y otros riesgos cibernéticos.

La vida digital se ha vuelto más intensa y el anuncio de un ataque de ransomware puede incluso ser una cortina de humo para desviar la atención de algo que ya ha ocurrido y espera el momento adecuado para negociar inescrupulosamente el pago de “rescate” para evitar la divulgación parcial o total en entornos oscuros de los datos “secuestrados” de su cliente.

Entonces, ¿cómo puede la tecnología ayudar a las organizaciones a adaptarse a la LGPD? ¿Cómo preservar su imagen frente a los clientes, ya que, siendo los guardianes de la información, son vulnerables a los ciberataques?

La respuesta está en la infraestructura de ciberseguridad. Ha llegado el momento de realizar una revisión generalizada y en profundidad de los recursos disponibles internamente. Es necesario saber qué parte de la infraestructura de ciberseguridad está realmente en uso y qué tan efectiva es para protegerse contra los ataques. El control hoy es igual a costo, una cifra que puede ser alta dependiendo de la sanción que apliquen los jueces en las sentencias que consideren la LGPD.

Realice un Health Check, sin cargo, de su infraestructura de ciberseguridad. Nuestro equipo de especialistas accede de forma remota a su base a través de Webex y realiza un informe en horas. Su red privada virtual (VPN) no puede exponerse. Por ello, recomendamos controles avanzados integrados con el servicio de inteligencia internacional Talos, para que no solo tenga dominio del entorno de TI que soporta datos protegidos por LGPD, sino que también cuente con un canal seguro en caso de problemas. Comuníquese con un especialista de Cisco |

# Resiliencia de la fuerza laboral: extiende la seguridad a sus trabajadores remotos

por Juan Pablo Mongini

Algunos eventos son tan perjudiciales que nos obligan a repensar todo. Pero, con frecuencia, son una bendición disfrazada. Todo tipo de innovaciones surgen de preguntas como “¿Hay una mejor forma de hacer esto?” y “¿Realmente deberíamos hacer aquello?”.

Por ejemplo, muchas empresas pensaban que era imposible que toda su fuerza laboral cumpliera sus objetivos sin trabajar en la oficina. Pero, veamos lo que sucedió, frente a enormes cambios, nuestros empleados prosperaron. Muchos descubrieron que son más productivos en el hogar que en la oficina. Se beneficiaron de pasar más tiempo con sus familias y menos tiempo en estresantes y largos traslados hacia su oficina. Un estudio reciente concluyó que “casi el 90% de los empleados preferiría continuar trabajando desde casa en alguna capacidad y casi la mitad desean trabajar desde casa más a menudo o todo el tiempo”.

Las empresas también se vieron favorecidas con empleados más productivos, la reducción de gastos operativos (con oficinas vacías, sin reuniones de trabajo y sin viajes) y revalorizaron el acceso a personal calificado distribuido.

Esto plantea la pregunta: ¿es hora de rediseñar la red empresarial? Ya sea que su empresa requiera o no que sus empleados trabajen in situ, es probable que algunas veces tengan que trabajar remotamente. Incluso desde la perspectiva de la resiliencia empresarial, cuando suceda otro evento disruptivo, su organización debe tener la capacidad de extender su red de forma segura a todos los usuarios, independientemente de dónde se encuentren.

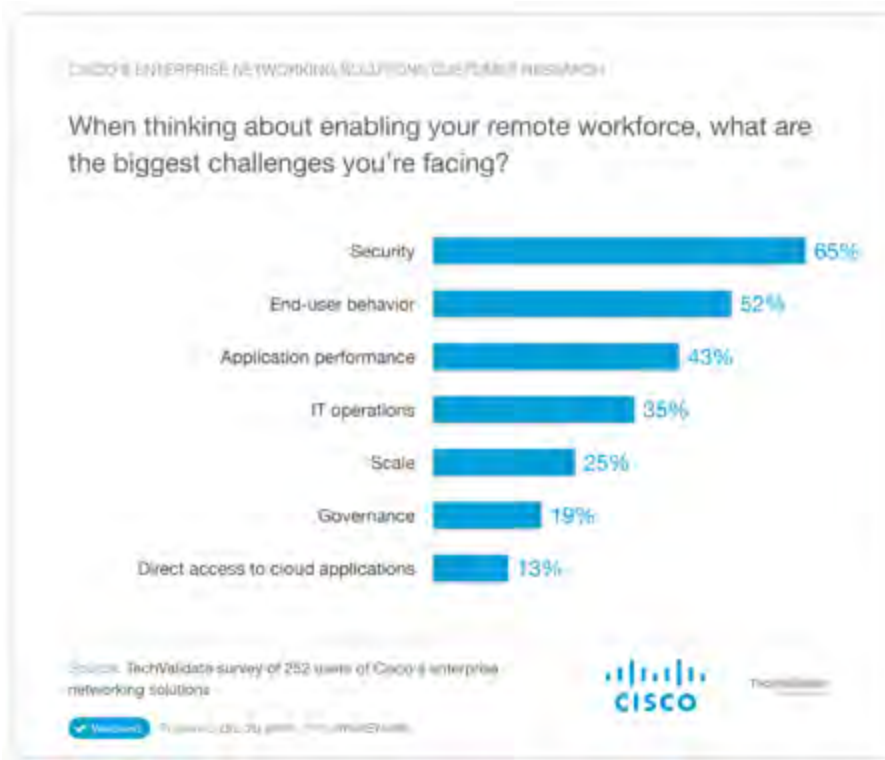
Suena fácil, parece bastar con ampliar su VPN, añadir unas cuantas aplicaciones en la nube y permitir que los empleados trabajen en cualquier sitio.

Lamentablemente, habilitar el trabajo remoto supone nuevos desafíos. El empleado remoto no siempre tiene el ancho de banda que consumen las aplicaciones empresariales de alta calidad. Asimismo, no siempre (cómo puedo decir esto sutilmente...) cuentan con las mejores prácticas de seguridad. Ingresan a redes no confiables, hacen click a enlaces de *phishing*,



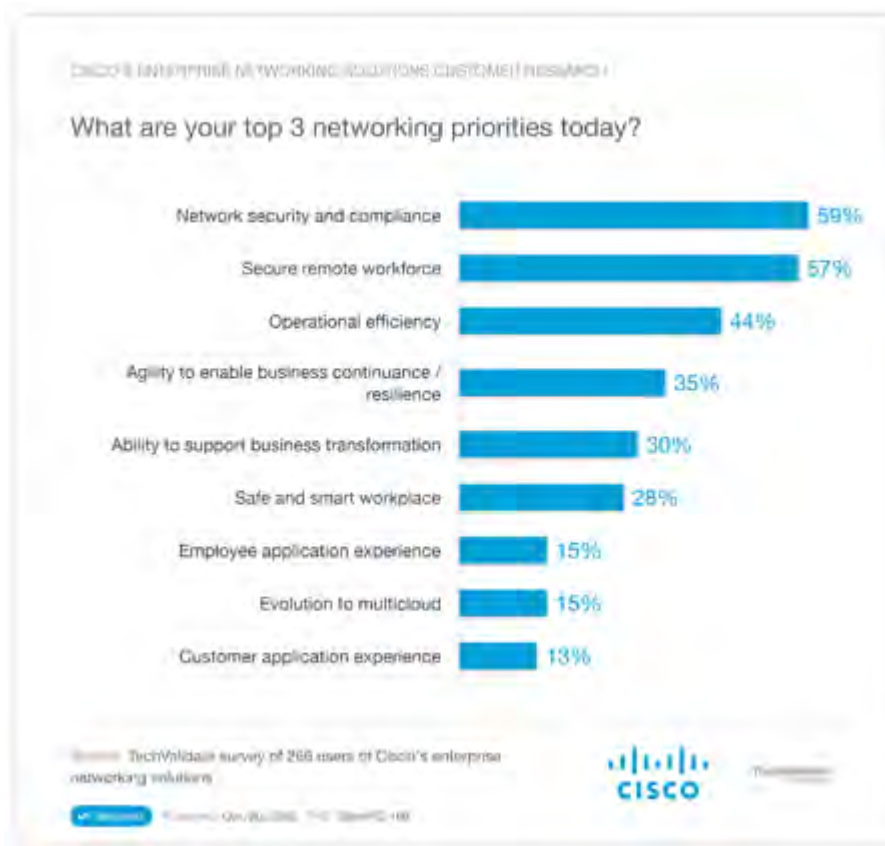
usan sus dispositivos personales y descargan aplicaciones no autorizadas (¿TI paralela?). Ni siquiera pensemos en casos como el usual "Password1". Y, solo porque usan una VPN, quizá los empleados

ni siquiera se dan cuenta de cuánto tráfico generan en la red empresarial al ejecutar aplicaciones no empresariales como YouTube, Netflix, FaceTime o Spotify.



En una reciente encuesta a clientes de Cisco, los comportamientos del usuario final presentan el segundo desafío más grande que el personal de TI tiene que encarar con respecto a la fuerza de trabajo remota. (La seguridad siempre gana en esta contienda).

Gráfica de desafíos que implica la fuerza laboral remota



Esta misma encuesta, realizada en septiembre, encontró que el 57% de las organizaciones afirmó que la seguridad de su fuerza de trabajo remota era una prioridad importante, un aumento del 23% contra el periodo antes de la pandemia. Es decir, solo cinco meses antes del éxodo de las oficinas en marzo.

Gráfica de las 3 principales prioridades de la red.

¿Qué podemos hacer? El área de TI debe implementar estrategias para ampliar la conectividad a la red de empleados remotos que trabajan desde casa o en microoficinas de forma segura, brindarles una experien-

cia ideal con aplicaciones, mediante soluciones administradas centralizadamente. TI debe brindar a los trabajadores remotos el mismo nivel de protección, gobernanza y rendimiento que disfrutaban en la oficina.



## Requisitos de la red para trabajadores remotos con seguridad empresarial

### Escalar las VPN para proteger a los empleados remotos

Las VPN son definitivamente una opción para ampliar el control a nivel empresarial y proteger a los empleados remotos. Los túneles divididos pueden también ayudar a reconectar las aplicaciones empresariales críticas con la red corporativa y desviar de internet las aplicaciones no empresariales.

### Mejor conectividad: puntos de acceso corporativos en el hogar

¿Desea llevar la experiencia a un nivel completamente nuevo? Los empleados que usan un punto de acceso corporativo justo detrás de su router personal no necesitan usar una VPN. Esta opción también optimiza las aplicaciones de voz y video y permite que los usuarios se conecten eficientemente desde diversos dispositivos como teléfonos IP y puntos terminales de video.

### El modelo Secure Access Services Edge (SASE) protege las aplicaciones multinube

La seguridad basada en la nube y el modelo SASE ayuda a defender contra las amenazas en Internet, independientemente de la conexión, el dispositivo o el entorno de nube que use el usuario.

## Conclusión

Al replantearse qué medidas serán necesarias para recuperarse ante cualquier interrupción, los empleados se sitúan en el epicentro. Extender la red a dondequiera que los usuarios estén, si bien no es fácil, es el futuro. Después de todo, la red brinda a nuestros empleados acceso seguro a las aplicaciones y los datos que requieren con el alto rendimiento que esperan, ya sea que trabajen desde casa o en la oficina

- 📶 Lea las cinco principales [tendencias de redes para 2021 en relación con la resiliencia empresarial](#).
- 📶 Conozca cómo puede [conectar a sus empleados que trabajan desde casa de forma segura](#).
- 📶 Conozca [las soluciones de redes de Cisco para garantizar la continuidad empresarial](#).

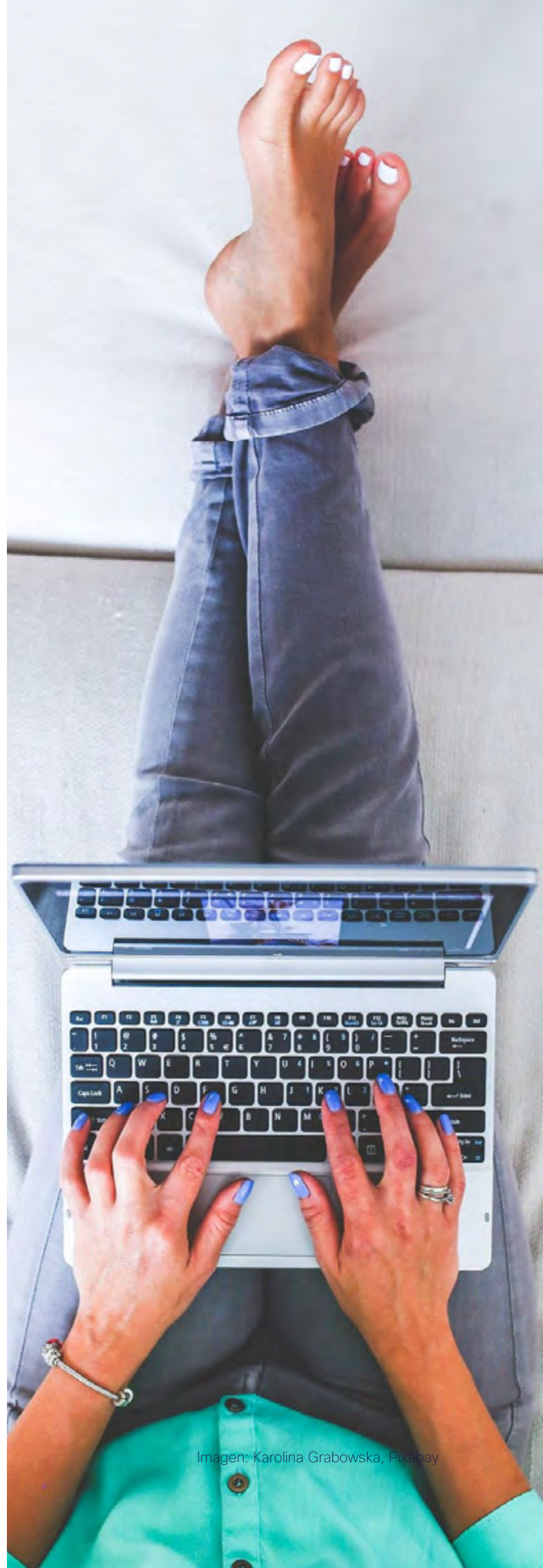


Imagen: Karolina Grabowska, Pixabay

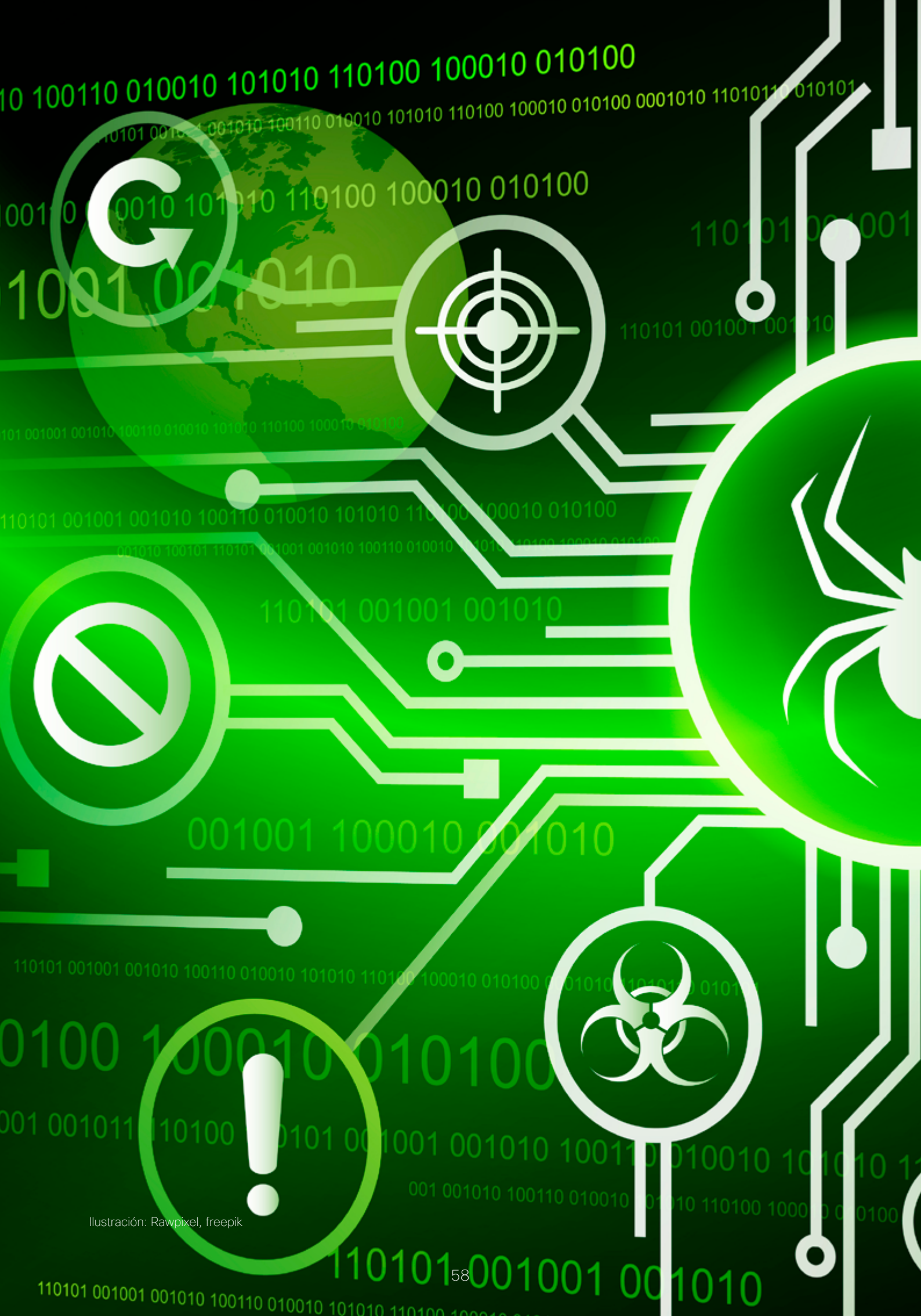


Ilustración: Rawpixel, freepik

# Guerra cibernética

por Marcelo Bezerra

En 2015, el presidente de China, Xi Jinping, y el entonces presidente de Estados Unidos, Barak Obama, firmaron lo que se considera el primer convenio entre naciones para controlar las acciones de ciberataques en la historia. En virtud del acuerdo, ambos países estipularon no patrocinar acciones de espionaje industrial y robo de actividad intelectual. El histórico pacto indudablemente nos lleva a pensar en lo que convencionalmente llamamos ciberguerra.

Hacer la guerra a través de Internet ha sido parte de nuestra imaginación durante mucho tiempo, gracias a las películas de Hollywood y a algunos hechos destacables como el famoso caso del virus Stuxnet, creado en 2010 especialmente para atacar los sistemas de control de las centrifugadoras de enriquecimiento de uranio de Irán. Aunque no trata literalmente de la ciberguerra, el acuerdo entre Estados Unidos y China confirmó lo que en 2015 aún no se admitía públicamente: que los países patrocinan acciones ofensivas a través de Internet contra otros países, enemigos o no.

Hoy la situación es bastante diferente. No solo sabemos que las acciones existen, sino también que son públicamente parte de la estrategia militar de varios países. En septiembre de 2019, el Departamento de Defensa de Estados Unidos publicó su plan estratégico con el propósito de utilizar armas cibernéticas para promover los intereses y la defensa de Estados Unidos. En el Reino Unido, un general confirmó que el país tiene armas para “degradar, interrumpir y destruir” infraestructura crítica, si fuera necesario en caso de guerra.

El tema, sin embargo, no es consensuado. Hay mucha discusión sobre lo que lo que se consideran un arma y una guerra cibernética, especialmente si tenemos en cuenta que las armas más sofisticadas de la actualidad incorporan cualquier número de sistemas y componentes electrónicos. Para el ex asesor del gobierno de EE.UU. Richard A. Clarke, autor del bestseller “Cyber War”, (2010), la ciberguerra se define como acciones patrocinadas por un estado nacional para penetrar redes o computadoras de otras naciones con el fin de causar daños o sabotajes. A la luz del mundo interconectado globalmente, la definición no deja dudas de que muchas acciones emprendidas o patrocinadas por un estado podrían considerarse entonces un acto de guerra.

## Inteligencia de amenazas para seguir el tema de cerca

Muy recientemente, dos acciones se han hecho públicas y se han atribuido a países, aunque no fueron admitidas por ellos. La primera fue la invasión a la empresa de seguridad FireEye y el robo de software creado por sus expertos para utilizarlo en sus contratos de consultoría. El hecho de que la empresa informara que no existía ninguna técnica o *malware* para explotar vulnerabilidades desconocidas entre el material robado no disminuye su importancia. La segunda fue el descubrimiento del compromiso del software de gestión ampliamente utilizado por empresas y organismos estatales del fabricante SolarWinds. Nuevamente asignado a un país y nuevamente no admitido.

Dos artículos en el blog de Talos, en <https://blog.talosintelligence.com>, ayudan a comprender los ataques y sus efectos potenciales. Talos, actualmente la organización privada más grande de inteligencia sobre amenazas, parte de Cisco Secure, ha estado siguiendo de cerca el problema. El equipo analizó una acción de espionaje contra diplomáticos con sede en Chipre, que identificó una campaña aún más amplia, que llegó a 40 organizaciones diferentes. Los ataques de los países suelen ser muy sofisticados y conllevan una variedad de riesgos si se filtran y atacan computadoras más allá de su objetivo inicial. El grupo también revisa continuamente la seguridad de los sistemas de infraestructura crítica, probablemente el mayor objetivo en caso de una acción de guerra real.

Los ataques de los países suelen ser muy sofisticados y conllevan una variedad de riesgos si se filtran y atacan computadoras más allá de su objetivo inicial. El grupo también revisa continuamente la seguridad de los sistemas de infraestructura crítica, probablemente el mayor objetivo en caso de una acción de guerra real.

## Armas cibernéticas: con el foco en las vulnerabilidades

La tecnología empleada en la guerra cibernética tiene características únicas. A diferencia de las armas tradicionales, un arma cibernética no tiene potencial destructivo. Su impacto dependerá del sistema atacado. Imagínese un programa de ataque capaz de penetrar en una computadora y permitir que se controle de forma remota. ¿Cuál es el efecto? Si está en nuestras casas, perderemos unos cientos de fotos, pero ¿y si es la computadora que controla el funcionamiento de una industria? ¿Y si se trata de una planta de energía nuclear? El efecto de un ciberataque también se desconoce hasta que ocurre, sin embargo, es posible que la víctima logre cubrir parte del impacto. Desde ese punto de vista parece un arma ineficaz, pero eso mismo es lo que la hace tan atractiva. Es totalmente fría. No hay explosiones ni muertes aparentes. No hay escenas emocionales ni soldados muertos. Es invisible y puede penetrar búnkeres completamente a prueba de ataques, incluso nucleares, por ejemplo a través de una simple memoria USB de un empleado desatento. Y, lo que es más importante, se puede negar fácilmente. Es poco probable que una nación pueda tomar represalias basándose únicamente en un ataque a sus sistemas informáticos, ya que los ataques bien hechos son difíciles de rastrear. ¿Cómo tomar represalias si no hay certeza absoluta?

Las armas cibernéticas tampoco se almacenan. En una guerra tradicional, el oponente con mayor cantidad de armas y mayor poder destructivo obtiene una clara ventaja. En la guerra cibernética no hay armas y, como ya se mencionó, su potencial de destrucción depende de su objetivo. Un ciber arsenal también es diferente porque está compuesto de técnicas y conocimientos. Las técnicas son las vulnerabilidades existentes en los sistemas y los programas de intrusión capaces de explotarlos. Cuanto más desconocidas, más valor tienen estas vulnerabilidades, llamadas día cero. Los programas son generalmente porciones de código de programación intercambiable que se pueden usar en diferentes situaciones para explorar vulnerabilidades. También existen programas específicos para evadir los sistemas de defensa digital, como los firewalls. Estas diferentes piezas de código se combinan luego en kits de ataque, sistemas de invasión complejos como en el mencionado caso de Stuxnet. Y para llevarlas a cabo solo es necesario el conocimiento de "genios" en informática, los hackers. Esta herencia intelectual es la base de la "reserva" de la guerra cibernética. Sin ella no hay ataque ni defensa. En una guerra totalmente científica, se cuentan los cerebros, no las ojivas |

# Spoiler Bridge N°4

## Hackeando Predicciones

Pasado pisado. Futuro, ¿hackeado? Cuando las predicciones no son buenas, podemos intervenir para desviar su rumbo. ¿Cómo podemos colaborar, reuniendo esfuerzos entre el sector público, privado y los proveedores de tecnologías y servicios de ciberseguridad? ¿Qué aporte hacen compañías como Cisco en el mundo para hacer posible una vida y economía digital resiliente?



En esta producción audiovisual y escrita, Juan Marino, Gerente Regional de Ciberseguridad de Cisco, hace un repaso por las principales predicciones de los analistas del mercado y da pistas para “hackearlas” o cumplirlas según convenga.

### Entrevistas

**Ángel Thomas Paulino C.**, CISO de Banco Caribe y Presidente del Comité de Ciberseguridad en la Asociación Bancos Comerciales de la República Dominicana (ABA).

**Juanita Rodríguez Kattah**, Vicerrectora de Innovación Académica Universidad EAN, Colombia.

### Ping Pong de preguntas y respuestas con Gary Becklund

En este encuentro, el líder que últimamente se desempeñó como Chief Operating Officer and Managing Sales Director, Americas Cybersecurity en Cisco, hace un repaso de sus veinte años de carrera en Cisco y comparte su experiencia y aprendizaje.

# Braycom

## Construimos Soluciones



Solucionamos las necesidades de negocio **aplicando tecnología.**

### Ciberseguridad

Diseñamos estrategias de ciberseguridad.

### Colaboración

Telefonía IP, Telepresencia.

### Cómputo

HCI, Storage, Backup.

### Networking

ROUTING/ SWITCHES/ WIRELESS.



Make **IT** Happen  
Consultanos.

