Año 1. Número 4.

# Bridge

cisco SECURE

Ciberseguridad

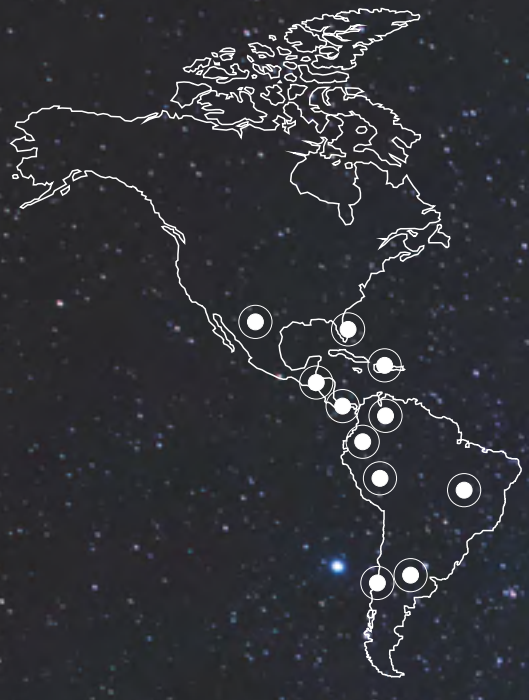
## Costa Rica
Con los ojos puestos en la Ciberseguridad

Especial
**Líderes en Ciberseguridad**

Conoce a **Laércio Albuquerque**
VP Cisco Latinoamérica

Contenido audiovisual

cisco The bridge to possible



# OCP TECH

## INGENIERÍA CONVERGENTE PARA SOLUCIONES PRÁCTICAS

*Expertos en soluciones de ciberseguridad*

CISCO Partner

OCP TECH

OCP.TECH


**US**

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

T +1.305.537.0800
F +1.305.537.0704

info@ocp.tech

**Panamá**

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

T +507.387.7300

**Taiwan**

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

T +886.953.656.967

# Editorial

Imagen: Adrien Tutin, Unsplash.

La vida es tal en tanto movimiento y cambio. Lo contrario es durar sin alteración, insistir en sostener lo estático y evitar el riesgo de lo impredecible, lo que no podemos asir como seguro. Estamos inmersos en procesos que nos despabilan, agitan y mutan. Cambia el entorno, cambiamos nosotros y al revés. Hay cambios que suceden de forma lenta, otros más drásticos, que exigen toda nuestra atención y creatividad. Los hay imperceptibles y ondulantes o enérgicos y vapuleantes. Somos en el cambio, por eso es tan importante acompañar ese proceso con un liderazgo sólido y confiable, sea propio e interno o proveniente de otra persona.

Definimos a un líder como aquella persona responsable de hallar el potencial en individuos y procesos y contribuir para llevarlo a cabo. Quien se atreve a la acción hacia un objetivo y construye una cultura de valentía donde "la armadura no sea necesaria ni recompensada". Quien acompaña en el recorrido y aporta positivamente. Quien insiste en soportar su creencia. Quien acepta el fracaso si sucede y se sobrepone enérgicamente a él, capitalizándolo.

En esta edición de Bridge damos un lugar destacado al concepto de liderazgo porque entendemos que el ¿quién? tiene la fortaleza de movilizar y producir aquello bueno que se busca. Por eso, toda la producción está cruzada por mujeres y hombres que llevan adelante equipos y procesos que requieren integrar en conciencia y acción la debilidad y la fortaleza en el camino de alcanzar un objetivo claro y bien definido. Cada cual con su estilo, guían, acompañan, son faro o soporte del todo hacia la meta.

Te invito a la aventura de conocerlos, ser testigo de sus experiencias y receptor de sus enseñanzas. Buen viaje.

Karina Basanta

# Staff


## Producción Integral
## Basanta Contenidos

Directora Editorial
Karina Basanta

Director de Arte
Nicolás Cuadros

Coordinadoras
Marta Pizzini
Marta Assandri

Producción audiovisual
Salpufilms

Locución
Loli Fahey

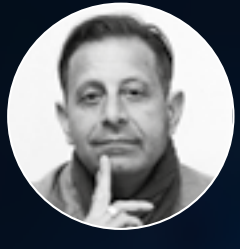
Colaboran en este número
Silvia Montenegro
Jorge Prinzo
Claudia Menkarsky
Freddy Macho
Soledad Clar

Fotografía e ilustración
Basanta Contenidos
Freepik
Pixabay
Unsplash

Agradecimientos
Jorge Cuadros
Isabella Cacciabue
Joaquín Cuadros
Nicolás Cacciabue
Santino Cuadros
Rodolfo Basanta

Foto de Tapa
Zdenek Machacek, Unsplash


Directora Editorial
Karina Basanta



Director de Arte
Nicolás Cuadros


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



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


Ilustración: Daniel Roberts, Pixabay.

## Cisco Latinoamérica

Cyber Security Director,
Americas Service Providers
and Latin America at Cisco
**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**
Adriano Gaudencio
Leticia Gammill
Jackeline Carvalho
María José Jiménez Domínguez
Nelson Brito
Militza González

## Marketing

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

Bridge Nº 4

# Sumario

# 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.

Braycom

in f **braycom**.com **ARG** *Bs As - Salta - Rosario - Córdoba* | **CHL** *Santiago de Chile* | **COL** *Bogotá* | **USA** *Miami*

# Lo Nuevo


Contenido audiovisual

**Drixit Technologies** revoluciona la industria al digitalizar y automatizar los procesos industriales. Gracias a su EPP digital, una solución IoT que combina *hardware* y *software*, mitiga y previene accidentes y logra potenciar la eficiencia operacional.

El EPP digital, compuesto por el Drixit Tag y Drixit Platform, viene con múltiples funcionalidades personalizables según las necesidades.

Para la seguridad de los equipos, el Drixit Tag está equipado con un botón antipánico, que brinda asistencia en el momento y lugar adecuados. Además, detecta y notifica de forma inmediata alturas de riesgo, caídas y golpes fuertes, gracias a la ubicación en tiempo real tanto en interiores como en exteriores.

A través de la Plataforma Drixit se pueden crear zonas con control de acceso automático, protegiendo a los equipos de entornos peligrosos. Además, cuenta con mapas históricos de información a fin de saber qué pasó y por qué, mejorando la seguridad y gestión de los equipos.

Finalmente, la plataforma mantiene los datos y análisis de la operación en un solo lugar, integrada con todas las plataformas, alarmas y sensores existentes, con el fin de tomar mejores decisiones e impulsar la operación

# Cisco

## La mejor empresa para trabajar en México

•Por cuarto año consecutivo recibe esta distinción.

•Para Cisco el eje central de la compañía lo componen sus empleados; ser certificados por Great Place to Work es sumamente importante para conocer las opiniones directas de los colaboradores.

CIUDAD DE MÉXICO, 14 de mayo de 2021.- Cisco obtuvo el primer lugar en el listado de Mejores Empresas para Trabajar realizado por Great Place to Work (GPTW) donde se consideran organizaciones con más de 500 empleados hasta 5,000. Por 12 años Cisco ha recibido esta certificación.

Great Place to Work Institute es una organización internacional que evalúa y certifica los ambientes de trabajo a través del análisis de datos obtenidos de encuestas respondidas directamente por los empleados de las organizaciones participantes.

Las áreas consideradas por Great Place to Work Institute para la certificación son: credibilidad, respeto, imparcialidad, orgullo y compañerismo. Adicionalmente, el Instituto analiza políticas, prácticas y procesos para cada una de las empresas participantes.

Para los integrantes de Cisco México, el orgullo y el compañerismo los destacan como los elementos más importantes que existen dentro de sus equipos de trabajo.

En opinión de Isidro Quintana, Director General de Cisco México, cada persona que integra la empresa es de suma importancia, son quienes constituyen Cisco. “Mantenemos una cultura consciente, en la cual nos preocupamos profundamente por ofrecer una experiencia positiva para todos, en la que el trabajo colaborativo y diverso permite generar nuevas ideas y explorar nuevas posibilidades para aprovechar el poder de la transformación digital e inspirar a la innovación”. Agregó que el ser reconocidos por cuarto año consecutivo el primer lugar por GPTW “nos compromete aún más para seguir mejorando nuestro ambiente laboral y sobre todo tener integrantes orgullosos por pertenecer a Cisco y con un fuerte compromiso por retribuir al entorno en el cual nos desempeñamos”

## Nombrada “Mejor empresa de seguridad” por SC Awards 2021

SC Media nombró recientemente a Cisco “Mejor empresa de seguridad” como parte de sus premios SC Awards 2021. “Este premio representa años de innovación y compromiso con la ciberseguridad además de la búsqueda constante para hacer que la seguridad sea menos compleja, más ágil y capaz de defender de las amenazas de hoy y de mañana”, indica Ghassan Dreibi, Cybersecurity Director, Americas Service Providers and Latin America at Cisco.
Como la empresa de ciberseguridad corporativa más grande del mundo, Cisco lidera con soluciones, que están impulsando la industria en SASE, XDR y Zero Trust. Cisco SecureX, su plataforma de seguridad integrada reúne a la perfección una amplia variedad de herramientas otorgando simplicidad, visibilidad y eficiencia a toda la infraestructura de seguridad de una organización. Además, a través de su centro de inteligencia de amenazas de clase mundial, Cisco Talos, respalda la operación de sus clientes manteniéndolos al día sobre el panorama de la ciberseguridad.
Adicionalmente al reconocimiento de “Mejor empresa de seguridad”, Cisco también ganó el premio SC Media a la “Mejor solución de seguridad para pequeñas y medianas empresas (pymes) basada en la nube, Cisco Umbrella y fue nombrada “Mejor solución de control de acceso ( NAC) a partir de su producto Cisco Identity Services Engine (ISE)

# Principios Rectores para la Ciberseguridad Ciudadana.

El pasado 15 de junio de 2021 se produjo el lanzamiento de los Principios Rectores para la Ciberseguridad Ciudadana, documento generado por el Laboratorio de Ciberseguridad de los Poderes Legislativos de la Organización de los Estados Americanos (OEA).

Estos postulados son el resultado de un esfuerzo co-creativo entre legisladoras y legisladores, asesores parlamentarios, expertos del sector privado en los campos de la ciberseguridad y la transformación digital, así como de académicos y líderes de sociedad civil, quienes bajo la coordinación del Laboratorio en materia de Ciberseguridad para los Poderes Legislativos, identificaron 10 lineamientos básicos para que todo Estado impulse la creación de políticas públicas, legislaciones, marcos normativos y reglamentos que le ofrezcan a las y los ciudadanos una mejor protección en su interacción con las actuales infraestructuras tecnológicas, como son la Internet, las redes sociales y los sistemas y/o plataformas de la información y de la comunicación

# Los 10 Principios Rectores de la Ciberseguridad Ciudadana son:

1. Resguardar y proteger los derechos y libertades individuales.
2. Preservar la soberanía en la democracia digital.
3. Consagrar la libertad de expresión y la privacidad por defecto en el ciberespacio.
4. Impulsar una cultura de la ciberseguridad.
5. Construir un entorno ciberseguro.
6. Asegurar la privacidad de los datos.
7. Establecer la responsabilidad compartida.
8. Fortalecer el desarrollo de aptitudes y habilidades.
9. Incorporar la educación para la vida en el ciberespacio.
10. Involucrar al ciudadano en los proceso de creación de marcos normativos que impulsen la innovación y la transformación digital.

Contenido Audiovisual

# Ciberseguridad que mejora la experiencia de usuario


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

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

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

# Entrevista

**Laércio Albuquerque**
VP Cisco Latinoamérica

Laércio Albuquerque es responsable de liderar la estrategia de la empresa para fomentar la innovación y la digitalización en toda la región. Apoyado por el equipo local y el ecosistema de partners de Cisco, se centra en ofrecer resultados positivos para los clientes, el gobierno y la sociedad, ayudándolos a resolver problemas, mejorando su productividad y negocios, y creando un mundo más inclusivo mediante el uso de la tecnología.

## ¿Qué significa para ti liderar América Latina desde una corporación mundial como Cisco?

Para mí, liderar Cisco Latam es un honor y un reto maravilloso. Estamos en una coyuntura regional muy interesante, apoyando hoy más que nunca a todos nuestros clientes en sus procesos de transformación digital. La pandemia demostró que la tecnología juega un papel crucial en los negocios, y que es necesaria para mantener de forma exitosa las operaciones en la economía digital.

Cisco tiene un compromiso firme, a largo plazo, con nuestra región a través de inversiones estratégicas y alianzas en todos los países. Estamos ahora en una posición única para impactar positivamente a empresas y organizaciones de cualquier tamaño, pequeñas o grandes, así como a la vida de millones de personas, aprovechando al máximo nuestras soluciones tecnológicas de primer nivel y nuestros programas de clase mundial como Cisco Networking Academy, que ha brindado habilidades digitales a casi 3 millones de personas en América Latina desde sus inicios; nuestras poderosas iniciativas sobre diversidad e inclusión y nuestros programas de aceleración digital para varios países, solo por nombrar algunas de las grandes cosas que nos distinguen como líderes de la industria.

## ¿Cuáles son los próximos pasos en tu gestión?

Mantener una escucha activa con nuestros clientes para apoyarlos y asistirlos en sus desafíos de negocio, que van desde el trabajo híbrido hasta retos en el manejo de datos y aplicaciones en forma segura. Al mismo tiempo, trabajamos de la mano con las comunidades y países donde operamos, llevando programas de educación en TI y otras iniciativas de responsabilidad social que tengan un impacto positivo en las personas.

A lo interno, seguir construyendo y liderando un equipo de clase mundial como el que tenemos en Cisco Latinoamérica, dándoles la visión y el apoyo para que sean los mejores asesores estratégicos de sus clientes. Y para que sigan sintiéndose orgullosos de lo que logran y de ser parte de un gran equipo humano.

por **Karina Basanta**

## ¿Cuál es el principal desafío?

Nuestro principal desafío como empresa líder en la región es mantenernos relevantes en la industria. Ir a la cabeza del mercado en los países, entendiendo sus transiciones y capturando todas sus oportunidades:

· Seguridad en la nube para ofrecer acceso a data, procesos y aplicaciones;

· Soluciones tecnológicas que apoyen la producción de bienes y la prestación de servicios;

· Una red robusta, segura que permita la conexión rápida y eficiente de personas y dispositivos, y que ayude a resolver exitosamente retos de negocio como la educación y el trabajo híbridos.

Si sabemos adelantarnos a lo que viene y actuamos en consecuencia, será más sencillo mantenernos en el camino hacia el éxito, enfocándonos siempre en lo que necesitan nuestros clientes y la experiencia que viven al trabajar con nosotros.

## Si digo la palabra ciberseguridad, ¿cuál es tu primera aproximación?

Ciberseguridad es la base de todo lo que ocurre en la economía digital. Debemos preguntarnos ¿por qué ciberseguridad? Para mí la respuesta es: porque debemos poner todo nuestro esfuerzo en enfrentar el terrorismo cibernético, que se ha convertido en un negocio multimillonario, poniendo en riesgo y afectando severamente países, servicios públicos, industrias, datos y personas.

Sin un contexto cibernéticamente seguro, los procesos de transformación digital que están atravesando muchos sectores, en especial producto de la pandemia, se pueden ver afectados. Vamos hacia un mercado global de 50 mil millones de dispositivos conectados, por lo tanto, puede haber 50 mil millones de agujeros de seguridad que debemos cerrar. Debemos entender la relevancia de esta situación y el rol que cumplen las regulaciones globales, regionales y locales para prevenir y atacar la situación.

Para Cisco, la ciberseguridad es un tema que abordamos de forma integral en varias dimensiones: trabajamos con gobiernos y autoridades para proveer conocimiento, experiencia y educación en ciberseguridad; ofrecemos a clientes de todos los sectores y tamaños soluciones y tecnología de punta para asegurar sus procesos de negocio; y estamos en constante innovación de nuestro portfolio, diseñado y construido sobre la base de una tecnología segura de punta a punta.

## Qué nuevo planteos trae Cisco a Latinoamérica en términos de seguridad y ciberseguridad.

Para nosotros es crítico ir a la vanguardia en estos temas de ciberseguridad. Estamos impulsando SASE (Secure Access Service Edge) que combina

funciones de red y seguridad en la nube para brindar un acceso seguro y sin problemas a las aplicaciones, en cualquier lugar donde trabajen los usuarios. El modelo SASE tiene como objetivo consolidar estas funciones en un único servicio integrado en la nube. Cisco proporciona todos los componentes básicos de una arquitectura SASE, reunidos en una única oferta.

Por otro lado, seguimos enfocados en Zero Trust, un modelo completo de seguridad de confianza cero, que permite mitigar, detectar y responder a los riesgos en las organizaciones, a fin de evitar incidentes de falsificación de credenciales, por ejemplo, en un modelo de trabajo híbrido.

Todos estos programas y soluciones de seguridad cuentan con el respaldo de inteligencia de amenazas de clase mundial de Cisco Talos, el mayor centro privado de inteligencia de amenazas global, que mantiene a los clientes y los actores de la industria al día con el panorama de la ciberseguridad, no solo en Latinoamérica sino en el mundo.

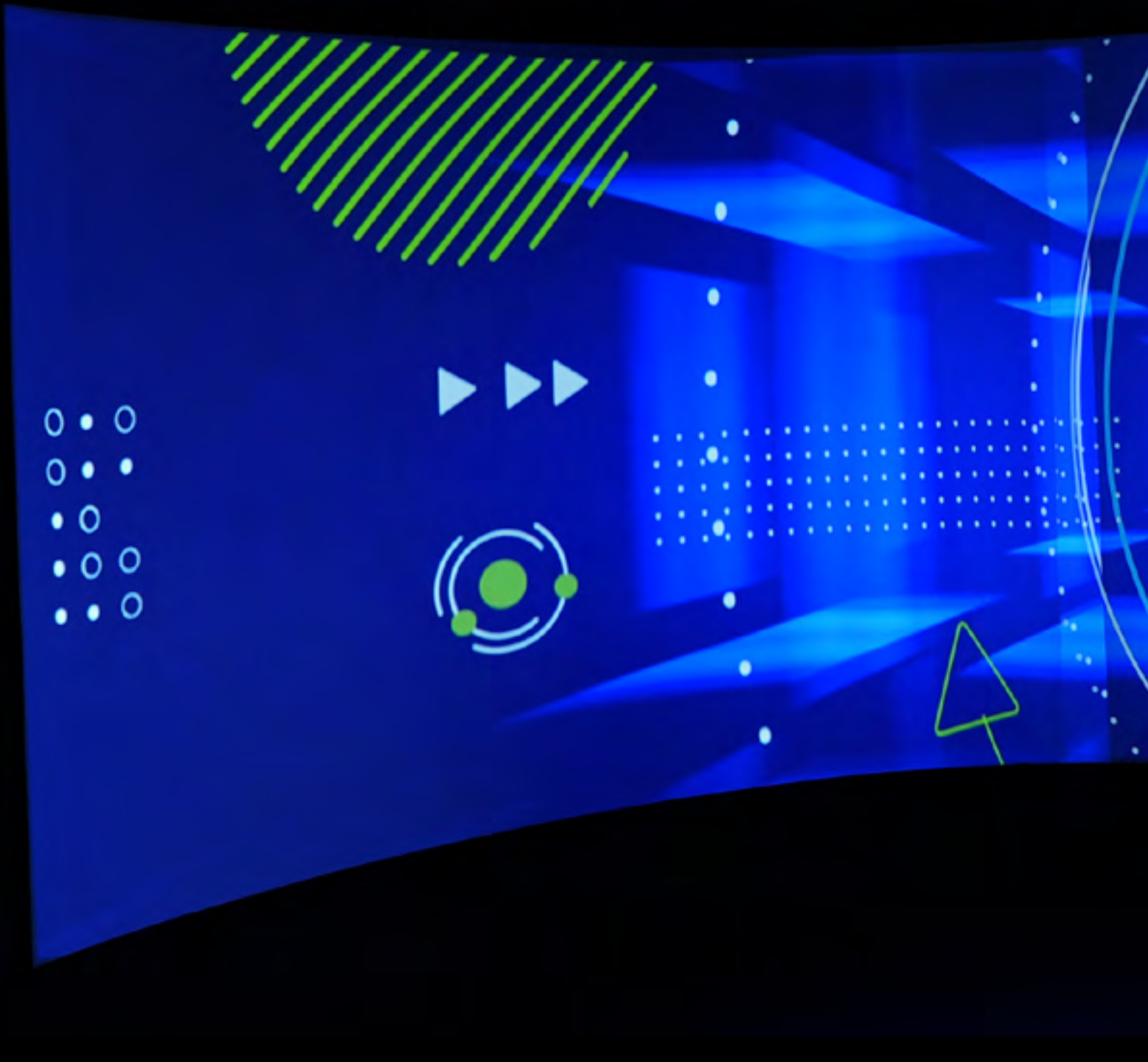
## En qué nuevas alianzas está trabajando Cisco para expandir la conciencia en ciberseguridad

Seguiremos apoyando la alianza regional con la Organización de Estados Americanos (OEA) a través de los Cibersecurty Innovation Councils, creados en 2019. Esta iniciativa es un espacio donde líderes y expertos del sector privado, sector público, academia, ONGs y proveedores de tecnología de seguridad colaboran para impulsar la innovación, crear conciencia y expandir las mejores prácticas, con el objetivo de ayudar a resolver los riesgos digitales y desafíos que afectan a la sociedad digital.
Adicionalmente, trabajamos con ONGs, cámaras de comercio, gremios, instituciones educativas de todo nivel, ministerios y agencias de gobierno, a fin de colaborar en la concientización sobre la relevancia de la educación en seguridad y ciberseguridad, a través de nuestro programa Cisco Networking Academy, que ha brindado habilidades digitales a casi 3 millones de personas en América Latina desde sus inicios

## Mini Bio

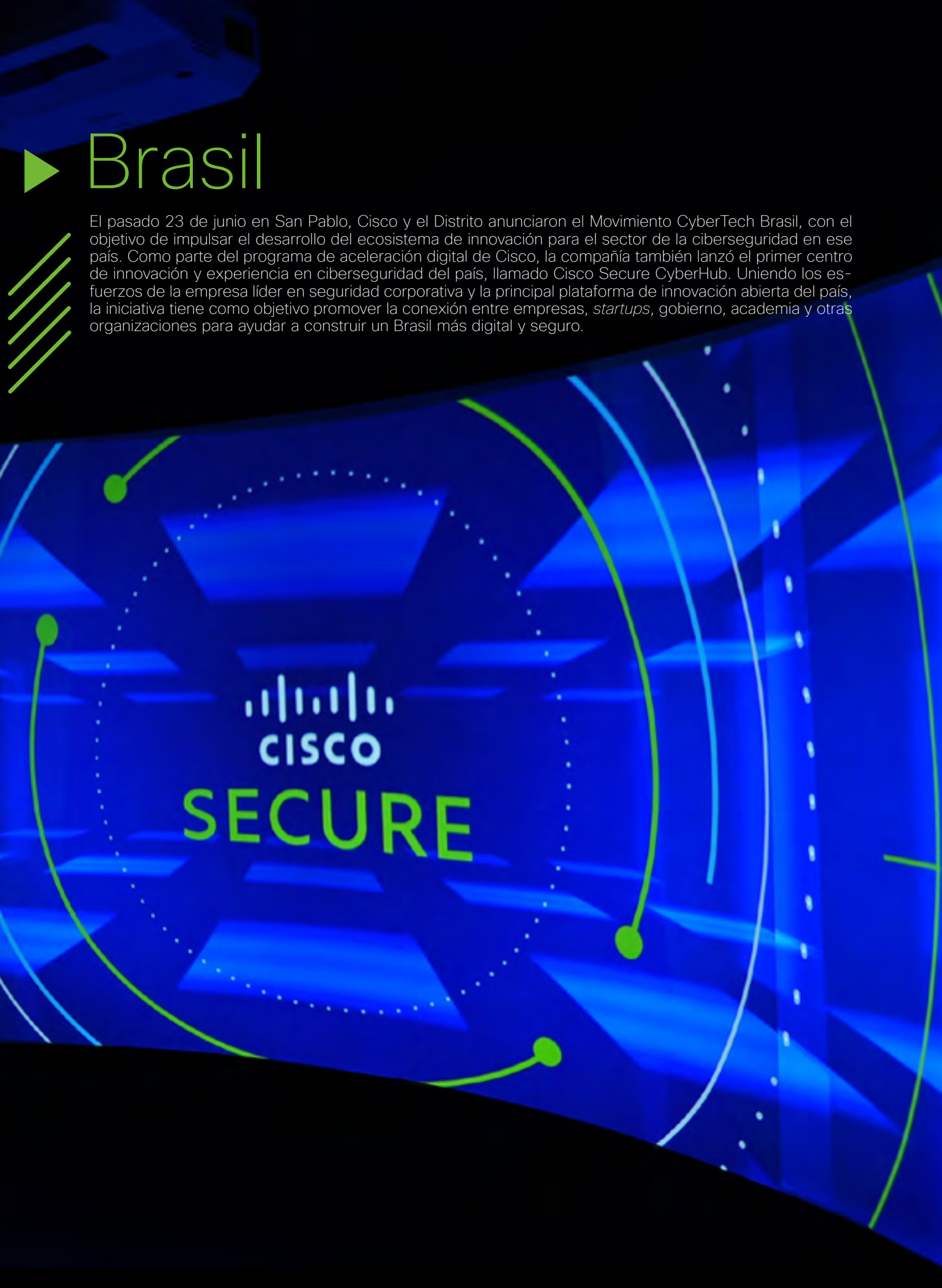
**Laércio** trabaja en el sector tecnológico desde hace unos 35 años. Antes de Cisco, ocupó importantes puestos de liderazgo en Brasil y América Latina. Trabajó en CA Technologies durante 20 años, donde ocupó distintas posiciones de liderazgo, incluida la de gerente de país en Brasil y presidente y gerente general para América Latina. El ejecutivo tiene una licenciatura en Análisis de Sistemas y Administración de Empresas de las Faculdades Associadas de São Paulo (FASP) y un MBA Ejecutivo de Insper.

# Movimiento CyberTech



# Brasil

El pasado 23 de junio en San Pablo, Cisco y el Distrito anunciaron el Movimiento CyberTech Brasil, con el objetivo de impulsar el desarrollo del ecosistema de innovación para el sector de la ciberseguridad en ese país. Como parte del programa de aceleración digital de Cisco, la compañía también lanzó el primer centro de innovación y experiencia en ciberseguridad del país, llamado Cisco Secure CyberHub. Uniendo los esfuerzos de la empresa líder en seguridad corporativa y la principal plataforma de innovación abierta del país, la iniciativa tiene como objetivo promover la conexión entre empresas, *startups*, gobierno, academia y otras organizaciones para ayudar a construir un Brasil más digital y seguro.



Con el mundo cada vez más hiperconectado y la digitalización de las empresas y los servicios en aceleración en los últimos años, el volumen y la complejidad de las amenazas cibernéticas también ha avanzado rápidamente. Una encuesta reciente de Cisco encontró que el 40% de las empresas en todo el mundo informó un incidente de seguridad significativo en los últimos dos años. Entendiendo la relevancia y necesidad de la ciberseguridad para que las empresas y el gobierno puedan continuar su camino de transformación digital, el Movimiento CyberTech Brasil pretende contar con la participación y colaboración de las principales organizaciones involucradas en el tema cibernético, impulsando acciones de difusión del conocimiento, formación de profesionales e innovación en el sector en el país.

Como parte de la iniciativa, Cisco y el Distrito planean promover una serie de eventos, reuniones, *hackatones* y programas de aceleración de *startups* enfocados en la ciberseguridad. Las empresas también pretenden colaborar en la construcción de la primera base de datos de *startups* de ciberseguridad del país, el CyberTech Digital Hub, además del monitoreo y producción continua de contenidos e informes sobre el sector en Brasil.

Esta iniciativa es parte del programa de aceleración digital de Cisco, Brasil Digital e Inclusivo, con Cisco Secure CyberHub como el principal espacio de innovación, experiencia y debate en ciberseguridad.

# Cisco Secure CyberHub

Ubicado dentro de las instalaciones de Distrito Fintech, en São Paulo, el nuevo centro permitirá la experimentación de escenarios complejos de ataque y defensa, trayendo conceptos y tecnologías de ciberseguridad. El espacio reunirá información en tiempo real sobre ataques, respuesta a incidentes y soluciones tecnológicas para empresas, *startups* y gobierno.

**CyberHub reúne tres entornos con recursos audiovisuales para experimentar la seguridad digital:**

## Red Room

Dedicada a demostrar la anatomía de un ataque, explorar sus etapas y los impactos del robo de datos en el *ransomware* con su consecuente riesgo para la vida.

## Blue Room

Entorno que simula el funcionamiento de las defensas, donde se destaca la importancia de la inteligencia, como el trabajo del grupo de investigación en ciberseguridad Cisco Talos y una arquitectura integrada que identifica y responde a los ataques en el menor tiempo posible.

## Sala de operaciones de seguridad

Entorno para demostraciones de soluciones, análisis de *malwares* y simulaciones de salas de crisis con orquestación de investigaciones de amenazas y automatización de respuestas.


Cisco Secure CyberHub también incluye un espacio para *startups* residentes interesadas en desarrollar soluciones basadas en tecnología y API de seguridad, Cisco SecureX/DevNet, que permite la integración y cooperación entre las soluciones de Cisco y las de sus socios. El nuevo espacio también ayudará a promover la formación de los profesionales de la ciberseguridad, complementando la capacitación ya ofrecida por Cisco Networking Academy.

Además, Cisco Secure CyberHub pretende ser un espacio de discusión y desarrollo de proyectos para mejorar la infraestructura de ciberseguridad de empresas, gobierno e infraestructuras críticas en Brasil.

## Lo que viene

Pronto, el Distrito lanzará el Informe Inside Cybertech, un estudio con datos de inversión de nuevas empresas en este segmento; Cybertech Digital Hub, plataforma de datos y conexión de empresas con *startups*; y Cybertech Summit, un evento de la industria que se celebrará en octubre en asociación con Cisco.

## Dixit

"Este es un paso de gran importancia para el programa Cisco Brasil Digital e Inclusivo. A través de CyberTech Brasil y el espacio Secure CyberHub, Cisco avanza en su objetivo de crear un ecosistema digital más conectado, innovador, inclusivo y, sobre todo, seguro. Tenemos mucha confianza en la importancia y calidad de las innovaciones generadas a partir de este movimiento", **Ricardo Mucci**, country manager de Cisco, Brasil.

"A medida que hacemos la transición a una sociedad ultraconectada, los desafíos de la seguridad cibernética se vuelven más grandes y complejos. El movimiento CyberTech Brasil y, en particular, Cisco Secure CyberHub, colaboran para difundir la cultura de ciberseguridad preventiva y receptiva, destacando las buenas prácticas y las herramientas necesarias para proteger empresas, datos y personas en un entorno en el que todos estamos sujetos a la acción de los criminales", **Fernando Zamai**, líder de Ciberseguridad de Cisco, Brasil.

"Con una economía cada vez más basada en la tecnología, el tema de la ciberseguridad se ha vuelto aún más urgente. Como uno de los mayores actores del ecosistema de innovación brasileño, el Distrito se siente obligado a participar en este movimiento", **Gustavo Araujo**, CEO y fundador del Distrito

Más sobre Cisco Secure CyberHub y Brasil Digital e Inclusivo.

# Hackeando predicciones

Contenido audiovisual

**Pasado pisado. Futuro, ¿*hackeado*? Cuando las predicciones no son buenas, podemos actuar para que no se cumplan. ¿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?**

Suele decirse "al pasado, pisado", pero creo que mirando retrospectivamente al 2020, cada uno lo pisó como pudo, y si bien hubo tropezones y algunas caídas, en general todos seguimos caminando, sin embargo en el apuro, la continuidad operativa se llevó por delante a la seguridad. Si seguimos caminando así, sin una gestión efectiva del riesgo cibernético, vamos a abonar a las estadísticas que dan sustento a las más temibles predicciones, como las que sentencian que a corto plazo 2 de cada 3 PyMEs que sufren una brecha quedan en la ruina en cuestión de meses; que el costo del cibercrimen va a crecer por encima del 1.5% del PBI Global y que puede escalar hasta el 6% si se atacaran infraestructuras críticas; o que vamos a llegar pronto a 4M de vacantes por falta de talento en ciberseguridad, de las cuales más de 600.000 son en Latinoamérica.

Si miramos a largo plazo, basta con escuchar los vaticinios del pensador Yuval Harari, que en el World Economic Forum recientemente se refirió a la disrupción tecnológica como uno de los 3 enemigos globales, dando cuenta de que quien controle los datos, controlará el mundo. En su visión, somos en estos tiempos animales *hackeables*, se pueden manipular nuestros deseos, nuestras posturas y por ende nuestras decisiones. Desde esta óptica, la ciberseguridad ocupa un lugar central para resguardar no solo los datos que le entregamos "voluntariamiente" al sistema, sino lo que podríamos llamar privacidad y libertad cognitiva.

Por supuesto que también están las predicciones positivas: gracias a la democratización del acceso a internet hay niños en todos los rincones del país y del mundo que posiblemente desarrollen nuevos conocimientos y resuelvan problemas globales. Esas predicciones mejor que sigan su camino y se cumplan.

## Situación actual

Si hay algo en que veo un consenso total es en que tenemos que hacer un esfuerzo mancomunado entre los sectores privado, público y fabricantes de tecnología para atravesar fronteras, porque está claro que las organizaciones cibercriminales saben colaborar muy bien y así ganan una ventaja ofensiva. Entonces más vale pensar el pasado que pisarlo y dejarlo en el olvido.

por **Juan Marino**

Imagen: kues, Freepik

Juan Marino en la previa del rodaje.

En el reporte Defending against critical threats: A 12 month roundup, 2021, corremos la cortina y revelamos las principales observaciones que han hecho los investigadores de Talos, centro de inteligencia de amenazas de Cisco, la organización no gubernamental de mayor envergadura a nivel global que bloquea 20.000.000.000 de amenazas por día. Sin embargo, lo bloqueado automáticamente ya no es un problema. El problema es lo desconocido. Y eso tiene ocupado a Matt Olney, líder de Talos, y a su equipo. El estudio da cuenta de la sofisticación que ha alcanzado el *ransomware*. Ya no solo lo sufre un desprevenido que se infecta con un *malware* y es extorsionado para pagar a fin de volver a tener acceso a sus datos, ahora cifrados e inalcanzables. Sino que ahora se transita una "Caza Mayor": los ataques son dirigidos y se valen de herramientas multi propósito. Por ejemplo, vemos el fenómeno de "doble extorsión", donde no solo se exige el pago para recuperar la información sino también para evitar su divulgación, que tendría un segundo impacto sobre la reputación de la organización o la persona. Además, sabemos que los criminales detrás de esto están bien organizados: hay brokers de acceso inicial que venden puertas abiertas a organizaciones que otros criminales compran para capitalizar los ataques de extorsión y robo de datos. De hecho, es posible que en este preciso momento alguno de estos brokers esté vendiendo acceso a tu organización.

## Tres predicciones que podríamos hackear

### 1 En algún momento tú o tu organización serán hackeados.

Para derribar esta predicción, la respuesta no es exclusivamente tecnológica. Veamos.

El Security Outcomes Study, 2021, encargado por Cisco, analizó la relación entre prácticas de seguridad y sus resultados positivos en 4800 organizaciones del mundo en 25 países, con buena representatividad de nuestra región. De allí surgió que el 45% de las prácticas sobre ciberseguridad, muestra algún grado de probabilidad de impacto positivo en el logro de objetivos. En cambio, el otro 55% de las prácticas parecen no dar resultado. Además indicó que de las 5 funciones de NIST (National Institute of Standars and Technology - Identificar, Proteger, Detectar, Responder, Recuperar), IDENTIFICAR, es la que muestra una mayor relación con el éxito en la seguridad, mientras que PROTEGER ocupa el 4to lugar. Esto quiere decir que, si bien las capacidades de protección son muy importantes, están sobrevaloradas en detrimento de las funciones IDENTIFICAR, DETECTAR y RESPONDER, que cuando son bien gestionadas muestran un incremento de probabilidad de éxito en la administración integral de la ciberseguridad.

El estudio también revela que las dos prácticas con un impacto más directo en el éxito de la seguridad son:

- Actualizar las tecnologías proactivamente.
- Lograr una buena integración tecnológica, lo cual se traduce en menor cantidad de productos por fabricante, que facilita la operación de seguridad e impacta positivamente en la retención de talento.

Entonces, ¿cómo hackeamos la mala predicción que nos dice que seremos *hackeados*?

- En primer lugar, trabajamos en un cambio de estrategia que no sobrevalore la protección.
- En segundo lugar revisamos el *framework* que mejor se acomode a tu organización y hacemos una evaluación de madurez, identificando los *gaps*.
- Y por último, trazamos un plan de acción de corto, mediano y largo plazo.

Las tecnologías van a ser un componente clave, pero un abordaje consultivo será fundamental. Ahora bien, si asumimos que la calamidad puede suceder en cualquier momento y no nos da tiempo a llevar adelante el plan, ¿qué deberíamos hacer de inmediato para estar mejor preparados?. Tenemos que valernos de los servicios de respuesta ante incidentes con los que podemos aumentar los recursos de la organización al sumar a los expertos de Talos.

### 2 En algún momento tu organización va a sufrir un comprometimiento de credenciales.

En el mismo reporte Defending against critical threats: A 12 month roundup, también hemos visto cómo el robo de credenciales es una parte fundamental de la cadena de ataque.

En este sentido pensemos que le estamos haciendo la vida bastante fácil a los adversarios en tanto y en cuanto seguimos dependiendo de las contraseñas como método único de autenticación. Hoy en día esto es un exceso de confianza. Por eso cobra tanta relevancia el paradigma de confianza-cero, que

El detrás de escena.

según mi perspectiva no debe entenderse en estricto rigor sino como un horizonte al que uno se aproxima reduciendo los excesos de credibilidad en el camino.

A nivel individual lo más probable es que el usuario y contraseña que hayas usado en algún servicio online ya fuera comprometido y esté circulando junto a una larga lista de víctimas en la *dark web*.

Entonces, ¿cómo hackeamos esta predicción? Propongo un desafío: ayudemos a un amigo o familiar a fortalecer su seguridad de dos maneras:
- Usando un gestor de contraseñas, de modo que tengan que recordar una sola bien robusta y el gestor genere otras fuertes y únicas para cada servicio.
- Adoptando un segundo factor de autenticación para los servicios más importantes, siempre que sea posible.

Por supuesto, además de ayudar a un amigo, lo primero es hacerlo uno mismo.

Será importante también llevar esta práctica a las organizaciones. Adoptar una solución *passwordless* o de Múltiple Factor de Autenticación (MFA) eleva la vara de seguridad muy rápidamente y es un gran paso en el camino a la confianza-cero. Al adoptarla, habrá que tener en cuenta que esta acción de seguridad impacta directamente en la experiencia de usuario entonces será importante analizar muy bien los casos de uso y considerar una solución que, más allá de MFA, permita construir políticas de acceso donde la validación de identidad sea dinámica y contextual, minimizando la fricción que le genera al usuario.

Listos para la acción.

En Cisco adoptamos nuestra propia solución Cisco DUO a escala global. En pocas horas, alrededor de 100.000 empleados comenzaron a validar sus accesos mayormente con una autenticación *push* al smartphone como segundo factor. Esto no generó sobresaltos y es un paso clave en la migración que hizo la compañía a servicios en la nube sin requerir conexión por VPN.

## 3 El aumento de la escasez de talento.

Diversos informes de diferentes fuentes dan cuenta de la necesidad creciente de personas idóneas para llevar adelante distintas funciones relacionadas a la ciberseguridad.
En ese sentido y para dar respuesta a la demanda, recomiendo tomar acción sobre la gran oferta de programas de educación e impulsarlos para acelerar la formación de los profesionales que necesitamos. En ese sentido, celebro que Cisco en conjunto con la OEA esté promoviendo nuestros programas de educación en ciberseguridad, aunque creo que aún podemos articular más con las universidades y poner a disposición lo que tenemos para ofrecer. A través de la Academia de Networking se han formado 12M de profesionales desde 1997 y esto es parte clave del programa de responsabilidad social corporativo.

## Democratizar la ciberseguridad

El presente y futuro de la vida digital se sostiene en la innovación de las grandes empresas tecnológicas. Por eso, casi 40 años después de la creación del router hoy tiene sentido que Cisco tenga el ambicioso propósito de habilitar un futuro inclusivo para todos, con la misión de inspirar nuevas posibilidades reimaginando aplicaciones, asegurando los datos, transformando la infraestructura y empoderando a los equipos de trabajo.
Vemos progresos y estamos involucrados en varios proyectos sin embargo, este es un tema en el que no podemos relajarnos y para *hackear* las malas predicciones debemos seguir promoviendo rápidamente las tecnologías de despliegue inmediato y gran escala como la seguridad por DNS, o Cisco Umbrella, que es, tal vez, una de las soluciones que permiten democratizar la seguridad y proteger a los hijos, y también a los padres en cualquier acceso a internet desde cualquier dispositivo.

## A modo de resumen

El reporte de la OEA de 2020 sobre Riesgos, Avances y el Camino a Seguir en América Latina y Caribe actualiza la información relevada por primera vez en 2016 sobre el estado de madurez de las naciones de la región. Allí, se ven los progresos en las 5 dimensiones que plantea el modelo; algunos países con grandes avances, otros no tanto.
Desde una perspectiva de muy alto nivel, la mejor forma de hackear las malas predicciones es logrando la mayor madurez posible en los 5 espacios planteados, a saber:

1. Política y Estrategia de Ciberseguridad.
2. Cultura Cibernética y Sociedad.
3. Educación, Capacitación y Habilidades en Ciberseguridad.
4. Marcos Legales y Regulatorios.
5. Estándares, Organizaciones y Tecnologías.

Y, sobre todo, una de las claves para avanzar es generar puentes que permitan vincular talento, conocimiento y experiencia. El año pasado comenzamos a reunir voces de distintas disciplinas e industrias y lo estamos volcando en esta publicación periódica que creamos localmente y bautizamos Bridge. Durante este año vamos a avanzar generando espacios de relacionamiento con Funcionarios y CISOs porque vemos que hacen mucha falta estas instancias.

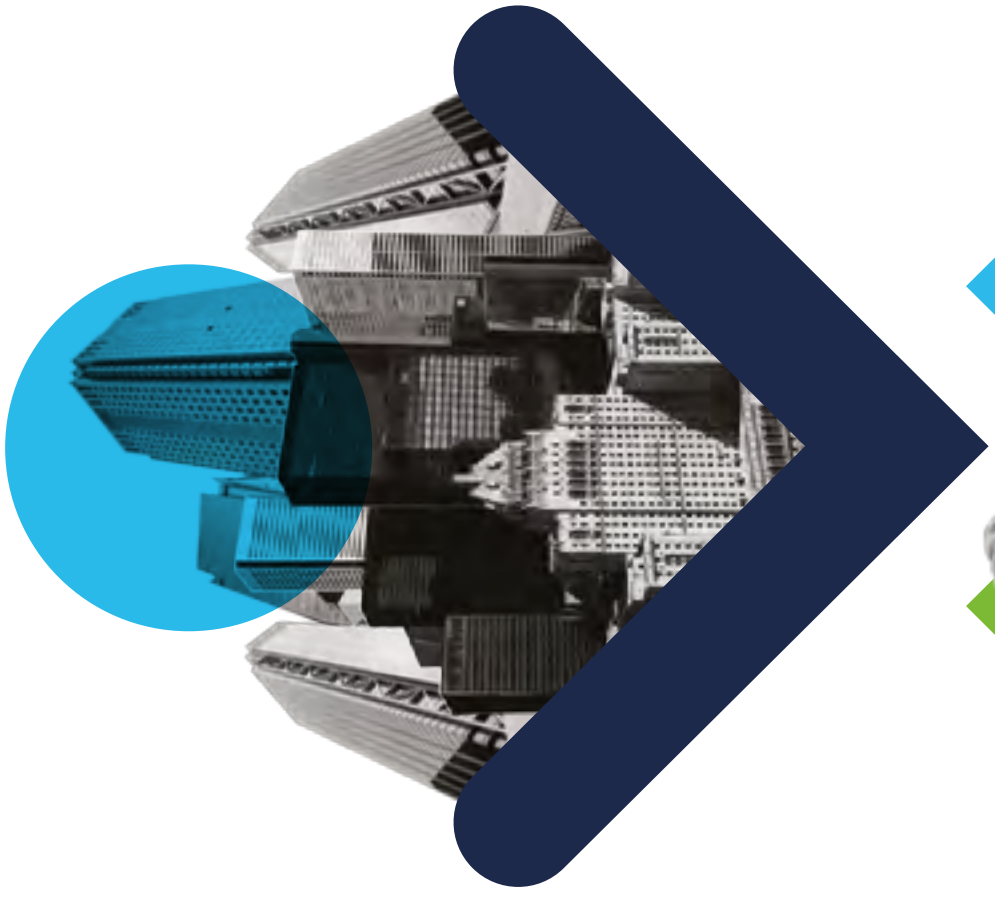
Los invito a conectar con nosotros, conmigo en nombre de Cisco, para buscar los espacios, las conversaciones correctas y que podamos trabajar juntos en *hackear* las predicciones

CISCO
SECURE X

# Experiencia simplificada

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

**Conozca más:**
**https://www.cisco.com/c/es_mx/products/security/securex**





CISCO The bridge to possible

# Autenticación sin contraseñas


Imagen: Jason Dent, Unsplash

**Futuro sin passwords: Cisco Secure introdujo la autenticación sin contraseña de Duo, que permite a los usuarios iniciar sesión de forma segura en aplicaciones en la nube a través de claves de seguridad o biometría de plataforma, sin necesidad del uso de tediosas contraseñas. La autenticación Duo sin contraseña es parte de la plataforma de confianza cero, de Cisco.**

## ¿Qué es la autenticación sin contraseña?

La autenticación sin contraseña es un método en el que un usuario puede iniciar sesión en un sistema informático sin ingresar (y luego tener que recordar) una contraseña o cualquier otro secreto basado en el conocimiento.
La biometría, las claves de seguridad y las aplicaciones móviles especializadas se consideran métodos de autenticación "sin contraseña" o "modernos"que proporcionan acceso seguro para cada caso de uso empresarial (aplicaciones híbridas, en la nube, locales y heredadas). Duo está innovando hacia un verdadero futuro sin contraseña que equilibra la usabilidad con una autenticación más sólida. Esta forma de autenticación brinda a los usuarios una experiencia de inicio de sesión sin fricciones, al tiempo que reduce la carga administrativa y los riesgos generales de seguridad para la empresa.
"MFA sin contraseña" es el término que se utiliza para designar la combinación del flujo de autenticación sin contraseña que utiliza múltiples factores, proporcionando el nivel de seguridad más alto cuando se implementa correctamente.

## ¿Cómo funciona?

La autenticación sin contraseña idealmente implica menos interacción del usuario durante el proceso de inicio de sesión que las formas tradicionales de autenticación. Utiliza criptografía de clave pública, que autentica al usuario con un par de claves criptográficas: una clave privada que es secreta y una clave pública que no lo es, y viene con un léxico de acrónimos y estándares nuevos (o relativamente nuevos), como el estándar FIDO2 (FIDO significa Fast IDentity Online y FIDO2 es solo un término general para la combinación de WebAuthn y Client to Authenticator Protocol (CTAP)).

## ¿Por qué es importante la tecnología sin contraseña?

La autenticación sin contraseña no es solo algo agradable de tener; en realidad, puede mejorar la postura de seguridad de una organización y reducir los costos asociados con la administración de contraseñas. Las contraseñas crean una mayor fricción para los usuarios, ralentizan la productividad empresarial y son inherentemente una forma débil de autenticación de usuarios.

## ¿Por qué implementarla?

La autenticación sin contraseña proporciona una garantía única y sólida de las identidades de los usuarios para lograr su confianza. Para las empresas, esto significa:
- Mejor experiencia de usuario.
- Reducción de la frustración del usuario y aumento de su productividad.
- Reducción de tiempo y costos de TI.
- Reducción de la carga administrativa de los *tickets* de la mesa de ayuda relacionados con las contraseñas y los restablecimientos de contraseñas.
- Postura de seguridad más fuerte.
- Eliminación de amenazas y vulnerabilidades relacionadas con las contraseñas (*phishing*, contraseñas robadas o débiles, reutilización de contraseñas, ataques de fuerza bruta, etc.).

## ¿Cómo implementarla?

La implementación "sin contraseña" no es una tarea fácil, especialmente cuando se trata de grandes poblaciones de usuarios, una cantidad sustancial de aplicaciones, infraestructuras híbridas y flujos de inicio de sesión complejos. Lograr un entorno completamente sin contraseña es un viaje que implica un enfoque por fases a medida que la tecnología continúa evolucionando y aumenta la adopción por parte de los usuarios. Aunque la eliminación completa de las contraseñas aún está lejos, reducir la dependencia de ellas ya es factible mediante la implementación de MFA, el establecimiento de confianza en los dispositivos, el aprovechamiento de SSO y la implementación de políticas de acceso adaptativas. En Cisco estamos listos para acompañar a las organizaciones a emprender este camino

**Pruebe la solución hoy: Cisco Secure Access by Duo, haga clic aquí.**

25º
Aniversario

por **Silvia Montenegro y Karina Basanta**

# Costa Rica

## El país de la cultura, del trabajo y el aprendizaje

Según un informe del Banco Mundial, Costa Rica posee una historia de éxito en términos de desarrollo, especialmente por su crecimiento económico sostenido durante los últimos 25 años. Está considerado como un país de ingreso medio alto, y se destaca por su política basada en la apertura de la inversión extranjera.

Se trata de un país reconocido por su consolidada democracia, por su política siempre a favor de la paz y el diálogo -no tiene Ejército-, y los altos estándares internacionales en el sistema educativo público. Este último valor se complementa con la cultura del trabajo impresa en el ADN del costarricense.

Con una población de alrededor de 5 millones de habitantes, posee una de las tasas de pobreza más bajas de América Latina y el Caribe, logro que está íntimamente relacionado con sus sólidos indicadores de desarrollo humano.

También se destacan sus logros ambientales, que han ayudado al país a construir su Marca Verde. Tienen ejercicio en convivir amigablemente con la

Imagen: visitcostarica.com

naturaleza y respetar su idiosincrasia y recursos. Impulsaron con éxito la transición energética, actualmente el suministro de Costa Rica es casi un 98% renovable. Además, supieron alcanzar una importante diversidad en su matriz energética, que facilita que el parque empresarial pueda ir adaptando nuevas energías a su quehacer cotidiano.

## Círculo virtuoso de desarrollo

En el año en que Costa Rica cumple 200 años de vida democrática, Cisco conmemora sus 25 años de fructífera trayectoria en el país, en los que supo cultivar un fuerte lazo de compromiso con el desarrollo de su economía y comunidad. Además de contribuir al desarrollo productivo y al impulso de la innovación y la digitalización del país, la compañía aporta a la creación y a las oportunidades de empleo de calidad y genera instancias de capacitación en áreas relacionadas.

Luis Carlotti, Country Leader Central America and Caribbean de Cisco Costa Rica, opina que el país tendrá un impacto importante en el futuro de Latinoamérica. Como símbolo de su performance destaca que, recientemente, el país centroamericano ingresó formalmente a la Organización para la Cooperación y Desarrollo Económicos (OCDE), reconocida por reunir a los países más ricos del mundo. Dice: "Ahora forma parte de este grupo de países privilegiados. Por eso, podemos decir que lideramos una operación pequeña en Latinoamérica, pero de Primer Mundo"

Fuente:

https://www.bancomundial.org/es/country/costarica/overview

https://twitter.com/OECD?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1397225089066807296%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.france24.com%2Fes%2Fprogramas%2FeconomC3ADa%2F20210526-costa-rica-ocde-cuarto-pais

https://www.france24.com/es/programas/econom%C3%ADa/20210526-costa-rica-ocde-cuarto-pais

https://www.oecd.org/greengrowth/costa%20rica.pdf

Imagen: Teatro Nacional, San José, Costa Rica


TEATRO NACIONAL

# 25º Aniversario de Cisco en Costa Rica

El 25° Aniversario de Cisco en Costa Rica es un acontecimiento notable en la historia de la compañía internacional líder en tecnología. Fundada en 1984, Cisco nació con la visión de inspirar nuevas posibilidades, brindar soluciones y herramientas innovadoras, ayudar a transformar a las comunidades y su gente hacia un futuro global e inclusivo. Este eje corporativo estratégico está presente con creces en la sede de Costa Rica, que abrió operaciones en 1996 y actualmente es liderada por Luis Carlotti, gerente general de Cisco para los mercados de América Central y Caribe. Dejando su impronta a través de la tecnología y la formación profesional, con un enfoque ético y transparente, la compañía contribuye todos los días en el desarrollo del hermoso país centroamericano, aportando competitividad y valor agregado.

# Luis Carlotti

## Country Leader Cisco Costa Rica & General Manager Central America and Caribbean Region.

**¿Qué significa liderar una empresa de la magnitud de Cisco en un momento de la historia como el actual, signado por la gran aceleración en la transformación digital, producto del contexto impactado por la pandemia?**

Es un momento complicado para el mundo y tenemos una gran responsabilidad. Cisco es una máquina asombrosa de innovación en todos los ámbitos y para mí es un privilegio poder ayudar, desde mi lugar, no solo a la corporación sino al gran equipo que nos acompaña. Con su calidad humana, su ética y su compromiso, el equipo trabaja arduamente para que las cosas salgan bien. Solo la oficina de Costa Rica tiene más de 200 empleados y, a través de nuestros socios de negocios, sumamos un poco más de 1.000 personas trabajando como un solo ecosistema. De aquí se da mucho servicio para América y el mundo. Tenemos colaboradores en Trinidad, Puerto Rico, República Dominicana, Guatemala, Panamá... Están lejos, pero estamos unidos. En este contexto tan complicado, nos toca apoyar a los empleados, conversar con todos, levantar el ánimo, entender las particularidades de cada uno. No es una tarea fácil, sino un gran desafío. Día a día vemos que, más allá de lo difícil, se sale adelante. En lo personal, lo tomo como un reto, que me llena de satisfacción. Estar en Cisco ayuda muchísimo, y eso lo recibo con mucha humildad.

**La pandemia puso a prueba a las empresas del mundo. ¿Cómo fue para Cisco Costa Rica?**

Como una empresa enfocada en el bienestar de las personas, desde el inicio de la pandemia, se venían tomando las medidas correctas. Desde el punto de vista del modelo de teletrabajo, Cisco se ha mantenido a la vanguardia ya que esta dinámica forma parte de nuestro ADN. En mi caso, por ejemplo, desde hace 10 años trabajo desde mi casa y mi oficina está en mi computadora. Es por ello que cuando nos toma por sorpresa la pandemia, trabajar en Cisco fue fácil, no hubo impacto en la forma de operar, nuestro objetivo entonces fue poner a las personas en primer lugar y ayudar a la sociedad de distintas maneras. Colaboramos en los procesos de migración al teletrabajo aportando nuestras herramientas de seguridad y de colaboración en diversos sectores del país.

**¿Cuál es la clave para ejercer el liderazgo que los llevó a encabezar el ranking 'Great Place to Work' en Costa Rica por 3er año consecutivo?**

Algunas variables ayudan. Por un lado, Cisco tiene una cultura corporativa maravillosa y por otro lado, Costa Rica es un país estupendo, su gente es encantadora, madura, con mucha inteligencia emocional, siempre están tratando de hacer las cosas bien. Mi primer objetivo al llegar al país hace 5 años fue incentivar al equipo, que se sintieran orgullos no solo de trabajar en Cisco, sino también en Cisco Costa Rica y que tuvieran claro el impacto de cada uno en la organización y el país. Para mí es un orgullo que durante los últimos tres años, Cisco Costa Rica se destaque por el capital humano que tiene, por la cultura que cada uno logra crear, por la calidad de sus socios de negocio y por los proyectos que impulsamos a través de la transformación digital segura en cada uno de nuestros clientes.

## ¿Cuál ha sido el impacto de la compañía en la comunidad costarricense?

Cisco y Costa Rica están vinculadas desde hace muchos años, de muchas maneras. Costa Rica es un país que abraza la tecnología, y Cisco ha invertido y ayudado significativamente a generar capital humano. Estamos presentes en el crecimiento de la sociedad y del aparato productivo del país. La empresa colaboró en su transformación digital, cualquier empresa y organización tiene algo de Cisco. Participamos en la penetración de la banda ancha en Costa Rica, en la interconexión de escuelas, en el proceso de transformación digital de las empresas y del sector público. Somos un referente en el área de Responsabilidad Social Corporativa, en términos de cómo se debe tratar al empleado, de transparencia, de devolverle al país no solo en los bienes que se venden, sino también en la formación y contratación de gente. Durante muchos años, miles de costarricenses se formaron en redes gracias a nuestro programa Cisco Networking Academy, esta formación le ha permitido a muchos jóvenes conseguir trabajo de calidad, especializarse. Y sentimos que en retribución el país abraza a Cisco.

Para ver el impacto de Cisco Costa Rica puedes acceder al Journal completo Aquí

## Cisco Networking Academy, un programa pionero en educación tecnológica, tiene una fuerte aceptación en Costa Rica. ¿Cómo fue el proceso de posicionamiento?

Por nuestras aulas presenciales y virtuales han pasado más de 91.000 alumnos y al día de hoy 21.000 personas son estudiantes activos. Con este programa hemos buscado contribuir en el desarrollo del país aportando competitividad a través de lo más importante que poseen los países: su capital humano. Cisco Networking Academy brinda mejores oportunidades laborales y de crecimiento a muchas

Imagen: Julie Duchesneau, Pixabay

personas, por ende también ofrece desarrollo para Costa Rica. El trabajo conjunto realizado de la mano de organizaciones, tanto públicas como privadas, han permitido llevar la tecnología a todos los rincones del país. Solo en Costa Rica contamos con una red de 152 aliados educativos, es decir, 152 instituciones imparten los cursos de la academia y con esto continuamos impulsando nuestra misión de fomentar el desarrollo de la fuerza laboral en las áreas promotoras de la digitalización del país.

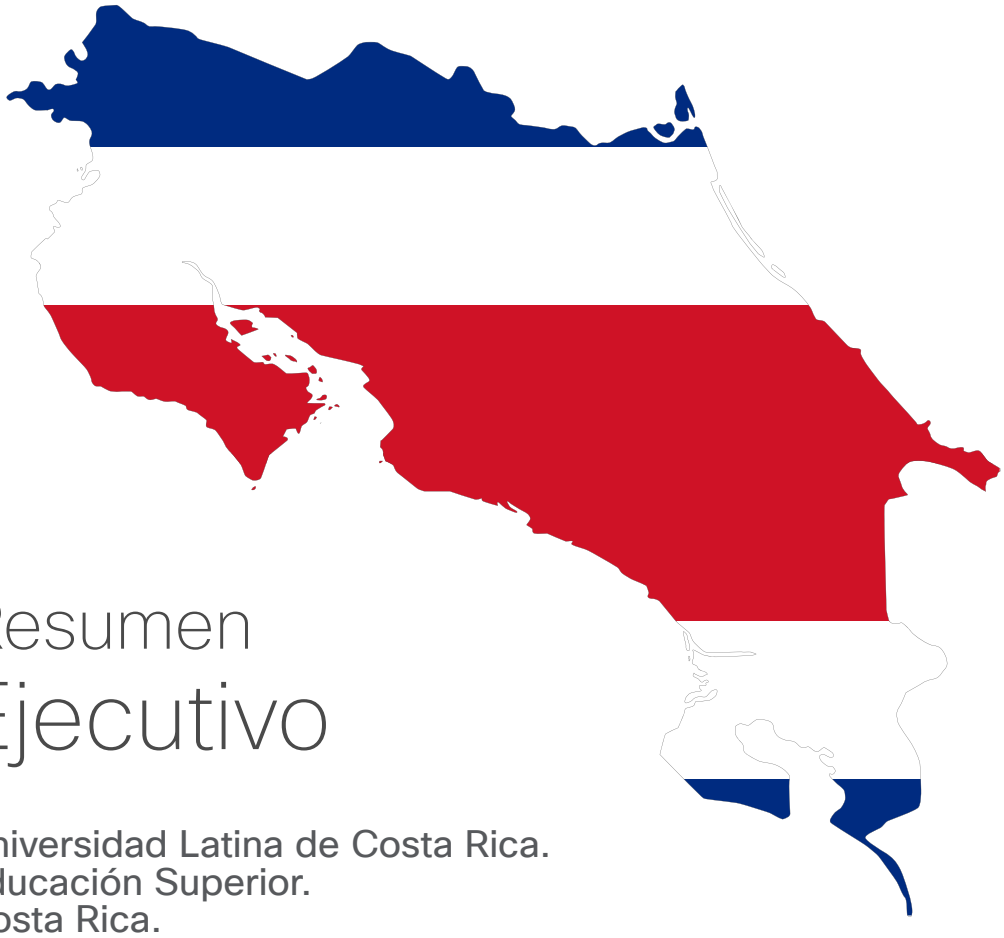
### Actualmente existe un déficit en cuanto a personas formadas en ciberseguridad, por ejemplo, a pesar de la demanda del mercado. ¿Crees que la experiencia de Cisco Networking Academy se puede extrapolar a otros países de Latinoamérica? ¿Cómo se puede incentivar el uso de estas herramientas que, además, son gratuitas?

Costa Rica es un ejemplo para seguir en términos de un modelo de exportación de servicios a través de su gente. El modelo seguramente podría ser replicado por otros países, porque es una buena idea invertir en programas que promuevan que los jóvenes aprendan las competencias del futuro, como lo es la ciberseguridad. Un país se hace competitivo en la medida que su gente crezca y se haga competitiva y Costa Rica lo está buscando con mucho foco, porque sabe que existe una gran brecha y en esa brecha hay una oportunidad para su gente. En este sentido hay consciencia que un país puede tener excelentes calles, seguridad, buena conexión de banda ancha, pero es importante que la gente esté calificada, que esté preparada para lo que las empresas requieren hoy. Es así como Costa Rica abre sus oportunidades ofreciendo buenos servicios para las empresas que invierten y poniendo a disposición personal altamente capaz para ser contratado.

### ¿Cuál es tu objetivo en esta etapa de tu trayectoria?

El gran desafío de Cisco en Costa Rica es mantener el ritmo de los últimos años y seguir creciendo. Cuando empezamos este proyecto éramos un grupo de un poco más de 100 personas en la oficina local, con una calificación en el ranking de Great Place to Work sobre el #11 y con un secreto bien guardado: Cisco Networking Academy. Hoy, 4 años más tarde, duplicamos la cantidad de empleados locales, hemos logrado mantener el nivel de excelencia por 3 años consecutivos como el mejor lugar para trabajar en el país, hemos formalizado nuestro programa de Cisco Networking Academy a través de acuerdos público-privados y nos convertimos en el hub para Centro América y el Caribe. Tenemos que seguir soñando y estar seguros de que Cisco Costa Rica puede lograr mucho más

UNIVERSIDAD LATINA DE COSTA RICA
POWERED BY Arizona State University



# Resumen Ejecutivo

Cliente: **Universidad Latina de Costa Rica.**
Sector: **Educación Superior.**
Ubicación: **Costa Rica.**

**Tamaño de la organización:** 8 sedes. + de 90 carreras entre programas de grado, certificaciones laborales y posgrados. + de 110.000 graduados.
Conjuntamente con la Universidad Americana, constituyen el mayor sistema universitario privado en Costa Rica con más de 25 mil estudiantes y aproximadamente ochocientos empleados administrativos.

**El desafío:** Implementar una solución integral de seguridad para mejorar y fortalecer la estructura de ambas universidades frente a ataques maliciosos y de día cero. Contar con un servicio que facilite y agilice la visibilidad y control de la red a fin de predecir su comportamiento y tomar acciones inmediatas ante un incidente.

**La solución:** Suite completa de seguridad en la nube a través de:

- Secure Email (suite de seguridad para email).
- Secure Endpoint (AMP for Endpoints).
- Umbrella (suite de seguridad para DNS).
- AnyConnect (suite de seguridad para conexiones VPN).
- SecureX (plataforma de integración).
- Implementación de todas las soluciones y gestión de la plataforma de seguridad de la Universidad a través del SOC de Altus.

# Caso de éxito

Imagen: Universidad Latina de Costa Rica

## La entidad

Con más de treinta años en el mercado, la Universidad Latina de Costa Rica es una de las pioneras en el desarrollo de la Educación Superior Privada en el país. Cuenta con ocho sedes ubicadas en San Pedro, Heredia, Grecia, Cañas, Santa Cruz, Ciudad Neily, Pérez Zeledón y Guápiles y su oferta está compuesta por más de noventa carreras entre programas de grado, certificaciones laborales y posgrados en las áreas de Ciencias de Salud, Ciencias Empresariales, Hospitalidad, Ciencias Sociales, Ingenierías y TIC's, Arte, Diseño y Comunicación. En la actualidad alcanza más de 110.000 graduados.

Desde la educación superior, promueve la formación de líderes éticos, innovadores y con visión global. Asimismo, apoya la investigación a través de la cooperación y el trabajo conjunto entre los sectores público y privado, con el objetivo de elevar la competitividad del país y el progreso social.

En el año 2020, la Universidad Latina se afilia a Arizona State University para convertirse en una universidad de impacto nacional.

Uno de los pilares de esta organización está basado en los valores sobre los que desarrolla su accionar: excelencia, compromiso, innovación, integridad y responsabilidad son una fortaleza que promueven y comparten con su comunidad.

## El desafío

Tanto la Universidad Latina de Costa Rica como la Universidad Americana, formaron parte del grupo Laureate hasta el año 2020. Ese año, se establecieron como afiliadas de Arizona State University. Este cambio dejó a ambas universidades con la responsabilidad de repensar toda su estructura de seguridad, tarea que requería celeridad en la implementación y robustez de la solución elegida debido al contexto mundial desatado por la pandemia.

"Lo primero que hicimos fue ver qué cobertura teníamos con Laureate. Luego definir nuestra propia arquitectura y bosquejar qué queríamos hacer de forma agnóstica. El paso siguiente fue avanzar con las fases de RFI y RFP donde invitamos a varios proveedores y, ya que teníamos la alternativa de la arquitectura de la solución, ampliamos con servicios y buscamos además quién hiciera el SOC", comenta Julio Galindo, Director de Tecnologías de Información de la Universidad Latina de Costa Rica y responsable de estructurar esta implementación.

## La solución

"El enfoque abordado junto a la universidad tiene que ver con una visión de solución y arquitectura, no está solamente basado en productos independientes. Cisco apoya y acompaña la estrategia y el plan de la universidad. El mensaje durante el proceso de evaluación estuvo relacionado a los conceptos de Automatización, Simplicidad e Integración, los tres pilares que busca la arquitectura", aclara Giovanni Calderón, Security Account Manager para Cisco Centroamérica y Caribe. Por tal motivo, la solución adquirida por la Universidad Latina refleja actualmente estos conceptos y está compuesta por la suite completa de seguridad en la nube de Cisco, a través de los siguientes productos y servicios:

Imagen: Universidad Latina de Costa Rica

- Secure Email (suite de seguridad para email).
- Secure Endpoint (AMP for Endpoints).
- Umbrella (suite de seguridad para DNS).
- AnyConnect (suite de seguridad para conexiones VPN).
- SecureX (plataforma de integración).
- Implementación de todas las soluciones y gestión de la plataforma de seguridad de la Universidad a través del SOC de Altus.

El proceso de venta y adquisición fue liderado por Altus Costa Rica, partner de Cisco reconocido en varias oportunidades por su gestión innovadora y a la vanguardia de la transformación digital.

Además de implementar las soluciones ofertadas, Altus gestiona toda la plataforma de seguridad de la universidad a través de su SOC. Incluso, se utilizan herramientas que complementan las soluciones de Cisco, sobre todo alrededor de las vulnerabilidades en los servidores.

**El servicio de soporte incluye**:

1. Protección contra cerca de 45mil correos maliciosos.
2. Bloqueo de cerca de 1.5MM dominios maliciosos.
3. Gestión de más de 200 servidores.
4. Reducción en la detección y remediación de vulnerabilidades en los servidores de varios meses a una semana, gracias a la automatización de los procesos de actualización de los servidores.

"Durante la pandemia logramos implementar un esquema de trabajo seguro donde la mayor parte del personal estuvo trabajando de forma remota sin ningún incidente de seguridad", aclara Alonso Bogarín, Gerente General, Altus Costa Rica.

Debido a que la seguridad es un proceso que transcurre de forma transversal a toda la organización, esta solución impacta directa y positivamente en todas las áreas de la universidad creando un sistema de protección y visibilidad superlativo en la industria.

> "El principal beneficio de esta suite de productos y servicios es la seguridad y la tranquilidad que nos brinda, tanto a quienes velamos por la seguridad de la información que se trafica a través de la universidad como a los alumnos, profesores y personal administrativo, usuarios de nuestros servicios."
>
> *afirma Julio Galindo*

Imagen: Universidad Latina de Costa Rica

Julio Galindo
Director de Tecnologías de Información de la Universidad Latina de Costa Rica

## ¿Por qué Cisco?

La elección de Cisco como aliado estratégico estuvo basada en su portafolio completo, robusto y confiable. "Cuando armas una arquitectura y necesitas la implementación rápida, lo más conveniente es optar por el proveedor que tenga el muro completo. Por ejemplo, SecureX nos permite tener el control de forma simple y los otros componentes son robustos e integrables", dice Galindo.

Como base para la decisión, la universidad contaba con su experiencia previa en otros productos de Cisco, ya que su parque de Access Point y Switches, son Cisco, también el Contact Center, el Call Manager y ahora la Seguridad.

## Próximos pasos en seguridad

La seguridad en la Universidad Latina de Costa Rica es apreciada como un proceso en constante evolución. En este sentido, Cisco es un socio de negocios que acompaña en cada paso del camino. Perfeccionar la seguridad lleva incluso a observar nuevos espacios que requieren atención. "Estamos avanzando en otros frentes que tienen que ver con este concepto. La seguridad está dentro de nuestro paradigma. Tengo más de 15 años en el sector, antes de Costa Rica estuve en Vietnam y antes en México y Brasil. Y siempre uno de los pilares en mis estrategias fue la seguridad, algo que nos cubra la espalda. Y el tener una arquitectura simple, robusta, nos hace más fácil la vida. En la universidad tenemos un plan de seguridad anual que incluye control de accesos, permisos, control de cambios, comunicación, entre otras funciones.", indica el director de Tecnologías de la Información de la casa de estudios.

Antes de la pandemia, el cisne negro que aceleró la transformación digital a nivel mundial, "la percepción de la seguridad en la dirección local se asemejaba a un concepto de lejano impacto, era algo que podía sucederle a alguien más e improbable para nosotros. A raíz del cambio producido, se ven con buenos ojos todos los temas relativos a esta disciplina, es por ello que se han autorizado los proyectos de los que hemos estado conversando. La pandemia ha provocado un cambio de cultura en este sentido para toda la organización, deberemos ser conscientes de los nuevos riesgos y aprender a utilizar las herramientas que nos permitan estar protegidos. Estas son adopciones paulatinas. El Comité de Dirección ahora ve a la seguridad como un habilitador para mantenerse en el mercado y más aún, para crecer", concluye Julio Galindo.

> "Nos sentimos honrados de tener a la Universidad Latina de Costa Rica como cliente y de que sea una voz en estos 25 años de Cisco en el país, ya que eso es reflejo de cómo hemos trabajado juntos como socios de negocios y del crecimiento que esperamos en la relación."
>
> *Jorge Mora,*
> *Account Manager Cisco.*

Imagen: Martín Lutze, Pixabay

# La Voz en la Comunicación Virtual

por **Claudia Menkarsky**

Vocal Coach, Terapeuta Psicovocal y Cantante Lírica

Hoy más que nunca, en pleno apogeo del modo virtual, nuestra voz -ese instrumento a través del cual nuestro mundo interno e invisible se hace audible con tonos y palabras para expresar pensamientos, sentimientos, estados anímicos, comunicándonos- toma extrema relevancia, ya que cada día es más importante facilitar la comunicación verbal y paraverbal a través de las pantallas.

Para transmitir de la manera más efectiva, afectiva y empática, es primordial considerar que, más allá de la propia disposición, condición y características vocales, podemos desinhibirnos, adquirir espontaneidad y confianza, empoderar nuestra voz con una vocalidad bien impostada y sonora, gestionar las emociones para crear el clima adecuado acorde al diálogo o exposición, conectar, comunicar.

La voz, la respiración y el sistema nervioso están íntimamente relacionados entre sí y son interdependientes. En la actualidad, cuando es habitual permanecer sentado durante largo tiempo, frente a un ordenador con auriculares, muchas veces utilizando tapabocas, se puede colapsar la respiración, se tiende a forzar la voz y elevar el tono para asegurarnos que somos escuchados. El uso de auriculares no permite recibir la señal adecuada para percibir si se está exigiendo la natural sonoridad de la voz. A su vez, se suma que el 80% de las personas no están conformes con su voz y sienten temor al hablar en público o a través de un video, por falta de entrenamiento y costumbre. Esta situación genera la inhibición de la respiración que colapsa el volumen y tensa la musculatura, generando en muchos casos bruxismo, contractura cervical, cefaleas, acidez estomacal y otras sintomatologías propias de no respirar profundo, en forma abdominal, aflojar la mandíbula y poder expresar espontáneamente aquello que deseamos transmitir, al igual que lo hacíamos en la niñez, con alma y corazón.

Así llegamos al entrenamiento vocal y expresivo, tal como la oratoria, el coaching de voz, y aprendizajes para hablar frente a otros, procurando ser realmente nosotros en nuestra voz, y no un puñado de nervios, con nudos en la garganta.

## ¿Cómo reconocer y mejorar nuestra **voz?**

Nuestra voz nos identifica y define, el estado de consciencia se refleja en la voz, cada voz es única, como la visión del mundo, como la verdad de cada uno. A continuación, compartimos algunos ejercicios para comenzar a reconocer la propia voz, mejorarla y hacerla oír, liberando su verdadero potencial, aquel que desde pequeños y a través de los años fue cambiando con cada "cállate, no grites", "haz silencio", "quédate quieto/a", "tú no sabes".
Hay tres factores que determinan una buena vocalidad: respirar profundo; abrir la boca, bajando la mandíbula en la A y en la O; y una buena impostación.

## Algunos **ejercicios**

Respirar nuevamente al vientre, como cuando nacemos: Bien sentado/a, erguido/a, con la espalda derecha, piernas sin cruzar, exhalar mientras nos inclinamos hacia adelante, apoyando los codos sobre las rodillas. Inspirar profundo. Allí se observa que el aire va inflando el vientre ya que baja el diafragma, y abre la parte intercostal. Así se logra respirar profundo. Inhalar por nariz en 5 tiempos, mantener el aire por otros 5 tiempos, y exhalar en 10 tiempos por la boca, soplando el puño de la mano, juntando los labios en forma de beso y procurando que el aire salga frío.
Si se realiza este ejercicio una vez al día, al cabo de una semana es posible identificar cuándo uno está respirando profundo y cuando no.
Aflojar la mandíbula. Hablar frente al espejo, mirando que la boca forme un huequito cada vez que se pronuncia la A y la O. Tanto cuando se afloja la mandíbula como al pronunciar las vocales, los labios deben cubrir naturalmente la dentición. Mientras no se habla, aún juntando los labios, con la boca cerrada, procurar dejar un pequeño espacio, poner la punta de la lengua entre los dientes para que se afloje la tensión que pueda haber en la mandíbula. Este ejercicio es de gran ayuda contra el bruxismo y las contracturas cervicales.
Impostar la voz. Realizar la siguiente prueba: juntar los labios y emitir un sonido. Si vibran y producen cosquillas es porque la impostación está descolocada. Se puede corregir, repitiendo el ejercicio y mientras se emite el sonido, bajar la cabeza, inclinándola suavemente hacia adelante. Así se observará que la vibración se siente en la punta de la nariz, se puede tocarla para comprobarlo. Luego, emitiendo el sonido, sonreír levemente e incorporarse con la cabeza bien erguida. Entonces es posible ver que ya está el sonido como en la "máscara", es decir el lugar del rostro en el que habitualmente ubicamos un antifaz; bien impostado, y sin sentir cosquilleo en los labios.
Para cuidar los oídos. Utilizar el auricular de un solo lado, alternándolo para no fatigar los tímpanos, y para poder sentir el volumen real de la voz mientras se habla, sin forzarla.

Procurar hablar en un tono de voz central, grave, dándonos tiempo para respirar. Hay que recordar que los momentos de atención se generan en los silencios que dan paso a la reflexión y no en un discurso rápido que, al poco tiempo, nadie atiende, sobre todo cuando no hay contacto con las miradas, ya que esta energía tan poderosa no existe tras la pantalla. Probar de hablar en alta voz, frente al espejo, para reconocer los gestos y poner las manos entre el pecho y el ombligo. Es buena idea grabarse o filmarse, ya que vernos y escucharnos es la mejor manera de detectar lo que se quiere cambiar y mejorar en la voz y expresión

La autora del artículo está disponible para contestar consultas o inquietudes relacionadas:
claudiamenkarskycoach@gmail.com

# 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**

# Ad Content


Hay que esperar lo inesperado. Esta premisa básica y universal, de aplicación válida en todo tiempo y lugar, se ha vuelto extraordinariamente presente y permanente en nuestras vidas a partir de los cambios recientes, que transformaron de una vez y para siempre el mundo tal como lo conocíamos. Poco queda de lo que hasta hace poco era el devenir cotidiano. Aún esperando lo inesperado, adaptarse a cambios tan extremos se hace difícil para cualquiera, especialmente si trata de desenvolver su actividad de manera individual. Transitar esta etapa se hace más fácil si se tienden puentes y se comparte el camino a recorrer. Es momento de comprender y aceptar las nuevas dificultades, y también a las nuevas soluciones que nos permitirán salir adelante.

Una de las herramientas disponibles es el modelo de negocios *Partner for Partners*, de Braycom, reconocido por Cisco. Este programa ofrece servicios profesionales de preventa, implementación y soporte a empresas del rubro, y que en lugar de competir trabajan en conjunto para potenciar sus posibilidades. De esta manera, Braycom pone a disposición de sus clientes su ingeniería y su formación profesional.

La confianza es la clave de *Partner for Partners* y hace más de 15 años que los partners más relevantes de Argentina y Chile confían en Braycom. Cuando un integrador la convoca a través de este programa, la empresa lo ayuda en la ingeniería de preventa sin costo, y le brinda sus servicios profesionales para implementar soluciones. Así, pone a su disposición ingenieros certificados, métodos y experiencias para minimizar riesgos en proyectos complejos, lo que le permite multiplicar su capacidad técnica y comercial.

El funcionamiento es simple: cuando un cliente convoca a un integrador de tecnología, éste se pone en contacto con Braycom, que lo ayuda sin costo alguno en el desarrollo consultivo y en la preventa de la solución apropiada para ese cliente. De esta manera, se acelera el ciclo de venta y el proyecto se concreta. En aquellos proyectos en que se requiera implementación, Braycom la realiza con sus ingenieros certificados y el servicio es previamente marginado como un producto más, así, ganan todos. *Partner for Partners* consigue resolver los desafíos para que el negocio del integrador pueda crecer sin correr riesgos, y asegurando siempre la fidelidad de sus clientes hacia su marca.

*Partner for Partners*, de Braycom, es una respuesta dinámica y efectiva para lo conocido y también para lo inesperado. Están todos invitados

Imagen: Mohamed Hassan, Pixabay

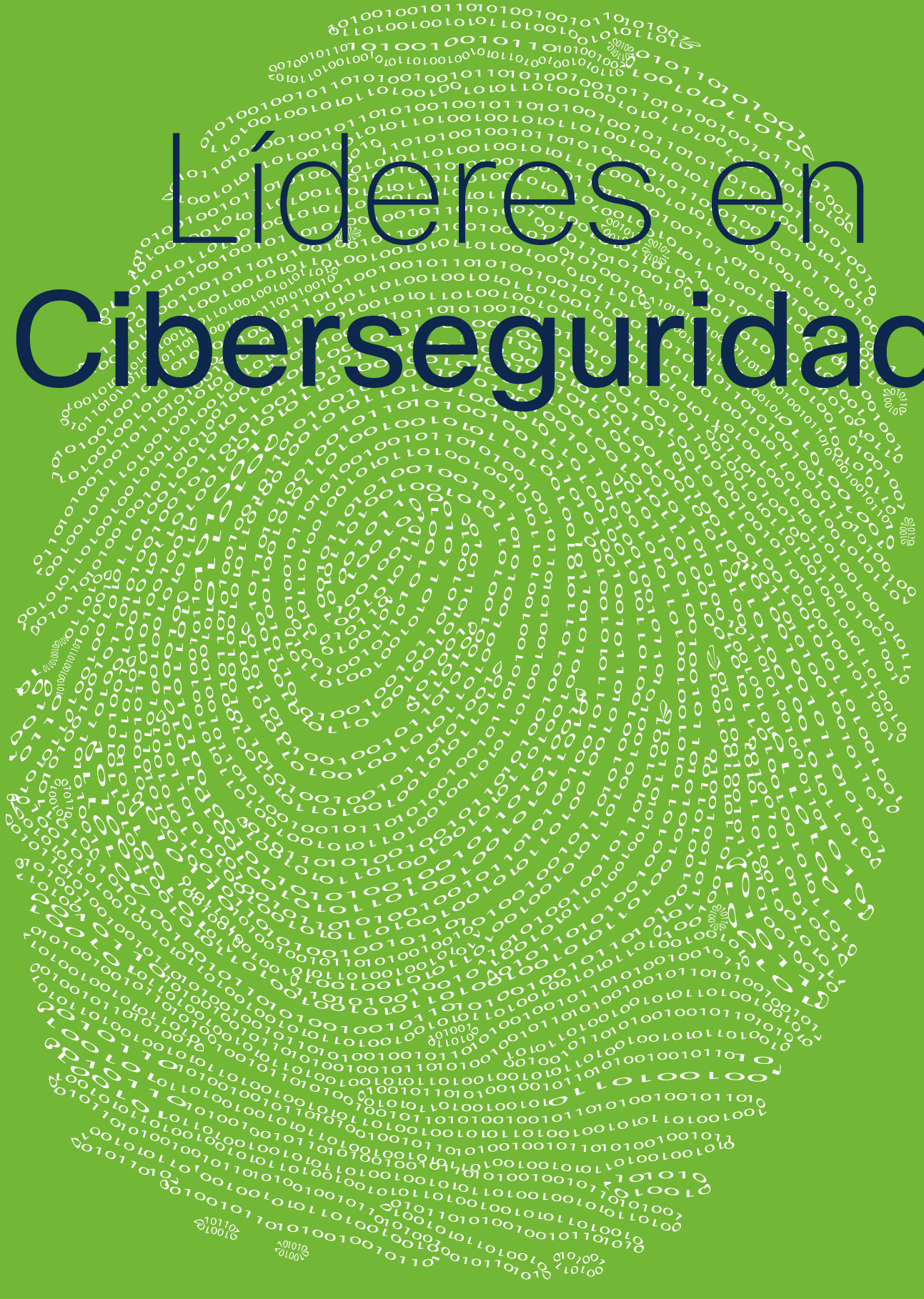
# PARTNER
## for **partners**

> *"Cuando comenzamos con este modelo muchos partners veían nuestra propuesta con escepticismo y desconfianza, solo bastó el primer negocio en conjunto, para convertirnos en un socio estratégico"*

por **Ing. Martín Marino**
CEO Braycom

Acceso
al servicio

# Líderes en Ciberseguridad



Los líderes en ciberseguridad suelen coincidir en que esta disciplina debe ser entendida como un proceso en constante adaptación. Cada uno con su estilo, guía a su equipo en el camino decisivo hacia una organización segura, que proteja no solo a sus integrantes y activos, sino también a sus colaboradores y a toda la cadena de valor. En esta edición de Bridge, tres líderes destacados en la materia comparten su conocimiento y experiencia y dan una aproximación sobre cómo abordar el futuro cambiante.

Nohemí **Moreno**

José Luiz **Santana**

Ricardo **Pérez D'Brot**

# Entrevista

# Nohemí **Moreno**

Applied Cybersecurity Services Lead Director at Accenture & Cybersecurity Specialization Professor at Latam Business School, México.
Top 50 Women In Cybersecurity, WOMCY, LATAM.

por **Karina Basanta**

Imagen: Flavio Moura, Pixabay
Cancún, Pirámide Maya

*La mirada de Nohemí abarca una amplia pluralidad de sectores: servicios financieros, retail, seguros, educación y telecomunicaciones son algunos de ellos. Su recorrido da cuenta de que su palabra tiene el sustento de la experiencia. En esta edición de Bridge compartimos su perspectiva sobre la ciberseguridad en el contexto actual y las recomendaciones para lograr una operación exitosa y resiliente.*

## En tu experiencia, ¿qué es lo que le quita el sueño de noche a una especialista en Ciberseguridad?

Depende el tipo de especialista, pero desde mi perspectiva considero que es el hacer un adecuado manejo de los riesgos con los recursos que tienes.
Generalmente, no se cuenta con todo el presupuesto necesario, la tecnología de punta o el personal con las habilidades y conocimientos actualizados. Más aún, cuando cada día hay nuevas amenazas y vulnerabilidades y estamos en un entorno totalmente cambiante.
Encontrar ese balance, comunicar y convencer sobre las necesidades críticas con claridad y estar bajo los niveles aceptables de riesgo establecidos por la organización, es un gran reto.

## ¿Ventaja ofensiva o defensiva en Ciberseguridad?

En el ambiente actual en el que nos encontramos, en donde los ciberataques están a la orden del día, no veo posible el no contar con mecanismos ofensivos y defensivos, en los que ambos proporcionen los *inputs* para reforzar o modificar las capacidades de una organización en materia de ciberseguridad.

## De acuerdo a tu recorrido ¿qué funciona y qué no en esta disciplina?

Lo que no funciona: creer que la seguridad es solo un problema técnico, que es inversión de una sola vez y asegurar que nada pasará en tu organización.
Lo que funciona: incluir en la organización una cultura de seguridad en todos los niveles, tomar el tiempo

para identificar y entender los posibles riesgos a los que se está expuesto de acuerdo al tipo de organización y los países en los que se opera. Estar preparado para responder y recuperar las operaciones ante un evento adverso y lo más importante, estar consciente sobre lo cambiante que es el entorno tecnológico, regulatorio y de negocio, y que la seguridad es un proceso continuo que requiere atención e intervención de la alta dirección.

## A tu entender, ¿qué lugar ocupa la privacidad en el planteo estratégico de Seguridad?

Es indispensable, y más ahora que la conciencia en materia de privacidad ha crecido exponencialmente debido a las diversas regulaciones en el mundo.
Durante la definición de una estrategia de seguridad es imprescindible saber qué es crítico para una organización y eso se define por los sistemas de misión crítica y los datos que se administran.
Por lo anterior, es necesario aplicar prácticas de privacidad y protección de datos para evitar el mal manejo y fuga de información que exponen a las organizaciones a diversos riesgos.

## Si digo la palabra “resiliencia” ¿qué significa para ti?

Tener las capacidades para recuperarse o adaptarse y continuar con el día a día ante un evento disruptivo.

## ¿Qué es lo que a tu entender debería estar haciéndose y no se hace en términos de ciberseguridad? Puedes tomar la pregunta desde cualquier punto de vista.

Estas prácticas se hacen en ciertos sectores y a diferentes niveles, pero considero deben reforzarse:

**1.** Gestionar minuciosamente los activos de información considerando aquellos que no pertenecen a la organización, aplicando las mismas políticas de seguridad sin importar la ubicación de la red.

**2.** Identificar y gestionar a los terceros, priorizando las prácticas de seguridad a emplear de acuerdo con el servicio que se proporciona y el tipo de acceso a los sistemas y datos.

Imagen: Carlos Alcazar, Pixabay
Los Toltecas de Tula, México

**3.** Accionar el proceso de gestión de riesgos de ciberseguridad utilizando información de ciber inteligencia.

**4.** La alta dirección debe involucrarse y entender los riesgos a los que se está expuesto en materia de ciberseguridad.

## Por favor comparte con nosotros tres recomendaciones sobre Seguridad teniendo en cuenta el contexto actual.

Los límites de una organización se han perdido, los dispositivos interconectados se han incrementado exponencialmente al igual que las identidades digitales utilizadas por humanos y no humanos. Por lo anterior, considero los siguientes tres puntos prácticas necesarias:

**1.** Poner el foco en proteger la información. Para ello es necesario saber qué y cómo se recopila, en dónde se almacena y con quién se comparte.

**2.** Catalogar y gestionar de manera efectiva los activos digitales en términos del riesgo potencial.

**3.** Implementar un programa para identificar, gestionar y monitorear las identidades digitales, activos y aplicaciones que acceden a dichos datos.

## ¿Hay algo que no te haya preguntado y te gustaría compartir?

En seguridad nada es infalible, por lo que es necesario contar con un plan de atención y respuesta ante incidentes claro y accionable, que involucre a las diferentes áreas de la organización e incluya aquellas de manejo de crisis y comunicaciones

# Entrevista


## José Luiz Santana

CISO, C6 Bank, Brasil

por **Nelson Brito**

*Aquí podrás leer un extracto de la entrevista. Te invito a acceder al contenido audiovisual completo desde el código QR en esta página.*

Imagen: Wanderson Teixeira, Pixabay
Cristo, Río de Janeiro

*Conversar con José es siempre muy enriquecedor. Sus ideas son tan claras y directas como sus acciones. En este bate papo pasamos revista sobre algunos de los puntos más sobresalientes de la disciplina que nos convoca.*

## José, ¿qué es lo que te quita el sueño de noche?

Para quien trabaja en seguridad, esa es una pregunta que no tiene una sola respuesta. Sin embargo, lo que más me preocupa, lo que busco intensamente día a día, es identificar los riesgos. Lo que más me quita el sueño es no saber que el riesgo existe, no estar consciente de dónde está alojado. Lo primero que debe saberse es dónde está para luego mitigarlo.

## ¿Ventaja ofensiva o defensiva en Ciberseguridad? ¿Dónde sueles poner el foco, en Blue Team o en Red Team?

Hago equilibrio, aunque suelo estar enfocado en Blue Team, en estrategias de defensa. Hay pocas personas de seguridad ofensiva en el equipo, aunque eso depende de cada corporación. Mas como todo en la vida: equilibrio. La seguridad ofensiva es muy importante, pero es imprescindible tener una estrategia de seguridad adecuada que consiga cerrar el círculo. Blue Team y Red Team son parte de ese círculo; la forma en que ellos se integren e interactúen definirá si la estrategia será o no exitosa. Al final, lo que más importa es una buena interacción entre estos equipos. Equilibrio.

## Teniendo en cuenta estas cuatro categorías sobre el rol de un líder de seguridad: tecnólogo, guardián, estratega, consultor, ¿con cuál te sientes más identificado y por qué?

Estratega. Pensar, construir, crear arquitecturas, tiene que ver con la estrategia. Ser vanguardista me motiva mucho, cómo hacer que todos vayamos en una dirección.

## ¿Qué funciona y qué no en Ciberseguridad?

No funciona querer hacer seguridad en algo que no conocemos profundamente. No funciona parar de estudiar. Para hacer seguridad en algo hay que profundizar siempre en cada nuevo mercado, en cada tecnología nueva, en cada herramienta. Asimismo, no funciona hacer ciberseguridad mientras los equipos de negocio y seguridad están separados.

## ¿Qué lugar ocupa la privacidad en el planteo estratégico de Seguridad del banco?

Un lugar muy crítico. Por eso la privacidad toca la seguridad, no está debajo de ella. La seguridad es un componente que está allí para ayudar. En mi opinión, privacidad no está dentro de seguridad.

## Si digo la palabra “resiliencia” ¿qué significa para ti?

Resiliencia es foco, fuerza, disciplina para cumplir la misión.

## Por favor comparte con nosotros tres recomendaciones teniendo en cuenta el contexto actual.

Primero y sobre todo, cuidar al equipo, cuidar al ser humano. Estamos pasando un momento difícil como sociedad y cada persona lo vive diferente, entonces quienes tenemos responsabilidad de liderazgo debemos procurar ponerlas en primer lugar y luego pensar en las demás cosas.
Segundo, entender que el trabajo remoto ya es realidad para mucha gente. La pandemia lo intensificó aún más y eso no tiene vuelta atrás. Esto significa que cualquier estrategia de ciberseguridad tiene que contemplar que las personas acceden a la red y trabajan desde cualquier lugar, es decir que ya no existe el perímetro y no volverá a existir, este es un punto a considerar.
Como tercer punto quiero cerrar con un mensaje positivo: la adversidad nos trae oportunidad. Lo mejor está por venir

Imagen: Ingrid Bezerra
Monumento a las banderas, Sao Paulo

# Ricardo Pérez D'Brot

Subgerente de Inteligencia y Respuesta de Ciberseguridad en Interbank, Perú.

por **Juan Marino y Jorge Prinzo**

Imagen: Goldbug, Pixabay
Machu Pichu, Perú.

*En este reality check con Ricardo, ponemos a jugar su vasta y enriquecedora experiencia luego de más de quince años de trayectoria en el mercado de la Banca en Perú. Los invitamos, queridos lectores, a acceder al reto de "desafiar al status quo" y revaluar su estrategia de ciberseguridad.*

Contenido audiovisual

**Hoy estás protegiendo a una de las principales entidades financieras de Perú; ¿cómo hackeás la predicción de que te van a robar credenciales?**

Es una realidad: definitivamente es algo que pasa. Las personas tienden a usar las mismas credenciales en múltiples servicios, o usan la clave corporativa cuando se registran en una página web... Entonces no es un tema del cómo sino del cuándo te va a pasar...

**Tienes que vivir con eso...**

Exacto: tienes que vivir con eso y por eso nuestro *aproach* se enfocó en reforzar la parte cultural, porque cuando eso pase necesitarás tener esa línea totalmente concientizada, totalmente preparada. Que las personas ya sepan: "esto es sospechoso", "esto es malicioso", "yo no lo he pedido", "yo no participé de este sorteo"... todas esas *red flags* que aparecen ante mensajes bastante tentadores. En los últimos años hemos estado dándole vueltas y vueltas, y fue motivo de muchas conversaciones cuando armamos presupuestos y cuando armamos la estrategia: podíamos invertir un montón de plata en infraestructura, en *firewalls*, en antivirus, *antimalwares* de última generación... pero siempre llegamos al factor humano.

**Cuando decidiste invertir, uno de los elementos que elegiste no dejar afuera es la conciencia de los usuarios.**

Así es: eso fue no negociable. Hemos tomado costos de oportunidad en otros proyectos, llevarlos a otros momentos u otros años, pero definitivamente el tema de cultura, una vez que comenzamos a reforzarlo ha sido un tema constante, y creo que es el que más frutos nos ha dado. Si nuestra superficie de ataque era de un veinticinco por ciento, hoy es de un dos o tres por ciento.

**Han podido medir eso...**

Sí; un dos por ciento no te hace inhackeable, pero tu superficie es menor.

**Leí un informe en el que cuentan que en Interbank hacen escenarios de simulación de crisis, por ejemplo qué pasaría si sufren una brecha de ciberseguridad. ¿Cómo les fue al hacer esos escenarios?**

Muy bien; participaron desde los mandos de toma de decisión hasta los mandos tácticos y operativos de la compañía, y a mí me sorprendió cómo se involucraron, cómo participaron en el primer ejercicio. No era para ellos algo así como "dos horas con la gente de seguridad... qué aburrido..."; no: se tomaron en serio ese juego de rol, asumieron el rol y plantearon "bien, ¿qué haríamos si nos pasa esto, que sería algo verdaderamente trágico para la organización?"; y "a ver, explícanos más". Empezaron a preguntar; obviamente no todos van a ser especialistas en ciberseguridad, pero les fue generando esa curiosidad, y a fin de cuentas, un *hacker* es siempre una persona muy curiosa, y de alguna manera los estamos metiendo en esa cultura *hacker*.

¿Hay alguna experiencia, o algo que hayas visto, de lo que hayas aprendido "esto funciona y esto no"?

Hace unos años era una práctica común en la industria la "seguridad por oscuridad"; era pensar "si encuentro algo, lo escondo, no hablo de eso, lo guardo bajo siete llaves", y eso nos ha demostrado que debería ser un tema de apertura, conversar sobre eso. Hay foros y foros, donde puedes hablar y dónde no; en un foro público no puedes decir "estos son mis *firewalls*, esto es lo que hago". No puedes exponer tu arquitectura porque te vuelves un *target*. Pero sí es una conversación sana decir "tenemos este problema, ¿cómo lo solucionamos?". No es algo solamente del equipo de seguridad, sino que es del equipo general de tecnología: involucras a tecnología, involucras a redes, involucras un montón de áreas, y se vuelve multidisciplinario, se vuelve enriquecedor. Tienes que hacer ese *shift*, un poco de *mindset* incluso en el equipo de seguridad, que puede ser receloso; tiene que ser más abierto para poder subsanar esos temas lo más rápido posible.

Pensando en el estado actual de madurez en ciberseguridad, ¿qué dirías: hay ventaja ofensiva o hay ventaja defensiva?

El atacante siempre va a tener la ventaja porque está constantemente atacando, constantemente estresando tu capacidad de dar respuesta. Nosotros podemos tener equipos que están tratando de prevenir eso, o adelantarnos a lo que pueda hacer el atacante, pero el atacante a fin de cuentas lo que necesita es una forma de hacerlo bien. Nosotros necesitamos sesenta y cinco mil quinientas treinta y cinco de esas formas en que él falle, pero a él le basta una.

Imagen: Patricia Van den Berg, Pixabay
Templo Coricancha, Cusco

Qué injusto eso, ¿no? Por último, teniendo en cuenta el contexto, en medio de una pandemia, con remotización del trabajo, por favor comparte con nosotros tres recomendaciones para elevar el nivel de seguridad el sector financiero y el sector público.

Primero, reforzar la cultura de seguridad para que las personas se vuelvan una capa más dentro del ecosistema. Definitivamente eso es algo con lo que nos ha ido bien, y creo que debería extenderse a todas las compañías, porque mientras más resilientes seamos como mercado en general, menos atractivos vamos a ser para los defraudadores. Usualmente lo que vemos es que el fraude es cíclico: van de prueba en prueba. Pero si todos empezamos a subir el nivel, no sólo colaboradores sino también clientes, entonces por ejemplo un tema de *phishing* va a ser cada vez menos atractivo para el delincuente porque ya no va a tener gente que caiga. Lo segundo es empoderar la seguridad del *endpoint*. Ahora, con la nueva forma de trabajar, el *endpoint* se ha vuelto totalmente crítico. Antes era una pieza importante pero no crítica dentro del esquema de ciberseguridad, porque se prefería priorizar temas perimetrales, un cien por ciento de visibilidad de los controles, y después ir bajando; la última línea de defensa era el *endpoint*. Ahora no, más bien la primera línea de defensa es el *endpoint*, de la mano con el usuario. Entonces ya no es negociable que tengas un antivirus desactualizado, un *firewall* de estaciones desactivado, el tema del control de dispositivos... Son temas que suenan básicos, pero tienes que hacer lo básico bien. Una vez que lo tienes maduro te empiezas a mover hacia todos los otros esquemas más complejos. Y lo tercero es no descuidar todas las otras líneas que tenías. Suena tal vez un poco contradictorio, pero estos son los momentos en los que se puede tratar de cambiar las cosas, de evolucionar. Si antes había ciertas restricciones porque las personas estaban en la oficina, bueno, hemos tenido todo este año y vamos a tener probablemente por un buen tiempo más a personas que no están conectadas a esa red. Quitemos algunos factores que nos restringen, y veamos qué podemos hacer. Podríamos desafiar esta parte del *status quo* y decir "voy a rehacer mi postura de seguridad". Ahora es cuando podemos tomar ese tipo de decisiones porque justamente las facilidades se están dando para que las personas hagan teletrabajo. Entonces probablemente no sea necesario un esquema de seguridad tan complejo en la red sino migrar a un esquema más predictivo, avanzado. Ahí depende de cada realidad, lo digo para que lo cuestionen, por qué no.

Súper claro, Ricardo, nos quedamos con esos tres puntos. Muchísimas gracias por habernos dedicado este tiempo valiosísimo y sobre todo por cuidar la banca, que es algo de lo que dependen mucho los ciudadanos. Así que, un placer y seguimos en contacto. Gracias.

El placer es mío, Juan. Muchas gracias

# Columna

Video:
Cisco IoT
Networking Overview

Imagen: Trevor Bobyk, Unsplash.

# El Gran Hermano IoT

## Ciberseguridad en ambientes hiperconvergentes


por **Freddy Macho**

Miembro Comisión Expertos
Laboratorio Ciberseguridad OEA
Presidente Centro de Investigación
de Ciberseguridad IoT – IIoT
Coordinador del Centro de
Ciberseguridad Industrial (CCI)
Chairman IoT Security Institute LATAM


El objetivo de esta columna es acercarnos a los diversos componentes que integran IoT, al igual que identificar los habilitadores que impulsan estos ambientes y sus mejores prácticas, los protocolos de comunicación y los estándares que existen en las diversas verticales de Internet de las cosas a nivel de ciberseguridad.

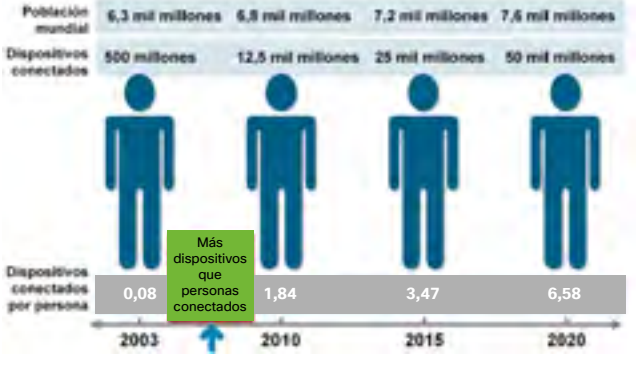
Los invito a transitar la lectura de esta primera entrega que busca incentivar, de alguna forma, la ávida necesidad que tenemos como seres humanos de alimentar con una pequeña cuota el conocimiento de estos ambientes.

El auge de Internet de las cosas o IoT proporciona un entorno donde los objetos cotidianos se alían y contribuyen juntos en un sistema que da paso a la convergencia de los dispositivos inteligentes y los dispositivos conectados convencionalmente. IoT se considera la tercera ola mundial de la industria de la información después de los inventos de la computadora e Internet.

En la actualidad, se encuentran conectados al Internet de las cosas una diversidad muy amplia de objetos que van desde automóviles, equipos médicos, termostatos, sistemas de iluminación y muchos otros dispositivos. La visión completa de una empresa de este rubro es que se diseñará, desarrollará e incorporará un mundo de sensores de bajo costo, los cuales se podrán programar para generar soluciones o servicios que podrán decirnos por ejemplo, que reduzcamos la cantidad de cafeína que consumimos después de las 8 p.m. o que se enciendan las luces de la habitación aumentando gradualmente su brillo en el preciso instante en el que se despierta de un sueño profundo al comenzar el día.

La presencia de Internet de las cosas es muy amplia en nuestras actividades tradicionales. Normalmente se divide en verticales. Mientras que para principios de la década del 2000 se consideraban seis de ellas, en la actualidad, se estima que existen cerca de 30 verticales, algunas de ellas robustas y en pleno funcionamiento, otras en desarrollo o de reciente creación. Es por este motivo que el concepto de IoT se considera como una definición viva, ya que su constante crecimiento y la incorporación de diversos aportes y virtudes proveen nuevas características a esta definición.

Aproximadamente 6.300 millones de personas vivían en el planeta en 2003 y 500 millones de dispositivos se encontraban conectados a Internet según un informe de Cisco en 2011. Esto indica que había menos de un dispositivo (0,08) para cada persona. En proyecciones de Cisco para el año 2020 se estimaba la existencia de 50 mil millones de dispositivos conectados a Internet, número, que en medio de la actualidad global enmarcada en una pandemia, impulsa la hipótesis de que esta proyección ha quedado corta.




Fuente: Cisco IBSG, Abril de 2011


Fuente: Fostec & Company

## Importacia de la ciberseguridad

Debido a lo antes expuesto, el probable impacto de no contar con el correcto nivel de ciberseguridad en el momento en que miles de millones de dispositivos inteligentes se conectan a Internet bajo el paraguas de IoT e interactúan entre sí para llevar la información correcta a las cosas correctas, en el lugar y momento precisos a través del canal correcto, sería simplemente catastrófico. Una falla de ciberseguridad podría impactar de forma muy diversa, por ejemplo en la posibilidad de que se creen espacios que faciliten la creación de ilícitos, la caída o indisponibilidad de servicios críticos, poner en riesgo la soberanía de un país o, más importante aún, causar la pérdida de vidas humanas.

Internet de las cosas es un nuevo cambio de paradigma en el mundo de la tecnología de la información (TI), donde las cosas tienen identidades digitales, funcionalidades de monitoreo con inteligencia artificial (IA) y se pueden ubicar, rastrear, seguir, controlar y automatizar.

La convergencia de las actividades de las tecnologías de la información (TI) tradicional, las tecnologías de

operación (OT) o redes industriales y la computación en la nube dan como resultado lo que he impulsado con el nombre de hiperconvergencia. Este proceso facilita la interacción entre la IoT y las smarcities y el IIoT (Industrial Internet of things) y las infraestructuras críticas, lo que amplía notablemente la complejidad de poder entregar niveles de ciberseguridad acordes a la necesidad que actualmente se requieren. La aceleración hacia la digitalización y el trabajo remoto han impulsado que el uso de la hiperconvergencia se incremente con enorme rapidez.

El despliegue del IoT plantea muchos problemas de ciberseguridad derivados de la propia naturaleza de los objetos inteligentes, por ejemplo, la adopción de algoritmos criptográficos ligeros, en términos de requisitos de procesamiento y memoria, y el uso de protocolos estándar, así como la necesidad de minimizar la cantidad de datos que pudieran quedar expuestos en el intercambio entre nodos.

La integración del mundo físico en el tejido de la web impone requisitos de ciberseguridad avanzados que deben satisfacerse para garantizar un control estricto sobre la interacción de los servicio en IoT.

La necesidad de elevar los niveles de ciberseguridad en los ambientes IoT – IIoT son inexcusables en Iberoamérica y por este motivo forman parte de los trabajos que son desarrollados por el grupo de Expertos del Laboratorio de Ciberseguridad para los Parlamentos de las Américas de la Organización de Estados Americanos (OEA), del cual tengo el gusto de participar. Uno de sus objetivos es generar un primer documento sobre "Principios Rectores de la Ciberseguridad IoT", cuyo fin es el impulso de la ciberseguridad en la región y al que podrás acceder desde esta edición de Bridge.

Por hoy, dejamos aquí. Hasta nuestro próximo encuentro

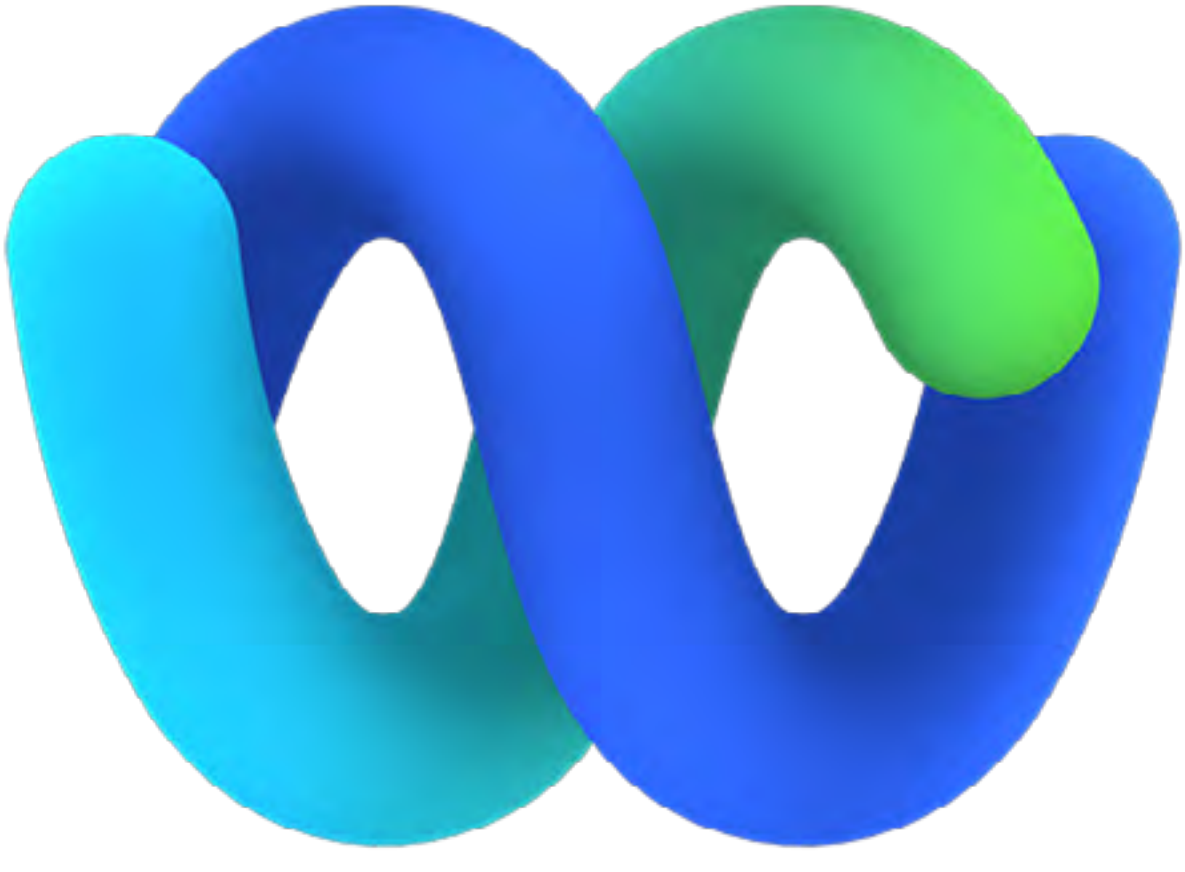
# Colaboración Segura

En 2020 la pandemia puso al mundo en modo online. En este artículo, el experto Adriano Gaudencio reflexiona sobre el modelo de trabajo en el corto plazo, que propone oficinas adaptadas a la modalidad híbrida y herramientas que ofrezcan una experiencia amigable, colaborativa y segura.

¿Cuáles son los retos que encaramos para la vuelta a la oficina? Cisco observa que, de ahora en adelante, el trabajo será híbrido. Acreditamos que el 98% de las reuniones ya no van a tener a todas las personas adentro de una oficina, sino que siempre habrá quienes sigan el encuentro online. El 54% de los empleados ya asumieron la posibilidad del trabajo remoto y están preparados para hacerlo. Según nuestras investigaciones, se estima que al menos ocho días del mes la mayoría de los empleados hará *home office*. Para alcanzar esta conclusión, Cisco entrevistó más de 1.000 empresas de distintos mercados. Consideramos que la muestra es significativa. Por otra parte, otra tendencia importante es la inclusión. Hoy, con la posibilidad de trabajo remoto, es posible abrir la búsqueda de talentos en distintas partes del mundo.

## El futuro es ahora

En esta instancia, una meta importante es asegurar una experiencia óptima y segura, tanto para la vuelta a las oficinas post cuarentenas, como para el



por **Adriano Gaudencio**

Líder de Ventas de Colaboración para América Latina de Cisco

trabajo remoto. Por eso Cisco está desarrollando la "Colaboración del Futuro". Se trata de alcanzar una colaboración inclusiva, que integre a todos, y habilite una experiencia remota 10 veces mejor que la presencial. Pero ¿puede ser la experiencia remota mejor que estar frente a frente con una persona, hablando, interactuando? Veamos con un ejemplo que, en algunos casos, sí: dentro de la aplicación, Cisco cuenta con la funcionalidad de traducción simultánea, en tiempo real, algo que tiene claramente una ventaja en caso de que los integrantes no hablen todos el mismo idioma. Recordemos que Cisco Webex es una plataforma de colaboración segura, que incluye aplicaciones para mejorar el trabajo en equipo de cada empleado, con herramientas de mensajería, intercambio de archivos, pizarra blanca y realización de tareas, entre otras muchas funciones, que van más allá del tiempo de una reunión o conferencia. En ella, Cisco integró varias aplicaciones en una sola, que se comparte en la nube y logra entregar variados servicios, como Webex Meetings, que es una plataforma para hacer videollamadas; Webex Teams, que permite enviar información a través de mensajes directos y de equipo; y el Contact Center. Podríamos decir que es el punto de partida del trabajo remoto. La idea es ofrecer una excelente herramienta para trabajar desde casa. Así como es necesario tener una buena silla o una computadora óptima, también es imprescindible la calidad de la voz o la imagen y acceder a distintos dispositivos que mejoran la experiencia del usuario. Cisco está avanzando en esta tarea.

A la vez, para nosotros es sustancial cuidar a los clientes de nuestros clientes. Por eso, lanzamos recientemente Cisco Webex Contact Center en la nube de Brasil, desde donde se atenderá a todos los clientes en América del Sur. Todas las integraciones con el cliente pueden ser gestionadas como una experiencia unificada directo de la pantalla, y es posible interactuar con las redes sociales, Facebook, Instagram, LinkedIn.

## El valor de la Seguridad

Cisco tiene políticas de seguridad muy avanzadas, por eso, una de las fortalezas de la plataforma Webex es su seguridad, que está presente de "punta a punta", no existe ningún quiebre en el proceso, ofreciendo una ventaja competitiva única. La Agencia Nacional de Seguridad de Estados Unidos publicó un informe que avala la política de seguridad de Cisco, confirmando que es *end to end*.

Con respecto a las vulnerabilidades, muchas veces están relacionadas a las credenciales, es decir, a la identificación de la persona que tiene acceso al sistema. La colaboración y la seguridad de Cisco se engloba en una solución completa. Ya sea que la persona trabaje desde la casa o desde la oficina, hay garantía de seguridad, se protege el acceso a Internet, los dispositivos, la confidencialidad de los archivos y de los datos, la autenticidad de las personas que trabajan. También se puede detectar lo que sucede en todas las soluciones para accionar una respuesta proactiva y garantizar que el trabajo remoto se haga en forma segura.

## ¿Cómo facilitar un regreso seguro a la oficina?

A través de la tecnología, Cisco garantiza el trabajo remoto, y también el presencial, certificando la seguridad y la calidad de la experiencia, controlando los procesos para aumentar la productividad y optimizar el trabajo.

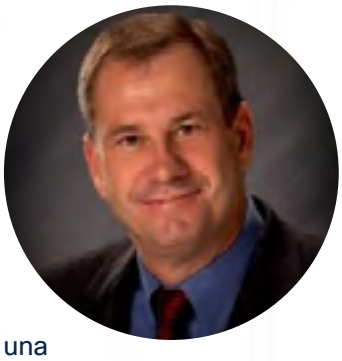
Estamos preparando ahora la vuelta a la oficina. En tiempos de distanciamiento y seguridad sanitaria, la herramienta de Cisco detecta, por ejemplo, si en una sala hay más personas que las recomendables, y avisa al responsable para que se pueda tomar una acción. También tiene sensores de temperatura, que detectan si un ambiente está con la temperatura ideal para que se pueda trabajar con comodidad; y un sistema que notifica si el ambiente se higienizó al finalizar una reunión y está en condiciones para el inicio de un nuevo encuentro.

El objetivo es tomar lo mejor del mundo analógico, y lo mejor del mundo digital, potenciando ambas áreas. Los dispositivos de Webex integran los dos procesos. Son herramientas de seguridad y colaboración, diseñadas para adaptarse a la coyuntura de la mejor manera; y permiten navegar por las distintas soluciones amigablemente, bajo el paraguas de la ciberseguridad de Cisco

Conozca y pruebe de forma gratuita las soluciones de seguridad de Cisco Secure

# Veinte años en el negocio con Gary Becklund

por **Soledad Clar**



**¿Por qué construiste una carrera de 20 años en Cisco?**

Cisco para mí, es una de esas pocas compañías en las que tienes realmente la oportunidad de expandir tus habilidades sin dejar nunca la empresa. Puedes cambiar de roles, adquirir nuevas responsabilidades y aprender cosas distintas siempre que estés dispuesto y abierto a hacerlo. Te da la satisfacción de expandirte sin necesidad de irte y hacerlo en otra compañía. Esa habilidad de Cisco es realmente lo que me mantuvo aquí por 20 años.

**¿Qué has aprendido de la diversidad cultural que existe en América?**

Primero debo decir que muchos años atrás, cuando comencé a relacionarme con el equipo de Latinoamérica, Ghassan Dreibi y otros miembros, estaba realmente abierto a las diferencias culturales con Estados Unidos.

Somos una compañía global pero muchos de nosotros solo nos habíamos dedicado a trabajar dentro del mercado de US, con muy poca exposición y entendimiento de otras culturas. La experiencia ha hecho realmente que abra mis ojos a la importancia de las originalidades de esta cultura. El equipo de Latinoamérica es uno de mis favoritos porque los latinoamericanos siempre han sido las personas más acogedoras y amorosas, ha sido siempre una alegría y un placer haberlas conocido.

Creo que si nos esforzamos encontraremos también esas características en otras culturas, pero nunca apreciaremos el valor y los beneficios de la diversidad cultural hasta el momento en que tengamos la posibilidad de sumergirnos en ese ambiente. Por eso estoy enormemente agradecido por la oportunidad que tuve de pasar mucho tiempo en América Latina.

**¿Mirando hacia atrás cuál es el mayor desafío que has visto en la industria?**
El mayor desafío es sin duda la velocidad del cambio que está ocurriendo. Y como nos hemos convertido en una compañía mucho más grande es dificultoso para nosotros mantenernos tan ágiles y flexibles como algunos de nuestros competidores de nicho. Entonces se trata de un balance, entre aprovechar el poder de Cisco y del mismo modo adoptar esa velocidad de cambio y ser capaces de modificar la dirección y adaptarse a esa celeridad. Creo que ese es el desafío más grande que pude ver en Cisco, es realmente un arduo balance.

**¿Cuál es el mayor desafío por venir?**
Voy a utilizar un dicho: "No sabemos lo que no conocemos" -"we don't know what we don't know"-. Los actores maliciosos y las amenazas evolucionan constantemente. Hemos visto tantos cambios en los últimos 5 ó 6 años que hemos creado GSSO (Global Security Sales Organization) dentro de Cisco. Mirando hacia atrás, como era la industria de Seguridad hace 5 años y cómo es hoy: hemos cambiado tanto, y las amenazas han cambiado tanto, que creo que el desafío será seguir el ritmo y mantenernos por encima de estas amenazas que evolucionan día a día.

**¿A qué se parece el éxito?**
Risas. Es una muy buena pregunta. Recuerdo que cuando recién ingresé a Cisco, le hice a mi primer jefe esa misma pregunta. En ese entonces éramos una cultura distinta, pero es igual de importante. Al hacer esta pregunta él me mira y me dice, "es muy simple, al final del día tienes que cumplir con los números". En ese momento me reí, pero hay mucha verdad en ello. Creo que cada uno de nosotros, de los que estamos en Cisco, estamos aquí porque creemos en la compañía. Creemos en la visión y en la dirección en la que Cisco se mueve. Entonces para mí el éxito no es sobre mi cargo, mi puesto de trabajo o sobre el reconocimiento, aunque todos disfrutamos del reconocimiento, el éxito es sobre la certeza de saber que hice todo lo que pude para contribuir cada cuatrimestre al éxito de Cisco. Cuando eso ocurre yo me siento exitoso, estoy orgulloso de Cisco cuando alcanzamos esos resultados y esos números. Entonces para mí el éxito se parece al sentimiento de que hice una contribución a la compañía durante cada cuatrimestre.

**¿Cuándo se ha sentido más valorado en cuanto a la relación con los clientes?**
Debo decir que es cuando estamos en la mesa discutiendo sobre resultados comerciales y no sobre soluciones tecnológicas. Porque ahí siento que hemos ganado la confianza del cliente como compañía, como equipo de trabajo, y también como persona, entonces allí siento que somos un socio de negocios del cliente y no solo un proveedor de tecnología.

**¿Qué significa productividad para usted hoy?**
Productividad tiene que ver con muchos aspectos dependiendo de cuál sea el rol o función que estemos cumpliendo aquí, en Cisco. Como es de esperar en el sector de ventas, productividad significa alcanzar los números requeridos. En cambio productividad dentro de SBG (Security Bussiness Group) tiene un significado distinto, allí productividad tienen que ver con innovación, con velocidad y *time to market* para satisfacer las necesidades de los clientes. Entonces el significado y la definición de productividad dependen realmente del rol y función que cada uno cumple en la empresa.

**¿Cuál es la mayor preocupación en seguridad?**
Creo que volvería a un comentario que hice anteriormente donde mencionaba "no sabemos lo que no conocemos" a medida que las amenazas evolucionan. Mi mayor preocupación sobre la industria de ciberseguridad tiene que ver con la capacidad de la industria de estar un paso adelante de la evolución de las amenazas y de los delincuentes informáticos.

**¿Cuál es la debilidad más común que interfiere en el camino al éxito?**
Permitir que los errores te paralicen. En Cisco decimos "si vas a fracasar hazlo rápido". Errores y fracasos nos van a suceder a todos nosotros, lo que hacemos con esos fracasos puede tanto reprimir como alimentar tu capacidad de ser exitoso. Entonces lo que hacemos con los errores y cómo los manejamos creo que es lo que más contribuye al éxito.

**¿Qué hace que alguien sea un buen líder?**
En primer lugar un líder te empodera para hacer tu trabajo. Tiene la seguridad y la confianza para dejarte desplegar en tu rol y permitirte hacer el trabajo para el cual te contrataron. Un líder muestra también empatía cuando suceden errores y te motivará.
Entonces para mí, es alguien que nos fortalece en nuestro trabajo, que muestra empatía cuando encontramos obstáculos y está ahí para alentarnos, guiarnos y motivarnos cuando lo necesitamos.

**Por favor, comparte con nosotros un consejo para quienes quieren crecer en su recorrido dentro de la compañía.**
Recuerdo un evento para líderes en San José, en algún momento cerca de cuando Cisco adquirió TANDBERG. Para esa época Chuck Robbins y Mark Patterson estaban liderando las oficinas de América. Chuck y Mark fueron a la cena de líderes que estábamos teniendo y al final hubo una sesión de Q&A (Preguntas y Respuestas por su sigla en inglés). Entonces uno de los managers le preguntó a Chuck por su carrera en Cisco y cómo llegó a donde estaba. Entonces Chuck dijo que si miraba hacia atrás se daba cuenta de que muchas veces en la carrera nos piden hacer cosas y a veces solo nos levantamos y las hacemos. Y nos tenemos que mover horizontal o lateralmente en la empresa antes de movernos hacia arriba. Y yo incorporé esa idea a mi carrera. Si miro hacia atrás realmente aproveché eso que dijo Chuck y comencé a desafiarme a mí mismo tomando diferentes puestos de liderazgo dentro de la compañía, algunos incluso nuevos e incómodos para mí que era un líder de ventas, ese fue un gran punto de inflexión dentro de Cisco. Entonces yo motivaría a todos a probar nuevas cosas dentro de la compañía, a expandir sus experiencias y capacidades, porque ahí es donde te conviertes en un recurso más valioso para Cisco. Y mientras me estoy retirando me gustaría pensar que yo fui un recurso valioso, pero más importante aún, que Cisco ha sido para mí un recurso valiosísimo para aprender y crecer

Imagen: Free-Photos, Pixabay

Estudio de resultados en materia de seguridad de 2021: edición para pequeñas y medianas empresas.

# Crecer con una estrategia sólida de ciberseguridad

El Estudio de resultados en materia de seguridad de 2021 de Cisco reúne las experiencias de más de 4800 profesionales de TI, seguridad y privacidad de todo el mundo y es una consecuencia del estudio más amplio que se centra en las pequeñas y medianas empresas (pymes).

La defensa de las organizaciones contra las amenazas cibernéticas es difícil para cualquier empresa, independientemente de su tamaño. Pero esto es particularmente cierto para las pymes porque sus recursos suelen ser limitados y deben centrarse en gran medida en hacer inversiones que generen resultados impactantes. Los riesgos son mayores y priorizar lo más importante es fundamental para el éxito. Ayudar a identificar esas prioridades es de lo que se trata este informe.

## Detallamos aquí los puntos más relevantes

### Hallazgos del estudio

**Las cosas buenas vienen en paquetes pequeños:** Casos convincentes de que el tamaño más pequeño de la empresa no obstaculiza la posibilidad de grandes triunfos a la hora de desarrollar enfoques de seguridad exitosos.

**La seguridad de las pymes se ocupa de los negocios:** Este estudio pone de manifiesto el concepto de que la seguridad y el negocio en general comparten una relación integral en las pymes.

**Prioridades:** Las pequeñas y medianas empresas que afirmaron contar con una estrategia sólida para guiar las iniciativas de seguridad fueron significativamente más propensas a informar resultados exitosos.

**El éxito radica en prepararse para el fracaso:** Entre las 25 prácticas de seguridad probadas, las capacidades de recuperación rápida tras un desastre fueron el mayor diferenciador de éxito entre las pymes y las organizaciones más grandes. La planificación de la resiliencia es una estrategia ganadora.

**Las amenazas modernas precisan tecnología moderna:** Las pymes que mantuvieron una pila tecnológica moderna lograron mayores tasas de éxito en cada uno de los 11 resultados de seguridad medidos.

**Los resultados que demuestran los factores de éxito en pequeñas y medianas empresas están organizados en tres categorías:**

- hacer posibles los negocios,
- administrar el riesgo y
- operar con eficiencia.

Te invitamos a acceder a estas conclusiones desde aquí

CISCO

# SECURE


The bridge to possible