Ano 1. Número 4.

Bridge

cisco SECURE

Cibersegurança

Costa Rica
De olho na cibersegurança

Especial
Líderes em cibersegurança

Conheça **Laércio Albuquerque**
VP Cisco América Latina

Conteúdo audiovisual

cisco The bridge to possible

CISCO Partner

OCP TECH

OCP.TECH

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

T +1.305.537.0800
F +1.305.537.0704

info@ocp.tech

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

T +507.387.7300

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

T +886.953.656.967

Editorial

Imagem: Adrien Tutin, Unsplash.

A vida é feita de movimentos e mudanças. O contrário seria atravessarmos ano a ano sem alteração, insistindo em sustentar o estático e evitando o risco do imprevisível. Estamos imersos em processos que nos despertam, nos agitam e nos transformam. O ambiente muda, nós mudamos e vice-versa. Há mudanças que acontecem lentamente, outras mais drásticas, que exigem toda a nossa atenção e criatividade. Há fatos imperceptíveis e ondulantes ou enérgicos e pulsantes. Estamos em mudança, por isso é tão importante acompanhar todos os fatos com uma liderança sólida e confiável, seja ela própria e interna ou de outra pessoa.

Definimos líder como a pessoa responsável por descobrir o potencial de outras, identificar novos processos e contribuir para a sua concretização. Quem ousa agir em direção a um objetivo e constroi uma cultura de bravura onde "armaduras não são necessárias nem recompensadas". Quem acompanha a evolução dos processos e contribui positivamente. Quem insiste em apoiar sua crença. Quem aceita o fracasso, se acontecer, e o supera com energia, capitalizando sobre ele.

Nesta edição da Bridge damos lugar de destaque à liderança, porque reconhecemos quem tem força para mobilizar e produzir o bem que se busca. Toda a edição é composta por mulheres e homens que formam equipes e realizam processos. Que unem fragilidade e força emocional e operacional para alcançar um objetivo claro e bem definido. Ao seu estilo, cada um orienta, acompanha, é um farol ou suporte do todo em direção à meta.

Convido você à aventura de conhecê-los, testemunhar suas experiências e receber seus ensinamentos. Boa Viagem.

Karina Basanta

Staff

Produção Integral
Basanta Contenidos

Diretor Editorial
Karina Basanta

Diretor de Arte
Nicolás Cuadros

Coordenadoras
Marta Pizzini
Marta Assandri

Produção audiovisual
Salpufilms

Locução
Loli Fahey

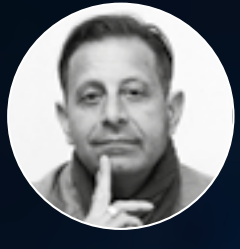
Colabore nesta edição
Silvia Montenegro
Jorge Prinzo
Claudia Menkarsky
Freddy Macho
Soledad Clar

Fotografía e ilustración
Basanta Contenidos
Freepik
Pixabay
Unsplash

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

Foto de Capa
Zdenek Machacek, Unsplash

Diretor Editorial
Karina Basanta



Diretor de Arte
Nicolás Cuadros

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

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

Ilustración: Daniel Roberts, Pixabay.

Cisco Latinoamérica

Cyber Security Director,
Americas Service Providers
and Latin America at Cisco
Ghassan Dreibi

Líderes Regionais de Cibersegurança

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

Obrigado
Adriano Gaudencio
Leticia Gammill
Jackeline Carvalho
María José Jiménez Domínguez
Nelson Brito
Militza González

Editor Geral
Juan Marino

Marketing

Taiane Belotti
Gerente de Marketing, Segurança Latam
Jimena Reyna Briseño
Gerente de Marketing de Conteúdos, Segurança, Latam

Bridge Nº 4

Sumário

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*

O novo

A Drixit Technologies revoluciona a indústria digitalizando e automatizando processos industriais, graças ao EPP digital, uma solução IoT (internet das coisas) que combina hardware e software, mitiga e previne acidentes e consegue aumentar a eficiência operacional.

O EPP digital, que integra o Drixit Tag e no Drixit Platform, vem com múltiplas funcionalidades personalizável de acordo com as necessidades.

Para a segurança do equipamento, o Drixit Tag é equipado com um botão anti-pânico, que fornece assistência na hora e no local certos. Além disso, ele detecta e notifica riscos imediatos, quedas e golpes pesados, graças à localização em tempo real dentro e fora de casa.

Através da plataforma Drixit você pode criar zonas com controle de acesso automático, proteger o equipamento de ambientes perigosos. Além disso, possui mapas de informações históricas para saber o que aconteceu e por quê, melhorando a segurança e o gerenciamento dos equipamentos. Por fim, a plataforma mantém os dados e análises da operação em um só lugar, integrado com todas as plataformas existentes, alarmes e sensores, a fim de tomar melhores decisões e conduzir a operação

Conteúdo audiovisual

Cisco

a melhor empresa para trabalhar no México

•Pelo quarto ano consecutivo recebe esta distinção; ser certificado pelo Great Place to Work é extremamente importante para saber a opinião direta dos colaboradores.

Cisco obteve o primeiro lugar na lista das Melhores Empresas para Trabalhar pelo Great Place to Work (GPTW) entre as organizações com 500 a 5 mil funcionários. Por 12 anos, a Cisco recebeu esta certificação.

O Great Place to Work Institute é uma organização internacional que avalia e certifica ambientes de trabalho por meio da análise de dados obtidos em pesquisas respondidas diretamente pelos funcionários das organizações participantes.

As áreas consideradas pelo Great Place to Work Institute para a certificação são: credibilidade, respeito, justiça, orgulho e camaradagem. Além disso, o Instituto analisa políticas, práticas e processos para cada uma das empresas participantes.

Para os membros da Cisco México, orgulho e camaradagem se destacam como os elementos mais importantes que existem em suas equipes de trabalho.

Na opinião de Isidro Quintana, CEO da Cisco México, cada pessoa que compõe a empresa é de extrema importância, porque são eles que constituem a Cisco: "Mantemos uma cultura consciente, na qual nos preocupamos profundamente em oferecer uma experiência positiva para todos. Um trabalho colaborativo e diversificado permite gerar novas ideias e explorar novas possibilidades para aproveitar o poder da transformação digital e inspirar a inovação". Ele acrescentou que ser reconhecido pelo quarto ano consecutivo como o primeiro lugar pelo GPTW "nos compromete ainda mais a continuar melhorando nosso ambiente de trabalho e, acima de tudo, ter membros orgulhosos de pertencer à Cisco e com forte compromisso em retribuir ao meio ambiente que operamos"

é nomeada a "Melhor Empresa de Segurança" pelo SC Awards 2021

Recentemente, a SC Media elegeu a Cisco como a "Melhor Empresa de Segurança" no SC Awards 2021. "Este prêmio representa anos de inovação e compromisso com a segurança cibernética, bem como a busca constante para tornar a segurança menos complexa, mais ágil e capaz de se defender contra as ameaças de hoje e de amanhã ", diz Ghassan Dreibi, diretor de vendas de segurança cibernética para a América Latina e o Caribe da Cisco. Como a maior empresa de cibersegurança corporativa do mundo, a Cisco lidera as soluções que estão impulsionando a indústria de SASE, XDR e Zero Trust.

A plataforma de segurança integrada Cisco SecureX, reúne uma ampla variedade de ferramentas, proporcionando simplicidade, visibilidade e eficiência para toda a infraestrutura de segurança de uma organização. Além disso, o Cisco Talos, por meio do Centro de Inteligência de Ameaças de classe mundial, oferece suporte à operação de seus clientes, mantendo-os atualizados sobre o cenário da segurança cibernética.

Além do reconhecimento de "Melhor Empresa de Segurança", a Cisco também ganhou o prêmio SC Media de "Melhor Solução de Segurança Baseada em Nuvem para Pequenas e Médias Empresas (PMEs), o Cisco Umbrella e foi nomeada" Melhor Solução de Controle de Acesso (NAC) com o produto Cisco Identity Services Engine (ISE)

Princípios orientadores para a segurança cibernética do cidadão

Em 15 de junho de 2021, foram lançados os Princípios Orientadores para a Cibersegurança Cidadã, documento gerado pelo Laboratório de Segurança Cibernética dos Poderes Legislativos da Organização dos Estados Americanos (OEA).

A iniciativa é resultado de um esforço cocriativo entre legisladores, assessores parlamentares, especialistas do setor privado nas áreas de cibersegurança e transformação digital, bem como acadêmicos e líderes da sociedade civil, que sob a coordenação do Laboratório de Cibersegurança para o Poder Legislativo, identificaram 10 diretrizes básicas para que cada Estado promova a formulação de políticas públicas, legislações, marcos regulatórios e normativos que ofereçam melhor proteção aos cidadãos em sua interação com as atuais infraestruturas tecnológicas, como internet, redes sociais e de informação e sistemas e / ou plataformas de comunicação

Os 10 Princípios Orientadores da Cibersegurança Cidadã são:

1. Salvaguardar e proteger os direitos e liberdades individuais.
2. Preservar a soberania na democracia digital.
3. Consagrar a liberdade de expressão e privacidade por padrão no ciberespaço.
4. Promover uma cultura de segurança cibernética.
5. Construir um ambiente cibernético seguro.
6. Garantir a privacidade dos dados.
7. Estabelecer responsabilidade compartilhada.
8. Fortalecer o desenvolvimento de competências e habilidades.
9. Incorporar a educação para a vida no ciberespaço.
10. Envolver os cidadãos no processo de criação de marcos regulatórios que promovam a inovação e a transformação digital.

Conteúdo Audiovisual

Cibersegurança que melhora a experiência do usuário

Resguardamos a identidade digital dos seus clientes para que seu negócio cresça.

- Prevenção de fraude
- Proteção de Identidade
- Biometria
- Gestão de risco

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

Entrevista

Laércio Albuquerque
VP da Cisco América Latina

Lidera a estratégia da empresa para fomentar a inovação e a digitalização em toda a América Latina. Apoiado pela equipe local e por todo o ecossistema de parceiros da Cisco, ele se concentra em oferecer resultados positivos aos clientes, ao governo e à sociedade, ajudando a resolver problemas, melhorando a sua produtividade e negócios, e criando um mundo mais inclusivo mediante o uso da tecnologia.

O que significa para você liderar a América Latina a partir de uma corporação global como a Cisco?

Para mim, liderar a Cisco Latam é uma honra e um desafio maravilhoso. Estamos em um momento regional muito interessante, atendendo a todos os nossos clientes hoje mais do que nunca em seus processos de transformação digital. A pandemia demonstrou que a tecnologia desempenha um papel crucial nos negócios e que é necessário manter com sucesso as operações na economia digital.

A Cisco tem um forte compromisso de longo prazo com nossa região por meio de investimentos e alianças estratégicas em todos os países. Estamos agora em uma posição única para impactar positivamente empresas e organizações de qualquer tamanho, pequeno ou grande, bem como a vida de milhões de pessoas, aproveitando ao máximo nossos programas e soluções de tecnologia de classe mundial de classe mundial, como o Cisco Networking Academy, que forneceu habilidades digitais a quase 3 milhões de pessoas na América Latina desde seu início; nossas poderosas iniciativas de diversidade e inclusão; e nossos programas de aceleração digital em vários países, apenas para citar algumas das grandes coisas que nos diferenciam como líderes do setor.

Quais são os próximos passos na sua gestão?

Manter um contato ativo com nossos clientes para apoiá-los e auxiliá-los em seus desafios de negócios, que vão desde o trabalho híbrido até os desafios no gerenciamento de dados e aplicativos de forma segura. Ao mesmo tempo, trabalhamos lado a lado com as comunidades e países onde operamos, liderando programas de educação em TI e outras iniciativas de responsabilidade social que gerem um impacto positivo às pessoas.

Internamente, continuar a construir e liderar uma equipe de classe mundial como a que temos na Cisco América Latina, dando-lhes a visão e o suporte para serem os melhores assessores estratégicos de seus clientes, e para que continuem a se orgulhar de fazerem parte de uma grande equipe humana e das nossas conquistas.

por **Karina Basanta**

Qual é o principal desafio?

Nosso principal desafio como empresa líder na região é nos mantermos relevantes no setor. À frente dos mercados em cada um dos países, entendendo suas transições e capturando todas as oportunidades, como:

• Segurança na nuvem para oferecer acesso a dados, processos e aplicativos;

• Soluções tecnológicas que apoiem a produção de bens e a prestação de serviços;

• Uma rede robusta e segura que permite a conexão rápida e eficiente de pessoas e dispositivos, e que ajude a resolver, com sucesso, desafios de negócios, como educação e trabalho híbridos.

Se soubermos antecipar o que está por vir e agirmos nesse sentido, será mais fácil nos mantermos no caminho do sucesso, sempre focando no que nossos clientes precisam e na experiência que eles têm ao trabalhar conosco.

Se eu disser a palavra cibersegurança. O que lhe vem à mente?

A cibersegurança é a base de tudo o que acontece na economia digital. Devemos nos perguntar por que a segurança cibernética? Para mim, a resposta é: porque devemos colocar todos os nossos esforços para enfrentar o terrorismo cibernético, que se tornou um negócio multibilionário, colocando países, serviços públicos, indústrias, dados e pessoas em risco e afetando gravemente os países.

Sem um contexto de segurança cibernética, os processos de transformação digital pelos quais muitos setores estão passando, especialmente como resultado da pandemia, podem ser afetados. Estamos caminhando em direção a um mercado global de 50 bilhões de dispositivos conectados, portanto, pode haver 50 bilhões de falhas de segurança que devemos fechar. Devemos compreender a relevância desta situação e o papel que as regulamentações globais, regionais e locais desempenham na prevenção e no combate à situação.

Para a Cisco, a segurança cibernética é uma questão que abordamos de forma abrangente em várias dimensões: trabalhamos com governos e autoridades para fornecer conhecimento, experiência e educação em segurança cibernética; oferecemos aos clientes de todos os setores e portes soluções e tecnologias de ponta para a segurança de seus processos de negócios; e estamos constantemente inovando nosso portfólio, projetando e construindo com base em uma tecnologia segura de ponta a ponta.

Quais são as novas abordagens que a Cisco traz para a América Latina em termos de cibersegurança.

É essencial para nós estarmos na vanguarda dessas questões de segurança cibernética. Estamos potencializando o SASE (Secure Access Service Edge), que combina recursos de segurança de rede e nu-

vem para fornecer acesso contínuo e seguro aos aplicativos, onde quer que os usuários trabalhem. O modelo SASE visa consolidar estas funções em um único serviço integrado à nuvem. A Cisco fornece todos os blocos de construção de uma arquitetura SASE, reunidos em uma única oferta.

Por outro lado, continuamos focados no Zero Trust, um modelo de segurança completo que permite mitigar, detectar e responder aos riscos nas organizações, de forma a evitar incidentes de falsificação de credenciais, por exemplo, num modelo de trabalho híbrido.

Todos estes programas e soluções de segurança são apoiados por inteligência de ameaças de classe mundial da Cisco Talos, o maior centro privado de inteligência de ameaças global, mantendo clientes e participantes da indústria atualizados com o cenário de negócios.

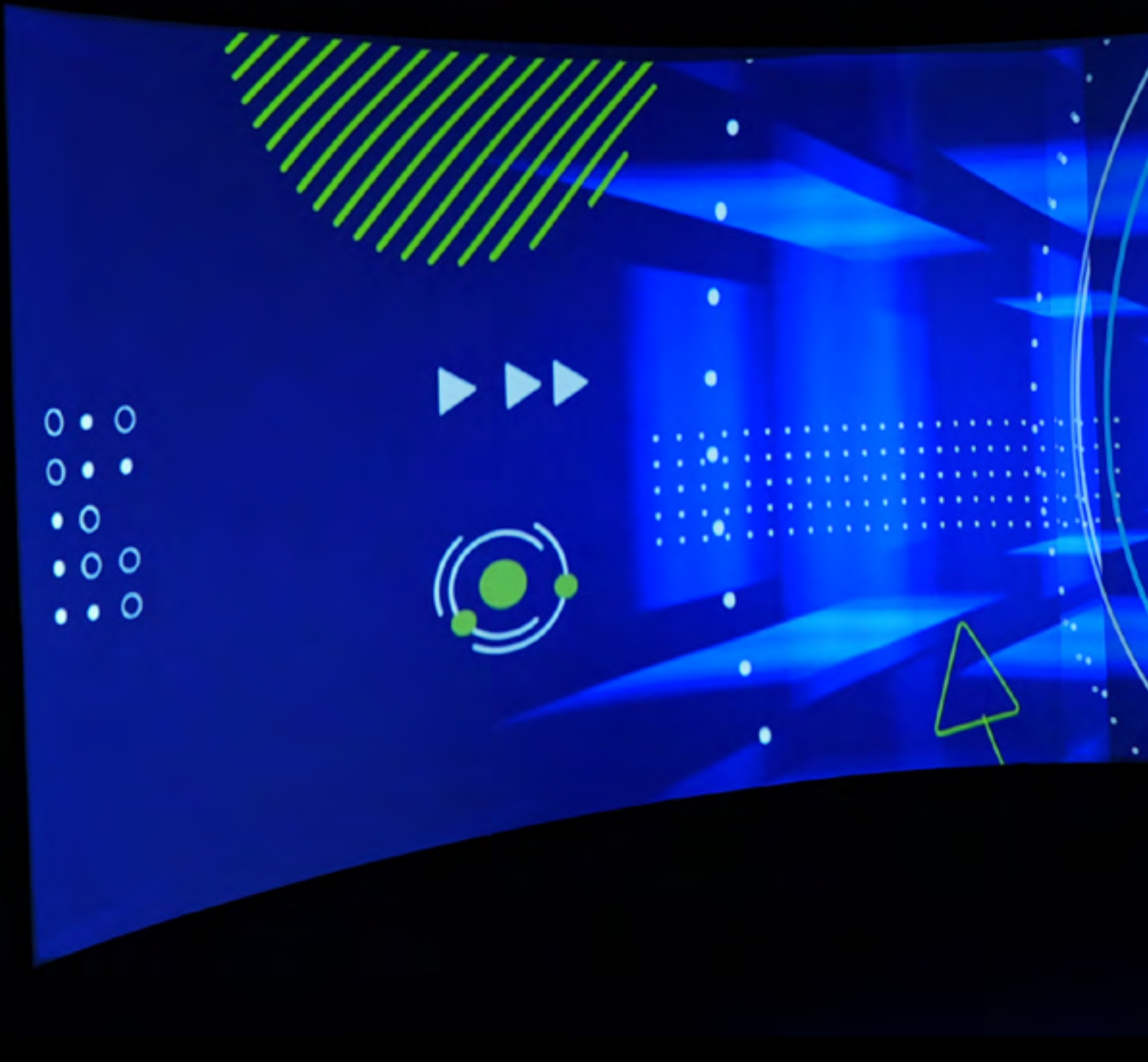
Em quais novas alianças a Cisco está trabalhando para expandir a conscientização sobre a segurança cibernética?

Continuaremos apoiando a aliança regional com a Organização dos Estados Americanos (OEA) por meio dos Conselhos de Inovação Cibersecurty, criados em 2019. Esta iniciativa é um espaço onde líderes e especialistas do setor privado, público, acadêmico, ONGs e fornecedores de tecnologia de cibersegurança vão colaborar para impulsionar a inovação, sensibilizar e expandir as melhores práticas, com o objetivo de ajudar a resolver os riscos e desafios digitais que afetam a sociedade digital.
Além disso, trabalhamos com ONGs, câmaras de comércio, sindicatos, instituições de ensino de todos os níveis, ministérios e agências governamentais, a fim de colaborar na conscientização sobre a relevância da educação em cibersegurança, por meio de nosso programa Cisco Networking Academy, que já forneceu habilidades digitais para quase 3 milhões de pessoas na América Latina desde o seu início

Mini Bio

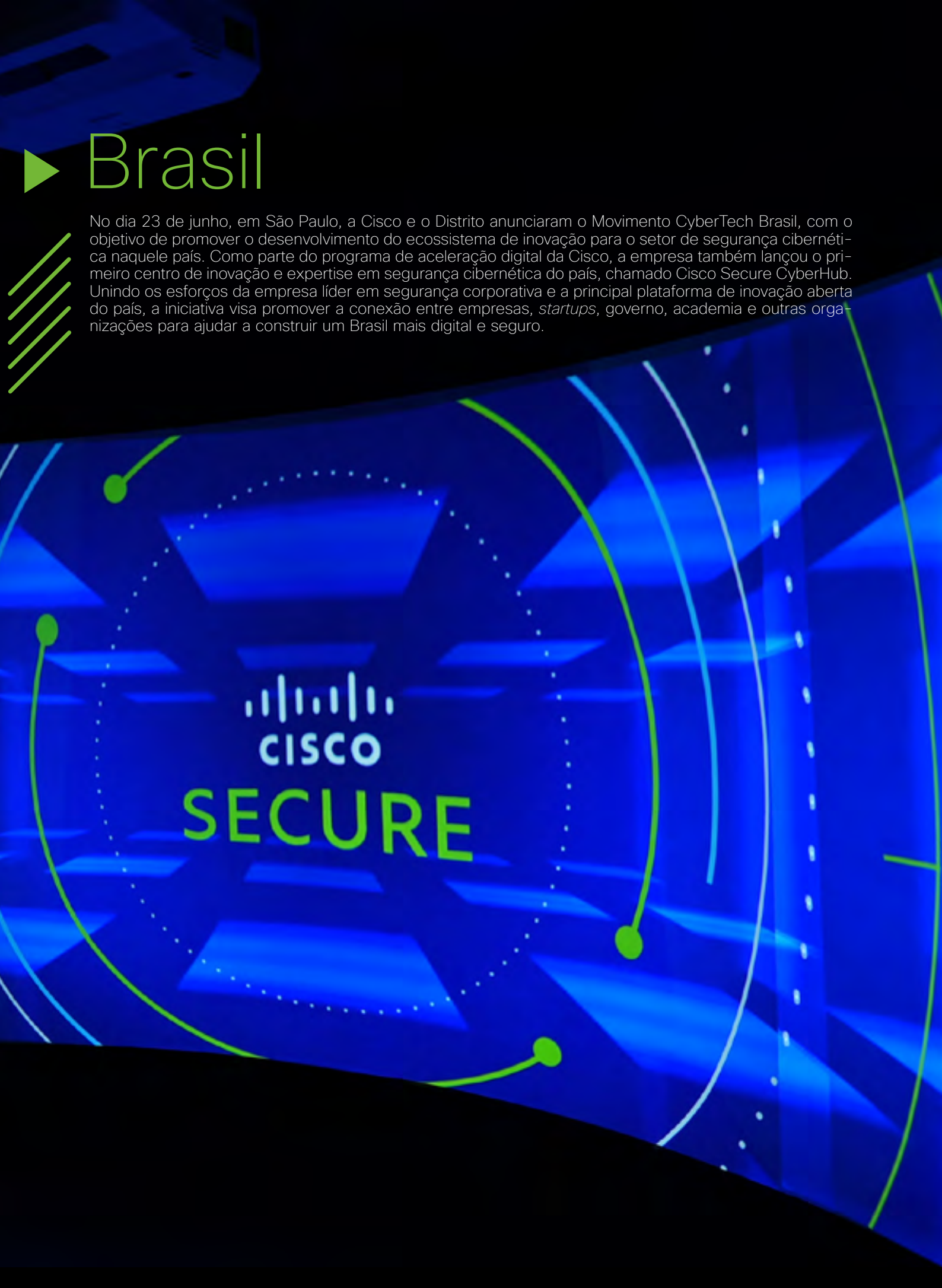
Laércio atua no setor de tecnologia há cerca de 35 anos. Antes da Cisco, ele ocupou importantes posições de liderança no Brasil e na América Latina. Trabalhou na CA Technologies por 20 anos, onde ocupou vários cargos de liderança, incluindo country manager para o Brasil, presidência e gerencia geral para a América Latina. O executivo é graduado em Análise de Sistemas e Administração de Empresas pelas Faculdades Associadas de São Paulo (FASP) e possui MBA Executivo pelo Insper.

Movimento CyberTech



Brasil

No dia 23 de junho, em São Paulo, a Cisco e o Distrito anunciaram o Movimento CyberTech Brasil, com o objetivo de promover o desenvolvimento do ecossistema de inovação para o setor de segurança cibernética naquele país. Como parte do programa de aceleração digital da Cisco, a empresa também lançou o primeiro centro de inovação e expertise em segurança cibernética do país, chamado Cisco Secure CyberHub. Unindo os esforços da empresa líder em segurança corporativa e a principal plataforma de inovação aberta do país, a iniciativa visa promover a conexão entre empresas, *startups*, governo, academia e outras organizações para ajudar a construir um Brasil mais digital e seguro.



Com o mundo cada vez mais hiperconectado e a digitalização de negócios e serviços acelerada nos últimos anos, o volume e a complexidade das ameaças cibernéticas também avançaram rapidamente. Uma pesquisa recente da Cisco descobriu que 40% das empresas em todo o mundo relataram um incidente de segurança significativo nos últimos dois anos. Entendendo a relevância e a necessidade da cibersegurança para que empresas e governo possam continuar sua trajetória de transformação digital, o Movimento CyberTech Brasil visa contar com a participação e colaboração das principais organizações envolvidas com o tema cibernética, promovendo ações de disseminação de conhecimento, capacitação de profissionais e inovação no setor no país.

Como parte da iniciativa, a Cisco e o Distrito planejam promover uma série de eventos, reuniões, hackathons e programas de aceleração de *startups* com foco na segurança cibernética. As empresas também pretendem colaborar na construção da primeira base de dados de *startups* de cibersegurança do país, o CyberTech Digital Hub, além do monitoramento contínuo e produção de conteúdo e relatórios sobre o setor no Brasil.

A iniciativa faz parte do programa de aceleração digital da Cisco, Digital and Inclusive Brazil, tendo o Cisco Secure CyberHub como principal espaço de inovação, experiência e debate em segurança cibernética.

Cisco Secure CyberHub

Localizado dentro das instalações do Distrito Fintech, em São Paulo, o novo centro permitirá a experimentação de complexos cenários de ataque e defesa, trazendo conceitos e tecnologias de segurança cibernética. O espaço reunirá informações em tempo real sobre ataques, resposta a incidentes e soluções tecnológicas para empresas, *startups* e governo.

CyberHub reúne três ambientes com recursos audiovisuais para experimentar a segurança digital:

Sala Vermelha

dedicada a demonstrar a anatomia de um ataque, explorando suas etapas e os impactos do roubo de dados em *ransomware* com seu consequente risco de vida.

Sala Azul

ambiente que simula o funcionamento das defesas, onde se destaca a importância da inteligência, como o trabalho do grupo de pesquisa de cibersegurança Cisco Talos e uma arquitetura integrada que identifica e responde a ataques no menor tempo possível.

Sala de operações de segurança

ambiente para demonstração de soluções, análise de *malware* e simulações de sala de crise com orquestração de investigações de ameaças e automação de respostas.

O Cisco Secure CyberHub também inclui um espaço para *startups* residentes interessadas em desenvolver soluções baseadas em tecnologia de segurança e API, Cisco SecureX / DevNet, que permite integração e cooperação entre as soluções Cisco e de seus parceiros. O novo espaço também ajudará a promover a formação de profissionais de segurança cibernética, complementando os treinamentos já oferecidos pela Cisco Networking Academy.

Além disso, o Cisco Secure CyberHub tem como objetivo ser um espaço de discussão e desenvolvimento de projetos para melhorar a infraestrutura de segurança cibernética de empresas, governo e infraestruturas críticas no Brasil.

O que vem

Em breve, o Distrito lançará o Inside Cybertech Report, um estudo com dados de investimentos de startups neste segmento; Cybertech Digital Hub, plataforma de dados e conexão de empresas com startups; e Cybertech Summit, um evento do setor a ser realizado em outubro em associação com a Cisco.

Dixit

"Esta é uma etapa muito importante para o programa Cisco Brasil Digital e Inclusivo. Por meio da CyberTech Brasil e do espaço Secure CyberHub, a Cisco avança em seu objetivo de criar um ecossistema digital mais conectado, inovador, inclusivo e, acima de tudo, seguro. Estamos muito confiantes na importância e na qualidade das inovações geradas a partir desse Movimento ", Ricardo Mucci, country manager da Cisco do Brasil.

"À medida que fazemos a transição para uma sociedade ultraconectada, os desafios da segurança cibernética se tornam maiores e mais complexos. O movimento CyberTech Brasil e, em particular, Cisco Secure CyberHub, colaboram para disseminar a cultura de segurança cibernética preventiva e responsiva, destacando as boas práticas e ferramentas necessárias para proteger empresas, dados e pessoas em um ambiente no qual todos estamos sujeitos à ação por criminosos ", Fernando Zamai, Líder de Segurança Cibernética da Cisco do Brasil.

"Com uma economia cada vez mais baseada em tecnologia, a questão da segurança cibernética se tornou ainda mais urgente. Como um dos principais players do ecossistema de inovação brasileiro, o Distrito se sente obrigado a participar desse movimento ", Gustavo Araujo, presidente e fundador do Distrito

Mais sobre Cisco Secure CyberHub y Mais sobre Brasil Digital e Inclusivo

Hackeando previsões

Conteúdo Audiovisual

Passado, passado. Futuro, *hackeado*? Quando as previsões não são boas, podemos agir para impedir que se concretizem. Como podemos colaborar, unindo forças entre os setores público e privado, provedores de tecnologias e serviços de segurança cibernética? Que contribuições empresas como a Cisco estão dando ao mundo para permitir vida e economia digital resilientes?

Costuma-se dizer "o que passou, passou". Acho que olhando para 2020, cada um fez o melhor que pôde e, embora tenha havido tropeços e algumas quedas, em geral todos continuamos caminhando. A pressa e a continuidade operacional foram alinhadas com a segurança. Mas, se continuarmos a caminhar assim, sem uma gestão eficaz do risco cibernético, vamos confirmar as previsões mais temíveis, como as que afirmam que a curto prazo 2 em cada 3 PMEs que sofrem uma violação serão arruinadas em questão de meses; que o custo do cibercrime crescerá acima de 1,5% do PIB global e que pode subir até 6% se infraestruturas críticas forem atacadas; ou que, em breve, atingiremos 4 milhões de vagas abertas por falta de talento em segurança cibernética, dos quais mais de 600.000 estão na América Latina.

Se olharmos a longo prazo, basta ouvir as previsões do pensador Yuval Harari, que no Fórum Econômico Mundial recentemente se referiu à ruptura tecnológica como um dos três inimigos globais, percebendo que quem controla os dados vai controlar o mundo. Em sua visão, somos animais hackable nestes tempos, nossos desejos, nossas posições e, portanto, nossas decisões podem ser manipuladas. Nesta perspectiva, a segurança cibernética ocupa um lugar central para proteger não apenas os dados, que "voluntariamente" entregamos ao sistema, mas o que poderíamos chamar de privacidade e liberdade cognitiva.

Claro, há também as previsões positivas: graças à democratização do acesso à internet, há crianças em todos os cantos do país e do mundo, possivelmente desenvolvendo novos conhecimentos e resolvendo problemas globais. É melhor que essas previsões continuem e se tornem realidade.

Situação atual

Se há algo em que vejo um consenso total, é que temos que fazer um esforço conjunto entre os setores público e privado e os fabricantes de tecnologia para cruzar as fronteiras, porque é claro que as organizações cibercriminosas sabem colaborar muito bem e, portanto, ganham uma vantagem ofensiva. Por isto, é melhor pensar no passado antes de pisoteá-lo e deixá-lo no esquecimento.

por **Juan Marino**

Imagem: kues, Freepik

Juan Marino na pré-sessão.

No relatório Defesa contra ameaças críticas: um rodeio de 12 meses, 2021, fechamos a cortina e revelamos as principais observações feitas por pesquisadores do Talos, o centro de inteligência de ameaças da Cisco, a maior organização não governamental global que bloqueia 20 milhões de ameaças por dia. No entanto, o bloqueio automático não é mais um problema. O problema é o desconhecimento. Algo que inexiste para Matt Olney, líder do Talos, e sua equipe ocupados. O estudo dá conta da sofisticação que o ransomware atingiu. Não apenas em relação a uma pessoa inocente que, infectada com malware, é extorquida a pagar para recuperar o acesso aos seus dados, agora criptografados e inacessíveis. Agora, um "Grande Jogo" está acontecendo: os ataques são direcionados e usam ferramentas multifuncionais. Por exemplo, vemos o fenômeno da "dupla extorsão", onde o pagamento não é apenas exigido para recuperar a informação, mas também para evitar sua divulgação, o que teria um segundo impacto na reputação da organização ou da pessoa. Além disto, sabemos que os criminosos por trás disso são bem-organizados: existem corretores de acesso inicial que vendem portas abertas para organizações que outros criminosos compram para capitalizar em ataques de extorsão e roubo de dados. Na verdade, é possível que neste exato momento uma dessas corretoras esteja vendendo acesso à sua organização.

Três previsões que poderíamos hackear

1 Em algum momento você ou sua organização serão hackeados.

Para reverter essa previsão, a resposta não é exclusivamente tecnológica. Vamos ver.

O Security Outcomes Study, 2021, encomendado pela Cisco, analisou a relação entre as práticas de segurança e seus resultados positivos em 4.800 organizações ao redor do mundo em 25 países, com boa representação de nossa região. A partir daí, constatou-se que 45% das práticas de cibersegurança apresentam algum grau de probabilidade de impacto positivo no cumprimento dos objetivos. Em contraste, os outros 55% das práticas parecem não ter sucesso. Indicou ainda que das 5 funções do NIST (Instituto Nacional de Normas e Tecnologia – Identificar, Proteger, Detectar, Responder, Recuperar), IDENTIFICAR é a que apresenta maior relação com o sucesso em segurança, enquanto PROTECT ocupa o 4º lugar. Isso significa que, embora as capacidades de proteção sejam muito importantes, elas são superestimadas em detrimento das funções IDENTIFICAR, DETECTAR e RESPONDER, que quando bem gerenciadas apresentam maior probabilidade de sucesso na gestão integral da segurança cibernética.

O estudo também revela que as duas práticas com impacto mais direto no sucesso da segurança são:

- Atualizar tecnologias de forma proativa.
- Atingir uma boa integração tecnológica, que se traduz em menos produtos por fabricante, o que facilita a operação de segurança e tem impacto positivo na retenção de talentos.

Então, como hackear a má previsão que nos diz que seremos *hackeados*?

- Em primeiro lugar, estamos trabalhando em uma mudança de estratégia que não supervalorize a proteção.
- Em segundo lugar, revisamos o *framework* que melhor se adapta à organização, e fazemos uma avaliação de maturidade, identificando os *gaps*.
- E, por último, traçamos um plano de ação de curto, médio e longo prazo.

As tecnologias serão um componente chave, mas uma abordagem consultiva será essencial. Agora, se presumirmos que a calamidade pode acontecer a qualquer momento e não temos tempo para levar a cabo o plano, o que devemos fazer imediatamente para estarmos mais bem preparados? Temos que usar serviços de resposta a incidentes com os quais podemos aumentar os recursos da organização, trazendo os especialistas do Talos.

2 Em algum momento sua organização sofrerá um comprometimento de credencial.

No mesmo relatório Defendendo-se contra ameaças críticas: um roundup de 12 meses, também vimos como o roubo de credenciais é uma parte fundamental da cadeia de ataques.

Nesse sentido, vamos pensar que estamos facilitando bastante a vida dos adversários, contanto que continuemos a depender das senhas como único método de autenticação. Hoje isso é excesso de

Por trás das cenas.

confiança. É por isso que o paradigma da confiança zero é tão relevante, que na minha perspectiva não deve ser entendido de forma estrita, mas como um horizonte ao qual se aproxima a redução dos excessos de credibilidade ao longo do caminho.

Em um nível individual, é mais provável que o nome de usuário e a senha que você usou em um serviço online já tenham sido comprometidos e estejam circulando com uma longa lista de vítimas na *dark web*.

Então, como hackeamos essa previsão? Proponho um desafio: vamos ajudar um amigo ou membro da família a fortalecer sua segurança de duas maneiras:
- Usando um gerenciador de senhas, para que eles tenham que lembrar apenas uma senha forte e o gerenciador gere outras fortes e exclusivas para cada serviço.
- Adotando um segundo fator de autenticação para os serviços mais importantes, sempre que possível. Claro, além de ajudar um amigo, a primeira coisa é fazer você mesmo.

Também será importante levar essa prática às organizações. A adoção de uma solução sem senha ou de autenticação de múltiplos fatores (MFA) eleva a fasquia muito rapidamente e é um grande passo no caminho para a confiança zero. Ao adotá-lo, será necessário levar em consideração que esta ação de segurança impacta diretamente na experiência do usuário, por isso será importante analisar muito bem os casos de uso e considerar uma solução que, além do MFA, permita a construção de políticas de acesso onde a validação de identidade é dinâmica e contextual, minimizando o atrito que gera para o usuário.

Pronto para a ação.

Na Cisco, adotamos nossa própria solução Cisco DUO em escala global. Em poucas horas, cerca de 100 mil funcionários começaram a validar seus acessos, principalmente com a autenticação push para o smartphone como segundo fator. Isso não gerou surpresas e é uma etapa fundamental na migração que a empresa fez para os serviços em nuvem sem a necessidade de uma conexão VPN.

3 O aumento da escassez de talentos.

Vários relatórios de diferentes fontes revelam a necessidade crescente de pessoas adequadas para desempenhar diferentes funções relacionadas à segurança cibernética.
Nesse sentido, e para atender à demanda, recomendo atuar sobre a grande oferta de programas de educação e promovê-los para acelerar a formação dos profissionais de que necessitamos. Nesse sentido, estou satisfeito que a Cisco, em conjunto com a OEA, esteja promovendo nossos programas de educação em segurança cibernética, embora acredite que ainda podemos nos articular mais com as universidades e disponibilizar o que temos a oferecer. Através da Networking Academy, os profissionais 12M foram treinados desde 1997 e esta é uma parte fundamental do programa de responsabilidade social corporativa.

Democratize a segurança cibernética

O presente e o futuro da vida digital são sustentados pela inovação de grandes empresas de tecnologia. Portanto, quase 40 anos após a criação do roteador, hoje faz sentido que a Cisco tenha um propósito ambicioso de permitir um futuro inclusivo para todos, com a missão de inspirar novas possibilidades ao reimaginar aplicativos, proteger dados, transformar a infraestrutura e capacitar os usuários e equipes.
Vemos progresso e estamos envolvidos em vários projetos. No entanto, este é um assunto em que não podemos relaxar, e para cortar as previsões ruins, devemos continuar a promover rapidamente tecnologias de implantação imediata e em grande escala, como segurança DNS ou Cisco Umbrella, é, talvez, uma das soluções que permitem democratizar a segurança e proteger as crianças e também os seus pais em qualquer acesso à internet a partir de qualquer dispositivo.

Resumindo

O relatório 2020 da OEA sobre Riscos, Progresso e Caminho a Seguir na América Latina e no Caribe atualiza as informações coletadas pela primeira vez em 2016 sobre o estado de maturidade das nações da região. Lá, o progresso é visto nas cinco dimensões propostas pelo modelo; alguns países com grandes avanços, outros nem tanto.
De uma perspectiva de alto nível, a melhor maneira de hackear previsões ruins é alcançando a maior maturidade possível nos cinco espaços propostos, a saber:

1. Política e Estratégia de Segurança Cibernética.
2. Cultura e sociedade cibernética.
3. Educação, treinamento e habilidades em Cibersegurança.
4. Estruturas Legais e Regulatórias.
5. Padrões, organizações e tecnologias.

E, sobretudo, uma das chaves para avançar é construir pontes que permitam unir talento, conhecimento e experiência. No ano passado, começamos a reunir vozes de diferentes disciplinas e setores e estamos transformando isso nesta publicação periódica que criamos localmente e batizamos de Bridge. Neste ano, vamos avançar gerando espaços de relacionamento com Funcionários e CISOs, pois vemos que estas instâncias são muito necessárias.

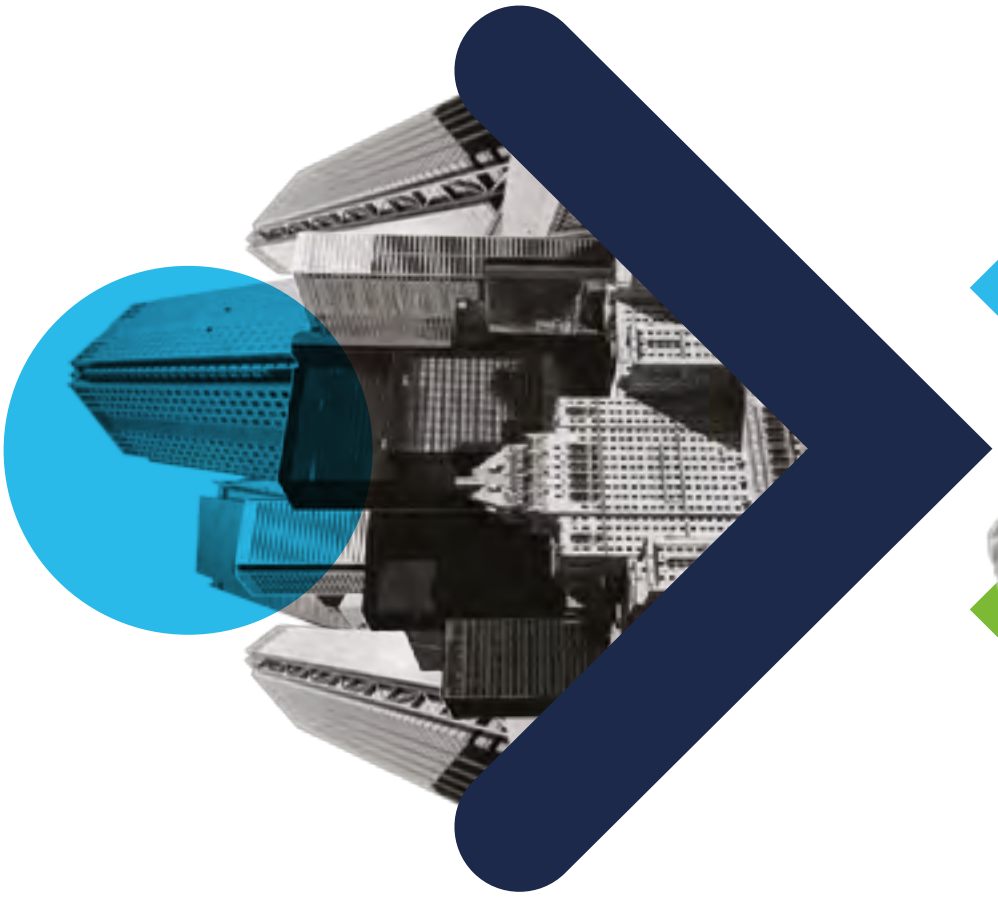
Convido você a se conectar conosco, comigo em nome da Cisco, para encontrar os espaços certos, as conversas certas e que possamos trabalhar juntos para hackear as previsões

CISCO
SECURE X

Experiência simplificada

A plataforma Cisco SecureX é uma experiência integrada de nosso portfólio de segurança que se conecta a toda a sua infraestrutura de segurança.

Explore mais:
https://www.cisco.com/c/pt_br/products/security/securex



Autenticação sem senha

Password:

sincontrase●●●●

Imagem: Jason Dent, Unsplash

Futuro sem senha: o Cisco Secure introduziu a autenticação sem senha Duo, que permite aos usuários fazer login com segurança em aplicativos em nuvem por meio de chaves de segurança ou biometria de plataforma, sem a necessidade de senhas tediosas. A autenticação Duo sem senha faz parte da plataforma Zero Trust da Cisco.

O que é autenticação sem senha?

A autenticação sem senha é um método no qual um usuário pode fazer login em um sistema de computador sem inserir (e então ter que se lembrar) uma senha ou qualquer outro segredo baseado em conhecimento.
Biometria, chaves de segurança e aplicativos móveis especializados são considerados métodos de autenticação "sem senha" ou "modernos" que fornecem acesso seguro para todos os casos de uso de negócios (aplicativos híbridos, em nuvem, locais e legados). O Duo está inovando em direção a um verdadeiro futuro sem senha que equilibra usabilidade com autenticação mais forte. Esta forma de autenticação fornece aos usuários uma experiência de login sem atrito, enquanto reduz a carga administrativa e os riscos gerais de segurança para a empresa.
"MFA sem senha" é o termo para a combinação do fluxo de autenticação sem senha que utiliza vários fatores, fornecendo o mais alto nível de segurança quando implementado corretamente.

Como funciona?

A autenticação sem senha idealmente envolve menos interação do usuário durante o processo de login do que as formas tradicionais de autenticação. Ele usa criptografia de chave pública, que autentica o usuário com um par de chaves criptográficas - uma chave privada que é secreta e uma chave pública que não é, e vem com um novo (ou relativamente novo) léxico de siglas e padrões. Como o padrão FIDO2 (FIDO significa Fast IDentity Online e FIDO2 é apenas um termo geral para a combinação de WebAuthn e Client to Authenticator Protocol (CTAP)).

Por que a tecnologia sem senha é importante?

A autenticação sem senha não é apenas uma coisa boa de se ter; pode realmente melhorar a postura de segurança de uma organização e reduzir os custos associados ao gerenciamento de senhas. As senhas criam maior atrito para os usuários, diminuem a produtividade dos negócios e são inerentemente uma forma fraca de autenticação do usuário.

Por que implementá-lo?

A autenticação sem senha fornece uma garantia única e forte de identidades de usuário para confiança. Para empresas, isto significa:

- Melhor experiência do usuário.
- Redução da frustração do usuário e aumento da produtividade.
- Redução de tempo e custos de TI.
- Reduzir a carga administrativa de tíquetes de help desk relacionados a senhas e redefinições de senha.
- Postura de segurança mais forte.
- Eliminação de ameaças e vulnerabilidades relacionadas a senhas (phishing, senhas roubadas ou fracas, reutilização de senhas, ataques de força bruta etc.).

Como implementar?

A implantação "sem senha" não é uma tarefa fácil, especialmente quando se trata de grandes populações de usuários, um número substancial de aplicativos, infraestruturas híbridas e fluxos de login complexos. Alcançar um ambiente totalmente livre de senhas é uma jornada que envolve uma abordagem em fases, conforme a tecnologia continua a evoluir e a adoção do usuário aumenta. Embora a eliminação completa de senhas ainda esteja muito longe, reduzir a dependência de senhas já é viável implementando MFA, estabelecendo confiança em dispositivos, aproveitando SSO e implementando políticas de acesso adaptáveis. Na Cisco estamos prontos para acompanhar as organizações a trilhar este caminho

Experimente a solução hoje: Cisco Secure Access by Duo,
Clique aqui

25º
Aniversário

por **Silvia Montenegro y Karina Basanta**

Costa Rica

O país da cultura do trabalho e da aprendizagem

De acordo com um relatório do Banco Mundial, a Costa Rica tem uma história de sucesso em termos de desenvolvimento, especialmente devido ao seu crescimento econômico sustentado nos últimos 25 anos. É considerado um país de renda média-alta e se destaca por sua política de abertura ao investimento estrangeiro.

É um país reconhecido por sua democracia consolidada, por sua política sempre em prol da paz e do diálogo - não tem Exército - e pelos elevados padrões internacionais no sistema público de ensino. Este último valor é complementado pela cultura do trabalho impressa no DNA da Costa Rica.

Com uma população de cerca de 5 milhões de habitantes, tem uma das taxas de pobreza mais baixas da América Latina e do Caribe, uma conquista intimamente relacionada a seus sólidos indicadores de desenvolvimento humano.

Suas conquistas ambientais, que ajudaram o país a construir sua Marca Verde, também são destacadas. Eles têm o exercício de conviver amigavel-

Imagem: visitcostarica.com

mente com a natureza e respeitar suas idiossincrasias e recursos. Eles promoveram com sucesso a transição energética, atualmente o abastecimento da Costa Rica é quase 98% renovável. Além disso, conseguiram alcançar uma diversidade significativa em sua matriz energética, o que facilita a adaptação do parque empresarial a novas fontes de energia.

Círculo virtuoso de desenvolvimento

No ano em que a Costa Rica comemora 200 anos de vida democrática, a Cisco comemora seus 25 anos de fecunda história no país, nos quais conseguiu cultivar um forte vínculo de compromisso com o desenvolvimento de sua economia e comunidade. Além de contribuir para o desenvolvimento produtivo e promover a inovação e digitalização no país, a empresa contribui para a criação e qualidade de oportunidades de emprego e gera oportunidades de formação nas áreas afins.

Luis Carlotti, Líder Nacional da América Central e Caribe da Cisco Costa Rica, acredita que o país terá um impacto importante no futuro da América Latina. Como símbolo de sua atuação, destaca-se que, recentemente, o país centro-americano aderiu formalmente à Organização para Cooperação e Desenvolvimento Econômico (OCDE), reconhecida por reunir os países mais ricos do mundo. Ele diz: "Você agora faz parte deste grupo de países privilegiados. Por isso, podemos dizer que lideramos uma pequena operação na América Latina, que está no Primeiro Mundo"

Fuente:

- https://www.bancomundial.org/es/country/costarica/overview
- https://twitter.com/OECD?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1397225089066807296%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.france24.com%2Fes%2Fprogramas%2FeconomC3ADa%2F20210526-costa-rica-ocde-cuarto-pais
- https://www.france24.com/es/programas/econom%C3%ADa/20210526-costa-rica-ocde-cuarto-pais
- https://www.oecd.org/greengrowth/costa%20rica.pdf

Imagem: Teatro Nacional, San José, Costa Rica


TEATRO NACIONAL

25º Aniversário da Cisco na Costa Rica

O 25º aniversário da Cisco na Costa Rica é um evento marcante na história da empresa líder em tecnologia internacional. Fundada em 1984, a Cisco nasceu com a visão de inspirar novas possibilidades, fornecer soluções e ferramentas inovadoras, ajudar a transformar comunidades e seus funcionários, em direção a um futuro global e inclusivo. Este eixo estratégico corporativo está amplamente presente na sede da Costa Rica, que abriu operações em 1996 e atualmente é liderada por Luis Carlotti, gerente geral da Cisco para os mercados da América Central e Caribe. Deixando sua marca por meio da tecnologia e da formação profissional, com uma postura ética e transparente, a empresa contribui a cada dia para o desenvolvimento do belo país centro-americano, proporcionando competitividade e valor agregado.

Luis Carlotti

Líder Nacional da Cisco Costa Rica e Gerente Geral da América Central e Caribe.

O que significa liderar uma empresa da magnitude da Cisco em um momento da história como o atual, marcado pela grande aceleração da transformação digital, em função do contexto impactado pela pandemia?

É um momento difícil para o mundo e temos uma grande responsabilidade. A Cisco é uma máquina incrível de inovação em todas as áreas e para mim é um privilégio poder ajudar, do meu lugar, não só a corporação, mas a grande equipe que nos acompanha. Com suas qualidades humanas, ética e comprometimento, a equipe da Cisco trabalha muito para que tudo corra bem. Só o escritório da Costa Rica tem mais de 200 funcionários e, por meio de nossos parceiros de negócios, agregamos um pouco mais de 1.000 pessoas trabalhando como um único ecossistema. A partir daqui, muitos serviços são prestados à América e ao mundo. Temos colaboradores em Trinidad, Porto Rico, República Dominicana, Guatemala, Panamá ... Eles estão longe, mas estamos unidos. Nesse contexto complicado, temos que apoiar os colaboradores, conversar com todos, levantar o ânimo, entender as particularidades de cada um. Não é uma tarefa fácil, mas um grande desafio. Dia a dia vemos que avançamos. Pessoalmente, considero um desafio, o que me enche de satisfação. Estar na Cisco ajuda muito e eu recebo isso com muita humildade.

A pandemia colocou os negócios do mundo à prova. Como foi para a Cisco Costa Rica?

Por ser uma empresa focada no bem-estar das pessoas, desde o início da pandemia, as medidas corretas foram tomadas. Do ponto de vista do modelo de teletrabalho, a Cisco tem se mantido na vanguarda, pois esta dinâmica faz parte do nosso DNA. No meu caso, por exemplo, trabalho em casa há 10 anos e meu escritório fica no meu computador. É por isso que quando a pandemia nos pegou de surpresa, trabalhar na Cisco foi fácil, não houve impacto na forma como operávamos. Nosso objetivo era colocar as pessoas em primeiro lugar e ajudar a sociedade de diferentes maneiras. Colaboramos nos processos de migração para o teletrabalho, disponibilizando as nossas ferramentas de segurança e colaboração em vários setores do país.

Qual é a chave para exercer a liderança que o levou ao topo do ranking “Great Place to Work” na Costa Rica pelo terceiro ano consecutivo?

Algumas variáveis ajudam. A Cisco tem uma cultura corporativa maravilhosa e, por outro lado, a Costa Rica é um grande país, seu povo é charmoso, maduro, com muita inteligência emocional, está sempre tentando fazer as coisas bem. Meu primeiro objetivo, quando cheguei ao país há 5 anos, era incentivar a equipe a sentir orgulho não só de trabalhar na Cisco, mas na Cisco Costa Rica e ter clareza sobre o impacto de cada um na organização e no país. Me orgulha o fato de, nos últimos três anos, a Cisco Costa Rica tenha conquistado destaque pelo capital humano que possui, pela cultura que cada um consegue criar, pela qualidade de seus parceiros de negócios e pelos projetos que promovemos por meio transformação digital segura em cada um de nossos clientes.

Qual foi o impacto da empresa na comunidade da Costa Rica?

A Cisco e a Costa Rica estão vinculadas há muitos anos, de várias maneiras. A Costa Rica é um país que abraça a tecnologia e a Cisco tem investido significativamente e ajudado a gerar capital humano. Estamos presentes no crescimento da sociedade e no aparelho produtivo do país. Participamos da expansão da banda larga na Costa Rica, da interconexão de escolas, do processo de transformação digital das empresas e do setor público, tanto que toda empresa e organização têm algo da Cisco, atualmente. Somos uma referência na área de Responsabilidade Social Corporativa, no tratamento do colaborador, na transparência, na retribuição ao país não só nas mercadorias que se vendem, mas também na formação e contratação de pessoas. Por muitos anos, milhares de costarriquenhos foram treinados em redes graças ao nosso programa Cisco Networking Academy. Esse treinamento permitiu que muitos jovens obtivessem um trabalho de qualidade e se especializassem. E sentimos que, em troca, o país abraça a Cisco.

Para ver o impacto da Cisco Costa Rica, você pode acessar o Jornal completo Aquí

A Cisco Networking Academy, um programa pioneiro em educação em tecnologia, tem uma forte aceitação na Costa Rica. Como foi o processo de posicionamento?

Mais de 91 mil alunos passaram por nossas salas de aula presenciais e virtuais e, até o momento, 21 mil pessoas são alunos ativos. Com este programa, buscamos contribuir para o desenvolvimento do país, proporcionando competitividade por meio do que há de mais importante nos países: seu capital humano. A Cisco Networking Academy oferece as melhores oportunidades de emprego e crescimento

Imagem: Julie Duchesneau, Pixabay

para muitas pessoas, portanto, também oferece desenvolvimento para a Costa Rica. O trabalho conjunto realizado pelas mãos de organizações, públicas e privadas, tem permitido que a tecnologia chegue a todos os cantos do país. Só na Costa Rica, temos uma rede de 152 parceiros educacionais, ou seja, 152 instituições ministram os cursos da academia. Com isso, continuamos promovendo nossa missão de promover o desenvolvimento da força de trabalho nas áreas que promovem a digitalização do país.

Atualmente, há um déficit em termos de pessoas treinadas em segurança cibernética, por exemplo, apesar da demanda do mercado. Você acha que a experiência da Cisco Networking Academy pode ser extrapolada para outros países da América Latina? Como você pode incentivar o uso destas ferramentas, que também são gratuitas?

A Costa Rica é um exemplo a seguir em termos de modelo de exportação de serviços por meio de seu povo. O modelo certamente poderia ser replicado por outros países, porque é uma boa ideia investir em programas que promovam os jovens a aprender as habilidades do futuro, como a segurança cibernética. Um país se torna competitivo à medida em que sua população cresce e se torna competitiva, e a Costa Rica o busca com muito foco, porque sabe que existe um grande gap que também gera oportunidade para seu povo. Nesse sentido, há consciência de que um país pode ter excelentes ruas, segurança, boa conexão de banda larga, mas é importante que as pessoas sejam qualificadas, que estejam preparadas para o que as empresas demandam. É assim que a Costa Rica abre suas oportunidades, oferecendo bons serviços às empresas que investem, e disponibilizando pessoal altamente capacitado para contratação.

Qual é o seu objetivo nesta fase da carreira?

O grande desafio da Cisco na Costa Rica é acompanhar o ritmo dos últimos anos e continuar crescendo. Quando iniciamos este projeto, éramos um grupo de pouco mais de 100 pessoas no escritório local, com 11ª posição no Great Place to Work e um segredo bem guardado: Cisco Networking Academy. Hoje, quatro anos depois, dobramos o número de funcionários locais, conseguimos manter o nível de excelência por três anos consecutivos como a melhor empresa para trabalhar no país, formalizamos nosso programa Cisco Networking Academy através de acordos público-privados e nos tornamos o centro da América Central e do Caribe. Precisamos continuar sonhando e ter certeza de que a Cisco Costa Rica pode realizar muito mais

UNIVERSIDAD LATINA DE COSTA RICA
POWERED BY Arizona State University

Sumário Executivo

Nome do cliente: **Universidad Latina de Costa Rica.**
Sector: **Ensino Superior.**
Local: **Costa Rica.**

Tamanho da organização: 8 locais. Mais de 90 carreiras entre programas de graduação, certificações trabalhistas e pós-graduação. Mais de 110.000 graduados. Junto com a American University, eles constituem o maior sistema universitário privado da Costa Rica, com mais de 25 mil alunos e aproximadamente 800 funcionários administrativos.

O desafio: Implementar uma solução de cibersegurança abrangente para melhorar e fortalecer a estrutura de ambas as universidades contra ataques maliciosos e de dia zero. Ter um serviço que facilite e agilize a visibilidade e o controle da rede, a fim de prever seu comportamento e agir imediatamente em caso de incidente.

A solução: pacote completo de segurança em nuvem por meio de:

- Email Security (suíte de segurança de email).
- AMP para Endpoints.
- Guarda-chuva (suíte de segurança para DNS).
- AnyConnect (suíte de segurança para conexões VPN).
- SecureX (plataforma de integração).
- Implementação de todas as soluções e gerenciamento da plataforma de segurança da Universidade através do SOC Altus.

Caso de éxito

Imagem: Universidade Latina da Costa Rica

A entidade

Com mais de trinta anos no mercado, a Universidad Latina de Costa Rica é uma das pioneiras no desenvolvimento do Ensino Superior Privado daquele país. Possui oito escritórios localizados em San Pedro, Heredia, Grécia, Cañas, Santa Cruz, Ciudad Neily, Pérez Zeledón e Guápiles e sua oferta é composta por mais de 90 cursos, incluindo graduação, certificações trabalhistas e programas de pós-graduação nas áreas da Saúde, Ciências Empresariais, Hotelaria, Ciências Sociais, Engenharia e TIC's, Arte, Design e Comunicação. Atualmente, possui mais de 110.000 graduados.

Desde a graduação, promove a formação de líderes éticos, inovadores e com visão global. Da mesma forma, apoia a pesquisa por meio da cooperação e do trabalho conjunto entre os setores público e privado, com o objetivo de aumentar a competitividade do país e o progresso social.

Em 2020, a Universidad Latina afilia-se à Arizona State University para se tornar uma universidade de impacto nacional.

Um dos pilares desta organização são os valores sobre os quais desenvolve as suas ações: excelência, compromisso, inovação, integridade e responsabilidade são uma força que promovem e partilham com a sua comunidade.

O desafio

Tanto a Universidad Latina de Costa Rica quanto a Universidade Americana fizeram parte do grupo Laureate até 2020. Naquele ano, foram estabelecidas como afiliadas da Arizona State University. Esta mudança deixou as duas universidades com a responsabilidade de repensar toda a sua estrutura de cibersegurança, tarefa que exigiu rapidez na implementação e robustez da solução escolhida devido ao contexto global desencadeado pela pandemia.

"A primeira coisa que fizemos foi ver que cobertura tínhamos com a Laureate. Em seguida, definimos a nossa própria arquitetura e esboçamos o que queríamos fazer agnosticamente. O passo seguinte foi avançar com as fases de RFI e RFP, para as quais convidamos vários fornecedores e, como tínhamos a alternativa da arquitetura da solução, ampliamos os serviços e também procuramos quem faria o SOC ", afirma Julio Galindo, Diretor de Tecnologias da Informação da Universidad Latina de Costa Rica e responsável pela estruturação desta implementação.

A solução

"A abordagem feita em conjunto com a universidade tem a ver com uma visão de solução e arquitetura, não se baseia apenas em produtos independentes. A Cisco apoia e acompanha a estratégia e o plano da universidade. A mensagem durante o processo de avaliação esteve relacionada aos conceitos de Automação, Simplicidade e Integração, os três pilares que a arquitetura busca", esclarece Giovanni Calderón, Gerente de Contas de Segurança da Cisco América Central e Caribe. Por isso, a solução adquirida pela Universidad Latina atualmente reflete esses conceitos e é composta pelo pacote completo de segurança em nuvem da Cisco, por meio dos seguintes produtos e serviços:

Imagem: Universidade Latina da Costa Rica

- Email Security (suíte de segurança de email).
- AMP para Endpoints.
- Guarda-chuva (suíte de segurança para DNS).
- AnyConnect (suíte de segurança para conexões VPN).
- SecureX (plataforma de integração).
- Implementação de todas as soluções e gerenciamento da plataforma de segurança da Universidade através do SOC Altus.

O processo de venda e aquisição foi liderado pela Altus Costa Rica, parceiro da Cisco reconhecido em diversas ocasiões por sua gestão inovadora e pela vanguarda da transformação digital.

Além de implementar as soluções oferecidas, a Altus gerencia toda a plataforma de segurança da universidade por meio de seu SOC. Ferramentas que complementam as soluções da Cisco também são usadas, especialmente para controle de vulnerabilidades nos servidores.

O serviço de suporte inclui:

1. Proteção contra cerca de 45 mil emails maliciosos.
2. Bloqueio de cerca de 1,5 bilhão de domínios maliciosos.
3. Gerenciamento de mais de 200 servidores.
4. Redução na detecção e remediação de vulnerabilidades nos servidores de vários meses para uma semana, graças à automação dos processos de atualização dos servidores.

"Durante a pandemia, pudemos implementar um esquema de trabalho seguro em que a maioria do pessoal trabalhava remotamente sem nenhum incidente de segurança", esclarece Alonso Bogarín, Gerente Geral da Altus Costa Rica.

Como a segurança é um processo que percorre toda a organização, esta solução impacta direta e positivamente todas as áreas da universidade, criando um sistema de proteção e visibilidade superlativo na indústria.

> "O principal benefício deste conjunto de produtos e serviços é a segurança e a tranquilidade que ele oferece, tanto para aqueles de nós que garantem a segurança das informações trafegadas pela universidade quanto para alunos, professores e funcionários administrativos, usuários de nossos serviços"
>
> *afirma Julio Galindo*

Imagem: Universidade Latina da Costa Rica

Julio Galindo
Diretor de Tecnologias
Informação Universitária
Latina da Costa Rica

Por que Cisco?

A escolha da Cisco como aliada estratégica baseou-se em seu portfólio completo, robusto e confiável. "Quando você constroi uma arquitetura e precisa de implementação rápida, a melhor coisa a fazer é ir com o fornecedor que tem a parede completa. Por exemplo, o SecureX nos permite ter controle de forma simples e os demais componentes são robustos e integráveis", diz Galindo.

Como base para a decisão, a universidade teve sua experiência anterior em outros produtos Cisco, já que seu Access Point e Switches park são Cisco, também Contact Center, Call Manager e agora Security.

Antes da pandemia, o cisne negro que acelerou a transformação digital global, "a percepção de segurança na direção local parecia um conceito de impacto distante, era algo que poderia acontecer com outra pessoa e era improvável para nós. Com a mudança, todos os assuntos relacionados a esta disciplina são bem-vindos, por isso os projetos de que falamos foram autorizados. A pandemia provocou uma mudança de cultura neste sentido para toda a organização. Devemos estar atentos aos novos riscos e aprender a utilizar as ferramentas que nos permitem estar protegidos. Estas são adoções graduais. O Steering Committee agora vê a segurança como um facilitador para permanecer no mercado e, mais ainda, para crescer", finaliza Julio Galindo

Próximas etapas na segurança

A segurança na Universidad Latina de Costa Rica é considerada um processo em constante evolução. Assim, a Cisco é um parceiro de negócios que o acompanha em cada etapa do projeto. Melhorar a segurança leva até mesmo à observação de novos espaços que requerem atenção. "Estamos avançando em outras frentes que têm a ver com este conceito. A segurança está dentro do nosso paradigma. Tenho mais de 15 anos no setor, antes da Costa Rica estive no Vietnã e antes no México e no Brasil. E sempre um dos pilares das minhas estratégias foi a segurança, algo que nos protege. E ter uma arquitetura simples e robusta torna a vida mais fácil para nós. Na universidade temos um plano anual de segurança que inclui controle de acesso, alvarás, controle de mudanças, comunicação, entre outras funções", afirma o diretor de tecnologia da informação da universidade.

> "Estamos honrados por ter a Universidad Latina de Costa Rica como cliente e por ela ser uma voz nestes 25 anos de Cisco no país, pois isso é um reflexo de como temos trabalhado juntos como parceiros de negócios e do crescimento que temos esperar na relação"

Jorge Mora,
Account Manager Cisco.

Imagem: Martín Lutze, Pixabay

A voz na comunicação virtual

por **Claudia Menkarsky**

Treinadora vocal, psicovocal terapeuta
e cantora lírica.

Hoje, mais do que nunca, no auge do modo virtual, nossa voz - aquele instrumento pelo qual nosso mundo interno e invisível se torna audível, com tons e palavras para expressar pensamentos, sentimentos, humores, comunicar - assume extrema relevância, já que todos os dias ela é o instrumento mais importante para facilitar a comunicação verbal e paraverbal por meio de telas.

Para transmitir da forma mais efetiva, afetiva e empática, é imprescindível considerar que, além de nossa própria disposição, condição e características vocais, podemos nos desinibir, adquirir espontaneidade e confiança, potencializar nossa voz com uma vocalidade sonora e bem definida, gerenciar as emoções para criar o clima certo de acordo com o diálogo ou exposição. Conecte-se, comunique-se.

A voz, a respiração e o sistema nervoso estão intimamente relacionados e são interdependentes. Hoje em dia, quando é comum ficar muito tempo sentado em frente a um computador com fones de ouvido, muitas vezes usando máscaras, a respiração pode entrar em colapso, a voz tende a ser forçada e o tom elevado para garantir que somos ouvidos. O uso de fones de ouvido não permite receber o sinal adequado para perceber se o volume natural da voz está sendo exigido. Por sua vez, acrescenta-se que 80% das pessoas não estão satisfeitas com a voz e têm medo de falar em público ou através de um vídeo, por falta de treino e hábito. Essa situação gera a inibição da respiração que colapsa o volume e tensiona os músculos, gerando em muitos casos bruxismo, contratura cervical, dores de cabeça, azia e outros sintomas de falta de respiração profunda, abdominal, afrouxamento da mandíbula e capacidade de expressar espontaneamente o que queremos para transmitir, como fazíamos na infância, com alma e coração.

Assim, chegamos ao treinamento vocal e expressivo, como falar em público, treinar a voz e aprender a falar na frente dos outros, tentando ser realmente nós mesmos em nossas vozes, e não um monte de nervos, com nós na garganta.

Como reconhecer e melhorar nossa voz?

Nossa voz nos identifica e nos define, o estado de consciência se reflete na voz, cada voz é única, como a visão do mundo, como a verdade de cada um. A seguir, compartilhamos alguns exercícios para começar a reconhecer a própria voz, aprimorá-la e fazê-la ouvir, liberando seu verdadeiro potencial, aquele que desde a infância e ao longo dos anos foi mudando a cada "cala a boca, não grita", "fique quieto", "fique quieto / a", "você não sabe."
Existem três fatores que determinam uma boa vocalidade: respiração profunda; abra a boca, baixando a mandíbula em A e O; e um bom ambiente.

Alguns exercícios

Respire novamente para o ventre, como ao nascer: bem sentado, ereto, com as costas retas, pernas descruzadas, expire inclinando-se para a frente, apoiando os cotovelos nos joelhos. Inspire profundamente. Lá, observa-se que o ar está inflando a barriga à medida que abaixa o diafragma, e abre a parte intercostal. É assim que você pode respirar profundamente. Inspire pelo nariz em 5 vezes, segure o ar por mais 5 vezes, e expire em 10 vezes pela boca, soprando o punho da mão, juntando os lábios em forma de beijo e garantindo que o ar saia frio.
Se você fizer este exercício uma vez ao dia, após uma semana é possível identificar quando você está respirando profundamente e quando não está.
Afrouxe a mandíbula. Falar em frente ao espelho, observando que a boca forma um pequeno orifício a cada vez que se pronuncia o A e o O. Tanto com a mandíbula solta quanto com a pronúncia das vogais, os lábios devem cobrir naturalmente a dentição. Enquanto não fala, ainda juntando os lábios, com a boca fechada, tente deixar um pequeno espaço, coloque a ponta da língua entre os dentes para que a tensão que possa existir na mandíbula seja aliviada. Este exercício é de grande ajuda contra bruxismo e contraturas cervicais.
Impor a voz. Faça o seguinte teste: junte os lábios e faça um som. Se vibram e fazem cócegas, é porque o cenário está fora do lugar. Pode ser corrigido, repetindo o exercício e enquanto o som é emitido, abaixe a cabeça, inclinando-a suavemente para frente. Desta forma, será observado que a vibração é sentida na ponta do nariz, pode ser tocado para verificar. Em seguida, fazendo o som, sorria levemente e sente-se com a cabeça erguida. Aí é possível perceber que o som já está lá como na "máscara", ou seja, o local da face onde costumamos colocar a máscara; bem implantado e sem sensação de cócegas nos lábios.
Para cuidar dos ouvidos. Use o fone de ouvido apenas de um lado, alternando-o para não cansar os tímpanos e para poder sentir o volume real da voz ao falar, sem forçá-lo.

Tente falar em um tom de voz profundo e central, dando-nos tempo para respirar. É preciso lembrar que momentos de atenção são gerados nos silêncios que dão lugar à reflexão e não em uma fala rápida que, depois de um curto espaço de tempo, ninguém atende, principalmente quando não há contato com o olhar, visto que essa poderosa energia não existe atrás da tela. Tente falar em voz alta, na frente do espelho, para reconhecer os gestos e coloque as mãos entre o peito e o umbigo. É uma boa ideia gravar ou filmar a si mesmo, pois nos ver e ouvir é a melhor maneira de detectar o que você quer mudar e melhorar na sua voz e expressão

A autora do artigo está à disposição para esclarecer dúvidas ou preocupações relacionadas:
claudiamenkarskycoach@gmail.com

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

Espere o inesperado. Essa premissa básica e universal, aplicável em todos os momentos e em todos os lugares, tornou-se extraordinariamente presente e permanente em nossas vidas desde as recentes mudanças que, definitivamente, transformaram o mundo como o conhecíamos. Pouco resta do que até recentemente era a vida cotidiana. Mesmo esperando o inesperado, adaptar-se a mudanças tão extremas é difícil para qualquer pessoa, em especial quando este esforço é solitário. Ou seja, passagem por esta etapa é menos dolorasa se houver pontes e se o caminho percorrido for compartilhado. É hora de compreender e aceitar as novas dificuldades e também as novas soluções que nos permitirão seguir em frente.

Uma das ferramentas disponíveis é o modelo de negócios *Partner for Partners*, da Braycom, reconhecido pela CISCO. Este programa oferece serviços profissionais de pré-venda, implementação e suporte para empresas da área e, em vez de competir, elas trabalham juntas para aumentar suas possibilidades. Desta forma, a Braycom coloca à disposição de seus clientes sua formação profissional e a experiência em engenharia.

A confiança é a chave para o *Partner for Partners* e por mais de 15 anos os parceiros mais relevantes na Argentina e no Chile confiaram na Braycom. Quando você é convocado por um integrador por meio deste programa, a empresa auxilia a engenharia de pré-venda sem nenhum custo, e oferece serviços profissionais para a implementação de soluções. Assim, coloca à sua disposição engenheiros certificados, métodos e experiências para minimizar riscos em projetos complexos, o que permite multiplicar sua capacidade técnica e comercial.

O funcionamento é simples: quando um cliente convoca um integrador de tecnologia, ele entra em contato com a Braycom, que o auxilia gratuitamente no desenvolvimento consultivo e na pré-venda da solução adequada para aquele cliente. Desta forma, o ciclo de vendas é acelerado e o projeto é concluído. Nos projetos em que a implantação é necessária, a Braycom a realiza com seus engenheiros credenciados e o serviço é previamente marginalizado como mais um produto. Assim, todos ganham. O *Partner for Partners* consegue solucionar os desafios para que o negócio da integradora cresça sem correr riscos e sempre garantindo a fidelização de seus clientes para com sua marca.

O *Partner for Partners* da Braycom é uma resposta dinâmica e eficaz tanto ao conhecido como ao inesperado. Todos estão convidados

Imagem: Mohamed Hassan, Pixabay

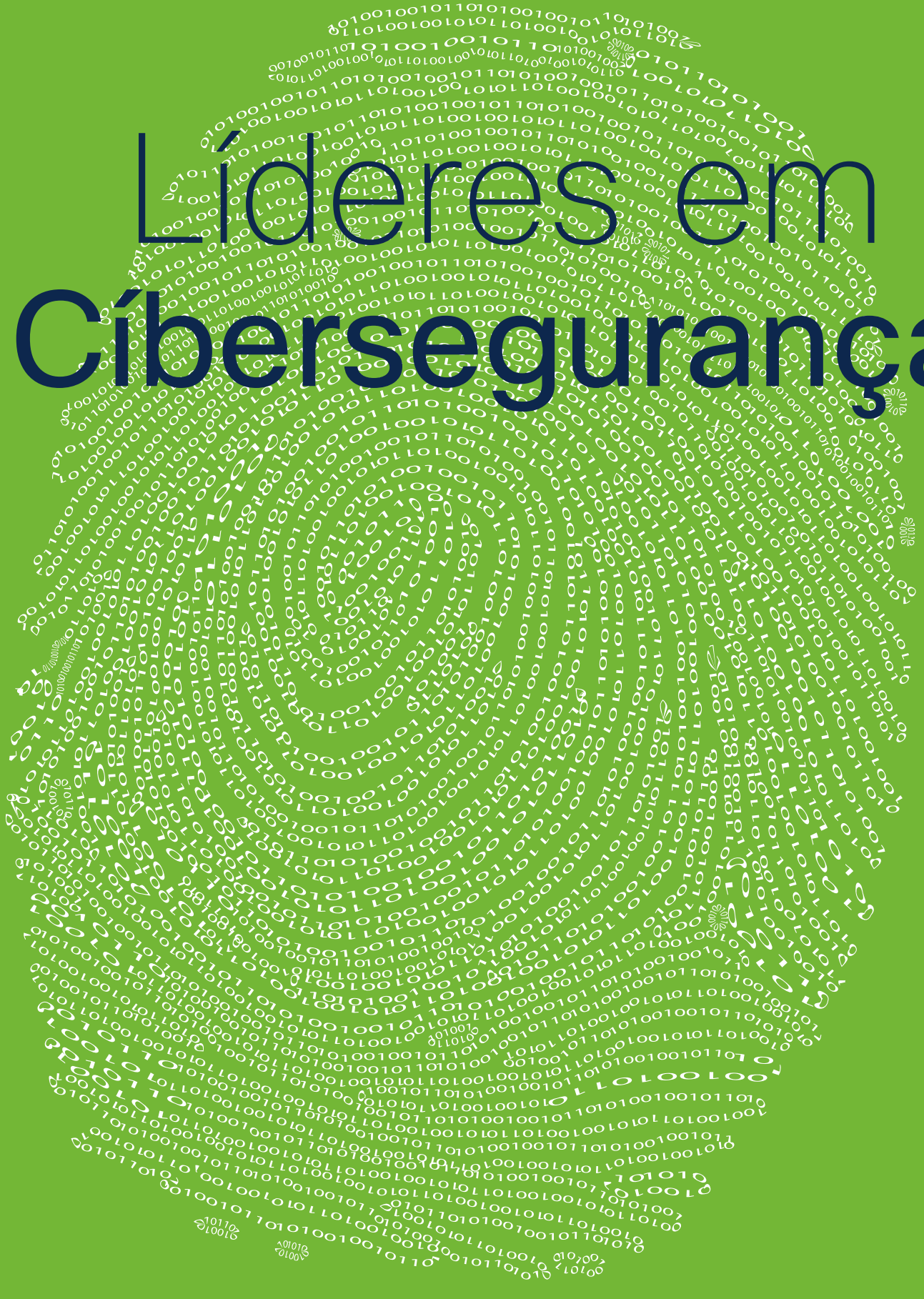
PARTNER
for **partners**

> *“Quando começamos com este modelo, muitos sócios viam nossa proposta com ceticismo e descon-fiança, mas bastou a primeira joint venture para o programa se tornar estratégico.”*

por **Ing. Martín Marino**
CEO da Braycom

Acesso serviço

Líderes em Cibersegurança



Muitas vezes, líderes de cibersegurança concordam que esta disciplina deve ser entendida como um processo em constante adaptação. Cada um ao seu estilo, guia sua equipe no caminho decisivo para uma organização segura, que protege não apenas seus membros e ativos, mas também os seus colaboradores e toda a cadeia de valor. Nesta edição da Bridge, três líderes proeminentes na área de segurança cibernética compartilham seus conhecimentos e experiências e dão indicações sobre como lidar com o futuro em mudança.

Nohemí **Moreno**

José Luiz **Santana**

Ricardo **Pérez D'Brot**

Nohemí **Moreno**

Diretora líder de serviços de segurança cibernética aplicada na Accenture e professora de especialização em segurança cibernética na Latam Business School, México.

por **Karina Basanta**

Imagem: Flavio Moura, Pixabay
Cancún, Pirámide Maya

O olhar de Nohemí alcança uma pluralidade de setores: serviços financeiros, varejo, seguros, educação e telecomunicações são alguns deles. Sua jornada e suas palavras são sustentadas pela experiência. Nesta edição da ***Bridge****, compartilhamos sua perspectiva sobre a segurança cibernética no contexto atual e as recomendações para uma operação resiliente e bem-sucedida.*

Pela sua experiência, o que hoje tira o sono de um especialista em segurança cibernética?

Depende da especialidade, mas na minha perspectiva considero que o mais crítico hoje é a dificuldade de fazer uma gestão de risco adequada com os recursos que se tem.
Geralmente, você não tem todo o orçamento necessário, tecnologia de ponta ou equipe com habilidades e conhecimentos atualizados. O que é ainda mais crítico quando, a cada dia, surgem novas ameaças e vulnerabilidades, e vivemos um ambiente totalmente em mudança, como o atual.
Encontrar um equilíbrio, comunicar e convencer sobre as necessidades críticas com clareza, estando dentro dos níveis aceitáveis de risco estabelecidos pela organização, é o grande desafio.

Vantagem ofensiva ou defensiva em Cibersegurança?

No ambiente atual em que nos encontramos, com os ataques cibernéticos na ordem do dia, não vejo como não haver mecanismos ofensivos e defensivos, nos quais ambos forneçam os insumos para reforçar ou modificar as capacidades de uma organização em segurança cibernética.

De acordo com a sua experiência, o que funciona e o que não funciona nesta disciplina?

O que não funciona:
çacreditar que segurança é apenas um problema técnico e que basta um único investimento para garantir que nada acontecerá à organização.

O que funciona:
incutir uma cultura de segurança em todos os níveis da organização; dedicar tempo à identificação e entendimento dos possíveis riscos de acordo com o tipo de organização e os países em que atua; estar preparado para responder e recuperar as operações em caso de evento adverso; e, o mais importante, estar ciente das mudanças nos ambientes tecnológico, regulatório e de negócios, e que a segurança é um processo contínuo que requer atenção e intervenção da alta administração.

No seu entendimento, qual é o lugar da privacidade na abordagem estratégica da Segurança?

É indispensável, e mais ainda agora que a consciência em relação à privacidade cresceu exponencialmente devido às várias regulamentações no mundo. Durante a definição de uma estratégia de segurança, é essencial saber o que é crítico para uma organização e o que é definido pelos sistemas de missão crítica e pelos dados gerenciados.
Portanto, é necessário aplicar práticas de privacidade e proteção de dados para evitar o manuseio incorreto e o vazamento de informações que expõem as organizações a vários riscos.

Qual é o significado da palavra “resiliência” para você?

Ter capacidade para se recuperar ou se adaptar e seguir a rotina diante de um evento perturbador.

O que, em sua opinião, deveria ser feito e não ser feito em termos de cibersegurança? Você pode aceitar a pergunta sob qualquer ponto de vista.

Essas práticas são feitas em determinados setores e em diferentes níveis, mas acho que devem ser reforçadas:

1. Gerenciar minuciosamente os ativos de informação, considerando aqueles que não pertencem à organização, aplicando as mesmas políticas de segurança independentemente da localização da rede.

2. Identificar e gerenciar terceiros, priorizando as práticas de segurança a serem utilizadas de acordo com o serviço prestado e o tipo de acesso aos sistemas e dados.

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

3. Ativar o processo de gerenciamento de riscos de segurança cibernética usando informações de inteligência cibernética.

4. A alta administração deve se envolver e compreender os riscos aos quais está exposta em termos de segurança cibernética.

Compartilhe conosco três recomendações sobre Segurança levando em consideração o contexto atual.

Os limites de uma organização foram perdidos, os dispositivos interconectados aumentaram exponencialmente, assim como as identidades digitais usadas por humanos e não humanos. Portanto, considero os seguintes três pontos práticos necessários:

1. Coloque o foco na proteção da informação. Isso requer saber o que e como é coletado, onde é armazenado e com quem é compartilhado.

2. Catalogue e gerencie efetivamente os ativos digitais em termos de risco potencial.

3. Implemente um programa para identificar, gerenciar e monitorar as identidades digitais, ativos e aplicativos que acessam esses dados.

Há algo que eu não perguntei e você gostaria de compartilhar?

Em segurança, nada é infalível, por isso é necessário ter um plano de atendimento e resposta a incidentes claro e acionável que envolva as diferentes áreas da organização e inclua as de gestão de crises e comunicação

Entrevista

José Luiz Santana

CISO, C6 Bank, Brasil

por **Nelson Brito**

Aqui você pode ler um trecho da entrevista. Convido você a acessar o conteúdo audiovisual completo a partir do código QR desta página.

Imagem: Wanderson Teixeira, Pixabay
Cristo, Río de Janeiro

Conversar com o José é sempre muito enriquecedor. Suas ideias são tão claras e diretas quanto suas ações. Neste bate-papo, revisamos alguns dos pontos mais marcantes da disciplina que nos une.

José, o que é que te mantém acordado à noite?

Para quem trabalha com segurança, esta é uma pergunta que não tem resposta única. Porém, o que mais me preocupa, o que procuro intensamente todos os dias, é identificar os riscos. O que mais me mantém acordado é não saber que o risco existe, não saber onde está alojado. A primeira coisa a saber é onde está e, em seguida, mitigar.

Vantagem ofensiva ou defensiva em Cibersegurança? Onde você costuma colocar o foco, Time Azul ou Time Vermelho?

Eu me equilibro, embora tenda a me concentrar no Time Azul, nas estratégias de defesa, porque existem poucas pessoas de segurança ofensiva na equipe. Mas, como tudo na vida: equilíbrio. A segurança ofensiva é muito importante, mas é essencial ter uma estratégia de segurança adequada que consiga fechar o loop. A Equipe Azul e a Equipe Vermelha fazem parte deste círculo; a maneira como eles se integram e interagem definirá se a estratégia será bem-sucedida ou não. No final das contas, o que mais importa é uma boa interação entre as equipes. Equilíbrio.

Levando em consideração essas quatro categorias da função de um líder de segurança: tecnólogo, guardião, estrategista, consultor, com qual você mais se identifica e por quê?

Estrategista. Pensar, construir, criar arquiteturas tem a ver com estratégia. Ser vanguardista me motiva muito, assim como fazer todos irem na mesma direção.

O que funciona e o que não funciona em Cibersegurança?

Não adianta querer fazer segurança em algo que não conhecemos profundamente. Não adianta parar de estudar. Para ter certeza de algo, você sempre tem que mergulhar em cada novo mercado, cada nova tecnologia, cada ferramenta. Além disso, fazer a segurança cibernética enquanto as equipes de negócios e de segurança estão separadas não funciona.

Que lugar ocupa a privacidade na abordagem de segurança estratégica do banco?

Um lugar muito crítico. É por isso que a privacidade toca a segurança, não está abaixo dela. A segurança é um componente que existe para ajudar. Na minha opinião, a privacidade não está dentro da segurança.

Se eu disser a palavra "resiliência", o que isso significa para você?

Resiliência é foco, força, disciplina para cumprir a missão.

Compartilhe conosco três recomendações levando em consideração o contexto atual.

Antes de mais nada, cuidar da equipe, cuidar do ser humano. Estamos passando por um momento difícil como sociedade e cada pessoa vive de maneira diferente. Então aqueles de nós que têm responsabilidades de liderança devem tentar colocá-los em primeiro lugar e depois pensar em outras coisas.
Em segundo lugar, entenda que o trabalho remoto já é uma realidade para muitas pessoas. A pandemia intensificou ainda mais e não há como retroceder. Isto significa que qualquer estratégia de cibersegurança deve contemplar que as pessoas acessem a rede e trabalhem de qualquer lugar, ou seja, o perímetro não existe mais e não existirá mais, este é um ponto a se considerar.
Em terceiro lugar, gostaria de encerrar com uma mensagem positiva: a adversidade nos traz oportunidade. O melhor está por vir

Imagem: Ingrid Bezerra
Monumento às Bandeiras, Sao Paulo

Entrevista

Ricardo Pérez D'Brot

Gerente Adjunto de Inteligência e Resposta de Cibersegurança, Interbank, Peru.

por **Juan Marino y Jorge Prinzo**

Imagem: Goldbug, Pixabay
Machu Pichu, Perú.

Nesta realidade confrontada com o Ricardo, evidenciamos a sua vasta e enriquecedora experiencia, após mais de 15 anos de experiência no mercado bancário no Peru. Convidamos vocês, caros leitores, a acessar o desafio de "desafiar o status quo" e reavaliar sua estratégia de segurança cibernética.

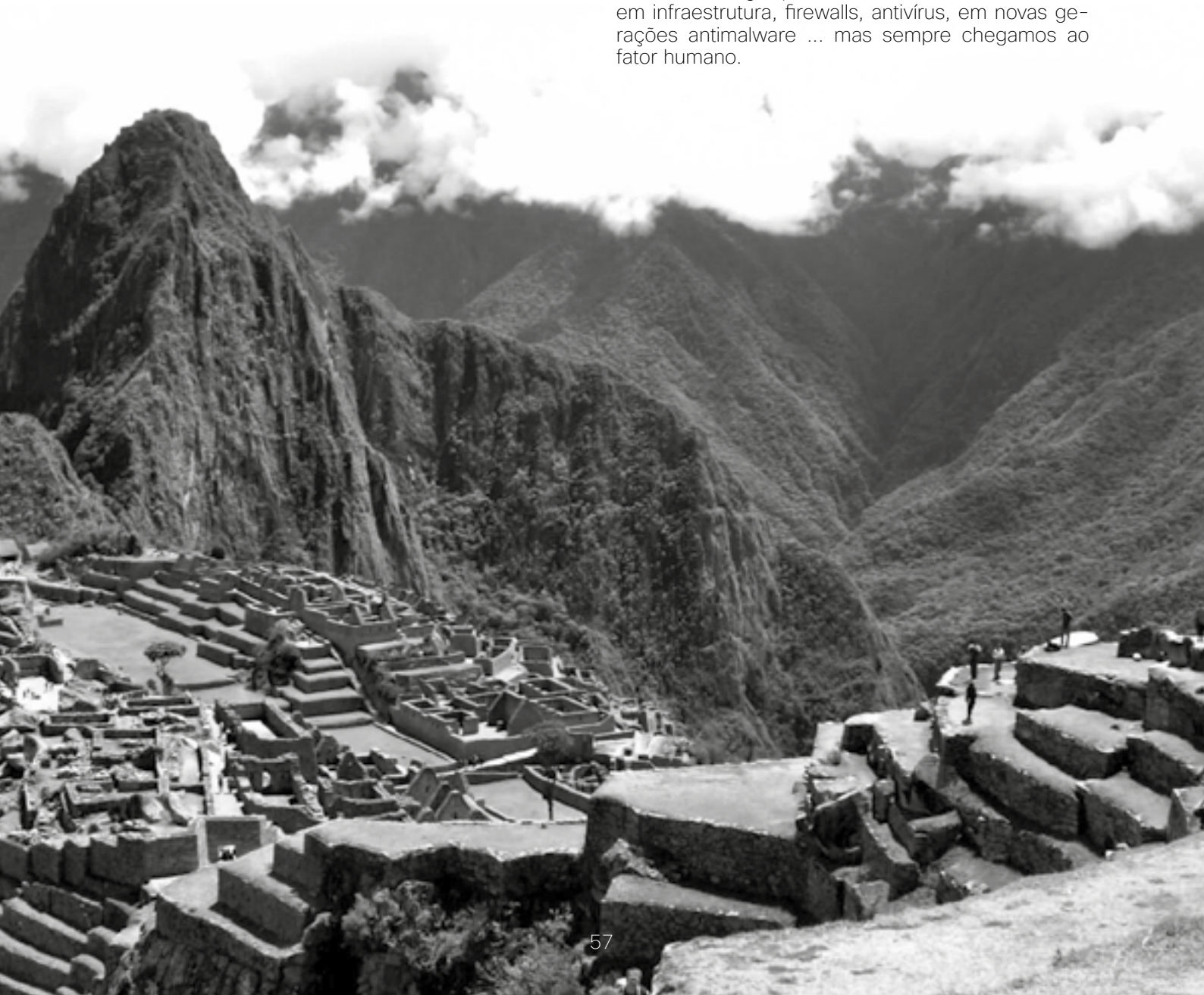
Conteúdo audiovisual

Protegendo uma das principais entidades financeiras do Peru, como você lida com a previsão de que suas credenciais serão roubadas?

É uma realidade: é definitivamente algo que acontece. As pessoas tendem a usar as mesmas credenciais em vários serviços, ou usam a senha corporativa ao se cadastrar em uma página da web ... Portanto, não é uma questão de como, mas de quando isso acontecerá com você ...

Você tem que conviver com isso ...

Exatamente: você tem que conviver com esta realidade e é por isto que nossa abordagem reforça a parte cultural. Desta forma, quando isto acontecer, você precisará estar totalmente atento e preparado. O que as pessoas já sabem: "isto é suspeito", "isto é malicioso", "Não pedi", "Não participei deste sorteio" ... todas aquelas bandeiras vermelhas que aparecem antes de mensagens bastante tentadoras. Nos últimos anos, a cultura do usuario foi assunto de muitas conversas quando montamos os orçamentos e a estratégia: poderíamos investir muito dinheiro em infraestrutura, firewalls, antivírus, em novas gerações antimalware ... mas sempre chegamos ao fator humano.



Então, na estratégia de investimento, um dos elementos de destaque é a consciência dos usuários.

Sim. Isto é inegociável. Temos aproveitado custos de oportunidade em outros projetos, transferindo-os para o futuro, mas definitivamente a questão da cultura, uma vez que começamos a reforçá-la, tem sido uma questão constante, e acho que é a que nos deu a maioria dos frutos. Se nossa superfície de ataque era de 25%, hoje é de 2% ou 3%.

Vocês estão capacitados para medir isto ...

Sim, 2% não nos torna imunes, mas sua área de superfície é menor.

Li um relatório que atesta que o Interbank traça cenários de simulação de crise, por exemplo, o que aconteceria se sofressem uma violação de segurança cibernética. Como estes cenários são definidos?

Muito bem. Participaram líderes decisórios, táticos e operacionais da empresa. Fiquei surpreso com a forma como eles se envolveram, como participaram do primeiro exercício. Não me pareceu algo como "duas horas com o pessoal da segurança... que chato..." Não: eles levaram a sério esta dramatização, assumiram o papel e perguntaram "bem, o que faríamos se isso acontecesse conosco, o que seria algo realmente trágico para a organização?"; e "vamos ver, conte-nos mais." Eles começaram a questionar; Obviamente, nem todos serão especialistas em ciberseguran-ça, mas esta curiosidade foi gerada e, no final das contas, um *hacker* é sempre uma pessoa muito curiosa. De alguma forma, estamos introduzindo-os nesta cultura *hacker*.

Há uma experiência ou algo que você viu e que te permita afirmar "isto funciona e isto não"?

Alguns anos atrás, "segurança por obscuridade" era uma prática comum. Era pensar "se eu encontro algo, escondo, não falo sobre isto, guardo a sete chaves". Isto nos mostrou o outro lado, que deveria ser um tema mais aberto. Existem vários fóruns nos quais é possível abordar este assunto. Mas, em um fórum público, você não pode dizer "estes são meus *firewalls*, é isso que eu faço", sob o risco de se tornar alvo. Por outro lado, é saudável asumir "temos este problema, como o resolvemos?" Não é um tema exclusivo da equipe de segurança. É algo que equipe de tecnologia em Geral debe lidar. Você envolve tecnologia, redes e outras áreas em um grupo multidisciplinar. Isto é enriquecedor e uma mudança necessária. É preciso mudar inclusive a mentalidade da equipe de cibersegurança para algo mais aberto e preparado para lidar com questões conhecidas e futuras o mais rápido possível.

Pensando no atual estado de maturidade da cibersegurança, o que você diria: existe uma vantagem ofensiva ou existe uma vantagem defensiva?

O atacante sempre terá a vantagem, porque está constantemente atacando, constantemente reforçando sua capacidade de responder. Podemos ter equipes tentando evitar isso ou antecipar o que o invasor pode fazer, mas o invasor precisa, em última instância, de uma maneira de fazê-lo corretamente. Precisamos de 65.535 maneiras para fazê-lo falhar, mas ele precisa de apenas uma brecha.

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

Que injusto. Por fim, consideração o atual contexto da pandemia e do avanço do trabalho remoto, compartilhe conosco três recomendações para elevar o nível de segurança no setor financeiro e no setor público.

Primeiro, reforce a cultura de segurança digital para que as pessoas se tornem mais uma camada dentro do ecossistema. Definitivamente, isto é algo que fizemos bem e acho que deveria ser estendido a todas as empresas, porque quanto mais resilientes formos, menos atrativos seremos para os fraudadores. Normalmente, o que vemos é que a fraude é cíclica: vai de teste em teste. Mas, se todos - colaboradores e clientes - começarmos a subir o nivel, um tópico de *phishing*, por exemplo será cada vez menos atraente para o criminoso, porque não haverá mais vítimas. A segunda é capacitar a segurança do endpoint. Agora, com a nova forma de trabalhar, o endpoint se tornou totalmente crítico. Antes era uma peça importante, mas não crítica dentro do esquema de segurança cibernética, porque era preferível priorizar questões de perímetro, visibilidade de 100% dos controles e, em seguida, diminuir. A última linha de defesa era o endpoing, mas ele se tornou a primeira, de mãos dadas com o usuário. Portanto, não é mais negociável que você tenha um antivírus desatualizado, um *firewall* de estação deshabilitado. A questão agora é o controle do dispositivo. Parece básico, mas você tem que fazer o básico bem feito. Depois de amadurecer, você começa a se mover em direção a todos os outros esquemas mais complexos. E a terceira coisa é não negligenciar todas as outras falhas que você já identificou. Pode parecer um pouco contraditório, mas este é o momento em que você pode tentar mudar as coisas, evoluir. Se antes havia certas restrições, porque as pessoas estavam no escritório, agora já tivemos um ano todo e provavelmente teremos por muito tempo mais pessoas que não estão conectadas à rede da organização. Vamos remover alguns dos fatores limitantes e ver o que podemos fazer. Poderíamos desafiar esta parte do status quo e dizer "vou rever minha postura de segurança". Agora é o momento ideal para tomarmos este tipo de decisão, porque as instalações estão sendo fornecidas para as pessoas teletrabalharem. Então, provavelmente não é necessário um esquema de segurança tão complexo na rede, o que abre espaço para migrarmos para um esquema avançado mais preditivo. Mas depende de cada realidade, minha recomendação é que questionem. Por que não?

Super claro, Ricardo, ficamos com estes três pontos. Muito obrigado por nos ter dedicado este precioso tempo e sobretudo por cuidar do banco, que é algo do qual os cidadãos dependem muito. Então, um prazer e continuamos em contato. Obrigado.

O prazer é meu, Juan. Obrigado

Coluna

Video:
Cisco IoT
Networking Overview

Imagem: Trevor Bobyk, Unsplash.

Big Brother IoT

Cibersegurança em ambientes hiperconvergentes

por **Freddy Macho**

Membro da Comissão de Peritos
Laboratório de Segurança Cibernética da OAS
Presidente do Centro de Pesquisa
Cibersegurança IoT - IIoT
Coordenadora do Centro
Cibersegurança industrial (CCI)
Presidente IoT Security Institute LATAM

O objetivo desta coluna é se aproximar dos vários componentes de IoT, bem como identificar os capacitadores que impulsionam estes ambientes e suas melhores práticas, os protocolos de comunicação e os padrões de cibersegurança que existem nas várias verticais de Internet das Coisas.

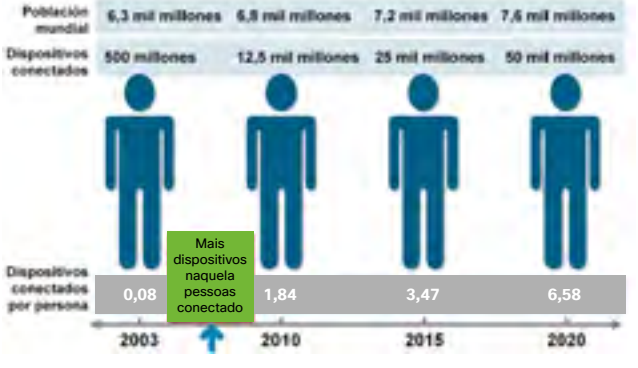
Convido você a fazer a leitura desta primeira parte que busca estimular, de alguma forma, a ávida necessidade que temos como seres humanos de nutrir o conhecimento sobre estes ambientes.

O surgimento da Internet das Coisas ou IoT fornece um ambiente onde os objetos do cotidiano se integram e contribuem juntos em um sistema que dá lugar à convergência de dispositivos inteligentes e dispositivos convencionalmente conectados. A IoT é considerada a terceira onda global da indústria da informação depois das invenções do computador e da Internet.

Hoje, uma grande variedade de objetos está conectada à Internet - carros, equipamentos médicos, termostatos, sistemas de iluminação e muitos outros dispositivos. A industria caminha rumo ao desenho, desenvolvimento e integração de um universo de sensores de baixo custo, que podem ser programados para gerar soluções ou serviços que nos possam dizer, por exemplo, como reduzir o consumo diario de cafeína ou registrar que as luzes da sala são acesas gradualmente, aumentando o brilho no momento em que você acorda de um sono profundo no início do dia.

A presença da Internet das Coisas é muito ampla em nossas atividades tradicionais. Geralmente, é dividido em verticais. No início dos anos 2000 tínhamos o registro de seis setores, mas atualmente estima-se que existam cerca de 30 verticais, algumas delas robustas e totalmente operacionais, outras em desenvolvimento ou criadas recentemente. O conceito de IoT é considerado uma definição viva, porque seu crescimento constante e a incorporação de várias contribuições e virtudes ainda seguem fornecendo novas características.

Em 2003, aproximadamente 6,3 bilhões de pessoas viviam no planeta e 500 milhões de dispositivos estavam conectados à Internet, de acordo com um relatório da Cisco em 2011. Isto indica que havia menos de um dispositivo (0,08) para cada pessoa. Nas projeções da Cisco para 2020, estimava-se que haveria 50 bilhões de dispositivos conectados à Internet, número que, em meio à situação global de pandemia, leva à hipótese de que esta projeção tenha ficado aquém da realidade.



Fuente: Cisco IBSG, Abril de 2011

Fuente: Fostec & Company

Importância de cíber segurança

Devido ao exposto, o provável impacto de não ter o nível correto de segurança cibernética no momento em que bilhões de dispositivos inteligentes se conectam à Internet, sob o guarda-chuva da IoT, e interagem entre si para levar as informações corretas para as coisas certas, no momento certo e colocado pelo canal certo, seria simplesmente catastrófico. Uma falha de segurança cibernética pode impactar de forma muito diversa, por exemplo, a possibilidade de criar espaços que facilitem a criação de atividades ilegais, a queda ou indisponibilidade de serviços críticos, colocar em risco a soberania de um país ou, mais importante, causar perda de vidas humanas.

A Internet das Coisas é uma nova mudança de paradigma no mundo da tecnologia da informação (TI), onde as coisas têm identidades digitais, recursos de monitoramento de inteligência artificial (IA) e podem ser localizadas, rastreadas, seguidas, controladas e automatizadas.

A convergência das atividades de tecnologia da informação tradicional (TI), tecnologias operacionais (OT) ou redes industriais e computação em nuvem resultam no que se convencionou chamar de hiper-

convergência. Este processo facilita a interação entre IoT e smarcities e IIoT (Industrial Internet of Things) e infraestruturas críticas, o que aumenta significativamente a complexidade de ser capaz de entregar níveis de segurança cibernética de acordo com a necessidade, o que é uma exigencia artual. A aceleração da digitalização e do trabalho remoto fez com que o uso da hiperconvergência aumentasse enorme e rapidamente.

A implantação da IoT levanta muitos problemas de segurança cibernética derivados da própria natureza dos objetos inteligentes, por exemplo, a adoção de algoritmos criptográficos leves, em termos de requisitos de processamento e memória, e o uso de protocolos padrão, bem como a necessidade de minimizar a quantidade de dados que podem ser expostos na troca entre nós.

Integrar o mundo físico à estrutura da web impõe requisitos avançados de segurança cibernética que devem ser atendidos para garantir um controle rígido sobre a interação de serviços na IoT.

A necessidade de elevar os níveis de segurança cibernética em ambientes IoT - IIoT são indesculpáveis na América Latina e por isso fazem parte do trabalho que é desenvolvido pelo grupo de especialistas do Laboratório de Segurança Cibernética para os Parlamentos das Américas da Organização do Estados Unidos Americanos (OEA), da qual tenho o prazer de participar. Um de seus objetivos é gerar um primeiro documento sobre "Princípios Orientadores da Cibersegurança IoT", cujo objetivo é promover a cibersegurança na região e que você poderá acessar a partir desta edição do Bridge.

Por hoje, ficamos por aqui. Até nosso próximo encontro

Colaboração Segura

Em 2020, a pandemia colocou o mundo em modo online. Neste artigo, o especialista Adriano Gaudencio reflete sobre o modelo de trabalho em curto prazo, que propõe escritórios adaptados à modalidade híbrida e ferramentas que oferecem uma experiência amigável, colaborativa e segura.

Quais são os desafios que enfrentamos ao voltar para o escritório? A Cisco observa que a partir de agora, o trabalho será híbrido. Podemos constatar que 98% das reuniões não terão mais todas as pessoas dentro de um escritório, mas que sempre haverá quem acompanhe a reunião online. 54% dos colaboradores já assumiram a possibilidade de trabalho remoto e estão preparados para tal. De acordo com nossa pesquisa, estima-se que pelo menos oito dias por mês a maior parte dos funcionários vá para casa. Para chegar a esta conclusão, entrevistamos mais de 1.000 empresas de diferentes mercados. Consideramos a amostra significativa. Por outro lado, outra tendência importante é a inclusão. Hoje, com a possibilidade de trabalho remoto, é possível abrir a busca por talentos em diferentes partes do mundo.

O futuro é agora

Nesse caso, uma meta importante é garantir uma experiência ideal e segura, tanto para o retorno aos escritórios pós-quarentena quanto para o trabalho

por **Adriano Gaudencio**

Líder de vendas de colaboração da Cisco
para a América Latina

remoto. É por isso que a Cisco está desenvolvendo a "Colaboração do Futuro". Trata-se de alcançar uma colaboração inclusiva que integre todos e possibilite uma experiência remota 10 vezes melhor do que a presencial. Mas pode a experiência remota ser melhor do que ficar cara a cara com uma pessoa, conversando, interagindo? Vejamos com um exemplo que, em alguns casos, sim: dentro da aplicação, a Cisco tem a funcionalidade de tradução simultânea, em tempo real, algo que claramente leva uma vantagem caso os membros não falem todos a mesma língua. Lembremos que Cisco Webex é uma plataforma de colaboração segura, que inclui aplicativos para melhorar o trabalho em equipe de cada funcionário, com ferramentas de mensagens, troca de arquivos, quadro branco e realização de tarefas, entre muitas outras funções, que vão além do horário de reunião ou conferência. Nele, a Cisco integrou diversos aplicativos em um, que é compartilhado na nuvem e consegue entregar diversos serviços, como o Webex Meetings, que é uma plataforma para realização de videochamadas; Webex Teams, que permite o envio de informações por meio de mensagens diretas e de equipe; e o Contact Center. Poderíamos dizer que é o ponto de partida do trabalho remoto. A ideia é oferecer uma excelente ferramenta para trabalhar em casa. Assim como é necessário ter uma boa cadeira ou um computador ideal, a qualidade da voz ou imagem e o acesso a diversos dispositivos que melhoram a experiência do usuário também são essenciais. A Cisco está progredindo nessa tarefa.

Ao mesmo tempo, é fundamental cuidarmos dos clientes dos nossos clientes. Por esse motivo, lançamos recentemente o Cisco Webex Contact Center na nuvem brasileira, de onde atenderemos todos os clientes da América do Sul. Todas as integrações com o cliente podem ser gerenciadas como uma experiência unificada diretamente da tela, sendo possível interagir com as redes sociais, Facebook, Instagram, LinkedIn.

O valor da segurança

A Cisco possui políticas de segurança muito avançadas, portanto, um dos pontos fortes da plataforma Webex é a sua segurança, que está presente de "ponta a ponta". Não há quebra no processo, o que oferece uma vantagem competitiva única. A Agência de Segurança Nacional dos Estados Unidos publicou um relatório que endossa a política de segurança da Cisco, confirmando que é de ponta a ponta.

No que se refere às vulnerabilidades, muitas vezes estão relacionadas às credenciais, ou seja, à identificação de quem tem acesso ao sistema. A colaboração e a segurança da Cisco estão reunidas em uma solução completa. Quer a pessoa trabalhe em casa ou no escritório, há garantia de segurança, o acesso à Internet, os dispositivos, a confidencialidade dos arquivos e dados, a autenticidade das pessoas que trabalham estão protegidas. Você também pode detectar o que está acontecendo em todas as soluções para acionar uma resposta proativa e garantir que o trabalho remoto seja feito com segurança.

Como facilitar um retorno seguro ao escritório?

Por meio da tecnologia, a Cisco garante o trabalho remoto, além do presencial, certificando a segurança e a qualidade da experiência, controlando os processos para aumentar a produtividade e otimizar o trabalho.

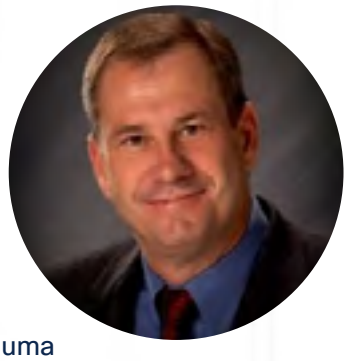
Estamos agora preparando o retorno ao escritório. Em tempos de distanciamento e segurança sanitária, a ferramenta Cisco detecta, por exemplo, se há mais pessoas em uma sala do que o recomendado, e avisa o responsável para que providências sejam tomadas. Também possui sensores de temperatura, que detectam se um ambiente está na temperatura ideal para que você possa trabalhar com conforto; e um sistema que avisa se o ambiente foi higienizado ao final de uma reunião e está pronto para o início de um novo evento.

O objetivo é absorver o melhor do mundo analógico e o melhor do mundo digital, valorizando ambas as áreas. Os dispositivos Webex integram os dois processos. São ferramentas de segurança e colaboração, desenhadas para se adaptar da melhor forma à situação; e permitem que você navegue pelas diferentes soluções de maneira amigável, sob o guarda-chuva da segurança cibernética da Cisco

Aprenda e experimente as soluções de segurança Cisco Secure gratuitamente

Vinte anos de negócios com Gary Becklund

por **Soledad Clar**



Por que você construiu uma carreira de 20 anos na Cisco?

Cisco para mim é uma daquelas poucas organizações onde você realmente tem a oportunidade de expandir suas habilidades sem nunca sair da empresa. Você pode mudar de função, assumir novas responsabilidades e aprender coisas diferentes, desde que esteja disposto e aberto para isto. Dá satisfação expandir sem ter que ir e fazer em outra empresa. Essa habilidade da Cisco é realmente o que me manteve aqui por 20 anos.

O que você aprendeu com a diversidade cultural que existe na América?

Em primeiro lugar, devo dizer que há muitos anos, quando comecei a interagir com a equipe latino-americana, Ghassan Dreibi e outros membros, estava realmente aberto às diferenças culturais com os Estados Unidos.

Somos uma empresa global, mas muitos de nós nos dedicamos apenas a trabalhar nos Estados Unidos, com pouca exposição e conhecimento de outras culturas. A experiência realmente abriu meus olhos para a importância das originalidades culturais. A seleção latino-americana é uma das minhas favoritas, porque os latino-americanos sempre foram as pessoas mais acolhedoras e amorosas, sempre foi uma alegria e um prazer conhecê-los.

Acredito que, se fizermos um esforço, também encontraremos estas características em outras culturas, mas nunca iremos apreciar o valor e os benefícios da diversidade cultural até que tenhamos a possibilidade de mergulhar naquele ambiente. É por isso que sou imensamente grato pela oportunidade que tive de passar muito tempo na América Latina.

Olhando para trás, qual é o maior desafio que você viu na indústria?
O maior desafio é, sem dúvida, a velocidade das mudanças que estão ocorrendo. E, como nos tornamos uma empresa muito maior, é difícil permanecermos tão ágeis e flexíveis quanto alguns de nossos concorrentes de nicho. Portanto, é um equilíbrio entre aproveitar o poder da Cisco e adotar esta velocidade de mudança e ser capaz de mudar de direção e se adaptar a esta velocidade. Acho que este é o maior desafio que pude ver na Cisco, é realmente um equilíbrio difícil.

Qual é o maior desafio que está por vir?
Vou usar um ditado: "Não sabemos o que não sabemos". Criminosos e ameaças estão em constante evolução. Vimos tantas mudanças nos últimos 5 a 6 anos em que criamos a GSSO (Global Security Sales Organization) dentro da Cisco. Olhando para trás, para como era o setor de segurança 5 anos atrás, mudamos tanto, e as ameaças mudaram tanto, que acho que o desafio será acompanhar e ficar acima destas ameaças que evoluem dia a dia.

Como é o sucesso?
Risos. Esta é uma pergunta muito boa. Lembro-me de quando entrei na Cisco pela primeira vez fiz a mesma pergunta ao meu chefe. Naquela época, éramos uma cultura diferente, mas tão importante quanto hoje. Ao fazer essa pergunta, ele olha para mim e diz: "É muito simples, no final do dia você tem que cumprir os números." Naquele momento eu ri, mas há muita verdade nisso. Acredito que cada um de nós que está na Cisco está aqui porque acredita na empresa. Acreditamos na visão e na direção que a Cisco está tomando. Então, para mim, sucesso não é sobre minha posição, meu trabalho ou reconhecimento, embora todos nós gostemos de reconhecimento. Sucesso é sobre a certeza de saber que fiz tudo o que podia para contribuir a cada trimestre para o sucesso da Cisco. Quando isto acontece, me sinto bem-sucedido. Me orgulho da Cisco quando alcançamos os resultados e os números. Então, para mim, sucesso é como a sensação de ter contribuído para a empresa a cada quadrimestre.

Quando você se sente mais valorizado em termos de relacionamento com o cliente?
Devo dizer que é quando estamos à mesa discutindo resultados de negócios e não soluções de tecnologia. Porque aí sinto que conquistamos a confiança do cliente como empresa, como equipe de trabalho e também como pessoa, aí sinto que somos um parceiro de negócio do cliente e não apenas um fornecedor de tecnologia.

O que produtividade significa para você hoje?
A produtividade tem vieses, depende da função que desempenhamos aqui na Cisco. Como seria de se esperar, no setor de vendas, produtividade significa atingir os números exigidos. Por outro lado, produtividade dentro do SBG (Security Business Group) tem um significado diferente: tem a ver com inovação, com rapidez e time-to-market para atender às necessidades dos clientes. Portanto, o significado e a definição de produtividade dependem muito do papel e da função que cada um desempenha na empresa.

Qual é a maior preocupação de segurança?
Acho que voltaria a um comentário que fiz anteriormente, quando mencionei "não sabemos o que não sabemos", à medida que as ameaças evoluem. Minha maior preocupação com o setor de segurança cibernética tem a ver com a capacidade do setor de se manter um passo à frente da evolução das ameaças e dos cibercriminosos.

Qual é a fraqueza mais comum que atrapalha o sucesso?
Permitir que os erros te paralisem. Na Cisco, dizemos: "se você vai falhar, que seja rápido". Erros e falhas acontecerão com todos nós, mas o que fazemos com estas falhas podem tanto nos sufocar quanto alimentar a nossa capacidade de ser bem-sucedido. Então, o que fazemos com os erros e como lidamos com eles é o que mais contribui para o sucesso.

O que torna alguém um bom líder?
Em primeiro lugar, um líder lhe dá poderes para fazer seu trabalho. Eles têm a segurança e a confiança para permitir que você se desenvolva em sua função e execute o trabalho para o qual foi contratado. Um líder também mostra empatia quando os erros acontecem e irá motivá-lo.
Então, para mim, ele é alguém que nos fortalece no nosso trabalho, que mostra empatia quando nos deparamos com obstáculos e está lá para nos encorajar, orientar e motivar quando precisamos.

Compartilhe conosco alguns conselhos para quem deseja crescer em sua trajetória dentro da empresa.
Lembro-me de um evento para líderes em San José, por volta de quando a Cisco adquiriu a TANDBERG (2009 de acordo com https://www.cisco.com/c/en/us/about/corporate-strategy-office/acquisitions/acquisitions- list- names.html). A essa altura, Chuck Robbins e Mark Patterson dirigiam os escritórios americanos. Chuck e Mark foram ao jantar dos líderes que estávamos realizando e no final houve uma sessão de perguntas e respostas (perguntas e respostas). Então, um dos gerentes perguntou a Chuck sobre sua carreira na Cisco e como ele chegou onde estava. Então Chuck disse que, se olhasse para trás, perceberia que muitas vezes, na corrida, somos solicitados a fazer coisas e às vezes apenas nos levantamos e fazemos. E temos que nos mover horizontalmente ou lateralmente na empresa antes de subir. E eu incorporei essa ideia na minha carreira. Se eu olhar para trás, realmente aproveitei o que Chuck disse e comecei a me desafiar assumindo diferentes posições de liderança dentro da empresa, algumas até novas e desconfortáveis para mim, que era um líder de vendas. Foi uma grande virada na Cisco. Então, eu motivaria todos a experimentar coisas novas dentro da empresa, para expandir suas experiências e capacidades, porque é aí que você se torna um recurso mais valioso para a companhia. E, agora que estou me aposentando, gostaria de pensar que fui um recurso valioso. Mas, o que é mais importante, que a Cisco foi um recurso inestimável para meu aprendizado e crescimento

Imagen: Free-Photos, Pixabay

Estúdio de resultados em matéria de segurança de 2021: edição para pequenas e medias empresas.

Cresça com uma estratégia de segurança digital sólida

O Cisco 2021 Security Outcomes Study reúne as experiências de mais de 4.800 profissionais de TI, segurança e privacidade de todo o mundo e é um recorte, de um estudo maior, focado em pequenas e médias empresas (PMEs).

Se defender de ameaças cibernéticas é difícil para qualquer empresa, independentemente do tamanho. Mas é particularmente desafiador para as PMEs, porque seus recursos são frequentemente limitados e elas devem se concentrar fortemente em fazer investimentos que gerem resultados impactantes. As apostas são maiores e priorizar o que é mais importante é fundamental para o sucesso. Ajudar a identificar estas prioridades é o objetivo deste relatório.

Detalhamos aqui os pontos mais relevantes.

Resultados do estudo

Coisas boas vêm de onde menos se espera: Casos convincentes em que o tamanho reduzido da empresa não impede a possibilidade de grandes ganhos no desenvolvimento de abordagens de segurança bem-sucedidas.

A segurança das PMEs tem a ver com os negócios: Este estudo destaca o conceito de que a segurança e os negócios em geral compartilham um relacionamento integral no caso das pequenas e médias empresas.

Prioridades: Pequenas e médias empresas que relataram ter uma estratégia forte para orientar as iniciativas de segurança foram substancialmente mais propensas a relatar resultados bem-sucedidos.

O sucesso está na preparação para o fracasso: Entre as 25 práticas de segurança comprovadas, os recursos de recuperação rápida de desastres foram o maior diferencial de sucesso não só entre pequenas e médias empresas como em organizações maiores. O planejamento para resiliência é uma estratégia vencedora.

Ameaças modernas exigem tecnologias modernas: As PMEs que mantiveram uma pilha de tecnologia moderna alcançaram taxas de sucesso mais altas em cada um dos 11 resultados de segurança medidos.

Os resultados que demonstram os fatores de sucesso em pequenas e médias empresas são organizados em três categorias:

- tornar os negócios possíveis;
- gerenciar risco;
- operar com eficiência.

Convidamos você a acessar essas conclusões a partir daqui

CISCO

SECURE

The bridge to possible