

# Bridge

CISCO  
SECURE

Cibersegurança



Smart  
Energy  
por Freddy Macho

Segurança  
na nuvem  
Entrevista  
Mariano O'Kon

Especial  
Como evitar a  
Síndrome de Burnout



Conteúdo  
audiovisual



The bridge to possible



# OCP TECH

ENGENHARIA CONVERGENTE  
PARA SOLUÇÕES PRATICÁS

*Especialistas em soluções de cibersegurança*



 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](mailto:info@ocp.tech)

#### Panamá

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

T +507.387.7300

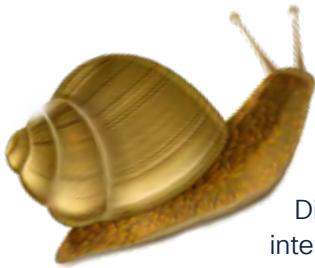
#### Taiwan

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

T +886.953.656.967

# Editorial

Esta é uma edição atípica de Bridge. O final de um ano intenso nos convida a desacelerar e a refletir sobre o que se viveu, sobre o que se segue, sobre como seguir. Desde a redação, escolhemos nos tornar mais conscientes e promovemos a consciência. Escolhemos perceber que o equilíbrio, a justiça sobre o nosso ser, as nossas escolhas baseadas no entendimento, na vontade, na responsabilidade e na escuta atenta de nós mesmos e do outro são os pilares de um trânsito baseado no justo meio.



Dito isto, cedo o tempo que levaria para ler esta página inteira a um período dedicado a você, para se concentrar em você, pacificamente. Você escolhe como, mas antes, respire fundo.

Um forte abraço.

A handwritten signature in black ink, appearing to read 'Kássia B.', with a horizontal line underneath.

# Staff

## Produção abrangente Basanta Contenidos

Diretora Editorial  
Karina Basanta

Diretor de Arte  
Nicolás Cuadros

Coordenadores  
Marta Pizzini  
Marta Assandri

Produção audiovisual  
Salpufilms

Locução  
Loli Fahey

## Colaboradores neste número

Silvia Montenegro  
Jorge Prinzo  
Claudia Menkarsky  
Freddy Macho  
Pablo Marrone

## Fotografia e ilustração

Basanta Contenidos  
Freepik  
Pixabay  
Unsplash

## Agradecimentos

Teatro Border  
Carlos Vieu  
Oswaldo Briscioli  
Nicolás Cacciabue  
Isabella Cacciabue  
Joaquín Cuadros  
Santino Cuadros

Foto de Capa  
Arek Socha, Pixabay



Diretora Editorial  
Karina Basanta



Diretor de Arte  
Nicolás Cuadros



**Impressão:** FP Impresora  
Antonio Beruti 1560, Florida Oeste,  
Provincia de Buenos Aires  
Tel: 11-4760-2300  
[www.fpimpresora.com.ar](http://www.fpimpresora.com.ar)

[basantacontenidos.com](http://basantacontenidos.com)  
[basanta@basantacontenidos.com](mailto:basanta@basantacontenidos.com)  
[@basantacontenidos](https://www.instagram.com/basantacontenidos)  
+54 911 5014-4510 / 5260-8723

## Cisco Latinoamérica

Cyber Security Diretor,  
Americas Service Providers  
and Latin America at Cisco

**Ghassan Dreibi**



Líderes Regionais  
Cibersegurança

Juan Marino  
Fernando Zamai  
Juan Orozco  
Yair Lelis  
Marcelo Bezerra

**Editor General**  
Juan Marino

### Agradecimentos

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

## Marketing

Taiane Belotti

Gerente de Marketing, Segurança Latam

**Jimena Reyna Briseño**

Gerente de Marketing de Contenidos, Segurança, Latam

---

O conteúdo dos anúncios e notas não é de responsabilidade do editor, mas das empresas e/ou signatários. A Editora reserva-se o direito de publicar pedidos de publicidade. Não é permitida a reprodução total ou parcial de qualquer um dos artigos, seções ou material gráfico desta revista.

Bridge Nº 5

# Sumário

Editorial	3	
	4	Staff
	6	Sumário
O novo CDA Country Digital Acceleration Chile - Colômbia	8	
	20	Coluna Smart Energy por Freddy Macho
Ad Content OCP Tech Hábitos de Cibersegurança: Prevenção e ação por Fabio Sánchez	28	
	32	Especial Como evitar a síndrome de burnout <b>Síndrome de burnout, uma patologia que ganhou tração durante a pandemia</b> por Silvia Montenegro <b>A capa de super-herói não existe: minha descoberta sobre a importância da saúde mental</b> por Laércio Albuquerque
		Tempo de música Voz: Noelia Munz Baixo: Sebastián Tozzola
		<b>Autoliderança: emoções vs. tarefas</b> por Pablo Marrone
		<b>Recursos Internos para o Bem-Estar</b> por Claudia Menkarsky
Um passeio seguro pelas nuvens Entrevista a Mariano O'Kon por Karina Basanta	50	
	56	Educação Programa de treinamento em segurança cibernética
25 anos Cisco Peru por Álvaro Rodríguez Larraín	58	

# Braycom

## Nós construímos Soluções



Nós resolvemos as necessidades de negócios **aplicando tecnologia.**

### Cíbersegurança

Desenhamos estratégias de segurança cibernética.

### Colaboração

Telefonia IP, Telepresença.

### Servers

HCI, Storage, Backup.

### Networking

ROUTING/ SWITCHES/ WIRELESS.



Make **IT** Happen  
Contate-nos.

  
**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

O novo

Em 17 de novembro passado, a Cisco Chile formalizou o lançamento de seu programa de aceleração digital em um evento virtual do qual participaram dirigentes da empresa e especialistas dos setores Comunidades Conectadas, Mineração e Energia.



Vive Acelera  
Cisco Chile

O programa [Country Digital Acceleration](#) (CDA) é uma iniciativa mundial de aceleração digital que busca gerar uma relação a longo prazo com o setor público, a indústria e a academia. No Chile e em outros países da região, esta iniciativa se materializa por meio do Advance Technology Center (ATC), um espaço de inovação virtual e presencial cujo objetivo é ajudar o país a alcançar todo o seu potencial digital e permitir que os participantes vivenciem experiências únicas através da articulação de diferentes tecnologias demonstradas em casos de uso prático.

## Por que o Chile?

A escolha do Chile como país apto para o investimento em aceleração digital, inovação, desenvolvimento de capital humano e novos modelos de negócio em Mineração, Energia e Comunidades conectadas foi dada basicamente por três pilares:

- É o país mais habilitado na América Latina para a transformação digital.
- É o primeiro produtor mundial de cobre e rênio e o segundo em lítio e molibdênio.
- O governo do Chile busca um ciberespaço livre, aberto, seguro e resiliente.

O impulso assim concebido contemplará a Cibersegurança como elemento imprescindível de qualquer desenvolvimento realizado.

# Acelera, o evento

Apresentado e coordenado por Bárbara Briceño, jornalista do Emol, o Acelera Cisco Chile 2021 contou com a presença de representantes da Cisco e de personalidades das três verticais escolhidas para o impulso transformador. Aqui você pode ler alguns dos destaques das palestras dos convidados e assistir ao evento completo a partir do QR incluído neste artigo:



**Claudio Ortiz**  
Gerente Geral, Cisco Chile.

*“Na Cisco estamos convencidos de que através da tecnologia podemos transformar e melhorar a vida das pessoas, os processos das instituições e acelerar os negócios nas empresas, portanto é um prazer para nós estar hoje apresentando o nosso programa CDA em conjunto com nosso centro de Co-inovação no qual procuramos gerar os espaços para a criação de novas ideias em prol da transformação digital do país.”*



**Ned Cabot**  
Diretor Sênior de Digitalização  
para Américas, Cisco.

*“A missão da Cisco é promover um futuro inclusivo para todos e o que fazemos na CDA para alcançar este objetivo é gerir a inovação e a colaboração em conjunto com parceiros. Nossa ideia é encontrar caminhos para coordenar a inovação para acelerar as agendas digitais entre os setores público, privado e a academia, a fim de gerar benefícios que derivam da transformação digital nas comunidades.”*

*“Tenho o privilégio de compartilhar que hoje participamos deste programa em 44 países e temos investido e impulsionado mais de 1000 projetos que conseguiram acelerar a digitalização e a criação de novas oportunidades de emprego.”*



**Sandra Eslava**

Diretora de Digitalização, Indústrias e Segmentos, Cisco América Latina.

*“O Chile tem um espaço único em sua visão de desenvolvimento em temas que aceleram a transformação digital. A razão da implementação deste programa no país é apoiar as diferentes indústrias e setores, avaliar as tecnologias necessárias para impulsionar o negócio e, assim, gerar impacto social. As diferentes organizações poderão contar com o apoio do nosso centro onde a tecnologia estará ao seu alcance para garantir os projetos de digitalização, inovação e inclusão.”*

*“No Chile, os principais casos de uso estão focados nos setores Energia, Mineração e Comunidades Conectadas, áreas centrais para dar impulso aos serviços que permitem otimizar o investimento no país, acompanhar a reserva dos recursos naturais e, sobretudo, que isto aconteça com base em desenvolvimentos seguros. A CDA também nos leva a abrir espaços educacionais e de desenvolvimento de competências através da Networking Academy.”*



**Painel Energía Trinidad Castro**

Diretora, WEC.

*“Novas tecnologias carimbaram os marcos históricos. No nosso país, estes têm a ver com o quadro regulamentar, a criação de institucionalidade do setor energético e a introdução das energias renováveis com uma força insuperável e grande vigor, já que hoje nos encontramos com uma matriz de 24% provida por energia renovável.”*

*“Os desafios da descarbonização são multifatoriais. Um deles tem a ver com a transmissão de energia para os lares a partir de diferentes fontes. Além disso, temos um enorme desafio em termos de armazenamento, ou seja, como concentrar energia durante um determinado período. Sem dúvida, a tecnologia pode colaborar muito para avançarmos neste sentido.”*





**Painel Comunidades Conectadas** Pelayo Covarrubias  
Presidente da Fundação País Digital.

*“Quando falamos de Comunidades Conectadas falamos de cidades que têm ferramentas digitais integradas. Por isso, é fundamental ajudá-las a fazê-lo de forma mais rápida.”*

*“As tecnologias já existiam. Com a pandemia, tivemos uma adoção mais rápida do que o esperado.”*

*“No Chile há a possibilidade de adoção tecnológica para aumentar a produtividade e melhorar a qualidade de vida... A pandemia nos levou a incorporar a mudança. Agora devemos entender como incorporar o que falta. Uma das áreas mais atrasadas é a educação, e penso que nesta área devemos concentrar um esforço especial. Devemos nivelar aqueles que tiveram menos possibilidades de aprender, a tecnologia nos permite isso.”*

*“Neste País Digital nos preocupam muito as PME, porque são as que estão no limite entre quebrar ou viver. Como consequência, precisamos ser capazes de as levar a uma maior adoção tecnológica.”*



**Víctor Toscanini**  
Gerente de Engenharia e Tecnologia,  
Cisco Chile.

*“Todo o desenvolvimento digital, definitivamente, se acelerou com a pandemia. Não tem*

*volta. No entanto, estas adoções tecnológicas devem colocar a pessoa no centro e as comunidades interligadas devem fazer o mesmo com o cidadão. Cada comunidade, cada cidade e cada governo conhece as necessidades de seus cidadãos, e a estratégia tecnológica deve se adequar a elas. Inclusive, todas as áreas que impactam as comunidades conectadas devem ser colaborativas entre si para que esta incorporação seja frutífera e em benefício das pessoas.”*



**Painel Minería** Diego Hernández  
Presidente da SONAMI

*“É muito importante a incorporação de tecnologia na mineração, particularmente no Chile, pois aqui temos minas mais maduras, o custo de produção aumentou e temos o desafio de manter as margens operacionais. Neste sentido, a inovação, a automatização e a incorporação da tecnologia digital são fundamentais, é a ferramenta que temos para melhorar a produtividade.”*

*“Hoje em dia, com a conexão e os sistemas de comunicação, a mineração se converteu em uma atividade colaborativa de muitos especialistas que se complementam, diferente de vários anos atrás, quando um mesmo trabalhador cumpria diferentes tarefas. Para isso, o apoio da tecnologia, que facilita o trabalho a distância, é fundamental.”*

*“Graças às diferentes formas de monitoramento, a tecnologia também nos permitiu prever riscos para os trabalhadores e evitar acidentes.”*

*“A mineração chilena está entrando em uma nova etapa tecnológica. E com excelentes perspectivas, já que o lítio e o cobre são indispensáveis para mitigar a mudança climática. Temos produção para muitos anos”*



# 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](https://www.cisco.com/c/es_mx/products/security/securex)



# CDA



Country

Digital

Acceleration

Imagen: Random Institute, Unsplash.

# Colômbia

O novo

## Cisco anuncia o primeiro Advanced Technology Center (ATC) na Colômbia

Como parte da chegada à Colômbia do programa [Country Digital Acceleration](#) (CDA), uma iniciativa mundial da Cisco que impulsiona a aceleração digital dos países através da inovação e da digitalização, no último dia 2 de dezembro foi anunciado o lançamento, em Bogotá, do centro de experiência e inovação Advanced Technology Center (ATC). Este espaço promove o uso de novas tecnologias em prol da modernização e digitalização do país, através da demonstração de usos práticos para as indústrias de Educação, Saúde e do Setor Público, bem como de todas as soluções de segurança.



Vive Accelerate  
day Colombia

O **Advanced Technology Center (ATC)** promove uma imersão digital através de um tour virtual 360° -até que a pandemia esteja controlada-, para demonstrar, com o uso de inteligência artificial, automação, análise de dados e cloud, as soluções mais disruptivas do portfólio da Cisco.

“Com este programa, reiteramos a confiança que a Cisco depositou na Colômbia durante estes 25 anos, apoiando o fortalecimento da transformação digital do país. Além disso, o investimento realizado no ATC em Bogotá permitirá alavancar o empreendedorismo e a inovação neste momento de mudança, bem como identificar novas oportunidades nas áreas de Educação, Saúde e Cibersegurança”; comentou Javier Castro, country manager da Cisco Colombia.

# 25 anos, e muito caminho pela frente

*“Desde o início, o trabalho da Cisco foi criar consciência sobre a importância de integrar a tecnologia nos negócios e comunidades para transformar vidas através da mudança digital. As alianças entre empresa privada e Governo foram fundamentais para a evolução tecnológica da Colômbia, permitindo construir uma sociedade melhor, um melhor ecossistema de parceiros de negócios e, portanto, um país com maior produtividade digital”, acrescentou Castro.*

O trabalho com o Estado, governo após governo, tem sido fundamental para o desenvolvimento tecnológico do país. Como um ator proativo, a Cisco tem colaborado com o desenvolvimento de projetos junto a entidades como o Comando Conjunto Cibernético das Forças Militares e a OEA, em aspectos relacionados à cibersegurança e à ciberdefesa, bem como no avanço de cidades inteligentes, tendo Barranquilla como um de seus pontos de aterrissagem entre as cidades que prioriza em seu projeto na América Latina.

É de salientar também que, nos últimos anos, a empresa acompanhou o plano de Transformação Digital e Inovação. Além disso, no contexto gerado pela pandemia, foram apoiados diferentes programas de educação ao utilizar a sua plataforma de Colaboração Webex em Universidades. Outra área de trabalho foi a Telesalud, facilitando a conexão de unidades de cuidado intensivo de hospitais regionais com hospitais em cidades principais, para permitir uma comunicação segura entre o corpo médico em nível nacional.

## Por que a Colômbia?

A aposta de investimento neste país foi dada principalmente pelas seguintes características:

- **Localização geográfica privilegiada, já que o país conta com fácil acesso a mercados globais.**
- **Investimento estrangeiro, pois a economia colombiana é uma das mais sólidas e estáveis da América Latina.**
- **HUB de inovação de produtos e serviços que geram valor agregado e emprego qualificado.**
- **Competitividade e equidade, já que se situa como o segundo país latino-americano com o melhor desempenho ambiental.**

# Cisco Accelerate day, o evento

Como impulso ao lançamento oficial, a Cisco organizou um evento digital que contou com a presença de líderes da empresa e representantes de organizações associadas e clientes. Assim, sob a apresentação de Inés María Zabarain, várias conversas e apresentações lançaram luz sobre esta iniciativa. Aqui compartilhamos as citações mais relevantes dos convidados. Além disso, você pode assistir ao evento completo a partir do QR incluído neste artigo.



**Santiago Pinzón**  
vice-Presidente de Transformación Digital, ANDI

*“A Cisco aposta em fazer coisas maiores no país: ajudar o trabalho remoto, para que tenhamos melhor conectividade, facilitar o desenvolvimento de territórios e cidades inteligentes. A Cisco apostou na Colômbia e hoje quer ajudar para que seja um país mais digital, mais influente e mais sustentável. Parabéns.”*



**Alberto Samuel Yonai**  
Presidente CCIT

*“A corporação Cisco tem sido uma peça-chave na modernização de diferentes setores da economia na Colômbia e com este novo esforço demonstra mais uma vez seu grande compromisso com o país. Obrigado Cisco, adiante com estas importantes iniciativas.”*





**Alison Treppel**  
Secretária Executiva  
do CICTE, OEA.

*“Nossa colaboração com a Cisco, particularmente nos últimos dois anos, tem impulsionado diversas iniciativas de cibersegurança e inovação na região, e é uma aliança da qual nos orgulhamos muito. Como resultado, temos três iniciativas de alto impacto: os Conselhos de Inovação em Cibersegurança (dois deles realizados na Colômbia), o Fundo de Inovação em Cibersegurança (que financiou 12 projetos na região, dois deles na Colômbia) e o lançamento dos Cursos de Fundamentos Essenciais de Cibersegurança. Estamos convencidos de que essas ações, entre muitas outras, contribuirão para construir um ciberespaço mais seguro para a Colômbia e para a região.”*



**Freddy Garcia**  
Líder de Estratégia,  
SENAsoft

*“Com as ferramentas de vanguarda que o Cisco nos deu, pudemos transferir conhecimento para os nossos instrutores, aprendizes e formandos, para se atualizarem e evoluírem ao ritmo da indústria. Além disso, com a Cisco conseguimos ter o suporte, não só profissional, mas também amigo, para operar de forma virtual, o que nos permitiu levar todos os projetos adiante sem que nada nos detenha.”*



**María Claudia Lacouture**  
diretora executiva  
AmCham, Colômbia.

*“A transformação digital é uma necessidade, uma realidade que está ajudando a reduzir brechas*

*em temas chave como a prestação de serviços médicos, a educação e o serviço público entre outros. Neste objetivo, devemos destacar a contribuição que por mais de 25 anos a Cisco desenvolveu em nosso país, acompanhando com inovação, boas práticas e suporte de qualidade para construir um desenvolvimento sustentável. Estamos certos de que virão outros 25 anos de valioso aporte. Muitas felicidades.”*



**Comandante Hans García**  
Anestesiologista,  
intensivista, Hospital  
Militar Central

*“Durante a fase mais forte da pandemia, em 2020, tinha preparado duas conferências relacionadas à via aérea e ventilação mecânica em pacientes afetados por COVID, previstas apenas para alguns membros do pessoal médico de nosso hospital. Graças à incorporação da plataforma Webex, pudemos massificar a capacitação e a interação entre diferentes centros e regiões e inclusive fora do país.”*



**Teniente Coronel Milena Realpe**  
Chefe do Mestrado  
em Cibersegurança  
e Ciberdefesa, Escola  
Superior de Guerra.

*“Tanto a partir da posição que desempenho atualmente, como em outras anteriores, a experiência que temos tido com projetos transformacionais em temas tecnológicos com a Cisco tem sido muitas e considero que tem sido uma prática muito satisfatória e com muito bons resultados. Além disso, desenvolvemos projetos que vão muito além e que têm a ver com a evolução de capacidades para compreender o ciberespaço, por exemplo, as Olimpíadas Cibernéticas Internacionais e vários exercícios de gestão de crises cibernética. Isso ajudou a fortalecer as capacidades no componente cibernético do nosso país. Estamos certos de que continuaremos a trabalhar de mãos dadas para conseguir um país cada vez mais empoderado e resiliente face a estes temas”*



# FAÇA PARTE DA WOMCY

**Somos uma organização sem fins lucrativos,  
formada por mulheres, com foco no  
desenvolvimento da Cibersegurança  
na América Latina.**

**WOMCY**

LATAM Women in Cybersecurity

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

# Smart Energy

a vertical do IoT/IIoT que impulsiona o desenvolvimento de nossas sociedades

A população mundial está crescendo de forma sustentada e, segundo estudos das Nações Unidas, aproximadamente 83 milhões de pessoas se somam à população global a cada ano. Estima-se que, atualmente, o número de habitantes da Terra seja de 7,3 mil milhões de pessoas e que seremos 9,7 mil milhões até 2050, com 68% vivendo em zonas urbanas, de acordo com o Departamento de Assuntos Econômicos e Sociais das Nações Unidas.

Devido a esta realidade, o conceito de eficiência energética é vital para o desenvolvimento das nossas sociedades, pois visa a otimização do consumo e a proteção do ambiente através da redução da intensidade energética, estimulando o usuário a consumir apenas o que precisa e, simultaneamente, a reduzir as emissões de CO2 na atmosfera com a migração progressiva para uma matriz energética renovável.

Com o avanço da adoção de soluções IoT - IIoT (Internet das Coisas e Internet das Coisas Industrial) estão surgindo diversas alternativas para impulsionar a descarbonização e a eliminação progressiva do consumo de combustíveis fósseis, com meta na neutralidade do carbono. As opções para uma matriz de energia renovável incluem:

- ✔ Energia eólica.
- ✔ Energia solar:
  - Energia solar térmica.
  - Energia solar fotovoltaica.
- ✔ Energia hidráulica ou hidrelétrica.
- ✔ Biomassa.
- ✔ Energia geotérmica.
- ✔ A energia das marés.
- ✔ Energia das ondas ou das ondas.
- ✔ Hidrogénio Verde.



por **Freddy Macho**

Presidente do Comitê IoT da Comissão  
Peritos Laboratório Cibersegurança OEA  
Presidente Centro de Pesquisa  
de Cibersegurança IoT - IIoT  
Coordenador do Centro de  
Cibersegurança Industrial (CCI)  
Presidente IoT Security Institute LATAM



¿Cómo funciona?



Assim surge o *Smart Energy*, um conceito que modifica a abordagem tradicional da produção em relação ao consumo de energia, buscando maximizar a eficiência do processo. Consiste na digitalização do setor energético, com o objetivo de mitigar a emergência climática e, conseqüentemente, solucionar um dos principais problemas associados ao modelo de consumo de energia. Para alcançar esta meta, une propriedades do vetor energético que, na sua transição para as energias renováveis, promove o desenvolvimento econômico e social sustentável. Com as novas tecnologias, recolhe-se informação para determinar um consumo eficiente e o melhor preço para a sociedade.

Por meio de ativadores, se aplicam métodos analíticos sofisticados nos ambientes energéticos: os sensores do Big Data recolhem a informação, a Inteligência Artificial a processa e, conforme os resultados, a Nuvem a transmite por meio de sinais enviados às máquinas, para que seja gerada a eletricidade adequada à demanda de energia. A interação de todos estes habilitadores descreve o uso dos ambientes hiperconvergentes IoT - IIoT. Este processo nos permite elaborar modelos sofisticados de informação que estimarão a necessidade de energia e, por outro lado, mostrar a capacidade de geração de cada consumidor a partir da sua

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

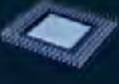
**Disruptions across 7 cross-industry trends**

Tech-trend clusters	Disruptions
<b>1 A. Next-level process automation</b>  Industrial IoT <sup>1</sup> Robots/cobots? <sup>2</sup> RPA <sup>3</sup>	<b>Self-learning, reconfigurable robots</b> will drive automation of physical processes beyond routine activities to include less predictable ones, leading to fewer people working in these activities and a <b>reconfiguration of the workforce</b> ; policy makers will be challenged to address labor displacement, even as organizations will need to rethink the <a href="#">future of work</a>
<b>B. Process virtualization</b>  Digital twins 3-D/4-D printing	<b>Advanced simulations and 3-D/4-D printing</b> will virtualize and dematerialize processes, shortening development cycles as ever-shorter product and service life cycles continue to accelerate, further <b>pressuring profit pools and speeding strategic and operational practices</b> that <a href="#">ignite corporate</a> with successful digital efforts
<b>2 Future of connectivity</b>  5G and IoT connectivity	With either high-band or low- to mid-band 5G reaching up to 80% of the global population by 2030, enhanced coverage and speed of connections across long and short distances will enable <b>new services</b> (eg, remote patient monitoring), <b>business models</b> (eg, connected services), and <b>next-generation customer experiences</b> (eg, live VR)
<b>3 Distributed infrastructure</b>  Cloud & edge computing	Wide availability of IT infrastructure and services through cloud computing could <b>shift demand for on-premise IT infrastructure</b> and reduce the need for IT setup and maintenance, while the democratization of infrastructure will help <b>shift competitive advantage</b> away from IT to software development and talent.

1. Internet of Things. 2. Collaborative robots. 3. Robotic process automation.

McKinsey & Company 8

**Disruptions across 7 cross-industry trends**

Tech-trend clusters	Disruptions
<b>4 Next-generation computing</b>  Quantum computing ASICs <sup>4</sup>	<b>High computational capabilities</b> allow new use cases, such as molecule-level simulation, reducing the empirical expertise and testing needed for a range of applications and leading to the following: disruption across industries such as materials, chemicals, and pharmaceuticals; highly <b>personalized product developments</b> , for instance in medicine; the ability to break the majority of <b>cryptographic security algorithms</b> , disrupting today's cybersecurity approaches; and the faster diffusion of <b>self-driving vehicles</b>
<b>5 Applied AI</b>  Computer vision, natural-language processing, and speech technology	As AI matures and continues to scale, it will enable <b>new applications</b> (eg, more rapid development cycles and detailed customer insights), <b>eliminate labor for repetitive tasks</b> (eg, filing, document preparation, and indexing), and support the <b>global reach of highly specialized services and talent</b> (eg, improved telemedicine and the ability of specialized engineers to work on oil rigs from the safety of land)
<b>6 Future of programming</b>  Software 2.0	Software 2.0 creates new ways of writing software and reduces complexity; however, as companies look to <b>scale their software-development capabilities</b> , they will need to <b>master DataOps and MLOps<sup>5</sup> practices</b> and technology to make the most of the future of programming
<b>7 Trust architecture</b>  Zero-trust security Blockchain	<b>Trust architectures</b> help commercial entities and individuals <b>establish trust and conduct business without need for intermediaries</b> , even as zero-trust-security measures address growing cyberattacks; countries and regulatory bodies may likely have to <b>rethink regulatory oversight</b> ; distributed-ledger technologies will <b>reduce cost and enable transformative business models</b>

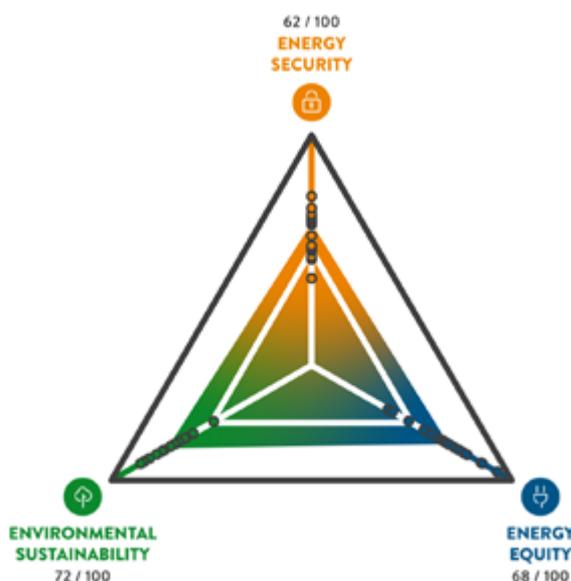
4. Application-specific integrated circuits.  
5. DataOps supports and enables better data analytics; MLOps combines infrastructure, tools, and workflows to provide faster and more reliable machine-learning pipelines.

McKinsey & Company 9

própria casa. A esta nova etapa energética global estão condicionadas as “5 D”: descarbonização, digitalização, desregulamentação, descentralização e democratização.

Na América Latina, segue crescente a implantação de energias renováveis, demonstrando que os países da região procuram diversificar a geração energética, como refletido no “Trilemma Index do

WORLD ENERGY COUNCIL”. O estudo indica que a região lidera o quadro mundial da Sustentabilidade na produção de energia devido à importante utilização de hidreletricidade e ao desenvolvimento e impulso da produção de hidrogênio, que utiliza energia renovável de baixo custo. As classificações de equidade energética melhoraram, principalmente através de subsídios, mas a ausência de uma regulamentação, a incerteza econômica e a instabilidade política, continuam a dificultar uma transição energética equilibrada.

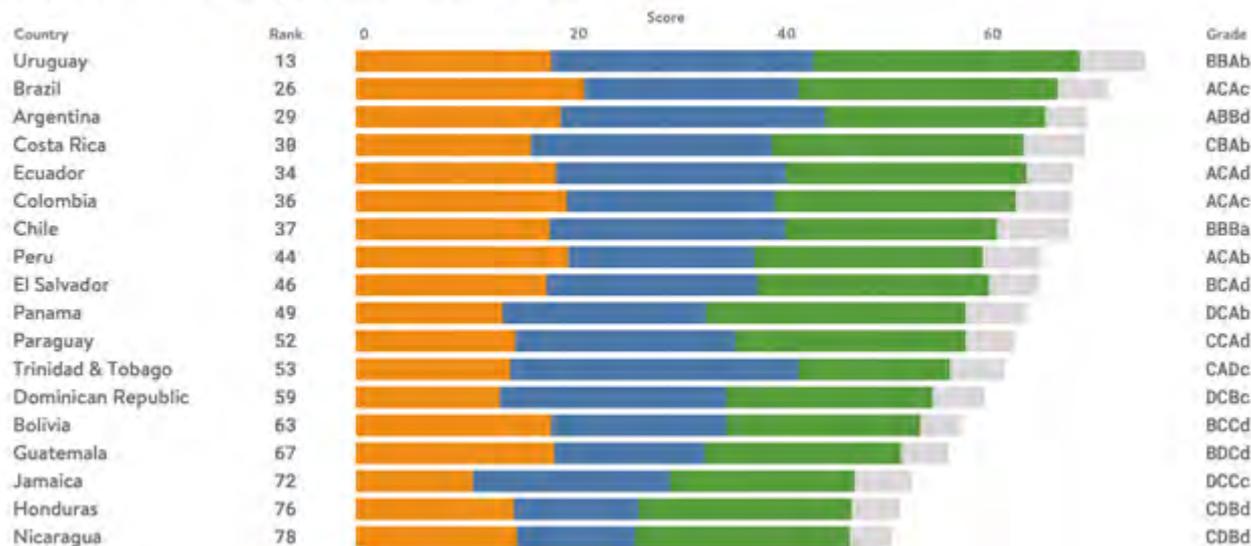


Source: World Energy Council

A busca de energias renováveis segue um crescimento proporcional à demanda por energia, em contraste com o consumo de petróleo e gás, que entrou em colapso. Este relatório reafirma que as energias renováveis dão forma ao futuro da energia na região. Brasil, Chile, Colômbia e México emitiram regulamentos que facilitam a compra de energia bilateral, acordos e mercados locais, oferecendo uma vantagem econô-

mica para os investidores, incluindo o preço a longo prazo. A expectativa é que estas políticas de investimento e de energia que apoiam a transição funcionem como um motor para a recuperação econômica da região. Os fatores mencionados anteriormente também oferecem oportunidades para estabelecer a produção de hidrogênio, que atualmente consta nas agendas dos governos do Brasil, Chile, Argentina e Uruguai.

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/>

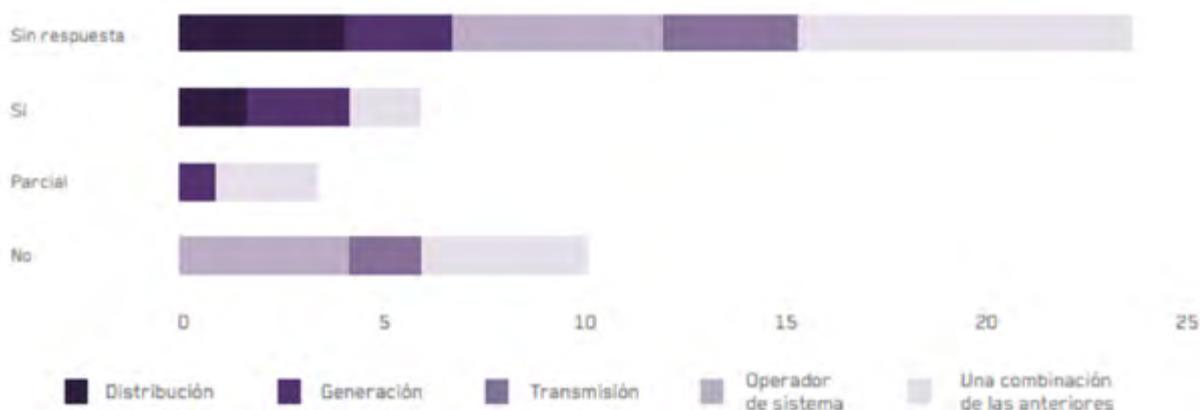
# Estado da Cibersegurança Industrial no setor elétrico na América Latina

O mundo se tornou totalmente dependente do fornecimento estável de eletricidade. As redes elétricas fazem parte das infraestruturas críticas de um país, tal como os principais hospitais, aeroportos etc. É por isso que as interrupções de energia são inaceitáveis e muitas vezes implicam sanções dos governos para os operadores de rede. As subestações elétricas do futuro serão digitalizadas, vão demandar

uma maior interoperabilidade e virão associadas a conceitos novos como virtualização de sensores, blockchain e machine learning.

Segundo o relatório “Estado de Preparação em Cibersegurança no setor elétrico na América Latina”, do Banco Interamericano de Desenvolvimento (BID), a compatibilidade com a normativa NERC dentro do ciclo elétrico em LATAM é baixa.

**FIGURA 51. Compatibilidad con NERC.**

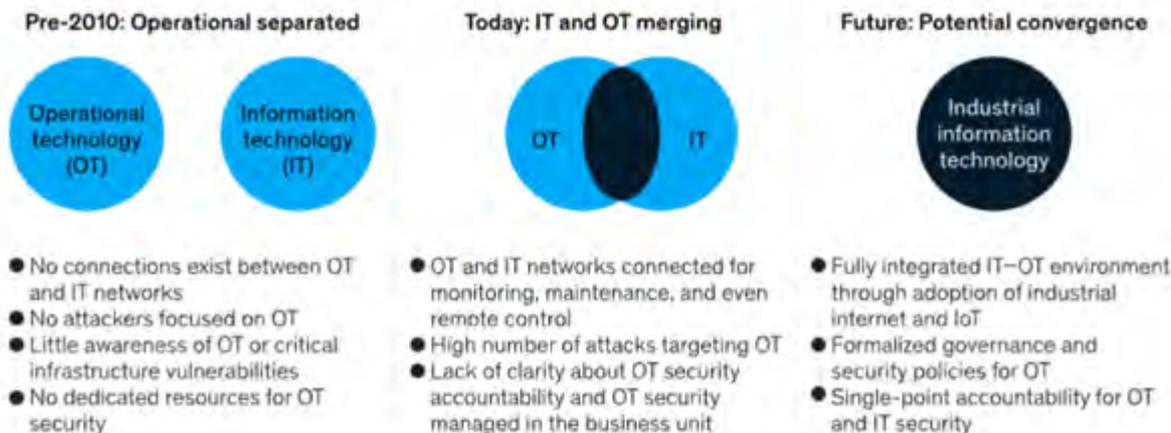


Fuente: <https://publications.iadb.org/publications/spanish/document/Estado-de-preparacion-en-ciberseguridad-del-sector-electrico-en-América-Latina.pdf/>

Os Sistemas de Controle Industrial (ICS) são vítimas frequentes de ataques, já que as ameaças são diversas e estes ambientes contam com diferentes características que abrem brechas para a exploração de possíveis vulnerabilidades, tais como a utilização de sistemas de manutenção a distância e a configuração incorreta do equipa-

mento. Em todos os casos, o código nocivo explorou vulnerabilidades conhecidas de software obsoleto e uma segmentação inadequada entre redes de escritório e redes de produção. Tudo parece indicar que este tipo de incidentes continuará a representar uma ameaça significativa para os ICS nos próximos anos.

## As data analytics drives convergence of OT and IT, organizations will need to rethink technology, policies, and operating model.



Source: Bengi Gregory-Brown and Derek Herz, Security in a converging IT/OT world, SANS Institute white paper, November 2016, <https://www.sans.org/white-papers/wp474/>

Atualmente, as novas redes inteligentes terão a oportunidade de conectar nós de rede com subestações digitalizadas, sistemas de informação geográfica, entre outros habilitadores. O nível de segurança da nova rede inteligente será comprometido pelo elo mais fraco da cadeia e, por esta razão, os operadores serão obrigados a substituir por completo os nós obsoletos para tentar elevar o nível da segurança digital. Em geral, quando os ataques são bem-sucedidos,

o prazo para comprometer o sistema de informação permanece muito curto. O tempo entre a primeira ação hostil e o comprometimento de um ativo é frequentemente medido em segundos ou minutos. No entanto, o prazo para a sua descoberta ou detecção, que depende em grande medida do tipo de ataque, é frequentemente expresso em dias, semanas ou meses. Estes tempos tendem a aumentar à medida que os ambientes se relacionam e dão lugar ao que eu gosto de chamar “ambientes hiperconvergentes”.

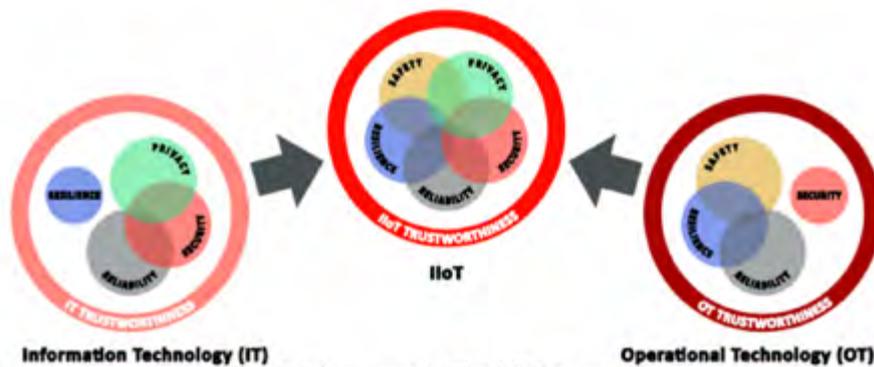


Figure 2-1: Convergence of IT and OT Trustworthiness

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

Embora seja difícil travar estes ataques avançados, é necessário disponibilizar todos os meios possíveis para detectar intrusões e travar as ações que possam comprometer as infraestruturas críticas de um país. Para combater os ataques às redes elétricas existem normas de segurança para o intercâmbio de informação e interoperabilidade, não só definir o nível de segurança e avaliar os riscos e as ameaças de um sistema de controle, como para determinar os requisitos de segurança a cumprir para se obter

um nível avançado. À medida que os sistemas de controle se tornam cada vez mais essenciais na cadeia de valor do setor da eléctrico (produção, transmissão e distribuição) e que os sistemas de tecnologia da informação estão cada vez mais ligados aos sistemas das tecnologias operacionais, aumentam os riscos em cibersegurança. Segundo o Fórum Econômico Mundial, os ciberataques representaram risco tecnológico nos últimos 9 anos.

**Top Global Risks by Likelihood**

	1st	2nd	3rd	4th	5th	6th	7th
2021	Extreme weather	Climate action failure	Human environmental damage	Infectious diseases	Biodiversity loss	Digital power concentration	Digital inequality
2020	Extreme weather	Climate action failure	Natural disasters	Biodiversity loss	Human-made environmental disasters		
2019	Extreme weather	Climate action failure	Natural disasters	Data fraud or theft	Cyberattacks		
2018	Extreme weather	Natural disasters	Cyberattacks	Data fraud or theft	Climate action failure		
2017	Extreme weather	Involuntary migration	Natural disasters	Terrorist attacks	Data fraud or theft		
2016	Involuntary migration	Extreme weather	Climate action failure	Intestate conflict	Natural catastrophes		
2015	Intestate conflict	Extreme weather	Failure of national governance	State collapse or crisis	Unemployment		
2014	Income disparity	Extreme weather	Unemployment	Climate action failure	Cyberattacks		
2013	Income disparity	Fiscal imbalances	Greenhouse gas emissions	Water crises	Population ageing		
2012	Income disparity	Fiscal imbalances	Greenhouse gas emissions	Cyberattacks	Water crises		

Fuente: [https://www3.weforum.org/docs/WEF\\_The\\_Global\\_Risks\\_Report\\_2021.pdf](https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf)

Global Risk	Description
<b>Adverse outcomes of technological advances</b>	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.
<b>Breakdown of critical information infrastructure</b>	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.
<b>Digital inequality</b>	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
<b>Digital power concentration</b>	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.
<b>Failure of cybersecurity measures</b>	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
<b>Failure of technology governance</b>	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](https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf)

## Iniciativas para impulsar o avanço da Cibersegurança industrial energética em nível global

### União Europeia

O projeto de Código de Rede da UE para a Cibersegurança no setor da energia estabelece regras setoriais específicas para os aspectos de cibersegurança dos fluxos transfronteiriços de eletricidade e foi publicado pela REORT-É para consulta pública. Uma vez que entre em vigor, anulará a diretiva NIS. O projeto do Código de Rede esteve em consulta pública até 10 de dezembro. Você pode ler aqui.

<https://consultations.entsoe.eu/system-operations/network-code-on-cybersecurity/>

### Índia

Sob a direção do Ministro da Energia Nova e Renovável, a Autoridade Central de Eletricidade e o Ministério da Energia preparou o Guia para a Segurança Cibernética no Setor Elétrico da Índia. Esta é a primeira vez que se formula um guia integral sobre segurança cibernética no setor da energia. O documento foi preparado a partir de contribuições de agências especializadas no campo como CERT-In, NCIIPC India, NSCS, Indian Institute of Technology e deliberações posteriores do Ministério de

Energia da Índia. O guia está disponível no site da CEA para download:

[https://cea.nic.in/wp-content/uploads/notification/2021/10/Guidelines\\_on\\_Cyber\\_Security\\_in\\_Power\\_Sector\\_2021-2.pdf](https://cea.nic.in/wp-content/uploads/notification/2021/10/Guidelines_on_Cyber_Security_in_Power_Sector_2021-2.pdf)

### EUA

Um novo projeto de lei bipartidário de “Relatório de Incidentes Cibernéticos” apresentado no Senado dos EUA exige que os proprietários e operadores de infraestruturas críticas informem à Agência de Segurança da Infraestrutura e da Cibersegurança (CISA) se sofrerem um ataque cibernético e se fizerem um pagamento por ataque. O novo projeto cria o requisito para que as organizações sem fins lucrativos, empresas com mais de 50 empregados e os governos estaduais e locais, notifiquem ao governo federal, no prazo de 24 horas, se realizarem um pagamento de resgate.

A legislação ordena às agências federais que sejam notificadas de ataques, que forneçam essa informação à CISA e criem um Conselho de Relatório de Inci-

dentos de Cibersegurança para coordenar os requisitos de relatório federal. Também dá à CISA autoridade para citar entidades que não relatam incidentes de cibersegurança ou pagamentos de ransomware.

O novo projeto de lei de Relatório de Incidentes Cibernéticos se baseia na legislação “Relatório de

Incidentes Cibernéticos para Infraestrutura Crítica de 2021”, que instava os proprietários e operadores de infraestruturas críticas a informarem um ataque cibernético à CISA, em no máximo 72 horas. O link do rascunho para download: <https://homeland.house.gov/imo/media/doc/Clarke-Discussion-Draft-082621.pdf>

## Desenvolvendo capacidades de Cibersegurança em ambientes hiperconvergentes

A crescente utilização de muitos tipos de dispositivos «inteligentes», combinada com a necessidade de apoiar as redes de comunicação subjacentes, revela a necessidade de criar novos mecanismos de cibersegurança. A aplicação de medidas como:

### ➤ Dispor de uma autoridade responsável pela cibersegurança no sector energético:

- ⦿ Criação de CSIRT setoriais ou criação de CSIRT do setor industrial.

### ➤ Desenvolvimento de regulações robustas para o setor industrial:

- ⦿ Criação de normas técnicas de Cibersegurança Industrial.
- ⦿ Definição e proteção prioritárias para as infraestruturas críticas.
- ⦿ Obrigatoriedade do envio de relatórios de incidentes no sistema.

### ➤ Desenvolvimento de capacidades de Cibersegurança Industrial e ambientes hiperconvergentes:

- ⦿ Educação, capacitação e criação de habilidades em Segurança Cibernética,
  - Sensibilização.
  - Quadro para a educação.
  - Quadro para a formação profissional.

Apesar da importância que a cibersegurança tem assumido como um dos pilares fundamentais da transformação digital, a ausência de competências técnicas e a escassez de profissionais continua a aumentar, sendo este o tópico principal e o ponto mais difícil de abordar para melhorar o nível de cibersegurança.

Segundo um estudo da ESG e da Information Systems Security Association (ISSA), 70% dos trabalhadores especializados acreditam que a sua organização é afetada pela falta de competências de cibersegurança. A diferença aumenta se falamos de segurança de aplicativos ou de cibersegurança na nuvem (todos no âmbito de TI), já que não se conta na atualidade com um estudo detalhado que avalie a brecha nos ambientes industriais (OT)

e os ambientes hiperconvergentes (IoT - IIoT). O Centro de Cibersegurança Industrial do qual tenho o prazer de participar, gerou um estudo chamado “Comparativo das Estratégias Nacionais de Cibersegurança na América Latina” que identifica as carências deste tópico na região.

[https://www.cci-es.org/activities/comparativa-de-las-estrategias-nacionales-de-ciberseguridad-en-latinoamerica/?doing\\_wp\\_cron=1637213260.0666239261627197265625](https://www.cci-es.org/activities/comparativa-de-las-estrategias-nacionales-de-ciberseguridad-en-latinoamerica/?doing_wp_cron=1637213260.0666239261627197265625)

Em contrapartida, diversos países da região começam a incorporar os requerimentos de cibersegurança industrial sob a norma NERC, o que impulsiona as seguintes perguntas:

Onde desenvolver as capacidades em nível académico ou de melhoria profissional em Cibersegurança Industrial e Cibersegurança IoT - IIoT?

Como é possível satisfazer a procura crescente de profissionais na América Latina, se apenas países como o Chile tem mais de 600 empresas reguladas pela prestação de serviços elétricos, e as quais, em sua maioria, devem contar com um responsável de cibersegurança industrial?

Quais são, atualmente, as pessoas que desempenham funções de elevada responsabilidade nestas organizações de infraestruturas críticas e quais são os skills de que dispõem?

Existem entidades especializadas em cibersegurança industrial que, por um lado, liderem as atividades de proteção das infraestruturas críticas, por um lado, e que, por outro lado, desempenhem a função de monitorar o cumprimento dos níveis mínimos?

Atualmente no Chile se iniciou o primeiro Diploma de Cibersegurança Industrial e se encontra em via de criação a primeira malha curricular que tem como objetivo desenvolver as capacidades sobre esta disciplina em ambientes hiperconvergentes. Além disso, a Cisco, através da Networking Academy, nos fornece diversas opções de cursos curtos que podem ser o ponto de partida para o crescimento no desenvolvimento profissional.

O caminho é longo, a estratégia é prioritária, mas começamos a dar os primeiros passos

# Hábitos de Cibersegurança: Prevenção e ação



Contenido  
audiovisual

por **Fabio Sánchez**

Diretor de Prática de  
Cibersegurança, OCP Tech.

## Ad Content

Cerca de 1250 a.C. ocorreu um acontecimento do qual certamente muitos ouviram falar: os gregos empreenderam uma guerra contra Tróia fundamentada no arrebatamento de Helena. Esta guerra deu origem a um dos conflitos mais lendários da antiguidade. Mas o interessante nesta história é o local, a cidade de Tróia. Ao longo de aproximadamente 9 anos, os gregos saquearam as cidades vizinhas, lutaram na praia e nos campos perto da cidade, mas apesar dos esforços não conseguiram tomar a cidade.

Foi nessas circunstâncias que os gregos aproveitaram o momento em que os troianos se achavam invencíveis e seguros de que não iam perder a sua cidade, e idealizaram um truque: um grande cavalo de madeira oco que ocuparam com soldados comandados por Odisseu; este cavalo foi dado aos troianos como oferenda à Atena e os gregos por sua vez fingiram partir. Os troianos, abrigados em sua cidade invencível e muito confiantes, entraram na oferenda e iniciaram uma grande celebração com vinho e comida para festejar a partida dos gregos e sua vitória. Os soldados que se encontravam dentro do cavalo aproveitaram a noite para abrir as portas da cidade e permitir a entrada de seu exército dando lugar a um saque impiedoso da cidade.

Mas vocês podem se perguntar: o que esta história tem de relevante, pois repete-se vezes sem conta nas empresas e nas organizações, independentemente da dimensão ou da indústria. Repete-se em cada empresa que não renova a sua estratégia de cibersegurança e que conserva os mesmos controles que a mantiveram segura durante os últimos anos. A organização normalmente se considera invencível e impenetrável como os cidadãos de Tróia, e é nessas circunstâncias que uma vulnerabilidade sutil e irrelevante pode se tornar a brecha que os atacantes esperaram pacientemente durante anos. É nestas que vivemos. As pessoas mudaram, mas os processos e controles seguem sendo os mesmos. Por isso que é necessário centrar esforços em reeducar, iniciando pela revisão e atualização dos riscos de cibersegurança e os ataques mais frequentes do último ano; também é necessário e urgente rever as práticas e controles da cibersegurança dos dispositivos e redes LAN caseiras. É na educação que estamos falhando, na minha opinião. Acreditamos estar seguros com os controles

e ferramentas que nos protegeram durante décadas, mas não nos apercebemos que a batalha se joga em nossos empregados e colaboradores, que, como pessoas, fazem parte essencial da estratégia de cibersegurança das empresas.

Por que colocar ênfase na cibersegurança nas redes LAN das nossas casas? Por que, se deveríamos estar mais preocupados com a rede da nossa empresa, das nossas sucursais, das sedes e escritórios em todo o mundo, que estão em risco? Por que devemos nos preocupar com redes caseiras e dispositivos fora da área de TI e segurança empresarial? Para dizer a verdade, o problema está nesta nova realidade que vivemos há um ano. As redes das nossas casas passaram a ser uma extensão da rede empresarial, porque uma grande parcela da força de trabalho das empresas está sob o modelo home office. A pandemia do coronavírus transformou algo que antes era desejável ou opcional a empregados e empreendedores: agora trabalhar em casa passou a ser algo quase mandatório e a vida laboral e a vida familiar se entrelaçaram muito mais, quase em nível imperceptível. Sem nos dar conta, passamos de atividades trabalhistas a nossa vida familiar sem nenhuma pausa. Começamos a revisar tarefas de nossos filhos, correios pessoais, páginas web de lazer, compras on-line, tudo com o mesmo computador portátil ou de mesa e usando o mesmo dispositivo celular, o que torna muito fácil para um atacante acessar por um meio eletrônico, como o email pessoal, a informação empresarial confidencial. Aqui está minha recomendação sobre a ênfase que devemos colocar em fortalecer a capacitação em cibersegurança de nossa equipe, colegas de trabalho e família, na prevenção e ação ante uma suspeita ou ataque efetivo por mais sutil ou irrelevante que pareça, dado que é certamente o início de algo muito mais elaborado e de maior impacto.

Proponho que você comece por criar e fortalecer os hábitos em torno das principais ameaças e ataques cibernéticos do ano passado e faça revisões semestrais de acompanhamento. Então, antes de passar a uma recomendação, listemos os ataques e ameaças mais populares e em aumento:

**Phishing:** Uma mensagem digital enviada com o propósito de enganar e fazer com que um indivíduo acesse um website falso apresentado como legítimo, com o objetivo de ativar um vírus ou instalar um malware que permita extrair informação sensível. Este tipo de mensagens pode chegar por meio de chats grupais com notícias falsas, websites de vacinação, informação e recomendação sobre o coronavírus, entre outros.

**Ransomware:** O roubo e o sequestro de dados é uma forma de extorsão que tomou força e é cada vez mais sofisticado. Iniciando pelo método de phishing, os atacantes criptografam parte ou todo um computador portátil de desktop ou servidor empresarial a fim de obter uma recompensa, geralmente em criptomoedas, que deverá ser paga ao atacante para a liberação dos dados.

**Arquivos políglotas:** Imagens que não são tais ou

arquivos compactados com executáveis que são ativados em sites maliciosos ou que ao baixar arquivos ilegais disparam ações e backdoors que os atacantes usarão posteriormente para exfiltração de informação ou instalação de malware com diferentes propósitos.

**Ataques IoT:** Com a proliferação da Internet das Coisas (IoT) cada vez temos mais dispositivos em casa conectados à Internet, como alto-falantes, hub ou hubs de lâmpadas, fechaduras inteligentes, que podem apresentar vulnerabilidades ou portas abertas e ficar à mercê de atacantes se não contam com uma correta e constante atualização de versão.

**Malvertising:** Palavra derivada de Malicious advertising (publicidade maliciosa, em inglês) que procura em diferentes redes sociais induzir o clique de uma possível vítima com publicidade falsa, mas credível para posteriormente instalar um malware com propósitos mais obscuros, abrindo uma brecha no nosso computador e nossa informação.

**Roubo de identidade:** Durante o último ano, o roubo de informações confidenciais de pessoas aumentou consideravelmente. Através dos métodos acima mencionados, os cibercriminosos aumentaram as solicitações de instituições bancárias e governamentais para obter créditos, subsídios e assinaturas de serviços que os têm como beneficiários e que a vítima terá que pagar posteriormente.

Estas são apenas algumas das ameaças e riscos a que estamos expostos e para as quais devemos criar uma série de hábitos de comportamento que nos permita prevenir e detectar qualquer impacto em nossas informações e dispositivos.

Vejamos alguns hábitos fáceis de implementar que nos ajudarão a fortalecer nossa postura contra os ciberataques:

**Duvidar e suspeitar de tudo:** A primeira coisa que devemos fazer é duvidar de qualquer mensagem, publicidade, correio de oferta ou de informação. Uma vez que os agressores se tornaram cada vez mais hábeis em falsificar sites de bancos ou de comércio eletrônico, é necessário duvidar sempre. Por mais seguro e real que seja a mensagem, devemos verificar o URL ou endereço da página web e corroborar que tenha um ícone com cadeado, ou seja, um certificado de segurança que garanta que o site é seguro e foi verificado por uma entidade certificadora. Se é uma mensagem de nosso banco ou instituição financeira de confiança revisemos que a direção seja a que sempre temos utilizado; ante a dúvida sempre devemos fechar o website, abstendo de fornecer informações e contactar imediatamente a entidade ou empresa para validar a veracidade da mensagem.

**Ser egoísta com a informação:** Devemos entender que a nossa informação é muito valiosa, e que todos os aplicativos gratuitos que baixamos e instalamos não são realmente grátis, estamos pagando-lhes com a nossa informação, dados básicos, contatos, localização on-line, sites que visitamos e rotinas de trabalho

entre muitas outras informações que compartilhamos; precisamos ser mais egoístas antes de dar permissão para aplicativos em nosso celular e rever o que estamos cedendo e compartilhando, ser egoístas quando preenchemos formulários de dados de inscrição em páginas web de sites de comércio eletrônico, sites de pesquisas etc. Sejamos egoístas e não demos nosso correio principal nem nossa informação básica, sem antes avaliar se é estritamente necessário.



Ilustración: Fotolia Xunantunich

**Ser rigoroso com as senhas:** Cada vez nos inscrevemos em mais sites, baixamos mais aplicativos em nosso celular, e todos estes pedem um usuário e senha. Para economizar tempo, nós geralmente caímos no hábito de colocar o nosso correio principal e a mesma senha fácil de lembrar. Daqui se destacam várias recomendações: primeiro não usar nosso correio principal se não for necessário, segundo usar aplicações de gestão de senhas que nos permitam guardar as credenciais de todos os sites e que proporcionam a autogeração de senhas fortes que incluam símbolos, maiúsculas, minúsculas. Desta forma, não será necessário memorizar e, se algum destes sites for exposto e as senhas e emails forem obtidas, não terão o nosso correio habitual nem a nossa única senha. Uma última recomendação é usar um segundo fator de autenticação: uma aplicação que gere um token de uso único ou autenticação biométrica que permita configurar-se nos nossos sites mais rigorosos, como correio eletrônico pessoal e empresarial e sites de comércio eletrônico habitual. Ser paciente e proativo com as atualizações também é prioritário, já que os computadores portáteis e de desktop, celulares e tablets geram periodicamente novas versões que proporcionam fechamento de brechas de segurança detectadas e não apenas novas funcionalidades. Geralmente são insistentes e irritantes as notificações e lembretes de atualização que surgem em janelas emergentes, mas que devemos enfrentar

com paciência e programar. Nós podemos proativamente silenciá-los e agendar uma hora por semana em que vamos fazer uma pausa do dispositivo ou aplicativo para iniciar e executar a atualização correspondente, mas é necessário e importante que como hábito estejamos permitindo que este processo seja realizado semanalmente, já que se não o fizermos estaremos expostos a numerosas vulnerabilidades de software e hardware que algum malware, vírus ou processo de um atacante vai aproveitar e usar para roubar, extorquir ou sabotar nossos dispositivos e informações.

Desde OCP TECH estamos em condições de prestar serviços para o desenho de uma estratégia integral que, junto com as ferramentas Cisco, ofereçam uma proteção sem fronteiras dos dados e ativos de sua empresa, incluindo não só as melhores práticas para a implementação de redes empresariais e soluções de software, mas também a experiência de um grupo de especialistas em segurança e processos que levarão a sua empresa ao próximo nível enquanto se concentra no negócio |

*O autor deste artigo está disponível para consultas em [fabio@ocp.tech](mailto:fabio@ocp.tech)*

# Síndrome de **burnout**, uma patologia que ganhou tração durante a pandemia

Esgotamento mental, emocional e físico. Demandas do trabalho que resultam em estresse. Atitude de indiferença e desapego ao trabalho. Desmotivação, frustração. Diminuição da produtividade. Estresse crônico. Insatisfação com o trabalho.



por **Silvia Montenegro**

Este quadro define o burnout ou síndrome do “queimado” ou de desgaste profissional, que, detectado pela primeira vez nas últimas décadas do Século XX, ganhou força com a conjuntura do século XXI. Os especialistas dizem que o aumento da concorrência global, os dispositivos digitais que normalmente obrigam muitos trabalhadores a estar em linha durante horários estendidos, somado a ambientes sociopolíticos instáveis e à possibilidade concreta de perder o trabalho ou estar sob a pressão de perdê-lo durante um tempo prolongado, desenham uma combinação que resulta em problemas psicológicos em grande parte da população. A crise mundial provocada pela pandemia de COVID-19 e as suas restrições apenas agravou o quadro.

Em 2019, a síndrome de burnout foi catalogada pela Organização Mundial da Saúde (OMS) como um risco laboral e, a partir de 1 de janeiro de 2022, integrará a Classificação Estatística Internacional de Doenças e Problemas de Saúde Relacionados (CIE-11), considerada uma boa oportunidade para visualizar a patologia presente na realidade laboral.

Trata-se de uma doença decorrente da interação do indivíduo com determinadas condições psicossociais no trabalho, que pode ser acompanhada de sintomas físicos. Também é reconhecida como um gatilho para outros problemas de saúde física ou mental mais graves.

## Cómo surge

Em seu livro “*Burnout: The High Cost of High Achievement*” (1974), Herbert Freudenberger foi o primeiro que utilizou o termo para definir o transtorno decorrente de um estresse trabalhista crônico. Este psicólogo americano, de origem alemã e ascendência judaica, observou as manifestações de esgotamento que apresentavam os psicoterapeutas de uma clínica de toxicómanos de Nova Iorque, e introduziu o conceito de mapeamento do processo de deterioração nos cuidados que davam aos seus pacientes. Definiu-o como “uma sensação de fracasso por sobrecarga de exigências de energia, recursos pessoais ou força espiritual do trabalhador”.

Alguns anos depois, a psicóloga Christina Maslach, que até hoje continua a investigar esta síndrome, elaborou um instrumento de medição universal, denominado MBI Maslach Burnout Inventory, ainda vigente, para detectar a presença de sinais de desgaste profissional, que é definido como um processo, em vez de um estado. Propôs diagnosticá-lo a partir de uma “tríade sintomatológica”, constituída pelo cansaço emocional, a despersonalização e a falta de realização pessoal.



Imagen: Morgan Basham, Unsplash.



## Sintomas e Profissões

As pessoas que experimentam a síndrome de burnout sentem que seus trabalhos são cada vez mais estressantes e frustrantes. Podem se distanciar emocionalmente, têm dificuldade em lidar com as tarefas diárias, têm desempenho reduzido. Sentem cansaço, dificuldades de concentração e falta de criatividade. Os sintomas físicos que geralmente acompanham o quadro são dores de cabeça e de estômago, problemas intestinais, distúrbios do sono, tensão muscular e exaustão física. A lista de sintomas associados é extensa, e o nível de alarme estabelece quatro estádios: leve, moderado, grave ou extremo.

Não existem dados precisos sobre grupos de maior risco. No entanto, com a descoberta da síndrome nos anos 70, algumas profissões ou atividades foram identificadas como as mais estressantes, incluindo profissionais de saúde, forças de segurança, assistentes sociais ou professores. Na década de 1990, o conceito do burnout foi ampliado, incluindo as pessoas que trabalham com clientes de trato direto.

Atualmente, o espectro inclui outros grupos ocupacionais, entre os quais se mencionam os profissionais que trabalham com dados, como os usuários de tecnologias e teletrabalhadores, o pessoal que lida com usuários problemáticos, ou aqueles afetados por uma cultura empresarial obsoleta ou complicada. Em um mundo onde tudo muda o tempo todo, convivem modelos de governança débeis: empresas e instituições com estruturas do Século XX e realidades do Século XXI.

## Pandemia e Vícios

Nora Revere, médica psicanalista, membro da International Psychoanalytic Association (IPA) e da Associação Psicoanalítica Argentina (APA), expressa que no contexto pandêmico a humanidade suportou medo, distanciamento físico e social, incerteza, novas formas

de trabalho a partir de casa ou desemprego: “Estamos confrontados com situações de muito estresse. Penso que, hoje, quase todos estamos um pouco ‘queimados’, ultrapassados pela forma como temos trabalhado em pandemia. Naturalizou-se trabalhar muitas horas por dia, ao que se acrescentou a impossibilidade de tirar férias pelas restrições. Dentro do estresse, a síndrome de burnout está focada na área de trabalho, mas podemos dizer que o problema é o estresse, que é mais abrangente”.

Um estudo internacional desenvolvido por pesquisadores da Universidade de Queensland, na Austrália, e publicado na revista *The Lancet*, estima que os casos globais de depressão maior e de transtorno de ansiedade aumentaram 28% e 26%, respectivamente, durante a pandemia.

A doutora Nora Revere acrescenta que as pessoas que sofrem da síndrome de burnout estão em desequilíbrio, fora de eixo. Muitas vezes esta situação está relacionada à intolerância, à frustração, à incapacidade de se adaptar às mudanças e, às vezes, a base pode ser a dependência do trabalho: “Creio que nesta época os seres humanos têm grande capacidade para a dependência, para o trabalho, para as séries, para a comida, e é produto da dependência emocional, da dificuldade de estar a sós com si mesmo, e o desafio não é preencher vazios, mas ter maior riqueza interna. Se trabalho 12 horas por dia, não tenho tempo para a família, para o lazer, para fazer exercício. Viciado significa escravo, e há um ditado que diz que não há escravo feliz. A gente pode ser feliz quando se apropria de si mesmo, da própria vontade”.

## E então...

Para recuperar da síndrome de *burnout*, recomenda-se apoiar-se na terapia psicológica para reconhecer as causas do estresse e buscar maneiras de combatê-las. Este é um processo, por isso, também é uma boa ideia usar a bateria de estratégias para enfrentá-lo.

Nora Revere acredita que, diante de uma situação de esgotamento laboral, em outro momento se aconselhava que a pessoa relaxasse, descansasse, tirasse férias. No entanto, hoje isto é impensável pela mesma dinâmica laboral do mundo competitivo. Por isso, o conselho falar com especialistas, ter interação social, buscar elementos que deem prazer, aumentar o lazer produtivo, a capacidade de desfrutar, estabelecer um lugar para o jogo, adotar hábitos saudáveis: “O tema seria ganhar o melhor dos tesouros, que é a felicidade. Se alguém tem uma vida íntegra, capacidade criativa, e possui recursos internos, o caminho para a felicidade é mais fácil, porque vai encontrar ferramentas para ter coragem, esperança, fé. Uma pessoa íntegra se focaliza em três aspectos de sua vida, a mente, o corpo e o espírito ou atitude frente à vida”. Marca a diferença entre a alegria, que é fugaz, e a felicidade, que persiste além de qualquer obstáculo, e coloca a ênfase

se no desafio de buscar constantemente a própria liberdade. Aqui uma pista: “Diz-se que a felicidade está nas coisas simples da vida”

## O desafio das Empresas

No que diz respeito às organizações e empresas, existem alguns fatores de risco que aumentam as chances de impactar negativamente na vida dos empregados. Entre eles contam-se uma estrutura muito hierarquizada e rígida, excesso de burocracia e falta de participação dos trabalhadores, falta de formação prática em novas tecnologias, desigualdade percebida na gestão do capital humano e estilo de direção inadequado.

Também existem fatores de risco relacionados com a concepção dos postos de trabalho, com perfis que suportam sobrecarga de trabalho, exigências emocionais na interação com o cliente, falta de apoio social, insatisfação no trabalho ou por temas relacionados com os salários.

Nora Revere destaca formas de prevenir o estresse do trabalho com base na oferta de apoio social e analisando as razões para a insatisfação. Além disso, destaca-se a oportunidade de treinar gestores e empregados através de conversações com especialistas que assessoram sobre o tema.



Imagem: Isabella and Zsa Fischer, Unsplash.



Imagem: M.T El Gassier, Unsplash.

## Cibersegurança: Especialistas à beira do colapso

Pelas características do trabalho de atuar sob pressão contra o crime cibernético e estar na primeira linha de defesa gerenciando e respondendo os alertas de ameaça – que evoluem para evadir a detecção –, os responsáveis da área formam um coletivo de trabalhadores predispostos a sofrer estresse. Vasta bibliografia e estudos falam da relação entre esgotamento laboral e rendimento, e sua relação com o erro humano em diferentes indústrias. Embora não existam estatísticas concretas sobre a proporção de erros em equipamentos de cibersegurança que respondem ao esgotamento, pode-se inferir que a síndrome de burnout influencia os resultados concretos dos profissionais de segurança. Este problema está também associado à elevada rotação que normalmente se verifica no setor.

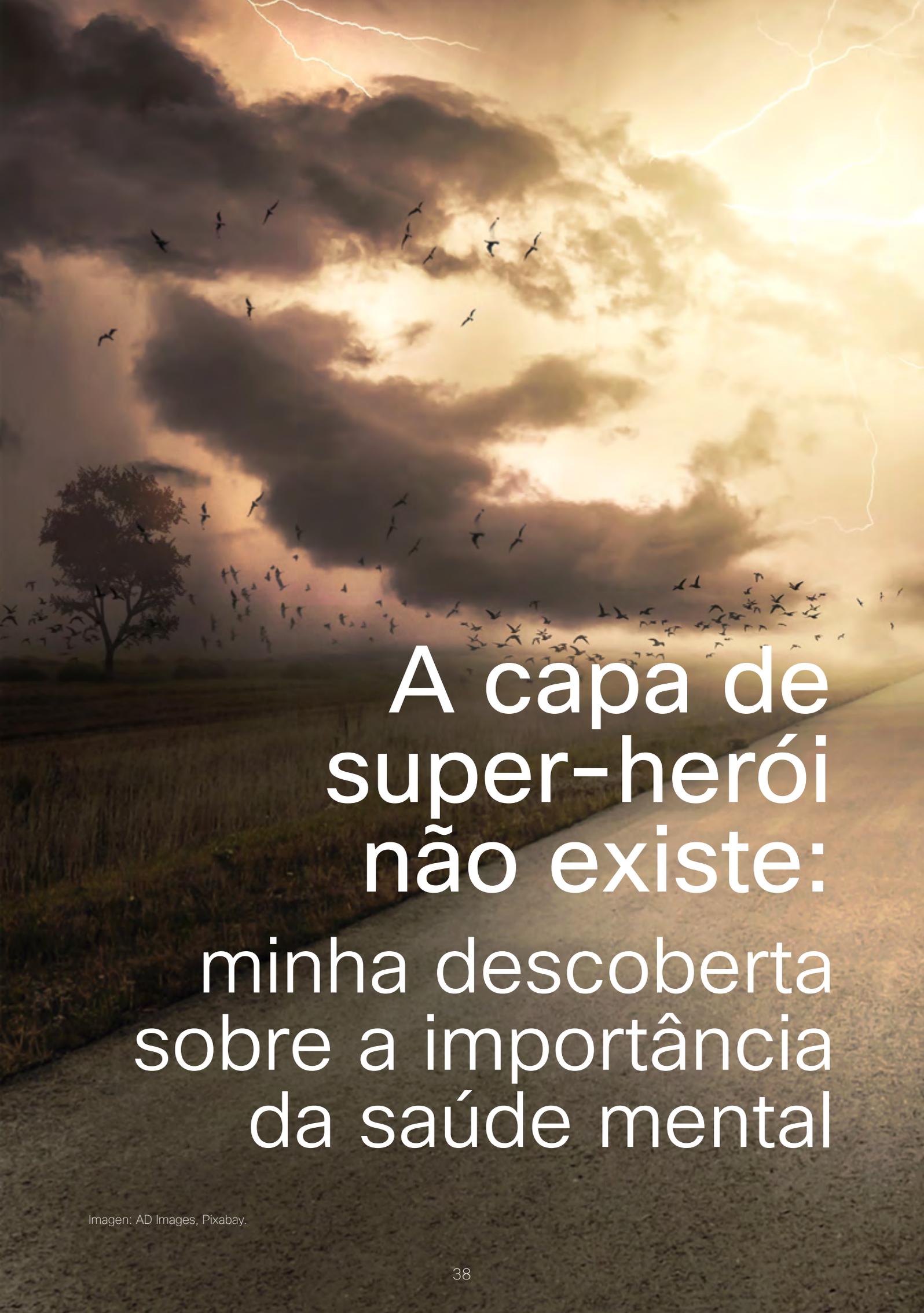
A Organização Mundial de Saúde (OMS) informa que, se EM um setor econômico há muitos trabalhadores com esgotamento laboral, torna-se menos produtivo, pelo que, além de ser um problema de saúde, gera impacto social e econômico.

Como em outras profissões, face a situações de estresse, é vital a implementação de políticas de apoio aos empregados, ter uma cultura empresarial efetiva e estabelecer métodos para prevenir e/ou contrariar quadros de desgaste profissional.



## Os jogos de vídeo na mira

A Classificação Estatística Internacional de Doenças e Problemas de Saúde Conexos (CIE) inclui também a perturbação da utilização de jogos de vídeo. Manifesta-se pela deterioração no discernimento do controle do jogo, como a duração, a intensidade ou a frequência; o aumento do grau de prioridade que se antepõe a outras atividades da vida diária; e o aumento do jogo apesar de identificar consequências negativas.



# A capa de super-herói não existe: minha descoberta sobre a importância da saúde mental



por Laércio Albuquerque,  
VP da América Latina



*Laércio em um momento de esparcimento, disfrutando de su perro y buena música.*

*Imagem: Gentileza L. Albuquerque.*

***Nós precisamos de pausa, nós não somos super-heróis, e eu acredito fortemente que as pessoas não querem super-heróis, elas querem apenas bons humanos.***

Ano passado eu escrevi sobre o meu processo forçado de Detox Digital, no qual fiquei 30 dias completamente desconectado, e me dei conta de que se eu tivesse feito pausas nos momentos adequados, não precisaria tomar medidas assim tão drásticas. Hoje, como simples exemplo, eu desligo meu celular duas horas antes de ir para a cama. Consegui vencer a tentação e já não dou mais aquela “olhadinha final” nos e-mails e mensagens antes de fechar os olhos para dormir.

A minha experiência pessoal com a saúde mental me ensinou muito. E como lembrança desta fase tão marcante, gostaria de dividir com vocês alguns aprendizados que levo para minha vida e que compartilho diariamente com os que estão ao meu redor:

## 1. Coloque seu ego de lado

Eu, assim como muitos de vocês, tenho algo que se chama ego. Aceitar, conviver e superar esse ego é algo difícil. Eu, como líder de uma das maiores empresas de tecnologia e conectividade do mundo, jamais quis aceitar que, apesar de extremamente feliz, estava sobrecarregado, cansado e a ponto de um colapso físico e mental.

***Eu queria dar conta de tudo, eu achava que eu podia dar conta de tudo, até porque amava e amo o que faço, e achava que nada ia acontecer, até sofrer um pico de arritmia e ir parar no pronto-socorro de um hospital.***

Quando você tiver problemas, deixe seu ego de lado, fale e busque ajuda. Tem muita gente que pode estar passando pelo mesmo que você, ou que já enfrentou esses mesmos problemas e podem te ajudar. E trabalhar numa companhia que realmente cuida de suas pessoas, também significou muito para mim.

## 2. Ponha as pessoas genuinamente em primeiro lugar

Tire os olhos de você e coloque nas pessoas. Seja autêntico e genuinamente interessado pelas pessoas, mas não porque você leu em algum lugar que “é preciso ser assim”, mas sim porque você quer.

A duras penas descobri que a nossa capa de super-herói simplesmente não existe. Entendi que você pode estar extremamente feliz e amar o que faz, mas tudo em excesso e sem suas devidas pausas pode ser um perigo. Neste artigo, divido um pouco sobre a importância da saúde mental e alguns aprendizados para não cair nesse buraco de novo.

**Qual conselho você daria para o seu eu do passado, de 20 ou 30 anos atrás?** Outro dia recebi uma pergunta como essa em uma entrevista, o que me fez pensar muito sobre a minha vida e refletir sobre tudo que aprendi nos últimos tempos. A minha resposta foi clara: “Eu diria que a capa de super-herói infelizmente não existe, não tente ser um super-herói.” O dia 10 de outubro foi instituído como o Dia Mundial da Saúde Mental, e eu não poderia deixar de comentar algo que é tão importante para mim e foi tão marcante na minha vida.

No meu caso, os desafios com a saúde mental vieram em um dos melhores momentos da minha carreira, em meados de 2020. Foi quando eu descobri que você pode estar feliz e amar o que está fazendo ou vivendo, mas tudo em excesso pode ser um perigo. Fazer mil coisas ao mesmo tempo sem as devidas pausas que seu corpo, mente e coração demandam, pode levá-lo para o buraco. E por experiência própria, eu digo que quando você tenta equilibrar vários pratos ao mesmo tempo com perfeição, é muito provável que alguns caiam. E está tudo bem.



Imagem: Myles Tan, Unsplash.

*Nesses meus mais de 20 anos como líder de pessoas, vi que elas não ligam para o quanto você sabe, mas querem saber o quanto você se importa com elas.*

Ser você, autêntico e vulnerável, faz com que as pessoas se aproximem e se conectem com você. Assim somos. Seja um líder que queira inspirar e, antes de tudo, seja feliz com você mesmo, sua posição e seus ideais. Você jamais conseguirá tocar outras pessoas se não estiver feliz consigo mesmo. Seja feliz com suas imperfeições, seja humano. E assim como eu falei acima, não você não precisa ser um super-herói, as pessoas buscam por outros seres humanos, com seus defeitos e virtudes.

### 3. Cuidado com o perfeccionismo

O perfeccionismo que me fez chegar à Vice-presidência América Latina da maior empresa de conectividade do planeta, é o mesmo perfeccionismo que já me levou ao hospital. Tudo precisa ter um balanço, um equilíbrio. Seja menos perfeccionista, se apegue menos aos detalhes, aprenda a delegar, e cuide com mais atenção apenas do que re-

almente importa. Para uma pessoa que se cobra tanto como eu, é difícil sentir que está “perdendo” o controle das coisas, mas tentar fazer tudo sozinho pode te levar a perder noites consecutivas de sono. Lembre-se de que em uma empresa, você nunca está só, você tem os demais da equipe, seu líder e outras pessoas que podem te apoiar. Busque ajuda e mentoria, mesmo que seja interna, para descobrir seus pontos de melhoria. O meu perfeccionismo me gerava (e ainda gera em partes) muita ansiedade, mas é libertador conseguir viver sem tanta pressão interna, além de fazer muito bem para nossa saúde mental.

### 4. Use a tecnologia de maneira correta

*Use a tecnologia como uma ferramenta nas suas mãos, não seja uma ferramenta nas mãos da tecnologia.*

A tecnologia é maravilhosa, nos ajuda muito, conecta pessoas, apoia comunidades, transforma vidas, gera empregos. Mas ao mesmo tempo que conecta as pessoas, também pode te distanciar



Imagem: Natalya Zaritskaya, Unsplash.

daqueles que estão ao seu lado, como da sua família naquele jantar importante, ou pode fazer com que você não preste atenção ao que seu filho contou sobre o dia na escola. Eu sempre digo que a mesma tecnologia que salva é a que cega. Os momentos com as pessoas que você ama não vão voltar, então preste atenção a sua vida real. Desconecte quando você tiver que desconectar, se é um fim de semana, aproveite o seu fim de semana. Se for feriado, esteja presente no feriado. A tecnologia pode ser uma benção ou uma maldição, e a escolha depende só de você. Não tente estar o tempo todo em mil lugares ao mesmo tempo. Quando sua mente, corpo e coração estão em lugares diferentes, em algum momento você vai sentir o impacto deste desequilíbrio em sua mente e seu corpo vai sofrer as consequências.

*Eu posso garantir que se você deixar sua família de lado numa data altamente significativa por uma reunião importante, em 10 anos, você não vai lembrar do que foi aquela reunião, mas irá sempre se lem-*

*brar de que não participou daquele inesquecível momento.*

Eu já cancelei uma reunião extremamente importante para a minha carreira para voltar para casa e estar presente no aniversário de 6 anos da minha filha (conto mais sobre essa história no meu Ted Talks). Por isso, valorize cada minuto com as pessoas que você ama, estabeleça prioridades e momentos de lazer. Descansar é necessário, ainda mais agora em um mundo completamente conectado. Lembre-se, a tecnologia vai automatizar tudo, mas jamais vai automatizar o calor de um abraço.

Minha paixão é usar a tecnologia para conectar os negócios e melhorar a qualidade de vida das pessoas, mas minha missão é fazer da tecnologia uma aliada. Eu amo tecnologia, dediquei toda a minha vida a isso, mas eu amo muito mais as pessoas e como a tecnologia pode ajudar e apoiar na melhoria da vida de cada um. Preste atenção aos seus sinais, a sua saúde mental e a você. Cuide de você e, somente assim, você poderá dar conta do resto 🌱

El secreto está en  
la transformación que  
surge a través de  
la mirada.



Contenidos Multiplataforma  
[basantacontenidos.com](http://basantacontenidos.com)



Basanta  
contenidos

Especial Mini recital

# Tempo de música

Voz: Noelia Munz  
Baixo: Sebastián Tozzola



Conteúdo  
audiovisual



O especial anti-burnout é um convite da redação de Bridge para você se conecte consigo mesmo, a partir de um lugar de consciência, reflexão, calma e prazer. Por isso, como conclusão, decidimos incluir um breve recital de dois artistas requintados, Noelia Munz e Sebastian Tozzola. Escaneando o QR presente tanto na capa como neste artigo você poderá acessar um vídeo de quatro temas musicais deste hipnótico duo de voz e baixo.

Por que os escolhemos? Para o conjunto precioso entre a voz de Noelia e os graves do baixo de Sebastian, que nos movem amavelmente a uma frequência de relaxamento prazeroso.

Para estar em sintonia com o tema que nos convoca, realizamos a filmagem no Teatro Border da cidade de Buenos Aires, o primeiro espaço sustentável deste tipo na Argentina.

**Com vocês, os artistas.**



Imagens: 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 doblaga 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 recalculer 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

Tecnologia e Inteligência  
Humana, Biológica e Natural:

# Recursos Internos para o Bem-Estar





por **Claudia Menkarsky**  
Vocal Coach, Terapeuta Psicovocal e  
Cantora Lírica

## Especial

Nestes tempos de agitação, confusão e mudança, nada melhor do que recorrer aos nossos recursos humanos para nos transformar em corpo e alma, alcançar o bem-estar e descobrir o próprio potencial para viver cada dia melhor?

Através de todos os tempos, temos adquirido múltiplos conhecimentos através de disciplinas orientadas a liberar o potencial humano-divino do nosso interior. De acordo com a nossa natureza, nos veremos mais ou menos inclinados às diferentes atividades, o importante é sentir e agir onde tudo flui com alegria; o que chamamos vocação, é uma grande orientação.

### Onde você está fluindo?

Todas as artes geram alegria para a alma e formidáveis emoções e hormônios de bem-estar.

Muitas vezes, nos dói relegar aquilo que gostamos, por dar tempo e prioridade a outras coisas, sem saber que com um par de horas por semana que dediquemos ao que nos é agradável e libertador teremos mais energia para fazer logo tudo aquilo que devemos.

Por isso, considere experimentar música, teatro, canto, dança, pintura, escrita, leitura, meditação, ioga, esportes, caminhadas, frequentar entes queridos, espaços naturais, dormir o necessário, alimentar-se bem para nutrir-se por dentro.

Grandes mudanças começam com pequenos passos ■

Entrevista

## Mariano O’Kon

Director, Architectures Sales,  
Cisco Latin America and the Caribbean



Imagen: Gerhard G., Pixabay.

Encontrei-me com Mariano via Webex em uma tarde cuja promessa de escutar coisas novas parecia esgotada para mim. Nossa conversa mudou não só essa premissa, mas Mariano lançou luz sobre vários pontos relacionados ao tema que nos convocava de uma forma sumamente didática e natural. O enxame de siglas se tornou um oásis de conhecimento e possibilidades. Convido-te a descobrir uma nuvem segura a partir das mãos firmes e confiáveis de Mariano O’Kon.

# Um passeio seguro pelas nuvens

por Karina Basanta



Temos os pés  
no chão, mas a  
informação na  
nuvem. Como  
chegamos a isso  
e por quê?

O conceito de transformação digital surgiu há mais de dez anos. Uma definição básica deste processo se refere ao uso da tecnologia na estratégia de negócios. Antes disso, a tecnologia era simplesmente um ativador, ou seja, permitia fazer as coisas mais baratas, mais rápido. Hoje também nos diferencia da concorrência, e em alguns casos, as empresas não existiriam sem a tecnologia, por exemplo, nos casos da Uber, Rappi. Costumamos falar da pandemia como geradora da mudança, porém a disponibilidade da conectividade começou como grande tendência há mais de 15 anos. No mercado, fala-se que 2/3 das compras começam pela internet (para escolher o produto, para comparar, para explorar) e 50% das delas ocorrem online, através do móvel. Se as pessoas usam tanto o dispositivo móvel, então é importante dar uma boa experiência de compra, porque diz-se que 60% dos consumidores estão dispostos a pagar mais por uma experiência digital superior e 50% muda de fornecedor, se a experiência digital for ruim. A lealdade às marcas em forma digital não existe se não se pode satisfazer o objetivo de alcançar o que se necessita em tempo e forma. É claro que a tolerância com as empresas é muito baixa em relação à satisfação do serviço. Atualmente, há uma interação constante entre a informação física e a virtual, e a experiência deve ser excepcional durante todo o processo de compra. Agora, se as empresas estão indo muito bem e começam a crescer em vendas digitais, elas vão precisar expandir seus data centers, porque sem isto seus serviços vão começar a declinar e perder clientes.

A reação das empresas para adaptar os recursos à demanda foi expandir o negócio para a nuvem, ou seja, aumentar os aplicativos para clientes em data centers públicos dos quatro maiores fornecedores, Microsoft, Google, Amazon, IBM, o que lhes permitiu obter rapidamente espaço de hospedagem dos dados. Segundo um estudo da IDC, até 2023 serão gerados 500 milhões de novas aplicações, o que reafirma que grande parte da população mundial opera através de aplicações para cobrir três grandes áreas:

**Produtividade:** são as que um empregado utiliza para fazer o seu trabalho, como Google, Office 365, box, Salesforce, SAP.

**Colaboraci3n:** que relaciona empregados com clientes e fornecedores, como Webex.

**Aplicaciones al consumidor:** s3o as que correm nas nuvens p3blicas do Google Cloud, AWS, Microsoft Azure, IBM e outras, ou na nuvem privada, em data centers pr3prios. Em todos os casos s3o utilizadas por consumidores finais.

A tua explica33o parece nos levar 3 nuvem h3brida.

Exato. A primeira tend3ncia que comeamos a ver h3 cerca de 10 anos foi precisamente a nuvem h3brida, onde as empresas se expandiram para a nuvem p3blica e comearam a consumir e a gerar aplica33es tanto nos data centers privados como p3blicos. A pandemia acelerou este processo. Como refer3ncia, na Am3rica Latina, metade dos clientes da Cisco j3 est3 usando pelo menos dois fornecedores de nuvem p3blica. Dois por uma quest3o de custos e para reduzir o risco de ter tudo com um s3 provedor.

## E a forma de trabalhar?

Com a chegada da pandemia, todos ficamos em nossas casas, e com as vacinas se comeamos a voltar aos escrit3rios. No entanto, a chegada das novas variantes do v3rus desarmou o esquema do retorno completo, fazendo com que as empresas tenham que contar com uma plataforma que lhes garantam que o trabalho remoto pode ser feito de forma correta. As empresas perceberam que “o trabalho n3o 3 aonde se vai, mas o que se faz”, como dizemos na Cisco h3 muitos anos. A pandemia nos mostrou que pod3amos usar o que estava dispon3vel atr3s da tecnologia para trabalhar remotamente, e uma das consequ3ncias que trouxe esta revela33o foi a ren3ncia maci3a de pessoas a seus trabalhos tradicionais quando lhes foi apresentada a obriga33o de voltar a cumprir um hor3rio dentro do escrit3rio. Por exemplo, de maio at3 hoje, nos EUA, 20 milh3es de pessoas renunciaram, e estima-se que na Am3rica Latina vai acontecer algo parecido, ainda que de forma mais lenta, pela menor oferta laboral. Hoje o trabalho se coloca em modo h3brido, ou seja, as pessoas v3o trabalhar no escrit3rio ou de sua casa de forma indistinta de acordo com a tarefa e a necessidade; seguramente o que nos for poss3vel fazer sozinhos o faremos, conforme o lar e o escrit3rio se transformam em espaos colaborativos.

## Vamos falar de tend3ncias.

Hoje temos duas fortes inclina33es: nuvem h3brida e trabalho h3brido. No entanto, o que acontece quando algo n3o funciona? A3 surge uma terceira tend3ncia, a observabilidade de todos os dispositivos aos quais se conectam todas as pessoas de todas as organiza33es para saber o que est3 funcionando mal. O desafio de tudo isso 3 garantir usu3rios, dispositivos, acesso 3 nuvem, detectar e responder a ameaas rapidamente. Se h3 5 anos a seguran3a era um tema cr3tico tendo todos os empregados dentro do escrit3rio, hoje eles est3o distribu3dos em diferentes espaos e o uso de mais dispositivos se tornou extremamente decisivo. Note-se que 80% do tr3fego corporativo sai para a nuvem, portanto n3o 3 poss3vel apenas garantir o escrit3rio. Garantir a nuvem torna-se imprescind3vel.



Imagem: Gentileza Mariano O’Kon

Estamos vivendo uma mudança cultural muito forte, a partir da disponibilidade e do uso da tecnologia da comunicação, o que implica grandes desafios em relação à segurança digital.

Quais são as tendências de segurança especificamente?

Podemos listar três:

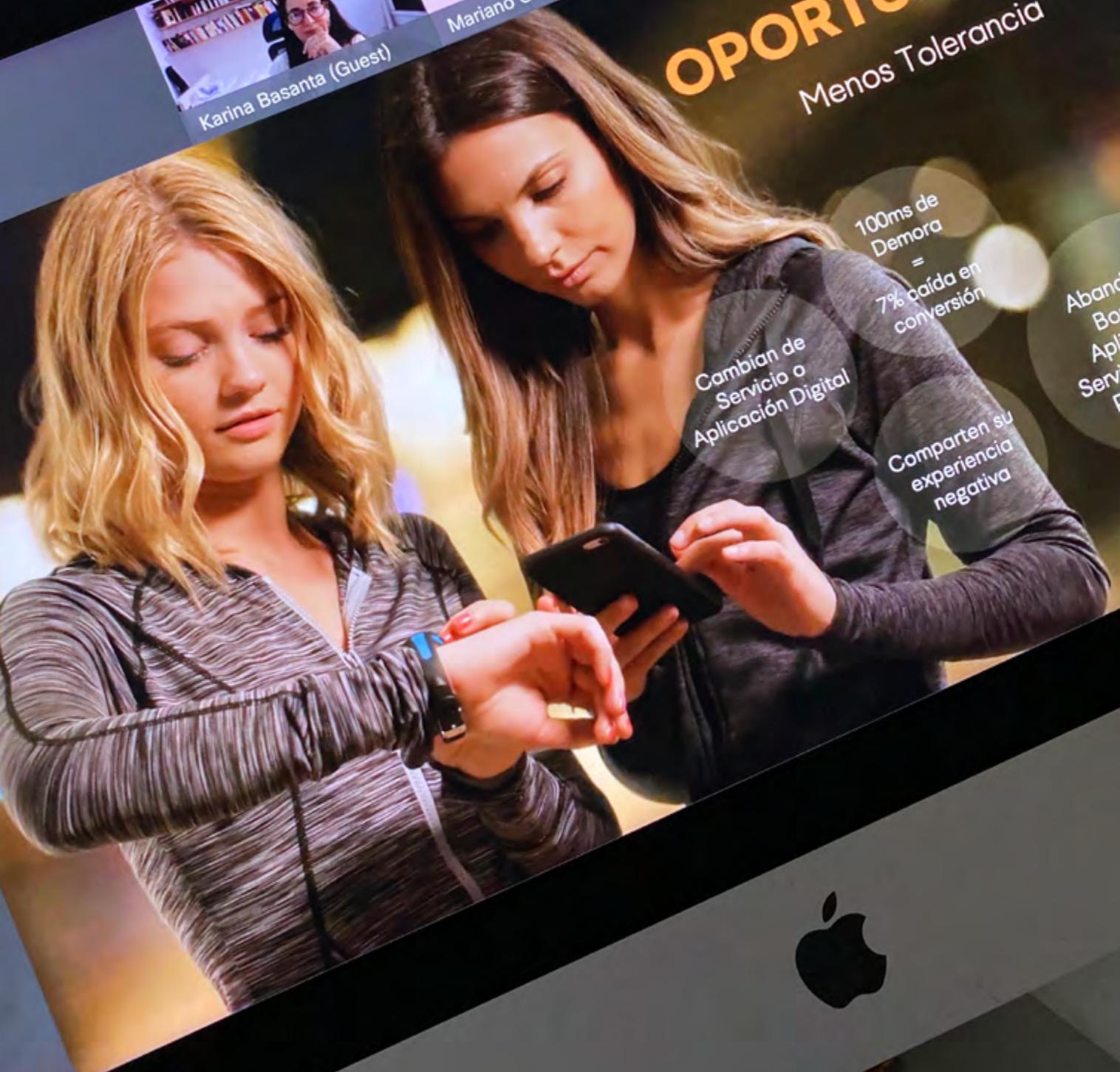
**Zero Trust**  
(confianza cero):

Antes o perímetro de segurança era fácil de delimitar. Se estávamos dentro do escritório, estávamos seguros, se estávamos fora, inseguros. Esta noção era incorreta, mas a maioria das empresas se manejava com este modelo. Assim, nos últimos anos, ocorreram ataques muito fortes, pois supunha-se que as redes eram seguras ainda sem sê-lo. Hoje não há mais dentro e fora, porque mesmo estando dentro do escritório, as aplicações não estão lá. O novo perímetro é a pessoa, que tem de ser autenticada na rede para ser validada. O Zero Trust nos



# UNA OPORTUNIDAD

Menos Tolerancia



Cambian de Servicio o Aplicación Digital

100ms de Demora = 7% caída en conversión

Comparten su experiencia negativa

Abandonan la Aplicación Servicio en Perno



Imagen: Karina Basanta

diz: “Não vou te deixar passar até que me digas com certeza quem és, com utilizador, password, dados biométricos ou validação considerada, e vou verificar se os seus aplicativos e sistemas operacionais estão em condições de entrar”. As permissões de acesso podem ser ajustadas ou completadas tanto quanto a organização o exigir, é claro. A confiança zero determina qual é o perímetro de entrada e qual o de defesa.

Na Cisco, estendemos o conceito de Zero Trust não só para as pessoas, mas também para as aplicações e os múltiplos dispositivos que se conectam à rede, como podem ser câmeras de segurança, sensores de IoT, entre outros, já que muitos dos ataques atuais entram através deste tipo de dispositivos que não contam com grandes medidas de segurança.

## SASE (Secure Access Service Edge):

Quando falamos de SASE, estamos falando de conectividade SD-WAN com segurança na nuvem, que, claro, inclui o Zero Trust, e seu objetivo é garantir o acesso aos aplicativos. Atualmente, a SD-WAN é crítica devido à expansão das empresas para a nuvem. Além disso, as empresas não só utilizam estas aplicações, como também as alteram com frequência e com elas as suas políticas de segurança. SD-WAN é sobre como se conectar de forma eficiente e economizando custos; se adicionarmos isso com segurança através da cloud security, chamamos a união de SASE.

Por que escolher Cisco para percorrer o caminho para SASE? Porque a Cisco tem o portfólio completo que requer SASE. O interessante quando se trata de um mercado tão dinâmico e exposto é reunir todos os elementos no mesmo Vendedor para reduzir riscos.

## XDR

Para entender o XDR, primeiro temos que entender o problema que queremos resolver. Todas as aplicações de software e dispositivos de hardware têm, em algum momento, uma falha (ou bug, como são conhecidos normalmente), que os desenvolvedores reparam e publicam em uma nova versão. A isto chamamos vulnerabilidade. O administrador de TI deve, então, atualizar o software para ter uma plataforma segura. Onde está o problema? Que toda empresa tem muitos, mas muitos, dispositivos e aplicações. E cada uma delas tem, potencialmente,

muitas vulnerabilidades. Então, o administrador de TI normalmente têm a visão de ser obrigado a resolver centenas, ou milhares de vulnerabilidades. Muitas destas, na realidade, não o afetam, talvez porque não se está utilizando a funcionalidade afetada ou porque já existe outra forma de atenuá-la.

O problema, então, é saber quais são as vulnerabilidades críticas que devemos resolver.

Aí aparece o XDR, que não é mais que uma forma de documentar as declarações de vulnerabilidades nas quais os Vendedores nos pomos de acordo. Na Cisco, temos soluções que olham todas as vulnerabilidades, no formato padrão XDR, de cada elemento que há na rede, tanto dispositivos de hardware como aplicações. Através do cruzamento dessas informações e dos algoritmos IA, se determinam quais são as informações críticas e expõe-nas de modo a permitir a atualização necessária para as cobrir. Podemos dizer que XDR é mais uma ferramenta na busca de dar ao departamento de Segurança um mapa de quais são as vulnerabilidades que precisam de uma atualização crítica.

Por último, Maria-  
no, de acordo com  
a sua experiência, o  
que não está sendo  
feito e deveria ser  
considerado nas  
organizações em  
relação à seguran-  
ça digital?

Penso que é preciso aumentar a conscientização. O antigo CEO da Cisco disse, há mais de oito anos, uma frase que ainda continua válida: “existem dois tipos de empresas, as que foram atacadas e as que não sabem que foram atacadas”. Acho que é muito importante conscientizar sobre o valor de ter uma equipe focada em cibersegurança, e se a equipe existe, fortalecê-la. O investimento nesta disciplina é geralmente visto como ingrato, porque se a prevenção procurada funciona, ninguém fica sabendo, é por isso que depois de grandes eventos como as Olimpíadas saem para comunicar todos os ataques dos quais a organização se defendeu. A segurança por definição é invisível e este é um dos fatores pelos quais não há consciência.

O trabalho levado pela equipe de cibersegurança da Cisco é admirável neste sentido, semear a conscientização e apoiá-la com os produtos e os serviços que a empresa tem para cobrir este espaço

Educação

# Programa de **treinamento** em segurança **cibernética**

Imagen: Andrew Neel, Unsplash.

## A cibereducação faz parte da estratégia de aceleração digital “Brasil Digital e Inclusivo” como uma forma de dar resposta à brecha de profissionais capacitados e disponíveis na disciplina.

No dia 16 de julho passado, a Cisco Brasil lançou um programa para desenvolver a nova geração de jovens profissionais em cibersegurança. Cibereducação Cisco Brasil combina os esforços da estratégia de aceleração digital “Brasil Digital e Inclusivo”, anunciada em maio, e o programa global de responsabilidade social na educação Cisco Networking Academy, que oferece capacitação, profissionalização e inclusão dos jovens no mercado tecnológico, incentivando os estudantes a adquirir novas competências de TI e a promover a sua empregabilidade.

O programa, dividido em duas vagas de formação – a primeira em agosto de 2020 e a segunda em fevereiro de 2021 – tem por objetivo proporcionar formação e preparação aos estudantes para o novo mercado de trabalho na era digital; formação para instrutores e oferta de oportunidades profissionais em parceiros e clientes da Cisco. O objetivo é criar um ecossistema consistente para o desenvolvimento de talentos em segurança da informação e satisfazer a crescente demanda de profissionais nesta área, tanto nos setores público como privado.

O programa de educação cibernética Cisco Brasil é 100% remoto, gratuito e tem quatro fases:

**Learn-A-Thon:** Uma maratona de conhecimento que tem como objetivo incentivar e capacitar os estudantes nos cursos exploratórios da Networking Academy “Introdução à cibersegurança” e “Fundamentos da cibersegurança”. Aberto a estudantes das academias da Cisco participantes, esta etapa inclui aprendizagem autodidata que dura um mês.

**Formação de instrutores:** Os instrutores da Cisco Academy Networking receberão formação em dois novos cursos: “CyberOps Associate” e “Network Security”. O objetivo desta fase é criar uma cadeia sustentável de educadores brasileiros em cibersegurança, onde os instrutores atuarão como multiplicadores do conteúdo da Networking Academy em suas instituições.

**Formação Profissional para Estudantes:** Dois mil estudantes selecionados da primeira fase serão formados no curso vocacional CCNA 1, com foco em redes, e em um dos cursos de formação profissional em cibersegurança – “CyberOps Associate”, que os prepara para a carreira de analistas em cibersegurança, ou “Network Security”, e depois para carreiras especializadas em segurança. Esta fase incluirá também for-

mação complementar em conjunto com os parceiros educacionais da Cisco Networking Academy.

**Estágio e oportunidade de trabalho:** Na última fase, os melhores alunos poderão por em prática os conhecimentos adquiridos. Os melhores talentos terão acesso a um estágio de 6 a 12 meses ou um programa de emprego efetivo, postos que serão oferecidos pelos sócios e clientes da Cisco.

Cibereducação conta com parceiros estratégicos como o Senai Nacional, o Centro Paula Souza e a Escola de Comunicações do Exército do Brasil, que contribuem para aproveitar o impacto positivo do Programa na sociedade, oferecendo bolsas para estudantes, entre outras iniciativas.

O público-alvo do programa são estudantes do último ano do ensino médio, graduados ou de ensino superior ou cursos técnicos, que estão interessados em trabalhar no segmento de cibersegurança.

### Dixit

“O Programa de Educação Cibernética da Cisco Brasil é outro passo importante na busca de um mercado de trabalho de TI mais inclusivo para todos neste país, oferecendo oportunidades para milhares de jovens interessados em ingressar em um segmento em constante crescimento”. Gabriel Bello Barros, líder da Cisco Networking Academy no Brasil.

“Ao aumentar a conscientização sobre a importância da cibersegurança e proporcionar um excelente treinamento aos estudantes, a Cisco busca criar um legado educacional na área de TI no Brasil, aumentando a empregabilidade e inclusão dos estudantes”. Gabriel Bello Barros

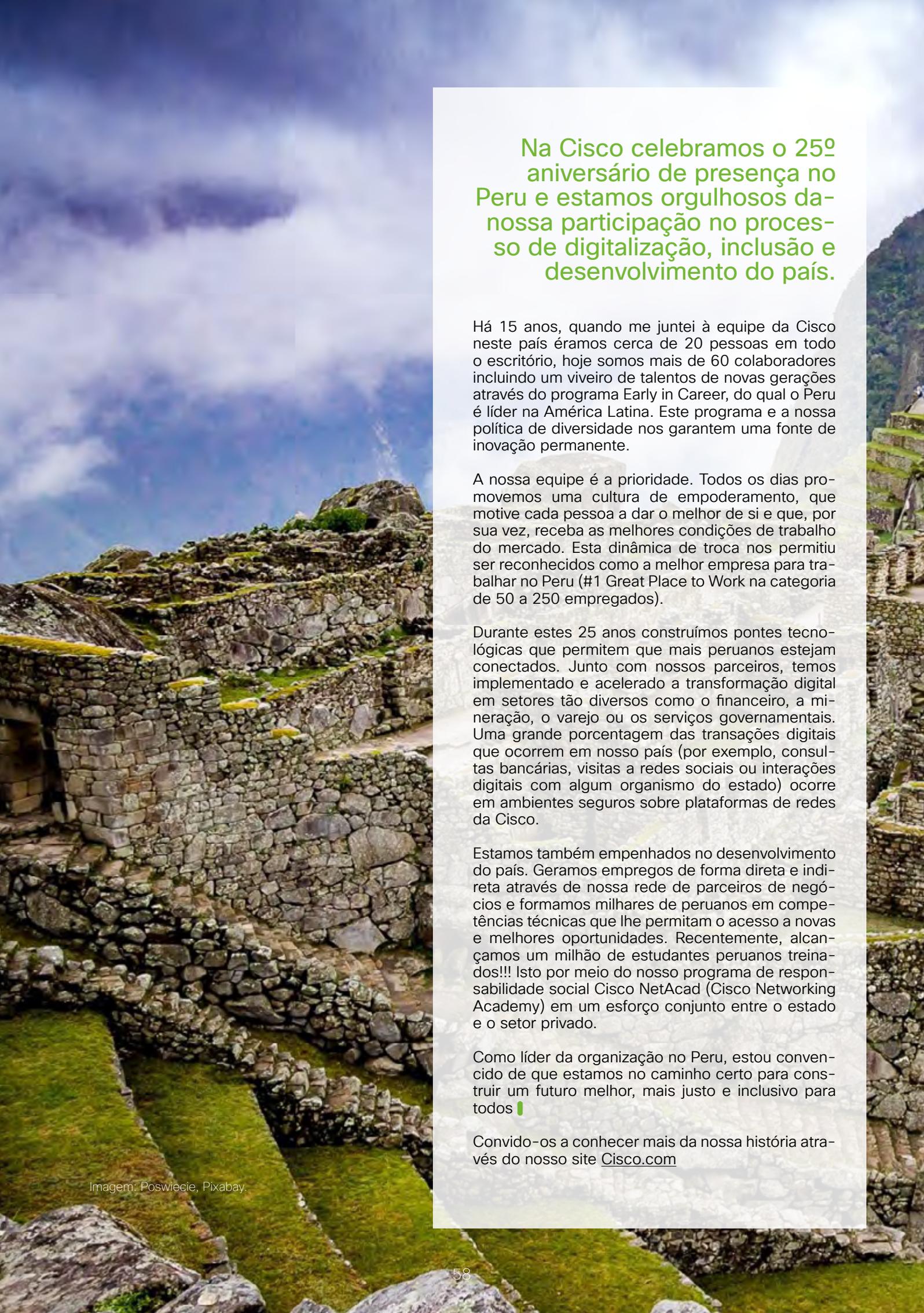
Para mais informações sobre o programa CiberEducation da Cisco Brasil, visite: [https://www.cisco.com/c/m/pt\\_br/brasil-digital-e-inclusivo/cibereducacao.html](https://www.cisco.com/c/m/pt_br/brasil-digital-e-inclusivo/cibereducacao.html)

## O programa em números (projetado para julho 2022)

- Estudantes participantes: 103.751
- Percentagem de mulheres 20%
- Número de estudantes para cursos de certificação: 34.559
- Número de instrutores: 895
- Percentagem de mulheres: 13%
- Academias Cisco (organizações parceiras oferecendo cursos): 521
- Empregabilidade: 97%

Parceiros estratégicos de educação cibernética Cisco Brasil:





## Na Cisco celebramos o 25º aniversário de presença no Peru e estamos orgulhosos da nossa participação no processo de digitalização, inclusão e desenvolvimento do país.

Há 15 anos, quando me juntei à equipe da Cisco neste país éramos cerca de 20 pessoas em todo o escritório, hoje somos mais de 60 colaboradores incluindo um viveiro de talentos de novas gerações através do programa Early in Career, do qual o Peru é líder na América Latina. Este programa e a nossa política de diversidade nos garantem uma fonte de inovação permanente.

A nossa equipe é a prioridade. Todos os dias promovemos uma cultura de empoderamento, que motive cada pessoa a dar o melhor de si e que, por sua vez, receba as melhores condições de trabalho do mercado. Esta dinâmica de troca nos permitiu ser reconhecidos como a melhor empresa para trabalhar no Peru (#1 Great Place to Work na categoria de 50 a 250 empregados).

Durante estes 25 anos construímos pontes tecnológicas que permitem que mais peruanos estejam conectados. Junto com nossos parceiros, temos implementado e acelerado a transformação digital em setores tão diversos como o financeiro, a mineração, o varejo ou os serviços governamentais. Uma grande porcentagem das transações digitais que ocorrem em nosso país (por exemplo, consultas bancárias, visitas a redes sociais ou interações digitais com algum organismo do estado) ocorre em ambientes seguros sobre plataformas de redes da Cisco.

Estamos também empenhados no desenvolvimento do país. Geramos empregos de forma direta e indireta através de nossa rede de parceiros de negócios e formamos milhares de peruanos em competências técnicas que lhe permitam o acesso a novas e melhores oportunidades. Recentemente, alcançamos um milhão de estudantes peruanos treinados!!! Isto por meio do nosso programa de responsabilidade social Cisco NetAcad (Cisco Networking Academy) em um esforço conjunto entre o estado e o setor privado.

Como líder da organização no Peru, estou convencido de que estamos no caminho certo para construir um futuro melhor, mais justo e inclusivo para todos ■

Convido-os a conhecer mais da nossa história através do nosso site [Cisco.com](https://www.cisco.com)

# 25 años Cisco Perú



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



