Año 2. Número 5.

Bridge

CISCO SECURE

Ciberseguridad

Smart Energy
por Freddy Macho

Seguridad en la nube
Entrevista Mariano O'Kon

Especial
Cómo evitar el síndrome de burnout

Contenido audiovisual

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

Esta es una edición atípica de Bridge. El final de un año intenso nos invita a andar más despacio y reflexionar sobre lo vivido, sobre lo que sigue, sobre cómo seguir. Desde la redacción, elegimos hacernos más conscientes y promovemos la toma de consciencia. Elegimos darnos cuenta de que el equilibrio, la justicia sobre nuestro ser, nuestras elecciones basadas en el entendimiento, la voluntad, la responsabilidad y la escucha atenta de nosotros mismos y el otro son los pilares de un tránsito basado en el justo medio.

Dicho esto, cedo el tiempo que tomaría leer esta página completa a un lapso dedicado a ti, a centrarte en ti pacíficamente. Tú eliges como, pero antes, respira profundo.

Te abrazo.

Imagen: Vectorpocket, Freepik.

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
Pablo Marrone

Fotografía e ilustración
Basanta Contenidos
Freepik
Pixabay
Unsplash

Agradecimientos
Teatro Border
Carlos Vieu
Osvaldo Briscioli
Nicolás Cacciabue
Isabella Cacciabue
Joaquín Cuadros
Santino Cuadros

Foto de Tapa
Arek Socha, Pixabay

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: Freepik.

Revista Bridge **Impresa / Digital**
Año 2. Número 5.

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

Editor General
Juan Marino

Agradecimientos
Laércio Albuquerque
Álvaro Rodríguez Larraín
Mariano O'Kon
Jackeline Carvalho
Militza González

Marketing

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

Bridge Nº 5

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*

CDA

Country Digital Acceleration

Imagen: Gonzalo Gallardo, Unsplash.

Chile

El pasado 17 de noviembre Cisco Chile formalizó el lanzamiento de su programa de aceleración digital con un evento digital del que participaron directivos de la empresa y expertos destacados de los sectores Comunidades conectadas, Minería y Energía.

Vive Acelera
Cisco Chile

El programa Country Digital Acceleration (CDA) es una iniciativa mundial de aceleración digital que busca generar una relación a largo plazo con el sector público, la industria y la academia. En Chile y otros países de la región esta iniciativa se materializa mediante el Advance Technology Center (ATC), un espacio de innovación virtual y presencial que tiene como objetivo ayudar al país a alcanzar todo su potencial digital y permitirá a los asistentes vivir experiencias únicas a través de la articulación de distintas tecnologías demostradas en casos de uso prácticos.

¿Por qué Chile?

La elección de Chile como país apto para la inversión en aceleración digital, innovación, desarrollo de capital humano y nuevos modelos de negocio en Minería, Energía y Comunidades conectadas estuvo dada básicamente por tres pilares:

- Es el país mejor habilitado en Latinoamérica para la transformación digital.

- Es el primer productor de cobre y renio a nivel mundial y el segundo en litio y molibdeno.

- El Gobierno de Chile busca contar con un ciberespacio libre, abierto, seguro y resiliente.

El impulso así concebido contemplará la Ciberseguridad como elemento imprescindible de cualquier desarrollo a llevarse a cabo.

Acelera, el evento

Presentado y coordinado por Bárbara Briceño, periodista de Emol, Acelera Cisco Chile 2021 contó con la presencia de representantes de la empresa y personalidades destacadas de las tres verticales elegidas para el impulso transformador. Aquí podrás leer algunos de los puntos sobresalientes de las ponencias de los invitados y vivir el evento completo desde el QR incluido en este artículo.

Claudio Ortiz
Gerente General, Cisco Chile

"En Cisco estamos convencidos de que a través de la tecnología podemos transformar y mejorar la vida de las personas, los procesos de las instituciones y acelerar los negocios en las empresas, por lo tanto es un placer para nosotros estar hoy presentando nuestro programa CDA conjuntamente con nuestro centro de co-innovación en el cual buscamos generar los espacios para la creación de nuevas ideas en pro de la transformación digital del país".

Ned Cabot
Director Senior de Digitalización para Américas, Cisco

"La misión de Cisco es impulsar un futuro inclusivo para todos y lo que hacemos en CDA para alcanzar este objetivo es manejar la innovación y la colaboración conjuntamente con socios. Nuestra idea es buscar cómo coordinar la innovación para acelerar las agendas digitales entre los sectores público, privado y la academia a fin de generar beneficios que deriven de la transformación digital en las comunidades".

"Tengo el privilegio de compartir que hoy estamos presentes con este programa en 44 países y hemos invertido e impulsado más de 1000 proyectos que lograron acelerar la digitalización y la creación de nuevas oportunidades de empleo".

Imagen: Juan Pablo Ahumada, Unsplash.

Sandra Eslava
Directora de Digitalización, Industrias y Segmentos, Cisco América Latina

"Chile tiene un espacio único en su visión de desarrollo en temas de acelerar la transformación digital. La razón de la implementación de este programa en el país es apoyar a las distintas industrias y sectores, evaluar las tecnologías necesarias para impulsar el negocio y, a través de ello, generar impacto social. Las distintas organizaciones podrán contar en el apoyo de nuestro centro donde la tecnología estará a su alcance para asegurar sus proyectos de digitalización, innovación e inclusión".

"En Chile, los principales casos de uso están enfocados en los sectores Energía, Minería y Comunidades conectadas, centrales para dar impulso a los servicios que permiten optimizar la inversión en el país, acompañar la reserva de los recursos naturales y, sobre todo, que esto suceda sobre la base de desarrollos ciberseguros. CDA nos lleva, además, a abrir espacios educativos y de desarrollo de competencias en talento humano a través de Networking Academy".

Panel Energía

Trinidad Castro
Directora, WEC.

"Nuevas tecnologías han marcado hitos históricos. En nuestro país, éstos tienen que ver con el marco regulatorio, la creación de institucionalidad del sector energético y la introducción de las energías renovables con una fuerza insospechada y gran vigor, ya que hoy día nos encontramos con una matriz de 24% proveída por energía renovable".

"Los desafíos de la descarbonización son multifactoriales. Uno de ellos tiene que ver con la transmisión de la energía a los hogares proveniente de distintas fuentes. Además, tenemos un desafío gigantesco en almacenamiento, es decir cómo concentrar energía por un período determinado. Sin duda, la tecnología puede colaborar mucho para lograr avanzar en este sentido".

Panel Comunidades Conectadas

Pelayo Covarrubias
Presidente de Fundación País Digital

"Cuando hablamos de Comunidades conectadas hablamos de ciudades que tienen integradas herramientas digitales, por eso es fundamental ayudarlas a hacerlo de forma más veloz".

"Las tecnologías estaban, con la pandemia lo que hicimos fue hacer una adopción más rápida de lo esperado".

"En Chile está la posibilidad de adopción tecnológica en pro de aumentar la productividad y mejorar la calidad de vida... La pandemia nos empujó a incorporar el cambio. Ahora debemos ver cómo desde nosotros adoptamos lo que falta. Uno de los sectores que ha quedado más rezagado es la Educación y creo que es ahí donde debemos poner un especial esfuerzo. Debemos nivelar a aquellos que han tenido menos posibilidades de aprender, la tecnología nos permite eso".

"Desde País Digital nos preocupan mucho las pymes, porque son las que están en el límite entre quebrar o vivir. Por lo tanto tenemos que ser capaces de empujarlas a una mayor adopción tecnológica".

Víctor Toscanini
Gerente de Ingeniería y Tecnología, Cisco Chile.

"Todo el desarrollo digital, definitivamente se aceleró con la pandemia. No tiene vuelta atrás. Sin embargo, estas adopciones tecnológicas tienen que poner a la persona en el centro y las comunidades conectadas deben hacer lo mismo con el ciudadano. En ese sentido cada comuna, cada ciudad y cada gobierno sabe las necesidades que tienen sus ciudadanos y la admisión tecnológica se tiene que adecuar a ellos. Incluso, todas las áreas que impactan las comunidades conectadas deben ser colaborativas entre sí para que esta incorporación sea fructífera y en beneficio de las personas".

Panel Minería

Diego Hernández
Presidente de SONAMI

"Es muy importante la incorporación de tecnología en minería, particularmente en Chile, pues aquí tenemos minas más maduras, nos ha subido el costo de producción y tenemos el desafío de mantener los márgenes operacionales. En este sentido la innovación, automatización e incorporación de tecnología digital es fundamental, es la herramienta que tenemos para poder mejorar la productividad".

"Hoy día con la conexión y los sistemas de comunicación la minería se ha convertido en una actividad colaborativa de muchos expertos que se complementan, diferente a hace varios años donde un mismo trabajador cumplía distintas tareas. Para esto el apoyo de la tecnología que facilite el trabajo a distancia es fundamental".

"Gracias a las distintas formas de monitoreo, la tecnología también nos ha permitido prever riesgos para los trabajadores y evitar accidentes".

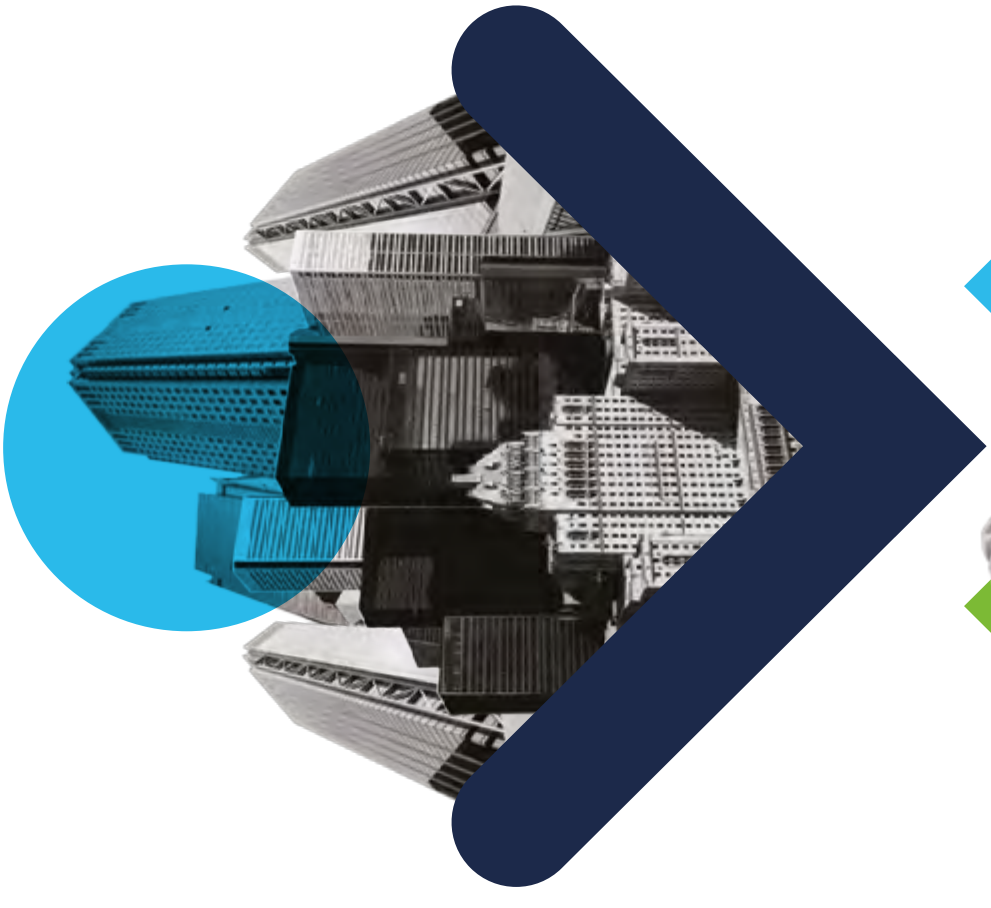
"La minería chilena está entrando en una nueva etapa tecnológica, además con muy buenas perspectivas ya que el litio y el cobre son indispensables para mitigar el cambio climático. Tenemos producción para muchos años"

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

CDA

Country Digital Acceleration

Imagen: Random Institute, Unsplash.

Colombia

Cisco anuncia el primer Advanced Technology Center (ATC) en Colombia

Como parte de la llegada a Colombia del programa Country Digital Acceleration (CDA), una iniciativa mundial de Cisco que impulsa la aceleración digital de los países a través de la innovación y digitalización, el último 2 de diciembre se anunció el lanzamiento en Bogotá del centro de experiencia e innovación Advanced Technology Center (ATC). Este espacio promueve el uso de nuevas tecnologías en pro de la modernización y digitalización del país, a través de la demostración de usos prácticos para las industrias de Educación, Salud y del Sector público, así como de todas las soluciones de seguridad.

Vive Accelerate day Colombia

El **Advanced Technology Center (ATC)** promueve una inmersión digital a través de un tour virtual 360° -hasta tanto esté controlada la pandemia- para mostrar con el uso de demos de inteligencia artificial, automatización, análisis de datos y cloud, las soluciones más disruptivas del portafolio de Cisco.

"Con este programa, reiteramos la confianza que ha depositado Cisco en Colombia durante estos 25 años, apoyando el fortalecimiento de la transformación digital del país. Asimismo, la inversión realizada en el ATC en Bogotá, permitirá apalancar el emprendimiento y la innovación en este momento de cambio; así como identificar nuevas oportunidades en las áreas de Educación, Salud y Ciberseguridad en el país ", comentó Javier Castro, country manager de Cisco Colombia.

25 años, y mucho camino por delante

"La labor de Cisco, desde un principio, fue crear conciencia sobre la importancia de integrar la tecnología en los negocios y comunidades para transformar vidas a través del cambio digital. Las alianzas entre empresa privada y Gobierno fueron fundamentales para la evolución tecnológica de Colombia, permitiendo construir una mejor sociedad, un mejor ecosistema de socios de negocios y, por ende, un país con mayor productividad digital", agregó Castro.

El trabajo con el Estado, gobierno tras gobierno, ha sido clave para el desarrollo tecnológico del país. Como un actor proactivo, Cisco ha colaborado en el desarrollo de proyectos con entidades como el Comando Conjunto Cibernético de las Fuerzas Militares y la OEA, en aspectos relacionados con ciberseguridad y ciberdefensa, así como en el avance de ciudades inteligentes teniendo a Barranquilla como uno de sus puntos de aterrizaje entre las urbes que prioriza en su proyecto Latinoamérica.

Es de resaltar también que, durante los últimos años, la empresa ha acompañado en el plan de Transformación Digital e Innovación. Asimismo, dentro del contexto generado por la pandemia, se han apoyado diferentes programas de educación al utilizar su plataforma de Colaboración Webex en Universidades. Otra área de trabajo ha sido Telesalud, facilitando la conexión de unidades de cuidado intensivo de hospitales regionales con hospitales en ciudades principales y poder permitir una comunicación segura entre el cuerpo médico a nivel nacional.

¿Por qué Colombia?

La apuesta de inversión en este país estuvo dada principalmente por las siguientes características:

- Ubicación geográfica privilegiada, ya que el país cuenta con fácil acceso a mercados globales.

- Inversión extranjera, pues la economía colombiana es una de las más sólidas y estables de Latinoamérica.

- HUB de innovación de productos y servicios que generan valor agregado y empleo calificado.

- Competitividad y equidad, ya que se ubica como el segundo país latinoamericano con el mejor desempeño ambiental.

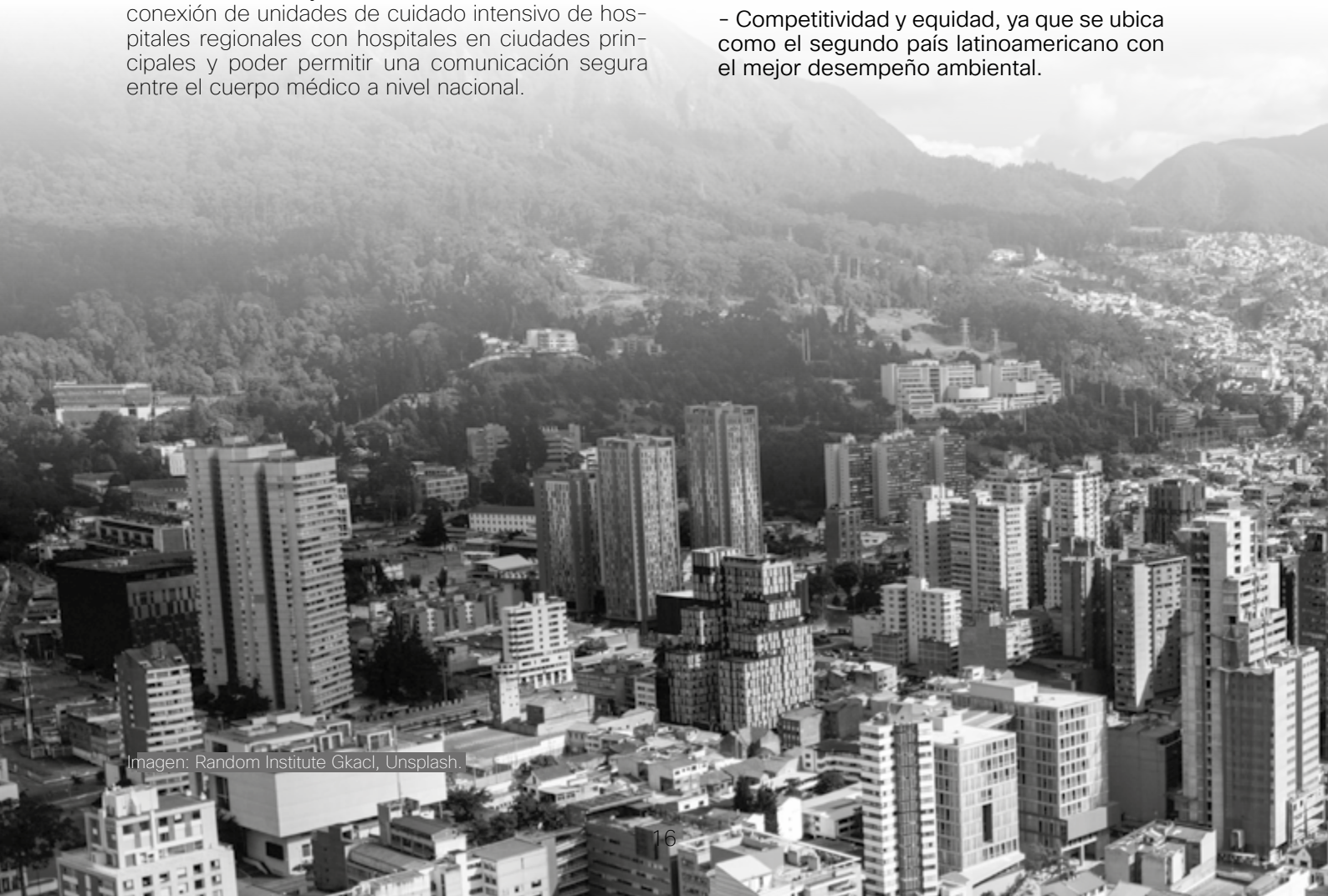


Imagen: Random Institute Gkacl, Unsplash.

Cisco Accelerate day, el evento

Como impulso al lanzamiento oficial, Cisco organizó un evento digital que contó con la presencia de líderes de la empresa y representantes destacados de organizaciones asociadas y clientes. Así, bajo la presentación de Inés María Zabaraín se fueron sucediendo las conversaciones que echaron luz sobre esta iniciativa. Aquí compartimos contigo las citas más relevantes de los invitados. Además, podrás vivir el evento completo desde el QR incluido en este artículo.

Santiago Pinzón
Vicepresidente de Transformación digital, ANDI

"Cisco apuesta a hacer cosas más grandes en el país: ayudar al trabajo remoto, a que tengamos mejor conectividad, a facilitar al desarrollo de territorios y ciudades inteligentes. Cisco le apostó a Colombia y hoy quiere ayudar a que sea un país más digital, más influyente y más sostenible. Felicitaciones".

Alberto Samuel Yonai
Presidente CCIT

"La corporación Cisco ha sido una pieza clave en la modernización de diferentes sectores de la economía en Colombia y con este nuevo esfuerzo demuestra una vez más su gran compromiso con el país. Gracias Cisco, adelante con estas importantes iniciativas".

Alison Treppel
Secretaria ejecutiva del CICTE, OEA.

"Nuestra colaboración con Cisco, particularmente en los últimos dos años, ha impulsado diferentes iniciativas de ciberseguridad e innovación en la región y es una alianza de la cual estamos muy orgullosos. Ésta ha derivado en tres iniciativas de alto impacto: los Consejos de Innovación en Ciberseguridad (dos de ellos realizados en Colombia), el Fondo de Innovación en Ciberseguridad (que ha financiado doce proyectos en la región, dos de ellos en Colombia) y el lanzamiento de los Cursos de Fundamentos esenciales de Ciberseguridad. Estamos convencidos de que estas acciones entre muchas otras contribuirán a construir un ciberespacio más seguro para Colombia y para la región".

Freddy Garcia
Líder de Estrategia, SENAsoft.

"Con las herramientas de vanguardia que Cisco nos ha entregado, hemos podido trasladarlas a nuestros instructores, aprendices y egresados para actualizarse y evolucionar al ritmo de la industria. Además, con Cisco hemos logrado tener el soporte, no solo profesional sino también amigo, para poder operar de forma virtual, lo que nos permitió sacar todos los proyectos adelante sin que nada nos detenga".

María Claudia Lacouture
Directora ejecutiva AmCham, Colombia.

"La transformación digital es una necesidad, una realidad que está ayudando a reducir brechas en temas clave como la prestación de servicios médicos, la educación y el servicio público entre otros. En este objetivo tenemos que resaltar el aporte que por más de 25 años ha desarrollado Cisco en nuestro país, acompañando con innovación, buenas prácticas y el soporte de calidad para construir un desarrollo sostenible. Estamos seguros que vendrán otros 25 años de valioso aporte. Muchas felicitaciones".

Comandante Hans García
Anestesiólogo intensivista, Hospital Militar Central

"Durante la etapa más fuerte de la pandemia en 2020, había preparado dos conferencias relacionadas a la vía aérea y ventilación mecánica en pacientes afectados por COVID, previstas solo para algunos miembros del personal médico de nuestro hospital. Gracias a la incorporación de la plataforma Webex hemos podido masificar la capacitación y la interacción entre diferentes centros y regiones e incluso fuera del país".

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

"Tanto desde la posición que desempeño actualmente como en otras anteriores, la experiencia que hemos tenido con proyectos transformacionales en temas tecnológicos con Cisco han sido muchas y considero que ha sido una práctica muy satisfactoria y con muy buenos resultados. Más allá de eso, hemos desarrollado proyectos que van mucho más allá y que tienen que ver con la evolución de capacidades para comprender el ciberespacio, por ejemplo las Olimpíadas Cibernéticas Internacionales y varios ejercicios de gestión de crisis cibernética, lo que ha contribuido a fortalecer las capacidades en el componente cibernético de nuestro país. Estamos seguros que seguiremos trabajando de la mano para lograr un país cada vez más empoderado y resiliente frente a estos temas"

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

Columna

Smart Energy

La vertical de IoT/IIoT que impulsa el desarrollo de nuestras sociedades.

La población mundial está creciendo de manera sostenida y según estudios de las Naciones Unidas, aproximadamente 83 millones de personas se agregan a la población mundial cada año. Se estima que actualmente el número de habitantes a nivel global es de 7.300 millones de personas y la misma alcanzará los 9.700 millones para el año 2050. De igual manera, el Departamento de Asuntos Económicos y Sociales de las Naciones Unidas ha lanzado un documento que prevé que el 68 % de la población vivirá en zonas urbanas de cara a 2050.

Debido a esta realidad el concepto de eficiencia energética es vital para el desarrollo de nuestras sociedades ya que busca la optimización del consumo y la protección del medio ambiente mediante la reducción de la intensidad energética, habituando al usuario a consumir solo la energía necesaria y a la vez, disminuir las emisiones de CO2 que se envía a la atmósfera por medio de la migración progresiva a una matriz energética renovable.

La adopción de soluciones IoT – IIoT crece constantemente y con ello las diversas alternativas para impulsar la descarbonización y la eliminación progresiva del consumo de combustibles fósiles, con meta en la carbono neutralidad. Entre las opciones que contempla una matriz energética renovable se encuentran:

- Energía eólica.
- Energía solar:
  - Energía solar térmica.
  - Energía solar fotovoltaica.
- Energía hidráulica o hidroeléctrica.
- Biomasa.
- Energía geotérmica.
- Energía mareomotriz.
- Energía undimotriz u olamotriz.
- Hidrógeno verde.

Ilustración: Freepik

por **Freddy Macho**

Presidente del Comité IoT de la 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

¿Cómo funciona?

Smart Energy es una filosofía que modifica el enfoque tradicional de la producción y el consumo de energía, buscando maximizar la eficiencia del proceso. Este concepto hace referencia a la digitalización del sector energético solucionando uno de los principales problemas asociados al modelo de consumo de energía. Su objetivo es mitigar la emergencia climática y para alcanzarlo, une propiedades del vector energético que, en su transición hacia las energías renovables promueve el desarrollo económico y social sostenible. A través de las nuevas tecnologías, se recopila información que luego se explota con el objetivo de determinar estados eficientes de consumo y el mejor precio para el conjunto de la sociedad.

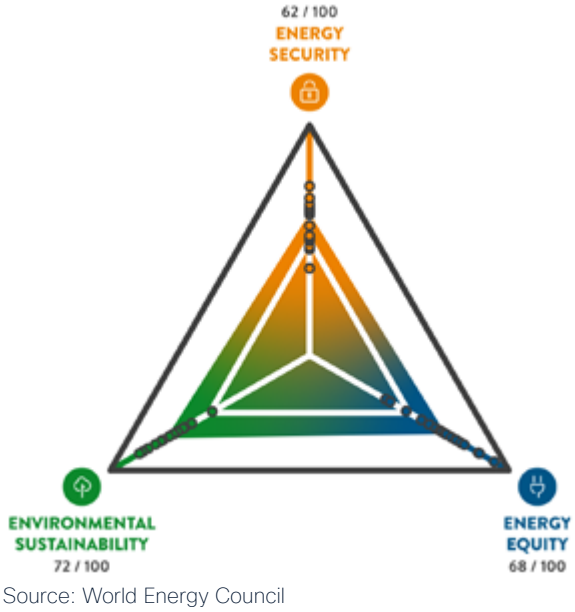
Por medio del uso de habilitadores se aplican métodos analíticos sofisticados en los ambientes energéticos: los sensores del Big Data recopilan la información, la Inteligencia Artificial la procesa y en función los resultados, Cloud la transmite a través de las señales que se envían a las máquinas, para que se genere la electricidad adecuada y así cubrir la demanda de energía. La interacción de todos estos habilitadores describe el uso de los ambientes hiperconvergentes IoT–IIoT. A través de este proceso

Seven cross-industry technology trends will disrupt company strategy, organization, and operations...

Fuente: McKinsey & Company

es posible elaborar modelos sofisticados que estimarán la necesidad de energía que, por otra parte, podrá incluso generar cada consumidor desde su propia casa. Esta nueva etapa energética global está condicionada por "las 5 D": descarbonización, digitalización, desregularización, descentralización y democratización.

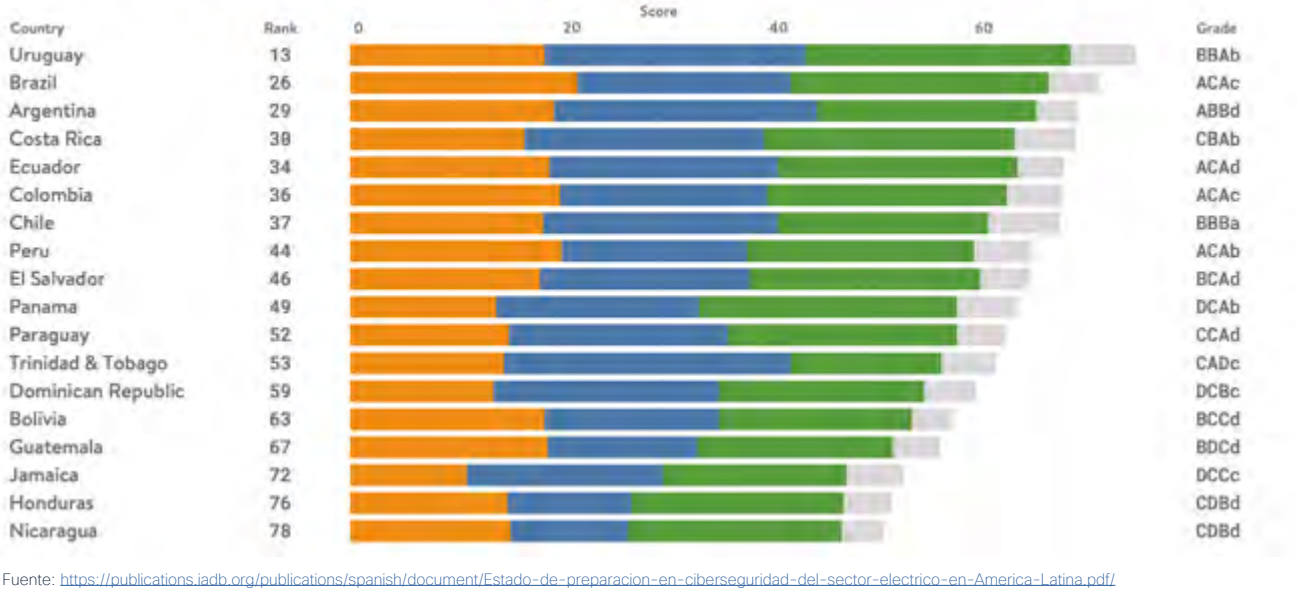
América Latina continúa el creciente despliegue de energías renovables demostrando que los países de la región buscan diversificarse en la generación energética, tal como lo refleja el Trilemma Index del WORLD ENERGY COUNCIL cuando afirma que la región lidera en la dimensión Sostenibilidad debido a su importante uso de hidroelectricidad y el desarrollo e impulso de la producción de hidrógeno, utilizando energía renovable de bajo costo. Los puntajes de equidad energética han mejorado, principalmente a través de subsidios, pero la falta de una reglamentación integral de marcos, incertidumbre económica y estabilidad política sigue obstaculizando la transición energética equilibrada.



Source: World Energy Council

La demanda de energías renovables sigue en aumento junto a la demanda de energía, en contraste con el petróleo y la demanda de gas, que se han desplomado. Este informe reafirma que las energías renovables dan forma al futuro de la energía en la región. Brasil, Chile, Colombia y México han emitido regulaciones que facilitan la compra de energía bilateral, acuerdos y mercados *spot*, que ofrecen una ventaja económica para los inversores, incluido el precio a largo plazo. Estas políticas de inversión y energía que apoyan la transición podrían funcionar como motor para la recuperación económica de la región. Los factores mencionados anteriormente también brindan oportunidades para establecer la producción de hidrógeno, que actualmente se incluye en las agendas de gobierno de Brasil, Chile, Argentina y Uruguay.

Figure 43: Country performances of LAC

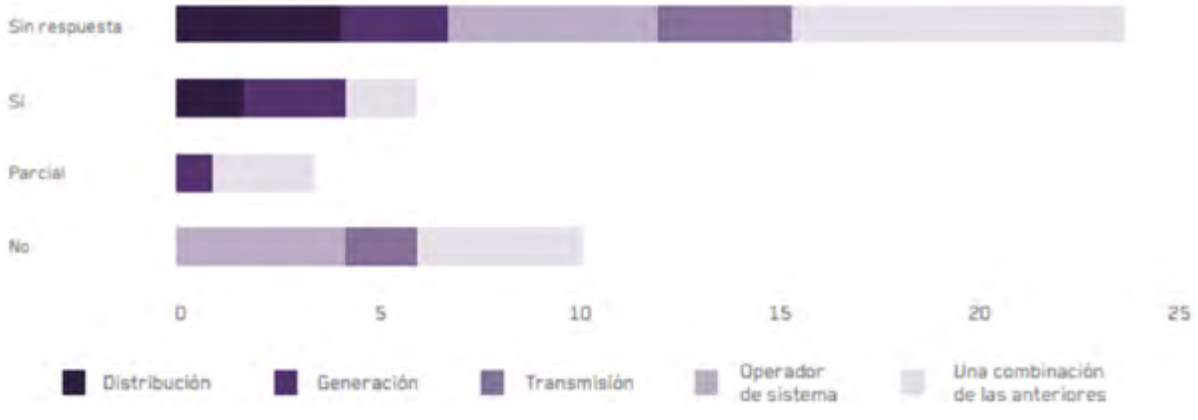


Fuente: https://publications.iadb.org/publications/spanish/document/Estado-de-preparacion-en-ciberseguridad-del-sector-electrico-en-America-Latina.pdf/

Estado de la Ciberseguridad Industrial en el sector eléctrico en América Latina.

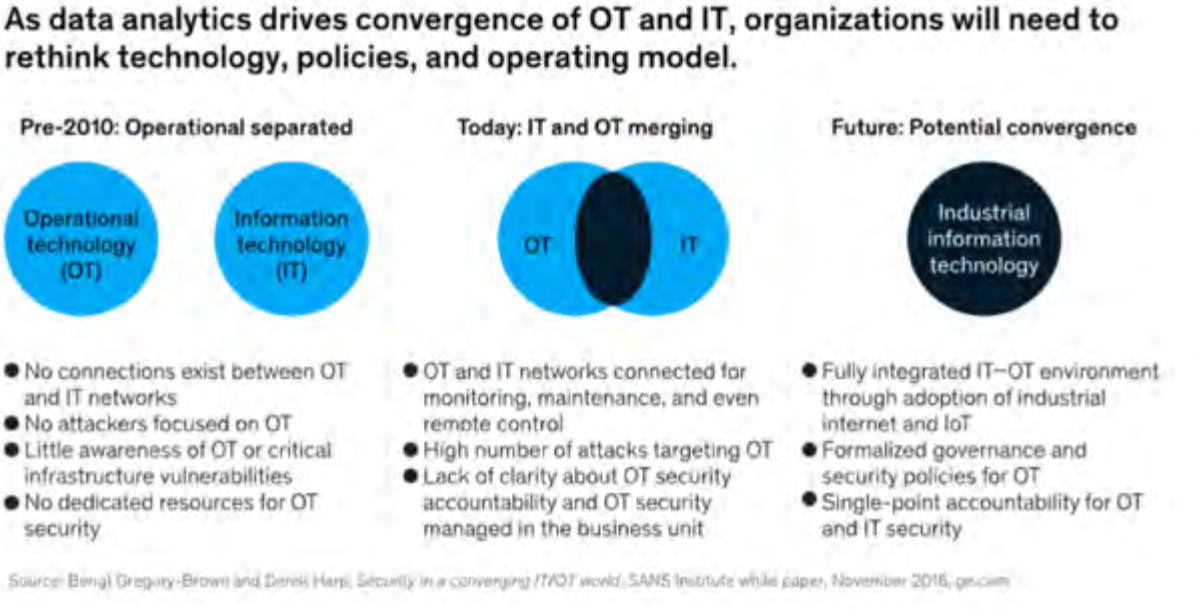
El mundo se ha vuelto totalmente dependiente del suministro estable de electricidad. Las redes eléctricas forman parte de las infraestructuras críticas de un país al igual que lo son los principales hospitales, aeropuertos, etc. Es por esto que las interrupciones de suministro eléctrico son inaceptables y a menudo conllevan sanciones de los gobiernos a los operadores de la red. Las subestaciones eléctricas del futuro serán digitalizadas, requerirán de una mayor interoperabilidad y vendrán asociadas a conceptos nuevos como virtualización de sensores, *blockchain* y *machine learning*. Según el informe "Estado de Preparación en Ciberseguridad en el sector eléctrico en América Latina" del Banco Interamericano del Desarrollo (BID) la compatibilidad con la normativa NERC dentro del ciclo eléctrico en LATAM es baja.

FIGURA 51. Compatibilidad con NERC.



Fuente: https://publications.iadb.org/publications/spanish/document/Estado-de-preparacion-en-ciberseguridad-del-sector-electrico-en-America-Latina.pdf/

Los Sistemas de Control Industrial (ICS) son víctimas frecuentes de ataques, ya que las amenazas son diversas y estos ambientes cuentan con diferentes características que facilitan que las posibles vulnerabilidades sean explotadas, tales como la utilización de sistemas de mantenimiento remoto y la configuración incorrecta de los equipos. En todos los casos, el código dañino explotó vulnerabilidades conocidas de software obsoleto y una inadecuada segmentación entre las redes de oficina y las redes de producción. Todo parece apuntar a que este tipo de incidentes continuará representando una amenaza significativa para los ICS en los próximos años.



Source: Bengi Gregory-Brown and Derek Harp, *Security in a converging IT/OT world*, SANS Institute white paper, November 2016, ge.com

Actualmente, las nuevas redes inteligentes, tendrán la oportunidad de conectar nodos con subestaciones digitalizadas, sistemas de información geográfica, entre otros habilitadores. El nivel de seguridad de la nueva red inteligente estará comprometido por el eslabón más débil de la cadena y por este motivo, los operadores se verán obligados a reemplazar por completo esos nodos obsoletos para apuntar a elevar el nivel de ciberseguridad.

En general, y cuando los ataques tienen éxito, el plazo para que se vea comprometido el sistema de información sigue siendo muy corto. El tiempo que media entre la primera acción hostil hasta el compromiso de un activo se mide, frecuentemente, en términos de segundos o minutos. Sin embargo, el plazo para su descubrimiento o detección, que depende en gran medida del tipo de ataque, suele expresarse en días, semanas o meses. Estos tiempos tienden a incrementarse en la medida que los ambientes se relacionan y dan paso a lo que me gusta llamar "ambientes hiper-convergentes".

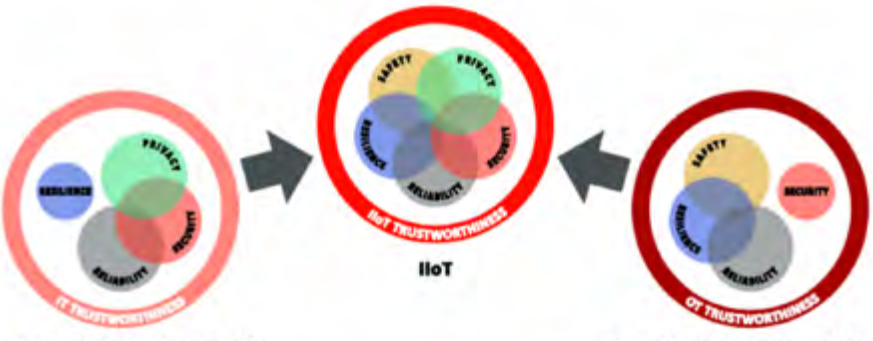


Figure 2-1: Convergence of IT and OT Trustworthiness

Fuente: Industrial Internet Consorium - Security Framework' (IISF)

Si bien parece difícil detener estos ataques avanzados, es necesario facilitar todos los medios posibles para detectar intrusiones y parar las acciones que puedan comprometer las infraestructuras críticas de un país. Para combatir los ataques a las redes eléctricas, existen estándares de seguridad para el intercambio de información e interoperabilidad en las redes eléctricas, a fin de definir el nivel de seguridad y evaluar los riesgos y amenazas de un sistema de control, y para determinar los requisitos de seguridad que se deben cumplir para alcanzar un nivel de seguridad avanzado.

A medida que los sistemas de control son cada vez más esenciales en la cadena de valor del sector eléctrico (generación, transmisión y distribución) y que los sistemas de tecnología de la información están cada vez más conectados a los de tecnología operativa, aumentan los riesgos en ciberseguridad. Según el Foro Económico Mundial, los ciberataques plantearon el riesgo tecnológico en los últimos 9 años.

Fuente: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

	Global Risk	Description
Technological	**Adverse** outcomes of **technological advances**	Intended or unintended negative consequences of technological advances on individuals, businesses, ecosystems and/or economies: AI, brain-computer interfaces, biotechnology, geo-engineering, quantum computing etc.
	Breakdown of critical information **infrastructure**	Deterioration, saturation or shutdown of critical physical and digital infrastructure or services as a result of a systemic dependency on cyber networks and/or technology: AI-intensive systems, internet, hand-held devices, public utilities, satellites, etc.
	Digital inequality	Fractured and/or unequal access to critical digital networks and technology, between and within countries, as a result of unequal investment capabilities, lack of necessary skills in the workforce, insufficient purchase power, government restrictions and/or cultural differences
	Digital power concentration	Concentration of critical digital assets, capabilities and/or knowledge by a reduced number of individuals, businesses or states, resulting in discretionary pricing mechanisms, lack of impartial oversight, unequal private and/or public access etc.
	Failure of **cybersecurity** measures	Business, government and household cybersecurity infrastructure and/or measures are outstripped or rendered obsolete by increasingly sophisticated and frequent cybercrimes, resulting in economic disruption, financial loss, geopolitical tensions and/or social instability
	Failure of **technology governance**	Lack of globally accepted frameworks, institutions or regulations for the use of critical digital networks and technology, as a result of different states or groups of states adopting incompatible digital infrastructure, protocols and/or standards

Fuente: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

Iniciativas para impulsar el avance de la Ciberseguridad industrial energética a nivel global

Unión Europea

El borrador del Código de Red sobre Ciberseguridad para el sector energético de la UE, establece normas sectoriales específicas para los aspectos de ciberseguridad de los flujos de electricidad transfronterizos y ha sido publicado por ENTSO-E para consulta pública. Una vez que entre en vigor, anulará la directiva NIS. El borrador del Código de Red está disponible para consulta pública hasta el 10 de diciembre. Puedes leerlo y compartir tus opiniones aquí.
https://consultations.entsoe.eu/system-operations/network-code-on-cybersecurity/

India

Bajo la dirección del ministro de Energía Nueva y Renovable, la Autoridad Central de Electricidad y el Ministerio de Energía ha preparado la guía para la Seguridad Cibernética en el Sector Eléctrico de la India. Esta es la primera vez que se formula una guía integral sobre seguridad cibernética en el sector de la energía. La Guía han sido preparada en conjunto por medio de aportes de agencias expertas en el campo como CERT-In, NCIIPC India, NSCS, Indian Institute of Technology y deliberaciones posteriores en el Ministerio de Energía de la India. Está disponible en el sitio web de CEA para descargar:
https://cea.nic.in/wp-content/uploads/notification/2021/10/Guidelines_on_Cyber_Security_in_Power_Sector_2021-2.pdf

EE.UU.

Un nuevo proyecto de ley bipartidista de "Reporte de incidentes cibernéticos" presentado en el Senado de EE.UU. requiere que los propietarios y operadores de infraestructura crítica informen a la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) si experimentan un ataque cibernético así como si realizan un pago por ataque. El nuevo proyecto crea el requisito para que las organizaciones sin fines de lucro, empresas con más de 50 empleados y los gobiernos estatales y locales, notifiquen al gobierno federal dentro de las 24 horas si realizan un pago de rescate.

La legislación ordena a las agencias federales que son notificadas de ataques que proporcionen esa información a CISA y creen un Consejo de Repor-

te de Incidentes de Ciberseguridad para coordinar los requisitos de reporte federal. También otorga a CISA la autoridad para citar a entidades que no reporten incidentes de ciberseguridad o pagos de *ransomware*.

El nuevo proyecto de ley de Reporte de Incidentes Cibernéticos se basa en la legislación "Reporte de Incidentes Cibernéticos para Infraestructura Crítica de 2021" que instaba a los propietarios y operadores de infraestructura crítica a informar a CISA dentro de las 72 horas si están experimentando un ataque cibernético. El link del borrador para descarga: https://homeland.house.gov/imo/media/doc/Clarke-Discussion-Draft-082621.pdf

Desarrolla capacidades de Ciberseguridad en ambientes hiperconvergentes

El creciente uso de numerosos tipos de dispositivos «inteligentes», combinado con la necesidad de dar soporte a las redes de comunicación que hay detrás, pone de manifiesto la necesidad de creación de nuevos mecanismos de ciberseguridad. Por ello, a la hora de abordar potenciales problemas, es fundamental la implementación de medidas tales como:

- Contar con una autoridad a cargo de la ciberseguridad en el sector energético:
  - Creación de CSIRT sectoriales o la creación de CSIRT del sector industrial.
- Desarrollo de regulaciones robustas para el sector industrial:
  - Creación de normativas técnicas de Ciberseguridad Industrial.
  - Definición y resguardo prioritario para las infraestructuras críticas.
  - Obligatoriedad de remitir informes de incidentes en el sistema.
- Desarrollo de capacidades de Ciberseguridad Industrial y ambientes hiperconvergentes:
  - Educación, capacitación y creación de habilidades en Seguridad Cibernética,
    - Sensibilización.
    - Marco para la educación.
    - Marco para la formación profesional.

A pesar de la relevancia que ha tomado la ciberseguridad como uno de los pilares fundamentales de la transformación digital, la ausencia de habilidades técnicas y la escasez de profesionales sigue en aumento, siendo este el principal tópico a cubrir y el punto más difícil de abordar para mejorar el nivel de ciberseguridad.

Según un estudio de ESG e Information Systems Security Association (ISSA) el 70% de los trabajadores especializados cree que su organización se ve afectada por la falta de habilidades de ciberseguridad. La diferencia se agiganta si hablamos de seguridad de aplicaciones o ciberseguridad en la nube (todos en el ámbito TI), ya que no se cuenta en la actualidad con un estudio detallado que evalúe la brecha en los ambientes industriales (OT) y los ambientes hiperconvergentes (IoT – IIoT). El Centro de Ciberseguridad Industrial del cual tengo el gusto de ser parte, generó un estudio llamado "Comparativa de las Estrategias Nacionales de Ciberseguridad en Latinoamérica" el cual identifica las carencias de este tópico en la región. https://www.cci-es.org/activities/comparativa-de-las-estrategias-nacionales-de-ciberseguridad-en-latinoamerica/?doing_wp_cron=1637213260.0666239261627197265625

Como contraste, en diversos países de la zona se empiezan a incorporar los requerimientos de ciberseguridad industrial bajo la norma NERC, lo cual impulsa las siguientes preguntas:

¿Dónde se pueden desarrollar las capacidades a nivel académico o a nivel de mejora profesional en Ciberseguridad Industrial y Ciberseguridad IoT – IIoT?

¿Cómo es posible cubrir la demanda creciente de profesionales en la región de LATAM cuando por ejemplo solo países como Chile tiene más de 600 empresas que son reguladas por la prestación de servicios eléctricos, las cuales en su mayoría deben contar con un responsable de ciberseguridad industrial?

¿Quiénes están desempeñando actualmente funciones de tan alta responsabilidad en estas organizaciones de infraestructura crítica y cuáles son los *skills* con los que cuentan actualmente?

¿Se dispone de entes especializados en ciberseguridad industrial que lideren las actividades de protección de la infraestructuras críticas por un lado, y que a la vez, cumplan la función de monitorear el fiel cumplimiento de los niveles mínimos?

Actualmente en Chile se ha iniciado el primer Diplomado de Ciberseguridad Industrial y se encuentra en vía de creación la primera malla curricular que tiene como objetivo desarrollar las capacidades sobre esta disciplina en ambientes hiperconvergentes. Sumado a lo anterior, Cisco a través de Networking Academy, nos facilita diversas opciones de cursos cortos que pueden ser el punto de partida para el crecimiento en el desarrollo profesional.

El camino es largo, la estrategia es prioritaria, pero empezamos a dar los primeros pasos

Hábitos de Ciberseguridad: Prevención y acción

Contenido audiovisual

Imagen: Photo Steff, Pixabay

Ad Content

por **Fabio Sánchez**
Director práctica de Ciberseguridad,
OCP Tech.

Cerca de 1250 a.C. ocurrió un acontecimiento del que seguramente muchos han escuchado: los griegos emprendieron una guerra contra Troya fundamentada en el rapto de Helena que dio origen a uno de los conflictos más legendarios de la antigüedad. Pero lo que es interesante de esta historia es el sitio a la ciudad de Troya que duró alrededor de 9 años, durante los cuales los griegos saquearon las ciudades cercanas, lucharon en la playa y los campos cerca de la ciudad y sin embargo a pesar de los esfuerzos, no lograron tomar la ciudad.

Fue en esas circunstancias cuando los griegos aprovecharon el momento en el que los troyanos se creían invencibles y seguros de que no iban a perder su ciudad, e idearon una treta: un gran caballo de madera hueco que ocuparon con soldados comandados por Odiseo; este caballo fue dado a los troyanos como ofrenda a Atenea y los griegos por su parte fingieron partir. Los troyanos, resguardados en su invencible ciudad y muy confiados, entraron la ofrenda e iniciaron una gran celebración con vino y comida para festejar la partida de los griegos y su victoria. Los soldados que se encontraban dentro del caballo aprovecharon la noche para abrir las puertas de la ciudad y permitir la entrada de su ejército dando paso a un saqueo impiadoso de la ciudad.

Se preguntarán qué tiene de relevante esta historia, pues que se repite una y otra vez en las empresas y las organizaciones sin importar el tamaño o la industria. Se repite en cada empresa que no renueva su estrategia de ciberseguridad y que conserva los mismos controles que la ha mantenido segura durante los últimos años. Suele creerse invencible e impenetrable como los ciudadanos de Troya, y es en esas circunstancias cuando un asalto sutil e irrelevante puede convertirse en la brecha que los atacantes esperaron pacientemente durante años. Y es que las condiciones del entorno en que vivimos y las personas han cambiado pero los procesos y controles siguen siendo los mismos, es por esto que es necesario enfocar los esfuerzos en reeducar, iniciando por la revisión y actualización de los riesgos de ciberseguridad y los ataques más frecuentes del ultimo año; también es necesario y urgente revisar las prácticas y controles de la ciberseguridad de los dispositivos y redes LAN caseras. Es en la educación donde en mi opinión estamos

fallando, creemos estar seguros con los controles y herramientas que nos protegieron durante décadas pero no nos percatamos que la batalla se juega en nuestros empleados y colaboradores, que como personas hacen parte esencial en la estrategia de ciberseguridad de las empresas.

¿Por qué poner énfasis en la ciberseguridad en las redes LAN de nuestras casas? ¿Por qué, si deberíamos estar más preocupados por la red de nuestra empresa, de las sucursales, de las sedes y oficinas en todo el mundo que están en riesgo? ¿Por qué debemos preocuparnos por las redes caseras y dispositivos fuera de la responsabilidad del área de TI y seguridad empresarial? A decir verdad, el problema subyace en esta nueva realidad que vivimos desde hace un año. Sucede que las redes de nuestras casas pasaron a ser una extensión de la red empresarial debido a que hoy un gran porcentaje de la fuerza laboral de las empresas está trabajando desde su casa. La pandemia del coronavirus transformó algo que antes era un deseable u opcional ofrecido a empleados y contratistas: ahora trabajar desde casa pasó a ser algo casi mandatorio y la vida laboral y familiar se entrelazó mucho más, casi a nivel imperceptible. Sin darnos cuenta pasamos de actividades laborales a nuestra vida familiar sin ninguna pausa, empezamos a revisar tareas de nuestros hijos, correos personales, páginas web de ocio, compras en línea, todo con el mismo computador portátil o de escritorio y el mismo dispositivo celular, siendo muy fácil para un atacante acceder por un medio electrónico como el email personal a información empresarial confidencial. Aquí radica mi recomendación sobre el énfasis que debemos poner en fortalecer la capacitación en ciberseguridad de nuestro equipo, compañeros de trabajo y familia, en la prevención y acción ante una sospecha o ataque efectivo por muy sutil o irrelevante que parezca, dado que seguramente es el inicio de algo mucho más elaborado y de mayor impacto.

Te propongo empezar por crear y fortalecer los hábitos alrededor de las principales amenazas y ciber ataques del último año y realizar revisiones semestrales de seguimiento. Entonces, antes de pasar a una recomendación, listemos los ataques y amenazas más populares y en aumento:

Phishing: Un mensaje digital enviado con el propósito de engañar y hacer que un individuo acceda a un *website* falso presentado como legítimo, con el objetivo de activar un virus o instalar un *malware* que permita extraer información sensible. Este tipo de mensajes puede llegar mediante chats grupales con noticias falsas, *websites* de vacunación, información y recomendación acerca del coronavirus, entre otros.

Ransomware: El robo y secuestro de datos es un modo de extorsión que ha tomado fuerza y es cada vez más sofisticado. Iniciando por el método de *phishing*, los atacantes encriptan parte o todo un equipo portátil de escritorio o servidor empresarial con el fin de obtener una recompensa, usualmente en criptomonedas, que deberá ser pagada al atacante para la liberación de los datos.

Archivos políglotas: Imágenes que no son tales o archivos comprimidos con ejecutables que se activan en sitios web maliciosos o que al descargar archivos ilegales disparan acciones y backdoors que los atacantes usarán posteriormente para exfiltración de información o instalación de malware con diferentes propósitos.

Ataques IoT: Con la proliferación de Internet de las cosas (Internet of Things) cada vez contamos con más dispositivos en la casa conectados a internet, como parlantes, hub o concentradores de bombillos, cerraduras inteligentes, que pueden presentar vulnerabilidades o puertos abiertos y quedar a merced de atacantes si no cuentan con una correcta y constante actualización de versión.

Malvertising: Palabra derivada de malicious adverstasing (publicidad maliciosa, en inglés) que busca en diferentes redes sociales inducir el click de una posible víctima con publicidad falsa pero creíble para posteriormente instalar un malware con propósitos más oscuros, abriendo una brecha a nuestro computador y nuestra información.

Robo de identidad: Durante el último año el robo de información confidencial de las personas aumentó considerablemente. A través de los métodos anteriormente mencionados, los ciberdelincuentes escalan solicitudes a entidades bancarias y gubernamentales para obtener créditos, subsidios y suscripciones a servicios que los tienen como beneficiarios y que luego la víctima tendrá que pagar posteriormente.

Las anteriores son solo algunas de las amenazas y riesgos a las que estamos expuestos y para las cuales debemos crear una serie de hábitos de comportamiento que nos permita prevenir y detectar cualquier impacto a nuestra información y dispositivos. Veamos algunos hábitos fáciles de implementar que nos ayudarán a fortalecer nuestra postura contra los ciberataques:

Dudar y sospechar de todo: Lo primero que debemos hacer es dudar de cualquier mensaje, publicidad, correo de oferta o de información. Dado que los atacantes cada vez se han vuelto más diestros en falsificar páginas web de bancos o de comercio electrónico, es necesario que siempre dudemos. Por más seguro y real que sea el mensaje, debemos verificar la url o dirección de la página web y corroborar que tenga un ícono con candado, es decir un certificado de seguridad que garantice que el sitio es seguro y ha sido verificado por una entidad certificadora. Si es un mensaje de nuestro banco o entidad financiera de confianza revisemos que la dirección sea la que siempre hemos utilizado; ante la duda siempre debemos cerrar el sitio web, abstenernos de suministrar información e inmediatamente contactar directamente a la entidad o empresa para validar la veracidad del mensaje.

Ser egoístas con la información: Debemos entender que nuestra información es muy valiosa, y que todas las aplicaciones gratuitas que descargamos e instalamos no son gratis en realidad, estamos pa-

gando brindándoles nuestra información, datos básicos, contactos, ubicación en línea, sitios web que visitamos y rutinas de trabajo entre otra mucha información que compartimos; tenemos que ser más egoístas antes de dar permisos a aplicaciones en nuestro celular y revisar qué estamos cediendo y compartiendo, ser egoístas cuando llenamos formularios de datos de inscripción en páginas web de sitios de comercio electrónico, sitios de encuestas

Ilustración: Fotolia Xunantunich

etc. Seamos egoístas y no demos nuestro correo principal ni nuestra información básica sin antes evaluar si es estrictamente necesario.

Ser estrictos con las contraseñas: Cada vez nos inscribimos a más sitios, descargamos más aplicaciones en nuestro celular y todos estos piden un usuario y contraseña. Para ahorrar tiempo, solemos caer en el hábito de colocar nuestro correo principal y la misma contraseña fácil de recordar. De aquí se desprenden varias recomendaciones: primero no usar nuestro correo principal si no es necesario, segundo usar aplicaciones de gestión de contraseñas que nos permitan guardar las credenciales de todos los sitios y que proveen la autogeneración de contraseñas fuertes que incluyan símbolos, mayúsculas, minúsculas, de esta manera no tendremos necesidad que memorizar y si alguno de estos sitios web es expuesto y las contraseñas y correos son obtenidas no tendrán nuestro correo habitual ni nuestra única contraseña. Una última recomendación es utilizar un segundo factor de autenticación: una aplicación que genere un *token* de único uso o autenticación biométrica que permita configurarse en nuestros sitios web más estrictos como correo electrónico empresarial y personal y sitios de comercio electrónico habitual. Ser pacientes y proactivos con las actualizaciones también es prioritario ya que los equipos portátiles y de escritorio, celulares y tablets generan periódicamente nuevas versiones que proveen cierre de brechas de seguridad detectadas y no solo nuevas funcionalidades. Generalmente son insistentes y molestas las notificaciones y recordatorios de actualización que surgen en ventanas emergentes, pero que debemos afrontar con paciencia y programar. Podemos proactivamente silenciarlas y agendar una hora a la semana en que vayamos a tomar un descanso del dispositivo o aplicación para que inicie y realice la actualización correspondiente, pero es necesario e importante que como hábito estemos permitiendo que se realice este proceso semanalmente dado que de no hacerlo estamos exponiéndonos a numerosas vulnerabilidades de software y hardware que algún *malware*, virus o proceso de un atacante aprovechará y utilizará para robar, extorsionar o sabotear nuestros dispositivos e información.

Desde OCP TECH estamos en condiciones de prestar servicios para el diseño de una estrategia integral que, junto con las herramientas Cisco, brinden una protección sin fronteras de los datos y activos de tu compañía, incluyendo no solo las mejores prácticas para la implementación de redes empresariales y soluciones de software sino también la experiencia de un grupo de expertos en seguridad y procesos que llevarán tu empresa al siguiente nivel mientras se enfoca en el negocio

El autor de este artículo está disponible para consultas en ***fabio@ocp.tech***

Síndrome de burnout, una patología que se potenció durante la pandemia

Agotamiento mental, emocional y físico. Exigencias laborales que resultan agobiantes. Actitud de indiferencia y desapego al trabajo. Desmotivación, frustración. Disminución de la productividad. Estrés crónico. Insatisfacción laboral.

Imagen: Spukkato

por **Silvia Montenegro**

Este cuadro define al *burnout* o síndrome del "quemado" o de desgaste profesional, que, detectado por primera vez en las últimas décadas del Siglo XX, la coyuntura del siglo XXI hace que cobre nueva vigencia. Los expertos dicen que el aumento de la competencia global, los dispositivos digitales que suelen obligar a muchos trabajadores a estar en línea durante horarios extendidos, sumado a entornos sociopolíticos inestables, y la posibilidad concreta de perder el trabajo o estar bajo la presión de perderlo durante un tiempo prolongado dibujan una combinación que deja como resultado gran cantidad de población con problemas psicológicos. La crisis mundial provocada por la pandemia de COVID-19 y sus restricciones no hizo más que aumentar el cuadro.

Ya desde 2019 el síndrome de *burnout* está catalogado por la Organización Mundial de la Salud (OMS) como un riesgo laboral y, a partir del 1 de enero de 2022, integrará la Clasificación Estadística Internacional de Enfermedades y Problemas de Salud Conexos (CIE-11), considerada una buena oportunidad para visualizar la patología, presente en la realidad laboral.

Se trata de una enfermedad derivada de la interacción del individuo con determinadas condiciones psicosociales en el trabajo, y puede estar acompañado por síntomas físicos. También se lo reconoce como un detonante de otros problemas de salud física o mental más graves.

Cómo surge

En su libro "*Burnout: The High Cost of High Achievement*" (1974), Herbert Freudenberger fue el primero que utilizó el término para definir al trastorno producto de un estrés laboral crónico. Este psicólogo estadounidense, de origen alemán y ascendencia judía, observó las manifestaciones de agotamiento que presentaban los psicoterapeutas de una clínica de toxicómanos de Nueva York, e introdujo el concepto para graficar el proceso de deterioro en los cuidados que impartían a sus pacientes. Lo definió como "una sensación de fracaso por sobrecarga de exigencias de energía, recursos personales o fuerza espiritual del trabajador".

Unos años después, la psicóloga Christina Maslach, quien hasta la actualidad sigue investigando sobre este síndrome, elaboró un instrumento de medición universal -denominado MBI *Maslach Burnout Inventory*-, aún vigente, para detectar la presencia de señales de desgaste profesional, que se define como un proceso, más que por un estado. Propuso diagnosticarlo a partir de una "tríada sintomatológica", constituida por el cansancio emocional, la despersonalización y la falta de realización personal.

Imagen: Morgan Basham, Unsplash.

Síntomas y Profesiones

Las personas que experimentan el síndrome del quemado sienten que sus labores son cada vez más estresantes y frustrantes. Pueden distanciarse emocionalmente, les cuesta hacer frente a las tareas diarias, tienen rendimiento reducido. Sienten agotamiento, dificultades para concentrarse y falta de creatividad. Los síntomas físicos que suelen acompañar el cuadro son dolores de cabeza y de estómago, problemas intestinales, trastornos del sueño, tensión muscular y agotamiento físico. La lista de síntomas asociados es extensa, y el nivel de alarma establece cuatro estadios: leve, moderado, grave o extremo.

No existen datos precisos sobre colectivos de mayor riesgo. Sin embargo, al descubrirse el síndrome en los pasados años ´70, se marcaron algunas profesiones u oficios como los más estresantes, entre quienes se contaban los profesionales sanitarios, fuerzas de seguridad, asistentes sociales o maestros. En la década del noventa el concepto del *burnout* se fue ampliando, incluyendo a las personas que trabajan con clientes de trato directo.

Hoy el espectro incluye otros grupos ocupacionales, entre los que se mencionan a los profesionales que trabajan con datos, como los usuarios de tecnologías y teletrabajadores, el personal que trata con usuarios problemáticos, o los empleados que padecen una cultura empresarial obsoleta o complicada. En un mundo donde todo cambia todo el tiempo, conviven modelos de gobernanza débiles: empresas e instituciones con estructuras del Siglo XX y realidades del Siglo XXI.

Pandemia y Adicciones

Nora Revere, médica psicoanalista, miembro de la International Psychoanalitic Asociation (IPA) y de la Asociación Psicoanalítica Argentina (APA), expresa que en el contexto pandémico la humanidad soportó miedo, distanciamiento físico y social, incertidum-

bre, nuevas modalidades de trabajo desde el hogar o desempleo: "Nos enfrentamos a situaciones de mucho estrés. Creo que, hoy, casi todos estamos un poco quemados, sobrepasados, por la forma en que estuvimos trabajando en pandemia. Se ha naturalizado trabajar muchas horas por día, a lo que se sumó la imposibilidad de tomarnos vacaciones por las restricciones. Dentro del estrés, el síndrome de *burnout* está focalizado en el área de trabajo, pero podemos decir que el problema es el estrés, que es más abarcativo".

Un estudio internacional desarrollado por investigadores de la Universidad de Queensland, Australia, y publicado en la revista The Lancet, estima que los casos de depresión mayor y trastorno de ansiedad en el mundo han aumentado un 28% y un 26%, respectivamente, durante la pandemia.
La doctora Nora Revere agrega que las personas que padecen el síndrome de *burnout* están en desequilibrio, fuera de eje. Muchas veces esta situación está relacionada a la intolerancia, a la frustración, a la incapacidad de adaptarse a los cambios, y en ocasiones la base puede ser la adicción al trabajo: "Creo que en esta época los seres humanos tenemos gran capacidad para la adicción, al trabajo, a las series, a la comida, y es producto de la dependencia emocional, de la dificultad de estar a solas con uno mismo, y el desafío no es llenar vacíos sino tener mayor riqueza interna. Si trabajo durante 12 horas por día, no tengo tiempo para la familia, para el ocio, para hacer ejercicio. Adicto significa esclavo, y hay un dicho que dice que no hay esclavo contento. Uno puede ser feliz cuando se adueña de sí mismo, de su propia voluntad".

Y entonces...

Para recuperarse del síndrome de *burnout*, se recomienda apoyarse en la terapia psicológica para reconocer las causas del estrés y buscar maneras de contrarrestarlas. Se trata de un proceso, por eso, también es buena idea recurrir a la batería de estrategias para hacerle frente.

Nora Revere opina que, frente a una situación de agotamiento laboral, en otro momento se aconsejaba que la persona se relaje, descanse, se tome vacaciones. Sin embargo, hoy eso es impensado por la misma dinámica laboral del mundo competitivo. Por eso, aconseja hablar con especialistas, tener interacción social, buscar elementos que den placer, aumentar el ocio productivo, la capacidad de disfrute, establecer un lugar para el juego, adoptar hábitos saludables: "El tema sería ganar el mejor de los tesoreros, que es la felicidad. Si uno tiene una vida íntegra, capacidad creativa, y posee recursos internos, el camino hacia la felicidad es más fácil, porque va a encontrar herramientas para tener coraje, esperanza, fe. Una persona íntegra se focaliza en tres aspectos de su vida, la mente, el cuerpo y el espíritu o actitud frente a la vida". Marca la diferencia entre la alegría, que es fugaz, y la felicidad, que persiste más allá de cualquier obstáculo, y pone el acento en el desafío de buscar constantemente la propia libertad. Da una pista: "Se dice que la felicidad está en las cosas simples de la vida"

El desafío de las Empresas

Con respecto a las organizaciones y empresas, existen algunos factores de riesgo que aumentan las posibilidades de impactar negativamente en la vida de los empleados. Entre ellos se cuenta tener una estructura muy jerarquizada y rígida, exceso de burocracia y falta de participación de los trabajadores, falta de formación práctica en nuevas tecnologías, desigualdad percibida en la gestión del capital humano y estilo de dirección inadecuado.

También existen factores de riesgo relacionados al diseño de los puestos de trabajo, con perfiles que soportan sobrecarga de labores, exigencias emocionales en la interacción con el cliente, falta de apoyo social, insatisfacción en el trabajo o por temas relacionado a los salarios.

Nora Revere destaca formas de prevenir el estrés laboral basado en la oferta de apoyo social y revisando los motivos de insatisfacción. Además, subraya la oportunidad de capacitar a directivos y empleados a través de charlas con especialistas que asesoren sobre el tema.

Imagen: Isabella and Zsa Fischer, Unsplash.

Imagen: M.T El Gassier, Unsplash.

Ciberseguridad: Estadística al borde del colapso

Por las características del trabajo de actuar bajo presión contra el delito cibernético y estar en la primera línea de defensa gestionando y respondiendo las alertas de amenaza -que evolucionan para evadir la detección-, los responsables del área conforman un colectivo de trabajadores predispuestos a sufrir estrés. Vasta bibliografía y estudios hablan de la relación entre agotamiento laboral y rendimiento, y su relación con el error humano en distintas industrias. Si bien no existen estadísticas concretas sobre la proporción de errores en equipos de ciberseguridad que responden al agotamiento, se puede inferir que el síndrome de *burnout* incide en los resultados concretos de los profesionales de seguridad. Este problema está asociado también a la alta rotación que suele haber en el sector.

La Organización Mundial de la Salud (OMS) informa que si en un sector económico hay muchos empleados con agotamiento laboral se vuelve menos productivo, por lo que, además de ser un problema a nivel salud, tiene impacto social y económico.

Como en otras profesiones, frente a situaciones de estrés es vital la implementación de políticas de apoyo a los empleados, tener una cultura empresarial efectiva y establecer métodos para prevenir y/o contrarrestar cuadros de desgaste profesional.

Los videojuegos en la mira

La Clasificación Estadística Internacional de Enfermedades y Problemas de Salud Conexos (CIE) incluye también el trastorno por uso de videojuegos. Se manifiesta por el deterioro en el discernimiento del control del juego, como la duración, la intensidad o la frecuencia; el aumento del grado de prioridad que se antepone a otras actividades de la vida diaria; y el incremento del juego a pesar de identificar consecuencias negativas.

La capa de superhéroe no existe:

cómo descubrí la importancia de la salud mental

Imagen: AD Images, Pixabay.

por **Laércio Albuquerque, vicepresidente Latinoamérica, Cisco**

Laércio en un momento de esparcimiento, disfrutando de su perro y buena música.
Imagen: Gentileza L. Albuquerque.

A duras penas descubrí que nuestra capa de superhéroe simplemente no existe. Comprendí que puedes estar extremadamente feliz y amar lo que haces, pero cualquier cosa en exceso y sin los descansos adecuados puede ser un peligro. En este artículo, comparto un poco sobre la importancia de la salud mental y algunas lecciones para no volver a caer en ese agujero.

¿Qué consejo darías a tu yo del pasado, de hace 20 ó 30 años? El otro día recibí una pregunta como esta en una entrevista, que me hizo pensar mucho en mi vida y reflexionar sobre todo lo que he aprendido en los últimos tiempos. Mi respuesta fue clara: "Yo diría que la capa de superhéroe lamentablemente no existe, no intentes ser un superhéroe". El 10 de octubre se estableció como el Día Mundial de la Salud Mental y me gustaría compartir contigo qué tan importante se ha vuelto en mi vida.

En mi caso, los desafíos de salud mental llegaron en uno de los mejores momentos de mi carrera, a mediados de 2020. Fue entonces cuando descubrí que uno puede ser feliz y amar lo que está haciendo o viviendo, pero el exceso puede convertirse en algo peligroso. Hacer mil cosas a la vez sin tomar los descansos que tu cuerpo, mente y corazón necesitan pueden llevarte al abismo. Y por experiencia digo que cuando intentas equilibrar varios platos al mismo tiempo a la perfección, es muy probable que se caigan algunos. Y todo está bien.

Necesitamos un descanso, no somos superhéroes, y creo firmemente que la gente no quiere superhéroes, solo quiere buenos seres humanos.

El año pasado escribí sobre mi proceso forzoso de Detox Digital, en el que estuve completamente desconectado durante 30 días, y me di cuenta de que si hubiera tomado pequeños descansos en los momentos adecuados, no habría tenido que tomar medidas tan drásticas. Hoy, como un ejemplo sencillo, apago mi celular dos horas antes de irme a la cama. Logro vencer la tentación de dar un "último vistazo" en correos y mensajes antes de cerrar los ojos para dormir.

Mi experiencia personal con la salud mental me ha enseñado mucho. Como recuerdo de esta fase tan importante para mí, me gustaría compartir algunas lecciones que llevo conmigo y que comento a diario con quienes me rodean:

1. Deja tu ego a un lado

Yo, como muchos de ustedes, tengo algo que se llama ego. Aceptar, convivir y superar este ego es difícil. Como líder de una de las empresas de tecnología y conectividad más grandes del mundo, nunca quise aceptar que, a pesar de estar extremadamente feliz, estaba abrumado, cansado y al borde de un colapso físico y mental.

Quería manejar todo solo, pensé que podía hacerlo, incluso porque amaba y amo lo que hago, y pensé que no pasaría nada, hasta que sufrí un pico de arritmia y terminé en la sala de emergencias de un hospital.

Cuando tengas problemas, deja tu ego a un lado, habla y busca ayuda. Hay muchas personas que pueden estar pasando por lo mismo que tú, o que ya se han enfrentado estos mismos problemas y pueden ayudarte. Trabajar para una empresa que realmente se preocupa por su gente, también significó mucho para mí.

2. Pon a las personas en primer lugar

Quita los ojos de ti y ponlos en la gente. Sé auténtico y genuinamente interesado en cada persona, no porque hayas leído en alguna parte que "tiene que ser así", sino porque lo quieres.

Imagen: Myles Tan, Unsplash.

En mis más de 20 años como líder de personas, he visto que a ellos no les importa cuánto sabes, pero quieren saber cuánto de verdad te preocupas por ellos.

Ser tú, auténtico y vulnerable, acerca a las personas y hace que ellas se conecten contigo. Así somos. Sé un líder que quiera inspirar y, sobre todo, sé feliz contigo mismo, tu puesto y tus ideales. Nunca podrás tocar a otras personas si no estás contento contigo mismo. Sé feliz con tus imperfecciones, sé humano. Y como dije anteriormente, no hace falta ser un superhéroe, la gente busca a otros seres humanos, con sus defectos y virtudes.

3. Cuidado con el perfeccionismo

El perfeccionismo que me llevó a convertirme en vicepresidente para Latinoamérica de la empresa de conectividad más grande del planeta es el mismo perfeccionismo que me ha llevado al hospital. Para todo se necesita balance y equilibrio. Sé menos perfeccionista, mantente menos apegado a los detalles, aprende a delegar y ocúpate solamente de lo que realmente importa. Para alguien que se exige mucho como yo, es difícil sentir que está "perdiendo" el control de las cosas, pero intentar hacer todo por ti mismo puede llevarte a perder noches consecutivas de sueño. Recuerda que en una empresa nunca estás solo, tienes a los demás del equipo, tu líder y otras personas que pueden apoyarte. Busca ayuda y mentoría, aunque sea interna, para encontrar tus puntos de mejora. Mi perfeccionismo me generó (y aún genera en partes) mucha ansiedad, pero es liberador poder vivir sin tanta presión interna, además de muy bueno para mantener nuestra salud mental.

4. Usa la tecnología correctamente

Utiliza la tecnología como una herramienta en tus manos, no seas una herramienta en manos de la tecnología.

La tecnología es maravillosa, nos ayuda mucho, conecta a las personas, apoya a las comunidades, transforma vidas, genera puestos de trabajo. Pero si bien conecta a las personas, también pue-

Imagen: Natalya Zaritskaya, Unsplash.

de alejarte de quienes te rodean, como por ejemplo, de tu familia en una cena importante, o puede hacer que no pongas atención a lo que tu hijo te dijo sobre el día en la escuela. Siempre digo que la misma tecnología que salva es la que ciega. Los momentos con las personas que amas no volverán, así que presta atención a tu vida real. Desconéctate cuando tengas que desconectar, si es fin de semana, disfruta tu fin de semana. Si es un día festivo, quédate ahí para el día festivo. La tecnología puede ser una bendición o una maldición, solo depende de ti. No intentes estar en mil lugares al mismo tiempo. Cuando tu mente, cuerpo y corazón estén en lugares diferentes, en algún momento sentirás el impacto del desequilibrio en tu mente y tu cuerpo sufrirá las consecuencias.

Te puedo garantizar que si dejas a tu familia en una fecha muy significativa para asistir a una reunión importante de trabajo, en 10 años, no recordarás de qué fue la reunión, pero siempre te acordarás de que no estuviste en ese momento inolvidable.

Yo cancelé una reunión extremadamente importante para mi carrera para volver a mi casa y asistir al sexto cumpleaños de mi hija (cuento más sobre esta historia en mi Ted Talks). Por eso, valora cada minuto con las personas que amas, establece prioridades y momentos de ocio. El descanso es necesario, aún más ahora en un mundo totalmente conectado. Recuerda, la tecnología va a automatizar todo, pero jamás podrá automatizar el calor de un abrazo.

Mi pasión es usar la tecnología para conectar negocios y mejorar la calidad de vida de las personas, pero mi misión es hacer de la tecnología una aliada. Amo la tecnología, le he dedicado toda mi vida, pero amo mucho más a las personas y cómo la tecnología puede ayudar y respaldar la mejora de la vida de todos. Presta atención a tus señales, tu salud mental y a ti mismo. Cuídate y, solo así, podrás hacer el resto

Contenidos Multiplataforma

basantacontenidos.com

Basanta
contenidos

Especial Mini recital

Tiempo de música

Voz: Noelia Munz
Bajo: Sebastián Tozzola

Contenido audiovisual

Imagen: Karina Basanta

El especial anti *burnout* es una invitación de la redacción de Bridge a conectar contigo mismo desde un lugar consciente, de reflexión, de calma y disfrute. Por eso, decidimos incluir un recital breve de dos artistas exquisitos, Noelia Munz y Sebastián Tozzola. Escaneando el QR presente tanto en la tapa como en este artículo podrás acceder a un video de cuatro temas musicales de este hipnótico dúo de voz y bajo.

¿Por qué los elegimos? Por el precioso ensamble entre la voz de Noelia y los graves del bajo de Sebastián, que nos mueven amablemente a una frecuencia de relajación placentera.

Para estar a tono con el tema que nos convoca, realizamos la filmación en el Teatro Border de la ciudad de Buenos Aires, el primer espacio sustentable de este tipo en Argentina.

Con ustedes, los artistas.

Imagenes: Nicolás Cuadros

Playlist

Alma mía, autora *María Grever*.
Se te olvida, autor *Álvaro Carrillo*.
Amor completo, autora de *Mon Laferte*.
Samba da utopia, autor *Jonathan Silva*.

Autoliderazgo: emociones vs. tareas

¿Te animas a mirarte y preguntarte cuánto te afecta una pandemia de COVID que se alarga y doblega tus esperanzas de "por fin" volver a la vida "normal"?

¿Te animas a hacerle frente a la idea de que será un mal endémico? O sea que lo "normal" es lo que creíamos "excepcional".

A nivel individual, nuestra cabeza (y hablo en primera persona) no siempre lo resiste, y de repente se "quema", nos deja apáticos, desangelados, descreídos de nuestras propias facultades.
A nivel grupal ocurren cosas equivalentes:

- Los líderes de equipos de trabajo ven a sus miembros oscilar en rendimiento y emociones.
- Los líderes de negocio no dejan de recalcular los escenarios y replantear posibilidades.
- Los inversores ven los riesgos crecer y los resultados postergarse.
- Los políticos ven radicalizarse a su electorado de un modo acelerado.
- Los educadores ven flaquear y perder el deseo de aprender de sus alumnos.
- Los empleados no quieren retornar a sus tareas.

A este respecto tengo mi propia opinión, parafraseando a Bill Clinton: "son las emociones, estúpido". Entonces, más que nunca:

- la capacidad de mirarnos, a nosotros y a quienes nos rodean; la capacidad de mantener conversaciones significativas; la capacidad de comunicarnos e inspirar se han tornado claves.
- la evasión que dan las redes y los dispositivos nos aleja de cualquier solución, al contrario, nos sumerge más en el torbellino del aislamiento. Tal vez la única excepción sea el uso del dispositivo para rescatarnos del dispositivo, como son los casos de las aplicaciones de meditación, o los consumos culturales que expanden nuestro universo emocional.

Lo que a nivel corporativo es la "colaboración" productiva, a nivel humano es la colaboración emocional: el **tiempo**, el **tono de voz**, y el **gesto** pasan a ser las "herramientas" que nos rescatan y rescatan al prójimo.

Anímate a mirarte, con calma, con profundidad. Anímate a preguntar y preguntar-te en serio "cómo estás" y compartirlo. A ayudar, y dejarte ayudar. Y a inspirar a quienes lo necesitan.

Las tareas se hacen mejor si antes, alineamos las emociones

por **Pablo Marrone**
Asesor en CX y Comunicación

Imagen: No longer here, Pixabay

Tecnología e Inteligencia Humana, Biológica y Natural:

Recursos Internos para el Bienestar

Imagen: Steve Johnson, Unsplash.

por **Claudia Menkarsky**

Vocal Coach, Terapeuta Psicovocal y Cantante Lírica

¿Qué mejor en estos tiempos de agitación, confusión y cambio que recurrir a nuestros recursos humanos internos para transformarnos en cuerpo y alma, lograr bienestar y descubrir el propio potencial para vivir en cada día, la mejor vida?

A través de todos los tiempos, hemos adquirido múltiples conocimientos a través de disciplinas orientadas a liberar el potencial humano-divino de nuestro interior. Acorde a nuestra naturaleza, nos veremos más o menos inclinados a las distintas actividades, lo importante es sentir y actuar allí donde todo fluye con alegría; lo que llamamos vocación, es una gran orientación.

¿Dónde fluye?

Todas las artes generan regocijo para el alma y formidables emociones y hormonas de bienestar.

Muchas veces, se suele relegar aquello que nos gusta, por dar tiempo y prioridad a otras cosas, sin saber que con un par de horas a la semana que dediquemos a lo que nos resulta placentero y liberador tendremos más energía para hacer luego todo aquello que debemos.

Por esto, considera probar con música, teatro, canto, baile, pintura, escritura, lectura, meditación, yoga, deportes, caminatas, frecuentar seres queridos, espacios naturales, dormir lo necesario, alimentarte bien y así nutrirte desde dentro.

Lo grandes cambios, comienzan con pequeños pasos

Entrevista

Mariano O'Kon

Director, Architectures Sales,
Cisco Latin America and the Caribbean

Imagen: Gerhard G., Pixabay.

Me encontré con *Mariano* vía Webex una tarde donde la promesa de escuchar cosas nuevas parecía agotada para mí. Nuestra conversación cambió no solo esa premisa, sino que Mariano echó luz sobre varios puntos relacionados con el tema que nos convocaba de una forma sumamente didáctica y natural. El enjambre de siglas se volvió un oasis de conocimiento y posibilidades. Te invito a descubrir una nube segura de la mano firme y confiable de *Mariano O'Kon*.

Un paseo **seguro** por las nubes

por **Karina Basanta**

Tenemos los pies en la tierra pero la información en la nube. ¿Cómo llegamos a esto y por qué?

El concepto de transformación digital surgió hace más de diez años. Una definición básica de este proceso se refiere al uso de la tecnología en la estrategia de negocios. Antes de esto, la tecnología era simplemente un habilitador, es decir permitía hacer las cosas más baratas, más rápido, hoy además nos permite diferenciarnos de la competencia, incluso en algunos casos, las empresas no existirían sin la tecnología, por ejemplo en los casos de Uber, Rappi. Solemos hablar de la pandemia como generadora del cambio, sin embargo la disponibilidad de la conectividad inició como gran tendencia hace más de quince años. En el mercado se habla de que 2/3 de las compras empiezan por internet (para elegir el producto, para comparar, para explorar) y el 50% de las compras que se hacen online, se hacen a través del móvil. Si las personas utilizan tanto el dispositivo móvil entonces es importante dar una buena experiencia de compra, pues se dice que el 60% de las personas están dispuestas a pagar más por una experiencia digital superior y el 50% cambia de proveedor si la experiencia digital es mala. La lealtad a las marcas en forma digital no existe si no se puede satisfacer el objetivo de lograr lo que se necesita en tiempo y forma. Está claro que la tolerancia hacia las empresas es muy baja con relación a la satisfacción del servicio. En la actualidad hay una interacción constante entre la información física y la virtual y la experiencia debe ser excepcional durante todo el proceso de compra. Ahora, si a las empresas les va muy bien y empiezan a crecer en ventas digitales necesitarán ampliar sus *data centers*, pues si no lo hacen sus servicios comenzarán a declinar y perderán clientes.

La reacción de las empresas para poder adaptar los recursos a la demanda fue expandirse hacia la nube, es decir subir las aplicaciones para clientes en *data centers* públicos de los cuatro proveedores más grandes, Microsoft, Google, Amazon, IBM, lo que les permitió crecer en demanda y obtener rápidamente espacio de alojamiento de los datos. Según un estudio de IDC, para 2023 se van a generar 500 millones de nuevas aplicaciones, lo que reafirma que gran parte de la población mundial opera a través de aplicaciones para cubrir tres grandes áreas:

Productividad: son las que utiliza un empleado para hacer su labor, como Google, Office 365, box, salesforce, SAP.

Colaboración: que relaciona empleados con clientes, proveedores, como Webex.

Aplicaciones al consumidor: son las que corren en las nubes públicas de Google Cloud, AWS, Microsoft Azure, IBM y otras, o en la nube privada en data center propios. En todos los casos son utilizadas por consumidores finales.

Tu explicación parece llevarnos a la nube híbrida

Exacto. La primera tendencia que comenzamos a ver hace alrededor de diez años fue precisamente la nube híbrida, donde las empresas se expandieron hacia la nube pública y comenzaron a consumir y generan aplicaciones tanto en los *data centers* privados como públicos. La pandemia aceleró este proceso. Como referencia, en Latinoamérica la mitad de los clientes de Cisco ya está utilizando por lo menos dos proveedores de nube pública. Dos por una cuestión de costos y achicar el riesgo de tener todo con uno solo.

¿Qué pasa con la forma de trabajo?

Con la llegada de la pandemia, todos quedamos en nuestras casas y con las vacunas se empezó a volver a las oficinas. Sin embargo, la llegada de las nuevas variantes del virus desarmó el esquema del regreso completo por lo tanto las empresas tienen que contar con una plataforma que les garantice que el trabajo remoto puede hacerse de forma correcta. Las empresas se dieron cuenta que "el trabajo no es dónde uno va, sino lo que uno hace", como decimos en Cisco desde hace muchos años. La pandemia nos demostró que podíamos utilizar lo que estaba disponible a través de la tecnología para trabajar remotamente y una de las consecuencias que trajo esta revelación fue la renuncia masiva de personas a sus trabajos tradicionales cuando se les presentó la obligación de volver a cumplir un horario dentro de la oficina, por ejemplo, de mayo a hoy, en EE.UU. renunciaron 20 millones de personas y se estima que en Latinoamérica va a pasar algo parecido aunque en forma más lenta por la menor oferta laboral.
Hoy el trabajo se plantea en modo híbrido, es decir que las personas van a trabajar en la oficina o desde su casa en forma indistinta según la tarea y la necesidad; seguramente lo que podamos hacer solos lo hagamos en el hogar y la oficina se transforme en un espacio colaborativo.

Hablemos de tendencias

Hoy tenemos dos inclinaciones fuertes: nube híbrida y trabajo híbrido. Sin embargo, ¿qué pasa cuando algo no funciona? Allí surge una tercera tendencia, la observabilidad de todos los dispositivos a los que se conectan todas las personas de todas las organizaciones para saber qué es lo que está funcionando mal. El desafío de todo esto es asegurar usuarios, dispositivos, el acceso a la nube y detectar y responder a las amenazas rápidamente. Si hace 5 años la seguridad era un tema crítico teniendo a todos los empleados dentro de oficina, hoy, que están distribuidos en diferentes espacios y haciendo uso de más dispositivos se ha vuelto sumamente decisivo. Tengamos en cuenta que el 80% del tráfico corporativo sale a la nube, por lo tanto no se puede asegurar solo la oficina y asegurar la nube se vuelve imprescindible.

Imagen: Gentileza Mariano O'Kon

Estamos viviendo un cambio cultural muy fuerte a partir de la disponibilidad y el uso de la tecnología de la comunicación y ello trae aparejado grandes retos en relación a la seguridad digital.

¿Cuáles son las tendencias en seguridad específicamente?

Podemos hablar de tres:

Zero Trust (confianza cero):

Antes el perímetro de seguridad era fácil de delimitar. Si estábamos dentro de la oficina estábamos seguros, si estábamos afuera, inseguros. Esa noción era incorrecta, pero la mayoría de las empresas se manejaba con ese modelo. Así, en los últimos años, sucedieron ataques muy fuertes pues se asumía que las redes eran seguras aún sin serlo. Hoy ya no hay adentro y afuera porque aún estando dentro de la oficina, las aplicaciones no están allí. El nuevo perímetro es la persona, que se tiene que autenticar en la red para validarse. Zero Trust nos dice "yo no te

Imagen: Karina Basanta

voy a dejar pasar hasta que no me digas con certeza quién eres, con usuario, *password*, datos biométricos o la validación que se considere, y además voy a comprobar que tus aplicaciones y sistemas operativos están en correctas condiciones para ingresar". Los permisos de acceso se pueden ajustar o complejizar tanto como la organización lo requiera, por supuesto. La confianza cero determina cuál es el perímetro de entrada y cuál el de defensa.

En Cisco, extendemos el concepto de Zero Trust no solamente hacia a las personas sino también a las aplicaciones y los múltiples dispositivos que se conectan a la red, como pueden ser cámaras de seguridad, sensores de IoT, entre otros, ya que muchos de los ataques actuales entran a través de este tipo de dispositivos que no cuentan con grandes medidas de seguridad.

SASE (Secure Access Service Edge):

Cuando hablamos de SASE nos referimos a conectividad SD-WAN con seguridad en la nube que, por supuesto, incluye a Zero Trust, y su objetivo es asegurar el acceso a las aplicaciones. Actualmente, SD-WAN es crítico debido a la expansión de las empresas a la nube. Además, las empresas no solo usan estas aplicaciones, sino que las cambian seguido y con ellas sus políticas de seguridad. SD-WAN se trata de cómo conectarnos de forma eficiente y ahorrando costos; si agregamos hacerlo de forma segura a través de *cloud security*, a la unión la llamamos SASE.

¿Por qué elegir Cisco para recorrer el camino hacia SASE? Porque Cisco tiene el portfolio completo que requiere SASE. Lo interesante cuando se trata de un mercado tan dinámico y expuesto es congregar todos los elementos en el mismo *vendor* para reducir riesgos.

XDR

Para entender XDR, debemos entender primero el problema que queremos resolver. Todas las aplicaciones de software y dispositivos de hardware tienen, en algún momento, alguna falla (o *bug*, como se los conoce normalmente), que los desarrolladores reparan y publican en una nueva versión. A esto lo llamamos vulnerabilidad. El administrador de TI debe, entonces actualizar el software para poder tener una plataforma segura. ¿Dónde esta el problema? Que toda empresa tiene muchos, pero muchos, dispositivos y aplicaciones. Y cada una de estas tiene, potencialmente, muchas vulnerabilidades. Entonces el administrador de TI se encuentra, normalmente, con el panorama de tener que resolver cientos, o miles de vulnerabilidades. Muchas de estas, en la realidad, no le afectan, quizás porque no se está utilizando la funcionalidad afectada o porque ya tiene otra forma de mitigarla.

El problema, entonces, es saber cuáles son las vulnerabilidades críticas que debemos resolver.

Ahí aparece XDR (Extended Detection and Response), que no es más que una forma de documentar las declaraciones de vulnerabilidades en las que los *vendors* nos ponemos de acuerdo. En Cisco tenemos soluciones que miran todas las vulnerabilidades, en el formato estándar XDR, de cada elemento que hay en la red, tanto dispositivos de *hardware* como aplicaciones. Con el cruce de esa información y a través de algoritmos de IA, determina cuáles de ellas son críticas y las expone de forma de que pueda realizarse la actualización necesaria para cubrirlas. Podemos decir que XDR es una herramienta más en la búsqueda de dar al departamento de Seguridad un mapa de cuáles son las vulnerabilidades que precisan de una actualización crítica.

Por último, Mariano, en tu experiencia ¿qué no se está haciendo y debería hacerse en las organizaciones en relación a la seguridad digital?

Creo que hay que lograr mayor toma de conciencia. El ex CEO de Cisco hace más de ocho años dijo una frase que aún sigue siendo válida: "existen dos tipos de empresas, las que fueron atacadas y las que no saben que fueron atacadas". Creo que es muy importante concientizar sobre el valor de tener un equipo enfocado en ciberseguridad, y si el equipo existe, fortalecerlo. La inversión en esta disciplina suele percibirse como ingrata, ya que si la prevención buscada funciona, nadie se entera, es por eso que luego de grandes eventos como por ejemplo las Olimpíadas se salen a comunicar todos los ataques de los que la organización se defendió. La seguridad por definición es invisible y este es uno de los factores por el cual no hay conciencia.

La labor que lleva el equipo de ciberseguridad de Cisco es admirable en este sentido, sembrar la concientización y apoyarla con los productos y los servicios que tiene la empresa para cubrir este espacio

Educación

Programa de capacitación en seguridad cibernética

Imagen: Andrew Neel, Unsplash.

La cibereducación es parte de la estrategia de aceleración digital "Brasil Digital e Inclusivo" como una forma de dar respuesta a la brecha de profesionales capacitados y disponibles en la disciplina.

El 16 de julio pasado, Cisco Brasil lanzó un programa para desarrollar la nueva generación de jóvenes profesionales en ciberseguridad. CiberEducación Cisco Brasil combina los esfuerzos de la estrategia de aceleración digital "Brasil Digital e Inclusivo", anunciada en mayo, y el programa global de responsabilidad social en educación Cisco Networking Academy, que brinda capacitación, profesionalización e inclusión de jóvenes al mercado tecnológico, alentando a los estudiantes a adquirir nuevas habilidades en TI e impulsar su empleabilidad.

El programa, dividido en dos olas formativas - la primera tuvo lugar en agosto de 2020 y la segunda en febrero de 2021 - persigue el objetivo de ofrecer formación y preparación de estudiantes para el nuevo mercado laboral en la era digital, formación para instructores y la oferta de oportunidades profesionales en socios y clientes de Cisco. El objetivo es crear un ecosistema consistente para el desarrollo de talento en seguridad de la información y satisfacer la creciente demanda de profesionales en esta área, tanto en los sectores público como privado.

El programa CiberEducación Cisco Brasil se lleva a cabo de forma 100% remota, es gratuito y cuenta con cuatro fases:

Learn-A-Thon: Un maratón de conocimiento que tiene como objetivo alentar y capacitar a los estudiantes en los cursos exploratorios de Networking Academy "Introducción a la ciberseguridad" y "Fundamentos de la ciberseguridad". Abierto a estudiantes de las academias de Cisco participantes, esta etapa incluye aprendizaje autodidacta que dura un mes.

Capacitación de instructores: Los instructores de la academia de Cisco Networking Academy recibirán capacitación en dos nuevos cursos: "CyberOps Associate" y "Network Security". El objetivo de esta fase es crear una cadena sustentable de educadores brasileños en ciberseguridad, donde los instructores actuarán como multiplicadores del contenido de Networking Academy en sus instituciones.

Formación Profesional para Estudiantes: Dos mil estudiantes seleccionados de la primera fase serán formados en el curso vocacional CCNA 1, enfocado en redes, y en uno de los cursos de formación profesional en ciberseguridad - CyberOps Associate ", que los prepara para la carrera de analistas en ciberseguridad, o "Network Security", y luego para carreras especializadas en seguridad. Esta fase también incluirá capacitación complementaria en conjunto con los socios educativos de Cisco Networking Academy.

Prácticas y Oportunidad Laboral: En la última fase, los mejores alumnos podrán poner en práctica los conocimientos adquiridos. Los mejores talentos tendrán acceso a una pasantía de 6 a 12 meses o un programa de empleo efectivo, puestos que serán ofrecidos por los socios y clientes de Cisco.

CiberEducación cuenta con socios estratégicos como el Senai Nacional, el Centro Paula Souza y la Escuela de Comunicaciones del Ejército de Brasil, que contribuyen a aprovechar el impacto positivo del Programa en la sociedad ofreciendo becas para estudiantes, entre otras iniciativas.
El público objetivo del programa son estudiantes de último año de bachillerato, graduados o de educación superior o cursos técnicos, que estén interesados en trabajar en el segmento de ciberseguridad.

Dixit

"El Programa CiberEducación de Cisco Brasil es otro paso importante en la búsqueda de un mercado laboral de TI más inclusivo para todos en este país, brindando oportunidades para miles de jóvenes interesados en ingresar a un segmento en constante crecimiento". Gabriel Bello Barros, líder de Cisco Networking Academy en Brasil.

"Al generar conciencia sobre la importancia de la ciberseguridad y brindar una excelente capacitación a los estudiantes, Cisco busca crear un legado educativo en el área de TI en Brasil, aumentando la empleabilidad e inclusión de los estudiantes". Gabriel Bello Barros

Para obtener más información sobre el programa CiberEducation de Cisco Brasil, visite: https://www.cisco.com/c/m/pt_br/brasil-digital-e-inclusivo/cibereducacao.html

El programa en números (proyectado a julio 2022)

- Estudiantes participantes: **103.751**
- Porcentaje de mujeres **20%**
- Cantidad de estudiantes para cursos de certificación: **34.559**
- Cantidad de instructores: **895**
- Porcentaje de mujeres:**13%**
- Academias Cisco (organizaciones asociadas ofreciendo cursos): **521**
- Empleabilidad: **97%**

Socios estratégicos de CiberEducación Cisco Brasil:

En Cisco celebramos el 25º aniversario de presencia en Perú y estamos orgullosos de nuestra participación en el proceso de digitalización, inclusión y desarrollo del país.

Hace 15 años, cuando me uní al equipo de Cisco en este país éramos alrededor de 20 personas en toda la oficina, hoy en día somos más de 60 colaboradores incluyendo un semillero de talento de nuevas generaciones a través del programa Early in Career, del cual Perú es líder en Latinoamérica. Este programa y nuestra política de diversidad nos garantizan una fuente de innovación permanente.

Nuestro equipo es la prioridad. Día a día impulsamos una cultura de empoderamiento, que motive a cada persona a dar lo mejor de sí y que, a su vez, reciba las mejores condiciones laborales del mercado. Esta dinámica de intercambio, nos ha permitido ser reconocidos como la mejor empresa para trabajar en el Perú (#1 Great Place to Work en la categoría de 50 a 250 empleados).

Durante estos 25 años hemos construido los puentes tecnológicos que permiten que más peruanos estén conectados. De la mano de nuestros *partners* hemos implementado y acelerado la transformación digital en sectores tan diversos como el financiero, la minería, el *retail* o los servicios gubernamentales. Un gran porcentaje de las transacciones digitales que tienen lugar en nuestro país (por ejemplo: consultas bancarias, visitas a redes sociales o interacciones digitales con algún organismo del estado), ocurren en entornos seguros sobre plataformas de redes de Cisco.

Asimismo, estamos comprometidos con el desarrollo del país. Generamos empleo de forma directa e indirecta a través de nuestra red de socios de negocios y formamos a miles de peruanos en competencias técnicas que le permitan el acceso a nuevas y mejores oportunidades. Recientemente alcanzamos ¡¡¡El millón de estudiantes peruanos capacitados!!! Esto, a través de nuestro programa de responsabilidad social Cisco NetAcad (Cisco Networking Academy) en un esfuerzo conjunto entre el estado y el sector privado.

Como líder de la organización en Perú estoy convencido que estamos en el camino correcto para construir un futuro mejor, más equitativo e inclusivo para todos.

Los invito a conocer más de nuestra historia a través de nuestro sitio cisco.com

Imagen: Poswiecie, Pixabay.

25 años Cisco Perú

por **Álvaro Rodríguez Larraín**
Country Leader, Perú.


CISCO
SECURE