Ano 1. Número 3.

Bridge

cisco SECURE

Cibersegurança

Especial
Mulheres na cibersegurança

Contraponto
Taekwon-Do e Cibersegurança

Colômbia
Transformação digital segura em saúde

Conteúdo audiovisual

CISCO Partner

OCP TECH

OCP.TECH

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

T +1.305.537.0800
F +1.305.537.0704

info@ocp.tech

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

T +507.387.7300

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

T +886.953.656.967

Editorial

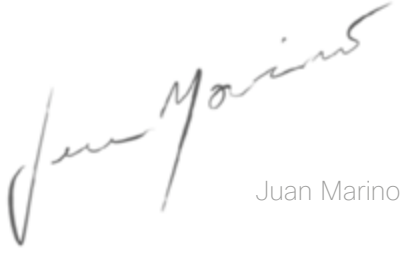
Durante anos, uma ideia muito simples assombrou minha cabeça, mas com um enorme poder de transformação: “cada pessoa está em uma posição única, privilegiada e irrepetível para ter sua melhor ideia.” A chave está no pronome possessivo “su”. O acúmulo de experiências, conhecimentos e desejos que nos diferenciam como indivíduos configuram a chave de acesso a essa ideia, que é como o fruto maduro que alguém pode alcançar antes de qualquer outro.

Sobre esta base, acredito que o verdadeiro significado de honrar a diversidade está em reconhecer o valor extraordinário da singularidade e capacitá-la de forma colaborativa, para inovar e resolver qualquer desafio que devemos enfrentar como uma comunidade.

A expulsão dos diferentes condena-nos não só a uma pobreza social e espiritual, mas também, desde uma lógica produtiva, a limitar as nossas possibilidades de inovação.

Nesta terceira edição de Bridge continuamos a enriquecer-nos na pluralidade de vozes e na procura da sabedoria, traçando pontes entre disciplinas que podem parecer tão divergentes como as artes marciais ou o trabalho dos Bombeiros Voluntários, mas que convergem, mais do que isso pode suspeitar, nos princípios que regem a cibersegurança.

Espero que esta leitura o alimente e o aproxime ainda mais de sua melhor ideia e que, ao virar a última página, você sinta o desejo de unir sua voz às vozes de mulheres e homens que compartilham suas perspectivas nesta publicação.



Juan Marino

Imagem: Pexels, Pixabay

Staff

Produção Integral
Basanta Contenidos

Diretor Editorial
Karina Basanta

Diretor de Arte
Nicolás Cuadros

Coordenador
Andrea Lecler

Produção audiovisual
Salpufilms

Colabore nesta questão
Silvia Montenegro,
Marta Pizzini, Jorge Prinzo

Fotografía e ilustración
Basanta Contenidos
Freepik
Pixabay

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

Foto de Capa
Alexandr Ivanov, Pixabay

Diretor Editorial
Karina Basanta

Diretor de Arte
Nicolás Cuadros

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

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

Cisco Latinoamérica

Director de Operações
de Cibersegurança
Ghassan Dreibi

Líderes Regionais
de Cibersegurança

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

Editor Geral
Juan Marino

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

Marketing

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

Bridge Nº 3

Sumário

VU

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

CISCO Engage

Brasil

Novas oportunidades: A democratização dos serviços financeiros na era da experiência.

Mais dados. Mais usuários móveis. Mais aplicações. Mais complexidade. Prepare-se para o futuro do banco digital com a Cisco. Estamos vivendo um momento inédito: nunca foi tão fácil o acesso a serviços financeiros. Milhões de brasileiros, que antes eram desbancarizados, hoje fazem parte de um grupo que já nasce digital.

Mais dados. Mais usuários móveis. Mais aplicações. Mais complexidade. Prepare-se para o futuro do banco digital com a Cisco. Estamos vivendo um momento inédito: nunca foi tão fácil o acesso a serviços financeiros. Milhões de brasileiros, que antes eram desbancarizados, hoje fazem parte de um grupo que já nasce digital.

Temário

PIX e OpenBanking

Painel sobre tecnologia, finanças e varejo **com João Bezerra e Ricardo Guerra-Itaú, Marino Aguiar (Santander), Jean Sigrist (Neon), e Carlos Alves (Riachuelo).**

Colaboração e o trabalho remoto

A complexidade pós-pandemia com times híbridos, **com Thiago Santanna (Cisco) e Estevam Carvalho (BTG Pactual).**

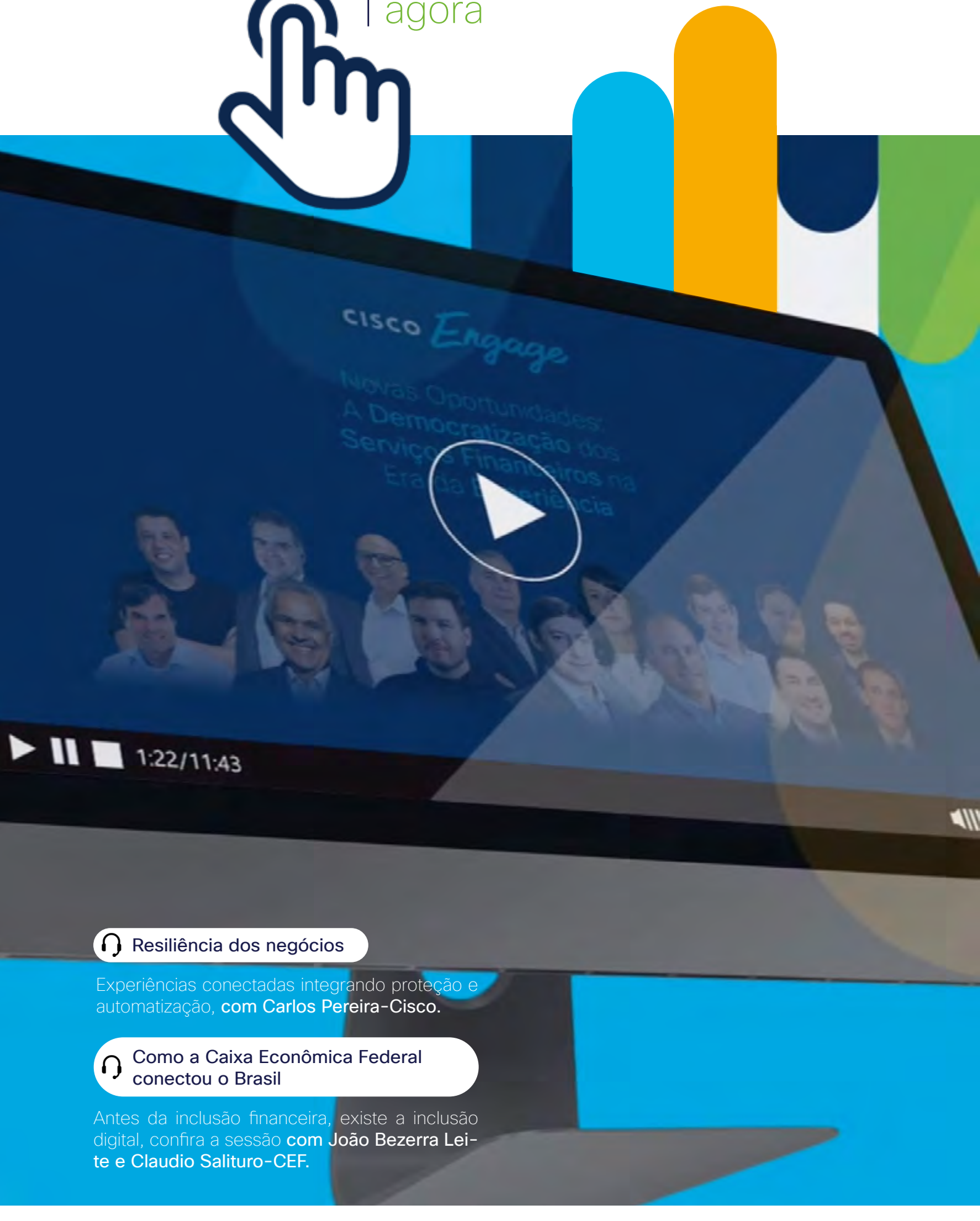
Transformação digital

A experiência do usuário e o crescimento exponencial da XP, **com João Valentin (AppDynamics), Eduardo Berti e Marcelo Vidu (XP Inc.).**

Maturidade em segurança

Como a tecnologia pode nos ajudar na retomada da economia, **com Ghassan Dreibi (Cisco Secure) e Renato Augusto (Bradesco).**

clique aqui | Assista agora



Resiliência dos negócios

Experiências conectadas integrando proteção e automatização, **com Carlos Pereira-Cisco.**

Como a Caixa Econômica Federal conectou o Brasil

Antes da inclusão financeira, existe a inclusão digital, confira a sessão **com João Bezerra Leite e Claudio Salituro-CEF.**

Em uma agradável palestra, Esteban Lus Bietti, CTO do Banco Supervielle, e os chefes do Corpo de Bombeiros Voluntários, General Sarmiento, Major Carlos Ramírez e Major Salvador Capano, encontram terreno comum em seus trabalhos. Tarefas diferentes, mas realizadas com a mesma responsabilidade, rapidez e paixão.

Imagem: Basanta Contenidos

Conversa

com os Bombeiros Voluntários de San Miguel

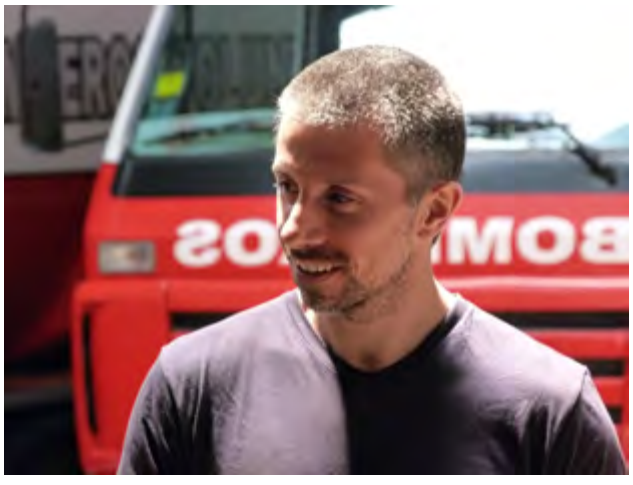
texto: **Silvia Montenegro**

vídeo: **Lus Bietti Ramírez Capano**

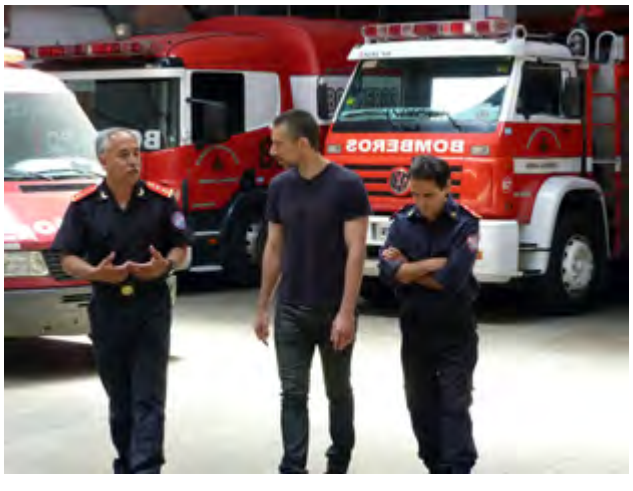
Hoje, em geral, organizações e empresas dependem de suas capacidades tecnológicas e de planos de contingência e serviços de proteção que garantem segurança para neutralizar riscos e oferecer confiança para resistir a um possível ataque cibernético. Além de elaborar planos de ação robustos, com normas, regras, protocolos, métodos e conhecimento da legislação vigente, os especialistas em tecnologia e cibersegurança devem estar preparados para "apagar incêndios digitais", relatar atividades suspeitas online, implementar estratégias de sustentação ou retomar um ambiente online seguro, manter e promover uma cultura de segurança digital.

Neste sentido, e respeitando as grandes diferenças, pode-se dizer que o trabalho dos responsáveis por tecnologia e cibersegurança está relacionado ao trabalho crítico do Bombeiro, profissional que realiza programas de segurança contra incêndio ou acidentes, a fim de salvar vidas e bens materiais.

Por isto, quando Esteban Lus Bietti, diretor de Tecnologia (CTO) do Banco Supervielle, o Major Comandante Carlos Ramírez, chefe do Quartel dos Bombeiros Voluntários General Sarmiento, e o Comandante Salvador Capano, 2º Chefe do Quartel, se reuniram. A conversa, fluente, destacou muitos pontos comuns. O encontro aconteceu nas instalações do Corpo de Bombeiros Voluntários General Sarmiento, em San Miguel, Província de Buenos Aires.



Esteban Lus Bietti
Quero te agradecer por este encontro. É a primeira vez que entro em um Corpo de Bombeiros. Acho que temos muitas coisas para trocar, compartilhar e aprender uns com os outros.



Carlos Ramírez
É um prazer conhecer aqui, conversar e compartilhar as experiências vividas nos serviços e trocar ideias.

Salvador Capano
O Quartel é nossa segunda casa. A comunidade se identifica muito com a gente, com o Corpo de Bombeiros. As pessoas se aproximam, veem como estamos equipados. Explicamos a eles que os recursos são muito importantes e que temos o que é justo e necessário para fazer frente às emergências, sempre enfatizamos isso.

Esteban Lus Bietti
Sim, os recursos são muito importantes, embora às vezes possam ser limitados, enquanto as tarefas que devemos realizar não o são. Pelo contrário, são muitas e de diferentes tipos. Temos que colocar muita cabeça e coração. Imagino que possa falar longamente sobre isto, porque são Bombeiros Voluntários...

Carlos Ramírez
Sim, nosso trabalho é especial. Nada é agradável para nós, conhecemos a dor do povo, o seu sacrifício, vemos as perdas que nos causam. Também temos a oportunidade de divulgar, de treinar. A parte humana é muito importante. Muitos de nós treinam o Bombeiro para que os elementos tenham o melhor desempenho, para otimizar o material disponível, para que o equipamento fique em operação por muito tempo. Comunicamos nossas necessidades às autoridades do Partido San Miguel. Eles nos ouvem, estamos em contato direto com a equipe técnica, que sabe da importância da prevenção. Agora, antes de aceitar um projeto, eles nos perguntam o que adicionar para segurança. Se houvesse um incêndio, quais elementos são necessários. Sei que é mais ou menos o que você também aplica na sua empresa...

Esteban Lus Bietti
Me sinto totalmente identificado, porque muitas vezes a gente tem que conseguir um orçamento para fazer algo que acaba sendo derivado para outra coisa que, a princípio, é mais importante até que aconteça alguma coisa, como você diz. Para nós também é muito importante trabalhar na prevenção do fato. Primeiro, porque é mais barato, é mais fácil remediar e ajuda a gente, como empresa, e o cliente final. E no seu caso toda a sociedade, que não precisa fugir e desperdiçar recursos. Para nós, é importante tentar gerar valor e participar desde o início do processo, quando as decisões são tomadas. Nesta fase, podemos projetar como eles são construídos ou quais medidas devem ser levadas em conta. E nos permite prevenir ao invés de agir ou reagir quando um incidente acontece. Devemos também ver como seguimos os procedimentos, o que fazer em cada caso. Não só é importante prevenir, mas uma vez que o evento se materialize ou aconteça, devemos saber qual é a primeira coisa a fazer, a quem devo ligar ou avisar para tentar não ocultar o que aconteceu, mas dar visibilidade para que ações possam ser tomadas e o incidente resolvido com o menor impacto possível. Eles devem ter muita experiência.

Salvador Capano
Sim, o recurso é importante e precisa ser modernizado. Hoje existe tecnologia, avanço, conforto. E nos Bombeiros, por meio do recurso e de protocolos, temos que ser atualizados e modernizados com tecnologia de ponta. Na área de combate a incêndios, devemos estar muito bem equipados, mas também devemos considerar que o equipamento tem validade. Hoje, os incêndios são de altíssima velocidade ou propagação, por isto, não podemos ter uma equipe treinada sob uma norma de cinco anos atrás. Precisamos acessar os equipamentos mais modernos para podermos enfrentar o incêndio sem mesmo saber que tipo de material está queimando, se madeira ou papel. Hoje se queima madeira, papel, ácido, plástico, cortiça, sintéticos, e tudo com um efeito de caça. Por isto os equipamentos de cinco anos ou mais não servem. Isto vale para uma escada rolante. Antes havia prédios de até 10 andares, hoje temos prédios de 25 andares. Então, temos um recurso muito caro, importante, caro de manter, mas em alguns casos obsoleto. As pessoas dizem que tem uma escada boa, mas se soubessem que somos limitados... Chegamos ao 8º andar e temos prédios de 20 andares.

Imagem: Ulrike Leone, Pixabay

Esteban Lus Bietti
No campo da segurança cibernética, uma das frases mais conhecidas é que o elo mais fraco é o usuário, portanto, o que podemos fazer é conscientizar as pessoas. Posso colocar várias medidas de segurança, mas se o usuário clicar ou entrar nos sites que ele não precisa entrar, a segurança acaba sendo violada e ocorre algum tipo de ataque. Como você convence o usuário? Como eles são treinados?

Carlos Ramírez
Você disse uma palavra importante. Trem. No momento em que algo aconteceu, devemos transmitir o motivo para evitar que volte a acontecer. E que as pessoas capitalizem com isto. Quando acontecer, sabendo como posso atacá-lo e, ao mesmo tempo, divulgar para que não se repita. Prevenção é treinamento e é isto que buscamos agora. A Prefeitura entendeu que a única forma é divulgar. Como fizemos isso? Por meio de relatórios, fotos, dados sobre os pontos fracos de uma construção e onde o fogo avança mais forte. Estamos fazendo o mesmo com a população. Nosso quartel tem pessoas que treinam em Reanimação Cardiopulmonar (RCP), e por lá já passaram 5 mil pessoas. Dizemos a vocês que hoje qualquer um é útil para colaborar com nosso trabalho na primeira instância do evento, na primeira cena. Em caso de incêndio, a primeira coisa a fazer é chamar imediatamente o Corpo de Bombeiros ou Emergência, pois o tempo é precioso. Há uma corrente que deve ser seguida e não pode ser cortada. O primeiro a ver o fogo tem que chamar. Assim que o sistema de emergência chega, a corrente é fechada.

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

Salvador Capano
As informações que damos são importantes para a comunidade. Informamos o vizinho. Aqui estão as áreas mais precárias e sabemos que talvez a casa não tenha extintor de incêndio, mas dizemos ao vizinho para ter um balde de areia, um balde de água, para abrir as janelas, para não jogar bitucas de cigarro no lixo. Estatisticamente, essa ação dá bons resultados. Internamente, prestamos muita atenção ao treinamento, que é obrigatório e constante. O Bombeiro não treinado não pode cumprir a função. Se temos equipamentos de última geração e não sabemos como usá-los... Em primeiro lugar, a segurança do bombeiro e a prestação do serviço, que é o nosso objetivo, salvar vidas e bens.

Imagem: Shutterbean, Pixabay

Carlos Ramírez
Portanto, o capital humano é importante. Depois de cada evento, temos que trabalhar com as pessoas. É nossa maior tarefa. Os bombeiros são treinados e seguimos os protocolos de cada classe de serviços. Não estamos preparados para perdas humanas. Quando há tragédias com perda de vidas, temos que trabalhar com os bombeiros para que voltem a atuar. Eles têm que estar muito preparados para não colocar a si próprios e seus colegas em risco.

Esteban Lus Bietti
Seu trabalho, onde vidas estão em jogo, tem um grande nível de complexidade. Nosso trabalho é parecido em muitos aspectos, como temos conversado, mas é claro que tem a ver com o trabalho com as máquinas e com as pessoas que fazem parte da equipe. Nesse sentido, é fundamental ter uma equipe consciente, treinada, motivada.

Escuta atenta foi uma das características mais salientes desta conversa.

Salvador Capano
Você disse outra palavra fundamental. Equipe. Somos seis que vão para as ruas, se um falha, todos nós falhamos. Alguns de nós podem saber mais sobre algum assunto, mas todos são fundamentais. E uma pessoa sozinha não apaga o fogo. Um corta a luz, outro resgata a vítima, tem um que aciona o carro de bombeiros e outro que puxa a mangueira. Somos uma equipe. Se um cair, temos que substituí-lo por alguém treinado e preparado. Não queremos heróis em uma placa de latão. Queremos uma equipe em que cada um atue. Todas as tarefas são importantes e, além disso, todos conhecemos todo o trabalho, porque fazemos rodízio. Hoje posso puxar a mangueira e amanhã tenho que me pendurar em uma corda resgatando a pessoa ou manejando o carro de bombeiros. Com as perdas humanas, a situação se complica. Embora o bombeiro tenha dado tudo, às vezes fica complicado. E é inevitável que o Bombeiro saia.

Carlos Ramírez
Nuestro lema es salen seis, vuelven seis.

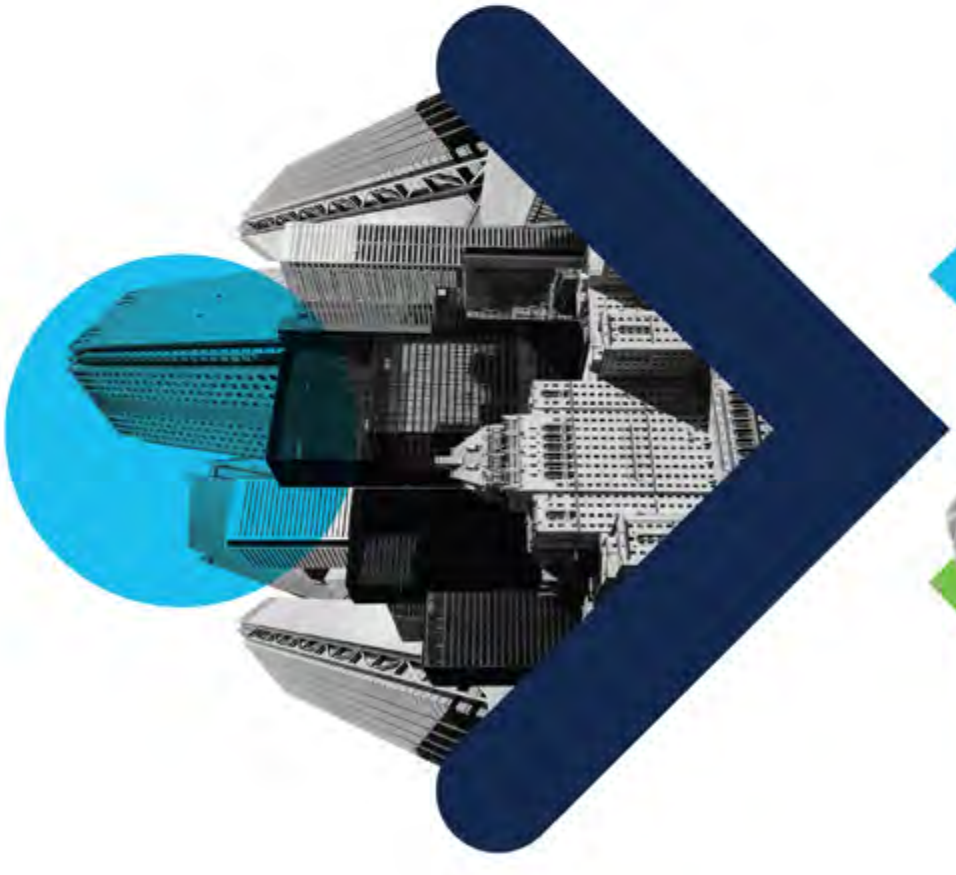
Esteban Lus Bietti
Muito interessante tudo o que compartilharam conosco. Agradeço o trabalho que você faz e por conversar neste momento. Aproveito muito para pensar e refletir e ver o que posso aplicar na minha equipe. Se pudermos trabalhar como bombeiros, certamente seremos melhores do que antes

CISCO
SECURE X

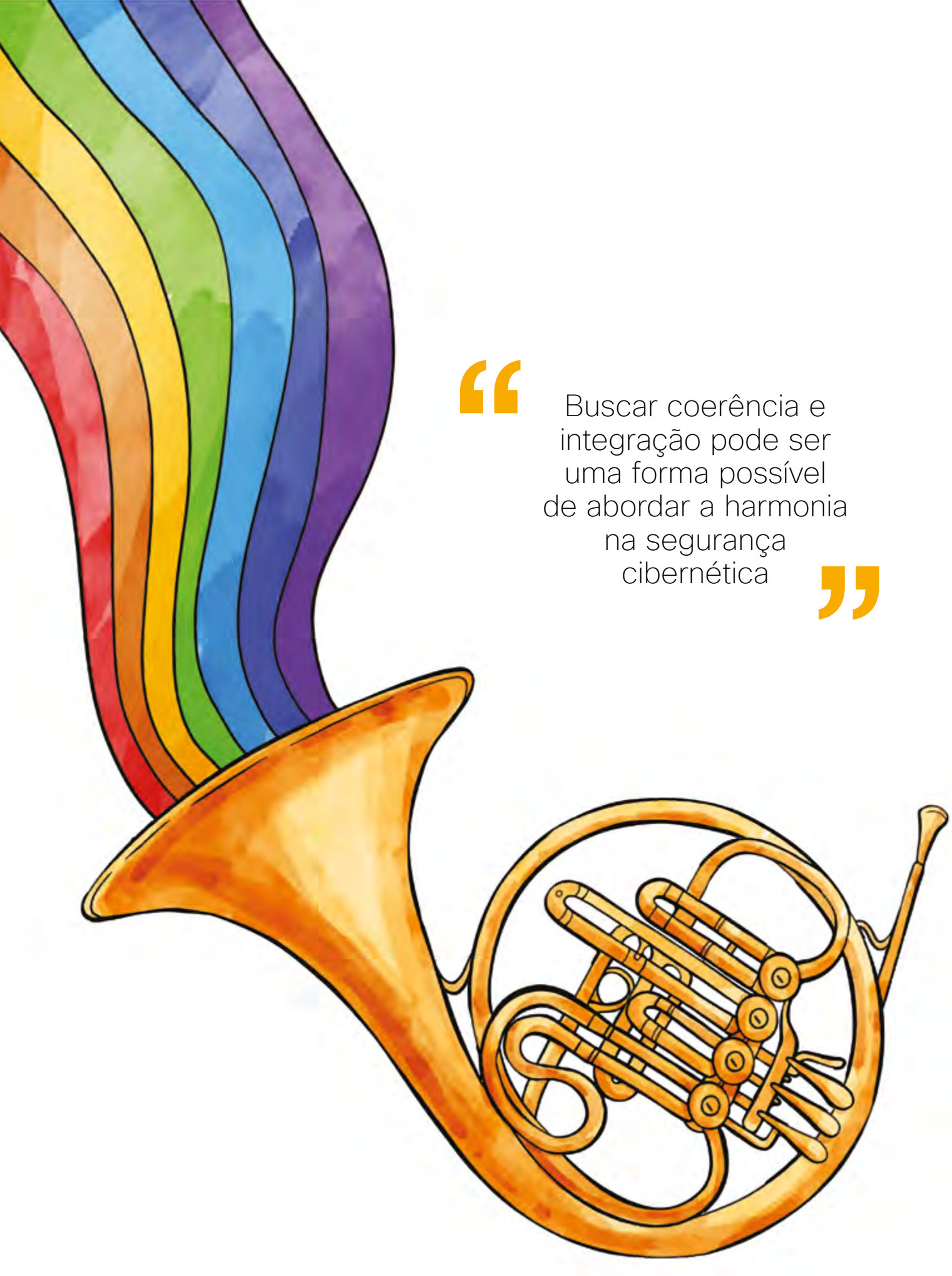
Experiência simplificada

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



CISCO The bridge to possible



> Buscar coerência e integração pode ser uma forma possível de abordar a harmonia na segurança cibernética

Imagem: Designed by Freepik

O desafio da harmonia

por **Walter Montenegro**

Harmonia é um termo comumente utilizado para descrever ou definir uma situação equilibrada, confortável, agradável, onde os elementos que a compõem estão perfeitamente alinhados naquele momento preciso, e que muitas vezes se deseja, para o bem-estar, manter ao longo do tempo. A palavra deriva do grego e significa acordo. De uma perspectiva geral, harmonia é o equilíbrio de proporções entre as diferentes partes de um todo, e seu resultado sempre denota beleza.

Na música, harmonia é o estudo da técnica de construção e ligação de acordes (notas simultâneas), bem como das progressões e princípios de conexão que os regem. Ele também cobre conceitos como ritmo harmônico. Ou seja, com a música, também temos a possibilidade de gerar harmonia, de produzir estes espaços agradáveis e de bem-estar, seja com um ou vários instrumentos.

Vamos pensar, por um momento, em uma peça musical complexa como um concerto, com vários instrumentos tocados ao mesmo tempo. Podemos ouvir alguns timbres claramente e outros podem passar despercebidos, porém todos juntos trarão beleza ao trabalho. As emoções começarão a fluir em comunhão com a percepção dos sons. Vamos imaginar que, de repente, um dos instrumentos comece a interpretar outra peça musical, em outro ritmo, em outro tom. Por mais insignificante ou mínimo que seja a participação deste instrumento, a harmonia será quebrada, as emoções passarão de algo agradável para algo totalmente incômodo e, com certeza, deixaremos de ouvir.

Na cibersegurança, como na música, precisamos ter harmonia. Se o nosso objetivo é reduzir os riscos, cada "instrumento" deve estar em sintonia com o seu par, com o qual se comunica e compartilha informações para gerar a colaboração necessária entre eles.

Muito se tem falado na indústria, nos últimos tempos, sobre o incrível número de soluções de segurança cibernética no mercado. Se nos referirmos à última Pesquisa de Benchmark CISO, 86% das empresas pesquisadas declararam ter entre 1 e 20 marcas fornecedoras para este segmento. Em outras palavras, é claramente mais complexo gerar a harmonia que buscamos entre 20 "instrumentos" do que apenas alguns.

Assim como na música, onde quanto mais instrumentos interagem, mais é necessário um maestro para conduzi-los, o mesmo acontece na segurança cibernética. O crescente número de soluções exige que haja um "condutor" que as organize, ordene os seus relatórios e por último permita a harmonia necessária para investigar um incidente num tempo limitado e responder rapidamente às ameaças detectadas por qualquer uma das soluções.

O desafio não é simples, mas devemos trabalhar nesta direção, em busca de coerência, confiança, integração, com o único propósito de nos aproximarmos da tão esperada "harmonia" da cibersegurança

SASE

Tudo o que você precisa saber sobre SASE (Secure Access Service Edge)

clique aqui

O que é SASE?

O Secure Access Service Edge (SASE) é uma arquitetura de rede que combina recursos VPN e SD-WAN com recursos de segurança nativos da nuvem, como gateways da web seguros, agentes de segurança de acesso à nuvem, firewall e acesso à rede de confiança zero. Estas funções são fornecidas a partir da nuvem pelo provedor SASE na forma de serviço.

Por que SASE?

Com a transformação digital das empresas, a segurança está migrando para a nuvem. Isto está gerando a necessidade de serviços convergentes para reduzir a complexidade, melhorar a velocidade e agilidade, habilitar redes com várias nuvens e proteger a nova arquitetura habilitada para SD-WAN.

Para que SASE?

O modelo SASE consolida inúmeras funções de rede e segurança, tradicionalmente entregues em soluções pontuais em silos, em um único serviço de nuvem integrado. Ao consolidar com SASE, as empresas podem:

- Reduzir custos e complexidade.
- Providenciar orquestração centralizada e otimização de aplicativos em tempo real.
- Ajudar a garantir o acesso perfeito para os usuários.
- Permitir acesso móvel e remoto mais seguro.
- Restringir o acesso com base no usuário, dispositivo e identidade do aplicativo.
- Melhorar a segurança aplicando uma política consistente.
- Aumentar a eficácia do pessoal de segurança e de rede com gerenciamento centralizado.

Como adotar o SASE?

O Gartner vê o SASE como uma visão para um futuro modelo de rede corporativa segura. Atualmente, esta não é a realidade de nenhum provedor. Hoje, o SASE é melhor representado pela convergência de SD-WAN gerenciado na nuvem e de segurança fornecida na nuvem.
A mudança para um modelo SASE será um processo gradual à medida que a TI reconsidere como conectar uma força de trabalho remota aos recursos de informação distribuídos de que precisam. Também é provável que haja uma demanda crescente por modelos de aquisição “como serviço” que ofereçam mais flexibilidade

Por que escolher a Cisco para adotar o SASE?

"SASE se refere à união entre networking e segurança, lado a lado. Isso me lembra quando, há alguns anos, a Cisco reuniu a rede de dados e a rede de voz, que estão totalmente integradas para nossos clientes hoje.
Já vimos este tipo de fusão, e a experiência de tantos anos nos permite ser mais eficazes, ter maior controle e visibilidade, mantendo uma arquitetura flexível para o futuro. SASE é a mesma jornada, a mesma jornada em que a Cisco tem ajudado seus clientes por 30 anos."

Vann Walters, VP, Vendas de Segurança nas Américas, Cisco.

"Porque adotar o SASE significa fazer uma jornada e, na Cisco, estamos nessa jornada há anos, todos os dias, ao lado de nossos clientes. A Cisco sempre focou na experiência do cliente e na prestação de serviços de qualidade e excelência. Em termos de nuvem, o que fizemos na América Latina, com o apoio da nossa organização em todo o mundo, foi criar uma infraestrutura local. Temos uma extensão de serviços globais na nuvem, e fazemos parte deste grande provedor para oferecer este tipo de soluções. Estamos dando aos nossos clientes uma melhor latência, uma melhor experiência. Se algo acontecer, temos um acordo de nível de serviço (SLA), um processo diferente de entrega de serviço, totalmente transparente para nossos clientes, muito diferente de outras ofertas de nuvem que só oferecem servidores muito básicos sem um alinhamento adequado, sem um processo de resiliência no negócio".

Ghassan Dreibi, Diretor de Operações de Cibersegurança, LATAM, Cisco.

"Nossa abordagem SASE ajuda as organizações a proteger o acesso, não importa onde residam os usuários e aplicativos, combinando segurança nativa da nuvem e recursos de rede fornecidos em modelos de consumo flexíveis 'as-a-service'.
Com foco na experiência do usuário, proteção de dados e simplificação das operações, somos um verdadeiro parceiro para nossos clientes em sua jornada para implementar aplicativos em ambientes multi-nuvem".

Juan Pablo Mongini, Chefe de Vendas de redes corporativas na LATAM, Cisco.

"Para cumprir a promessa do SASE, há uma infraestrutura e arquitetura de tecnologia 'nos bastidores' que difere profundamente entre os fabricantes. As empresas em transição para o SASE devem se aprofundar nisto, especialmente para reconhecer que a eficácia da segurança transcende a prevenção e depende da detecção e resposta em tempo hábil às ameaças que ocorrerão. Por outro lado, se o SASE aborda uma convergência da rede e da segurança e o Gartner recomenda 'idealmente um único fornecedor que possa oferecer a maioria dos componentes do SASE, fica claro que muito antes da proeza do conceito, a Cisco estava construindo as bases do que agora é denominado desta forma'".

Juan Marino, Gerente Regional para a LATAM, Cisco.

Ad content

Experiência de Edesa com Braycom

Imagem: Ananitit-Pixabay

Em primeira pessoa

por: **Diego Máspero**

Engenheiro de Sistemas e CIO da Edesa, Salta, Argentina.

Era 2016 quando na Edesa tomamos a decisão, e o risco, de fazer o que tínhamos que fazer: adaptar e otimizar nossos sistemas de TI. O desafio de melhorar o desempenho, reduzir os custos operacionais, obter maior confiabilidade da infraestrutura e facilidade de uso ficou claro desde o início. Este objetivo tornava iminente a migração de toda a infraestrutura do nosso data center, e as tarefas a serem realizadas implicavam muitas e grandes mudanças:

- Servidores com tecnologia Intel.
- Armazenamento para nova tecnologia SDS (Software Defined Storage).
- Unificação de hipervisores em VMware.
- Backup de HW para disco (facilidade de fazer futuras migrações) e backup de SW para Veeam (tecnologia simples de usar e amigável que já conhecíamos).
- Rede de alta capacidade.
- Sistemas operacionais de servidor para Linux e Windows Server.
- Motor BD Oracle 12g.

Foi neste contexto que analisámos o know-how de tecnologias que a Braycom tinha à disposição e trocávamos informações com eles. Ficamos satisfeitos em descobrir que eles tinham amplo conhecimento em VMware, rede e segurança, uma combinação rara no mercado de um único fornecedor.

Com o passar das reuniões, percebemos que a Braycom tinha algo diferente dos outros fornecedores que conhecíamos, percebemos que eles se sentaram ao nosso lado e analisaram as propostas a oferecer de um ponto de vista semelhante ao nosso, não tão interessados em vender um produto, mas para resolver o problema da melhor maneira e o mais economicamente possível.

Juntos, traçamos as expectativas econômicas, de desempenho, funcionalidade, facilidade de atualização, facilidade de uso e suporte após a entrada em produção. E, em todos os casos, todos os requisitos foram atendidos e superados.

Hoje temos uma solução totalmente redundante e um esquema ativo-ativo que nos permite ter um plano de continuidade de negócios (BCP), impensável com a infraestrutura que tínhamos anteriormente.

Ter um parceiro tecnológico estratégico como a Braycom, que está focado em como nos ajudar a resolver nossos problemas com um orçamento limitado como o que estamos acostumados em nosso país, nos permite enfrentar novos projetos como, por exemplo, viajar na jornada SASE em termos de cibersegurança, ou seja, a montagem de um site remoto que nos permita ter todo o data center 100% operacional em menos de 24 horas, em caso de um grande desastre de destruição de ambos os data centers.
Estamos nesse caminho

Taekwon-Do e Cibersegurança

Contraponto

texto: **Silvia Montenegro**
vídeo: **Juan Marino**

O que é Taekwon-Do?

Um método poderoso de combate desarmado. Uma arte marcial moderna enraizada em uma antiga tradição guerreira. Um estilo de vida. Nesta nota, Juan Marino entrevista o grão-mestre Néstor Galarraga.

Com o objetivo de mergulhar na essência do Taekwon-Do, que a partir de suas diretrizes se propõe a percorrer um caminho interior rumo à "sabedoria na mente, força no corpo e pureza no coração", Juan Marino, gerente regional de Cibersegurança da Cisco, visitou o Grão-Mestre Néstor Galarraga, que dirige uma organização com mais de 200 mil praticantes e é uma referência não só no esporte em si, mas também no seu ensino e divulgação. Seus trabalhos em diferentes áreas do Taekwon-Do são reconhecidos no meio internacional e valorizados por sua seriedade e originalidade.

No início do encontro, Juan Marino expressou a grande honra de desfrutar aquele momento e conversar com o autor do livro "El Poder del Guerrero", publicado pela Editora Tequisté em plena quarentena plena da COVID-19, e que inclui as reflexões, anedotas e conceitos do atleta argentino, após uma grande carreira: "Li seu livro com atenção, mas não posso deixar de lhe perguntar exatamente onde reside o poder do guerreiro?"

Para Néstor Galarraga, é uma construção interna, que fortalece o exterior e ilumina uma poderosa descoberta pessoal: "O verdadeiro poder está dentro. Aprender a se defender é um caminho pelo qual, irreversivelmente, se acaba introspectivo".

Tática e Estratégia

O paralelismo entre esporte e cibersegurança, que foi a hipótese que aproximou o representante da Cisco do Dojang-espaço físico para treinos de Taekwon-Do, foi revelado desde o início do encontro: "na cibersegurança nos defendemos de um atacante e de uma organização criminosa. Neste meio de defesa há muitas coisas a fazer. Em nosso campo dizemos que o atacante tem táticas, técnicas e procedimentos, como você joga isso no Taekwon-Do?

Federico Teissandier e Gonzalo Hauri
durante uma prática para ilustrar a entrevista.

Conteúdo audiovisual
com demonstração prática.

Integridade
Perseverança
Autocontrole **Cortesia**
Espírito indomável

O Grão-Mestre explicou que a abordagem é semelhante: "há uma estratégia geral, depois há a tática, que intervém para aplicar diferentes partes desta estratégia, que é, eu diria, universal. Existem 2 mil combinações de técnicas manuais e 1.800 combinações de técnicas em pé. Então, é muito amplo falar de estratégia, porque você tem que levar em consideração o contexto. Não é a mesma coisa se defender dentro de um transporte público ou em casa, não é a mesma coisa estar sozinho ou acompanhado de seus filhos. Se você sofrer uma agressão e estiver acompanhado de sua família, a reação defensiva é limitada. E se você estiver sozinho, talvez possa se dar a oportunidade de criar uma situação na qual você pode reagir e se defender, especialmente quando a integridade é percebida como estando em risco".

Percepção e Disciplina

Juan Marino fez uma consulta sobre a "fantasia" que costuma rodear as artes marciais e coloca o especialista como alguém capaz de enfrentar, com sucesso, qualquer situação perigosa: "Como você vê? Como é se preparar para o desconhecido? Na cibersegurança, de alguma forma, acontece a mesma coisa conosco, não sabemos como eles vão nos atacar...", consultou.

"É certo. Quando comecei a praticar, tive a ilusão de poder me defender de 10 pessoas armadas. Porém, a arte marcial realmente forma como não entrar em uma situação desvantajosa, ou seja, ela prepara o seu olho, o torna muito mais sensível, e daí se revela fundamentalmente um estado de percepção em relação à violência. Ao perceber, você pode decidir muito claramente onde se posicionar".

"Imagino que esta percepção evite entrar em pânico e saber como reagir", completou Juan Marino, acrescentando que os especialistas em tecnologia não podem permanecer apenas na teoria: "As organizações mais maduras simulam cenários de ataque e defesa. Qual é o papel da simulação e do jogo em uma arte marcial?".

Néstor Galarraga explicou que no Taekwon-Do tudo é prática: "O seu desenvolvimento não se dá por meio de um livro para se aprender, mas por meio da prática. É entrar em uma comunidade onde tudo se aprende com o trabalho. Estamos intimamente ligados ao jogo, tem alguém que ataca e outro que joga para se defender, e isto leva a estados muito próximos da realidade, porque, digamos, o conceito de marcialidade é essencial para se controlar a luta. Se tomarmos essa base, preparo duas pessoas para lutar praticamente até no

Marino e Galarraga durante a conversa.

estado natural, eu tenho controle, sei que quando gerar o stop posso detê-las, e isto porque há obediência e respeito ao instrutor, sob a proteção do disciplina".

A técnica

Juan Marino destacou três eixos sobre os quais o Taekwon-Do nasce: o ataque, o contra-ataque e a antecipação; e reconheceu que, em seu campo, a cibersegurança, o contra-ataque é raro: "pode ocorrer entre governos na forma de ciberataque como um futuro de guerra. Em vez disso, podemos entender como ocorrem os outros ataques e como se antecipar a eles. Você pode ve algum exemplo do que isto significa no Taekwon-Do? "

E então Federico Teyssandier entrou na sala, vestido com seu dobok - calça, paletó, cinto. E um sofisticado "jogo" foi montado entre ele e o Grão-Mestre, que colocou em cena a filosofia do esporte, da prática, do pensamento, da ação. Através da força dos dois adversários, dos seus movimentos estratégicos, da precisão dos seus pontapés ou contra-ataques, da sua agilidade e coordenação, o domínio do corpo se desenvolveu como uma espécie de xadrez corporal, muito harmonioso e ao mesmo tempo poderoso.

Mestre Galarraga, faixa-preta e IX Dan, mostrou sua habilidade, reflexos e equilíbrio com muita generosidade e predisposição. Enquanto lutava, ele dizia: "Eu o ataco com um soco, para obter uma resposta favorável nesta situação. Agora estou em desvantagem. Ele me ataca e eu fico vulnerável. Diante desse ataque, tenho que escolher uma posição melhor para mim. Eu poderia ir, é uma posição melhor, mas temporária, porque ele vai me alcançar com o outro punho. Mas terei uma ferramenta pronta para aquela ação que meu oponente vai gerar. É uma situação de antecipação, paro quando a técnica ainda não acabou de ser executada. Se eu conseguir conectá-lo nesta posição, vou usar algo que é fantástico em todas as artes marciais, ou seja, a adição da sua força no meu punho..."

Uma coisa é colocar em palavras, outra é ver. Neste jogo com o adversário, ele marcava movimentos de contra-ataque, técnicas lineares, formas de controle: "Tenho que levar em consideração quais ações ele pode gerar e o que devo fazer para controlá-las. Esta é uma situação de contra-ataque".

Superar a si mesmo

Através de chutes, golpes, bloqueios, saltos, equilíbrio e reflexo, o Taekwon-Do se torna uma ferramenta para o aprimoramento físico, mental e social. Néstor Galarraga acrescentou: "você sabe quando antecipar e quando contra-atacar. Se eles baterem em você em ação, a única possibilidade é tentar minimizar o dano. E veja que respostas dar, o dano não pode ser evitado".

Federico Teyssandier e Néstor Galarraga durante a demonstração. Você pode ver o conteúdo audiovisual completo através do código QR no início da nota.

Juan Marino falou sobre o conceito de resiliência: "na cibersegurança pensamos que o ataque acontecerá e, em muitos casos, não poderá ser evitado. Como o Taekwon-Do entende a resiliência?

"Taekwon-Do é resiliência. Entendemos que a verdadeira luta é consigo mesmo e uma das primeiras coisas que aprendemos é trocar a limitação pelo desafio", explicou o Grão-Mestre, acrescentando: "podemos aprender a nos acomodar com a limitação, se ela não for superável. Teremos sempre uma visão positiva". Ele falou sobre as limitações que cada um pode ter e, principalmente, aquelas que se baseiam no medo: "o medo imobiliza, ensinamos como superá-lo com uma ação inteligente".

Um mundo melhor

Esforço, perseverança, trabalho comprometido transformam as pessoas em lutadores pela vida. E a arte marcial é baseada em um programa técnico que exige respeito a códigos de conduta, como cortesia, integridade, autocontrole, valorização da cultura e tradição. Professores orientais dizem que quem praticou Taekwon-Do sabe que é beleza e crueza, facilidade e rigor, tradição e inovação, força e sensibilidade, obediência e criatividade, coragem e prudência, humildade e autoridade. Um meio, nunca um fim.

"Pode nos dedicar um último pensamento da marcialidade, Mestre, para nós, que estamos fora da disciplina, imersos no mundo, na esfera corporativa ou em outras organizações", propôs Juan Marino.

A mensagem foi: "por meio do Taekwon-Do ensinamos os alunos a abraçar, viver e compartilhar uma série de valores e princípios para tentar alcançar um mundo melhor. Ciência, técnica, tecnologia estão dentro do ser humano e o tornam insubstituível".

Antes de agradecer os ensinamentos e se despedir do Grão-Mestre, Juan Marino disse: "Interpreto então que a técnica do Taekwon-Do pode ser comparada com a tecnologia, e que o segredo não está aí, mas em tudo que os cerca: os princípios, os valores, uma forma de ver a vida, uma forma de ser"

A equipe no final da produção.

Imagem: Basanta Contenidos

Especial Mulheres na Cibersegurança

Produção abrangente conjunta WOMCY-Bridge

Ao delinearmos o resumo para esta edição da Bridge, procuramos integrar referências que proporcionem uma experiência diferente, com outra voz e um ponto de vista marcadamente diferente dos anteriores. Por isto decidimos incluir o olhar feminino e desenvolver um Especial Mulheres na Cibersegurança em conjunto com a WOMCY (Mulheres na Cibersegurança). Delineamos e produzimos o projeto junto com Leticia Gammill, Líder de Canais de Segurança da Cisco Latam e Presidente Fundadora da WOMCY Latam, a quem agradecemos profundamente.

WOMCY
LATAM Women in Cybersecurity

Leticia Gammill lidera a equipe de parceiros regionais de segurança cibernética da Cisco. Ela também é responsável pela estratégia, posicionamento e ativação da arquitetura e soluções de segurança cibernética para parceiros, provedores de serviços e revendedores da Cisco. Supervisiona a implementação, rastreamento e sucesso de programas de canal e iniciativas de lucratividade de parceiros na região.

Com 15 anos de experiência no setor de segurança cibernética, assessorando clientes e parceiros nas Américas em todas as fases de sua estratégia de segurança cibernética, a experiência em gestão e segurança cibernética de Letícia inclui estratégias de expansão regional e execução em empresas de primeira linha.

Ela é a fundadora e presidente da WOMCY, Latin America Women in Cybersecurity, uma organização focada em mentoria e desenvolvimento de programas especiais para promover carreiras em segurança cibernética e aumentar a presença de profissionais de segurança cibernética na América Latina. Formou-se na EHTP no Porto, Portugal, e possui MBA pela Kellogg School of Management da Northwestern University.

Martha Liliana Sánchez Lozano

De-
senvolveu
uma notável carreira
em Cibersegurança na
Colômbia, tanto na esfera
oficial como privada, e em
organizações não governamen-
tais. Para falar sobre este assunto,
sobre o caminho que ela percorreu
e os passos a seguir, Letícia Gammill,
Líder de Canais de Segurança Ciber-
nética da Cisco, a entrevistou para a
Bridge.
A conversa aconteceu por meio do
Webex, plataforma de colaboração da
Cisco.

Conteúdo
audiovisual

texto: **Jorge Prinzo**
vídeo: **Leticia Gammill**

O que é necessário para iniciar uma carreira em segurança cibernética? Treinamento técnico e experiência são essenciais?

Ee comecei pelo interesse de saber coisas novas. Sempre fui encorajada a agir sobre temas inovadores e às vezes até desconhecidos. A cibersegurança me interessa porque não afeta apenas a minha realidade, mas a forma como o mundo funciona. Os ataques que estavam surgindo afetavam o espaço digital e não havia ninguém para lidar com o problema. Isto me chamou a atenção: atuar em campos novos, estudando-os, entendendo-os, depois transmitindo estas informações e mudando o comportamento ao seu redor, criando novas formas de agir, assim como novos campos de trabalho e acadêmico.
É requisito fundamental para quem trabalha nestas carreiras ter atitude inovadora. Em relação à experiência e ao conhecimento, eu tinha base técnica e uma experiência profissional que me orientava. Porém, ao longo do caminho, percebi que não tinha tudo, que outras habilidades também eram necessárias. Não é algo apenas para engenheiros ou militares. Tive que interagir com administradores, advogados, sociólogos, representantes de organizações de direitos humanos... são tantos os interesses na cibersegurança que qualquer pessoa interessada, que queira criar coisas novas e mudar seu ambiente, é bem-vinda.

É imprescindível continuar estudando, porque são temas que evoluem muito rapidamente, são muito dinâmicos e precisam ser atualizados constantemente. Como você vê a segurança cibernética na Colômbia?

A implementação de políticas de segurança cibernética na Colômbia foi um processo que teve início em 2007, após o ataque cibernético contra a Estônia, quando ficou evidente que um país poderia ser paralisado, que poderia haver mortes ou afetar o sistema financeiro. Em resposta ao aumento da criminalidade, criamos uma política com leis específicas e uma infraestrutura contra ataques a computadores.
Em 2011, analisamos o panorama e percebemos que não havia programas de treinamento, que não haveria pessoas capazes de enfrentar estes novos desafios. Naquela época, eu era diretora de um programa de tecnologia na Escola Superior de Guerra. Entendemos que havia algo novo a fazer e criamos o primeiro Mestrado em Cibersegurança e Ciberdefesa da América Latina. Foi o ponto de partida para abrir novos caminhos e novos programas nas universidades. Hoje estamos focados em criar confiança e segurança digital, trabalhando com todas as áreas envolvidas, porque é um assunto de todos e de responsabilidade compartilhada.
De acordo com o índice nacional de cibersegurança, a Colômbia está localizada acima da média mundial e, na América Latina, em terceiro lugar, atrás do Chile e do Brasil. Avançamos, e podemos avançar ainda mais em inovação, proteção dos ativos essenciais e integração de todas as partes interessadas.

Quero destacar seu compromisso com o treinamento. Faltam profissionais tanto na Colômbia quanto em toda a América Latina. Além de responder às ameaças cibernéticas, precisamos pensar na falta de profissionais em nosso setor. Em um ambiente tão dinâmico, Martha, como é um dia típico na sua função?

Eu tenho funções diferentes, porque sempre há questões pendentes a resolver. Estou sempre lendo, estudando, procurando desafios. Tenho reuniões com diversos atores. Sou solicitada pela Academia, pela Defesa, por organizações de Direitos Humanos, para fazer eventos ou mesmo propor novas linhas de trabalho... Também preparo minhas aulas, agora me dedico mais tempo à Academia. Procuro passar para as pessoas que não conhecem estas questões, para quem acha que isto é apenas uma coisa técnica, que não é assim. Também participo de mesas setoriais para desenvolver e fortalecer políticas governamentais. E, finalmente, agora estou focada nos problemas sociais. Sou presidente da Internet Society Colombia, uma organização que pensa em como a Internet será segura e confiável para o mundo, com foco social, pensando em como levaremos conectividade às pessoas mais vulneráveis. Criei a entidade na Colômbia, sou a primeira presidente, e me dedico a buscar recursos para gerar projetos na Colômbia, para que possamos fazer as mudanças necessárias, porque ninguém virá resolver nossos problemas. Tento modificar o espaço em que estou, criando oportunidades para novas gerações. Com a criação do Master, consegui bolsas para 60 alunos estudarem de graça, e isto criou novos empregos. Isto não muda o setor, mas contribui com um grão de areia. Esta é a minha rotina.

Você conquistou seu próprio espaço em instituições rígidas em termos de diversidade de gênero. Qual foi o impacto de ser pioneira do setor em sua vida profissional?

MiniBio

Martha Liliana Sánchez Lozano, PhD, MBA, C|CISO, ISO 27001
Engenheira de Sistemas, MBA pela Universidad de los Andes, Master em Cyberdefense pela Universidade de Alcalá na Espanha, Doutora do programa de Direito Internacional da Universidade Alfonso X el Sabio, da Espanha, com menção "Cum Laudem" sobre o tema Pesquisa: os desafios do Direito Internacional Humanitário para os conflitos armados no ciberespaço.
Oficial da reserva ativa da Força Aérea Colombiana, na patente de Coronel. Em 2014, participou da mesa de especialistas nacionais com apoio da OEA para fortalecer a segurança cibernética, foi membro do comitê de defesa cibernética das forças militares colombianas e desde 2015 participa das mesas de construção do CONPES em segurança digital 3854 e 3995 do confiança e segurança digital. Desde 2015, lidera o processo de desenho e implementação do programa de cibersegurança e ciberdefesa da Escola Superior de Guerra da Colômbia, sendo a primeira Diretora do Master of Cybersecurity e Cyberdefense em 2016. Entre 2017 e 2018, atuou como Conselheira Nacional de Segurança Digital na Presidência da República da Colômbia. Autora do livro "Conflitos armados no ciberespaço: Desafios do Direito Internacional Humanitário" (2017, Colômbia). Atualmente é professora de pós-graduação internacional em segurança cibernética e defesa cibernética e membro executivo da Internet Society Colombia Chapter, da qual foi fundadora. Top WOMCY 2020.

Gosto de inovar, de sair do modelo que devo cumprir como mulher na sociedade. Estudei Engenharia de Sistemas, uma carreira que quando comecei era "para homens". Foi complicado, mas com esforço consegui me destacar. Como engenheira, resolvi entrar para a Aeronáutica. Naquela época, por exemplo, as mulheres não podiam ser pilotos, algo que só passou a ser permitido há dez anos. Comecei a trabalhar com radares, numa área ainda mais complicada do que quando estudava, em termos de equidade entre homens e mulheres, em relação à posição de poder que os homens têm e à desigualdade de gênero que existe. Fiz isso com dedicação, esforço e paciência. Não desisti, embora muitas vezes tenha pensado em fazê-lo; Muitas vezes me disse: "chega, não preciso agüentar isso". Mas continuei e consegui fazer minha carreira. Além disso, quando começamos com a segurança cibernética, havia um viés sexista. Homens de outros países vinham dar palestras e me chamavam para as conferências porque queriam que uma mulher participasse apenas para cumprir um compromisso, como se fosse necessário cobrir uma cota. Eu dizia a eles que havia muitas mulheres neste meio. Estas práticas tentam subestimar nosso conhecimento, nossa experiência, porque somos mulheres, ou porque sou mãe e tenho filhos e cuido deles.
Mas, por outro lado, também existem pessoas que me ajudaram. É um problema difícil, em todas as áreas, mas conheci pessoas com uma visão ampla, que disseram: "Confio em você e vamos em frente". Isto me permitiu avançar neste tema. Acima de tudo, ser pioneira no assunto me ajudou a assumir funções quase inatingíveis para as mulheres, e por meio das quais consegui ajudar a fortalecer a segurança cibernética na Colômbia.

Você poderia definir seu amor pela segurança cibernética em uma palavra?

Não uma, mas duas palavras: satisfação e desafio. Me permitiu sentir que nasci para isto e fui capaz de evoluir, talvez porque me sinta atraída pela novidade.

Quais são seus projetos para 2021?

Gosto de escrever. Escrevi o livro "Conflitos armados no ciberespaço", sobre os desafios do direito internacional na área cibernética, que faz parte do doutorado que fiz na Espanha. É o primeiro livro da América Latina sobre estes temas.
Agora estou trabalhando em meu segundo livro, sobre ciberdiplomacia na América Latina, tema que só foi desenvolvido na Europa. Estou mantendo contatos com a Comunidade Europeia e com universidades da Colômbia, para que tenha relevância e comece a se desenvolver nesta área. Espero me dedicar à escrita neste ano, e também gerar novas formações nas universidades. Fui convidada para ser professora de segurança cibernética e defesa cibernética em universidades no México. Além disso, continuarei buscando recursos para os projetos da organização que presido na Colômbia. Estes são os planos que tenho a curto prazo

A distância é sempre relativa,
depende da percepção. Somos donos de cada uma
das nossas distâncias: o espaço físico que nos separa pode
ser o terreno que nos une se a emoção que nos liga é a espe-
rança. O tempo eterno que passa durante a separação do ente
querido pode se tornar o momento que clama pela proximidade
entre duas pessoas que pensam uma na outra. Um livro pode nos
afastar quilômetros de nosso entorno imediato, uma palavra pode
nos prometer a proximidade do futuro. Nós escolhemos.
Somos donos de todas as nossas distâncias.

Conteúdo Multiplataforma

basantacontenidos.com

Andréa Thomé

No final do ano, entrevistar líderes empresariais pode se tornar uma tarefa difícil. No final do ano, as tarefas vão mal, as pessoas ficam agitadas e conseguir uma nova entrada na agenda pode ser um desafio intransponível. Porém, na entrevista com Andréa Thomé, estes pressupostos eram apenas parte de um imaginário, da experiência alheia. Se algo mostra força na liderança, é a capacidade de promover, distribuir, incentivar e agir com perspectiva de sucesso, características marcantes em nossa entrevistada. E também uma vantagem inesquecível: seu calor implacável, respeito e profissionalismo em todos os momentos.

por: **Karina Basanta**

Sua carreira mostra grande força e perseverança. O que significa empoderamento para você?

É ser autossuficiente para motivar, mobilizar, dar força e agilidade para alcançar resultados. Este processo nos permite descobrir que independentemente das adversidades, quando queremos, podemos e fazemos o que queremos.

E vice-versa, o que é fragilidade para Andréa Thomé?

A fragilidade nos diz que é preciso mais força e uma dose maior de fortalecimento para manter o equilíbrio. Nos leva a pesar as dificuldades, mas nos permite refletir. Em momentos de fragilidade nos desafiamos e crescemos, para voltar mais fortes ao marco zero.

Li recentemente uma entrevista com Tarja Halonen, ex-presidente da Finlândia, na qual ela argumenta que a questão de gênero acabou sendo um fator-chave para explicar a qualidade das respostas de governo à pandemia. Na sua opinião, o que as mulheres querem dizer ao afirmar que fazemos as coisas melhor?

Características como sensibilidade, foco, assertividade e capacidade analítica nos colocam em vantagem quando nos deparamos com as crises que vivemos nesta pandemia. Outro aspecto que admiro nas mulheres é a capacidade de desenhar cenários com base na análise crítica e na intuição que já nasce com elas.

Por que Womcy (Mulheres na Cibersegurança)?

WOMCY nasceu de uma necessidade que hoje impacta positivamente centenas de mulheres em mais de 18 países da América Latina e América Central. Ao procurar uma ONG na LATAM em 2019 para se juntar e contribuir, Letícia Gammill, nossa fundadora e CEO, simplesmente não encontrou e decidiu fundar a sua própria ONG.

Desde então, recrutamos líderes, definimos programas, ações, criamos equipes, alcançamos pessoas especiais e até conquistamos a simpatia de homens que nos ajudam como parte de nossa equipe WOMCY Ele por Ela.

Há pouco mais de um ano, quando recebi o convite da CEO, por indicação de um ex-líder que tive em uma fase da minha carreira, não pude deixar de admirar a abrangência da proposta que é fruto de 9 programas e do trabalho de 6 times no Brasil liderados por um grupo de mais de 50 talentos.

Percorremos o mundo corporativo, associações, universidades e escolas, com conferências, informações, tutorias, programas de treinamento, divulgação de vagas e muita recepção para executivos, gestores, especialistas, jovens, iniciantes, estudantes e profissionais em transição para a segurança cibernética.

Posso dizer que nunca aprendi tanto e nunca me senti tão útil em poder ajudar os necessitados em um setor tão promissor.

No seu entendimento, quais são as habilidades necessárias para se destacar em segurança cibernética?

Curiosidade, capacidade investigativa, busca contínua pelo conhecimento, visão crítica, pensamento inovador, equilíbrio e visão preditiva para minimizar incidentes.

Como você vê a segurança cibernética no Brasil e como está o posicionamento do país em relação à América Latina?

Temos muita experiência na prevenção e resposta a incidentes de segurança, especialmente porque passamos por muitos ataques. Ao mesmo tempo em que experimenta o sabor amargo dos incidentes, obtém-se a capacidade de conhecer suas características, aprender a evitar sua incidência e responder com agilidade e eficiência aos seus impactos adversos.

O setor, no Brasil, alcançou posição de destaque se compararmos com o cenário da última década. Hoje, a segurança cibernética faz parte da agenda estratégica de qualquer setor, embora não receba necessariamente a prioridade que merece. Já o IBGC – Instituto Brasileiro de Governança Corpora-

tiva, por exemplo, definiu em publicação o papel do Conselho de Administração em relação aos riscos cibernéticos.

Acredito que o assunto também tem ganhado relevância em outros países da América Latina, onde percebo a plena colaboração entre eles, seja na troca de conhecimentos, recursos e informações.

Acho que na pós-pandemia muito precisa ser revisto de acordo com os resultados que vivenciamos. A cultura de segurança cibernética deve ser intensamente mantida, as ferramentas de segurança devem ser desafiadas e complementadas e os processos devem ser aprimorados e transformados para oferecer o melhor custo-benefício às empresas.

Uma palavra para descrever seu amor pela segurança cibernética.

Desafío.

Quais são os próximos passos, em 2021, em termos de cibersegurança?

A pandemia nos ensinou e ao mesmo tempo nos expôs muito. Notamos em alguns ambientes que as medidas básicas de segurança não eram eficazes ou inexistentes durante as crises.

Compartilhe conosco uma breve mensagem final sobre o seu desejo por questões de segurança cibernética.

Quero ver mais mulheres neste setor que é tão promissor, que traz tantos benefícios para empresas, indivíduos e para o mundo. Desejo também que não haja diferença de remuneração, conhecimento ou oportunidades para os diversos gêneros em nosso mercado.

Por último, quero acima de tudo ser capaz de ver o setor crescer com mais reconhecimento, diversidade e defesas corporativas cada vez mais fortes contra fraudes e incidentes de segurança cibernética

MiniBio

Graduada em Ciência da Computação e MBA em Gestão de Negócios, Andréa atualmente atua como Diretora de soluções de Cibersegurança na everis. Além disso, é líder da operação da WOMCY Brasil (Mulheres na segurança cibernética) e mentora de negócios, CISM, Hardvard Manager Mentor, CobITF, PMBM, ORM Admin. Ele mora na cidade de São Paulo, Brasil.

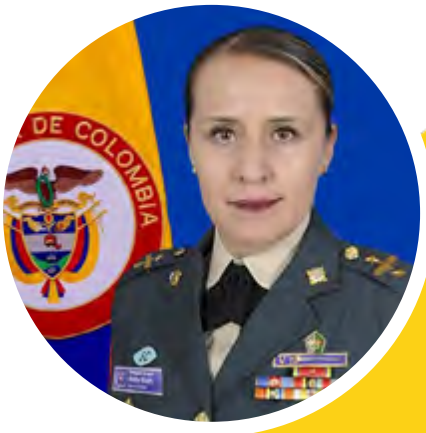
FAÇA PARTE DA WOMCY

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



Milena
Realpe Díaz

Entrevista com a Tenente Coronel Milena Realpe Díaz, Chefe do Mestrado em Cibersegurança e Ciberdefesa do Colégio de Guerra da Colômbia.

Conteúdo audiovisual

texto: **Jorge Prinzo**
vídeo: **Leticia Gammill**

O que é necessário para iniciar uma carreira em segurança cibernética? É essencial ter experiência e conhecimento técnico?

Sim, você tem que ter treinamento, e é melhor começar com Engenharia de Sistemas, Engenharia Eletrônica, qualquer engenharia relacionada a estes programas. O tema é muito emocionante e muda a cada dia, o que nos obriga a estar em constante treinamento. Este seria o começo: uma carreira de engenharia que dá o contexto geral, e então o aluno pode escolher a especialidade em segurança cibernética, ou defesa cibernética, no caso militar. Devemos necessariamente ter treinamento.

Como você vê a segurança cibernética na Colômbia e como está o posicionamento do país em relação à América Latina?

A Colômbia fez um trabalho muito importante. Começamos, em 2011, com o primeiro documento de segurança e defesa cibernética e tentamos dar continuidade a ele. Na verdade, já temos quatro políticas, atualizações e planos de ação. E funcionou. Conseguimos cumprir os planos de ação. Gostaríamos de ir mais rápido, mas isso depende de muitos fatores, econômicos, de recursos humanos... No ano passado, a OEA publicou a segunda edição de um estudo latino-americano, iniciado em 2016, comparando os países da região em diversos aspectos, como na política, na conscientização, na cultura da informática, nos regulamentos e nas leis. Na Colômbia, para a nossa alegria, crescemos em todos estes aspectos. Agora somos membros da Convenção de Budapeste, o que também foi um avanço para o nosso país. Nossa primeira política foi chamada de Diretrizes sobre Cibersegurança e Ciberdefesa. Em seguida, passamos para o tema em que fortalecemos a economia digital, e agora focamos na confiança das pessoas neste novo cenário em que vivemos, compartilhamos, trabalhamos... Este novo domínio, o ciberespaço, não mudou apenas a forma de fazermos negócios, mas também, fundamentalmente, as nossas vidas. Estamos avançando como país. Temos que continuar trabalhando, mas acho que estamos no caminho certo.

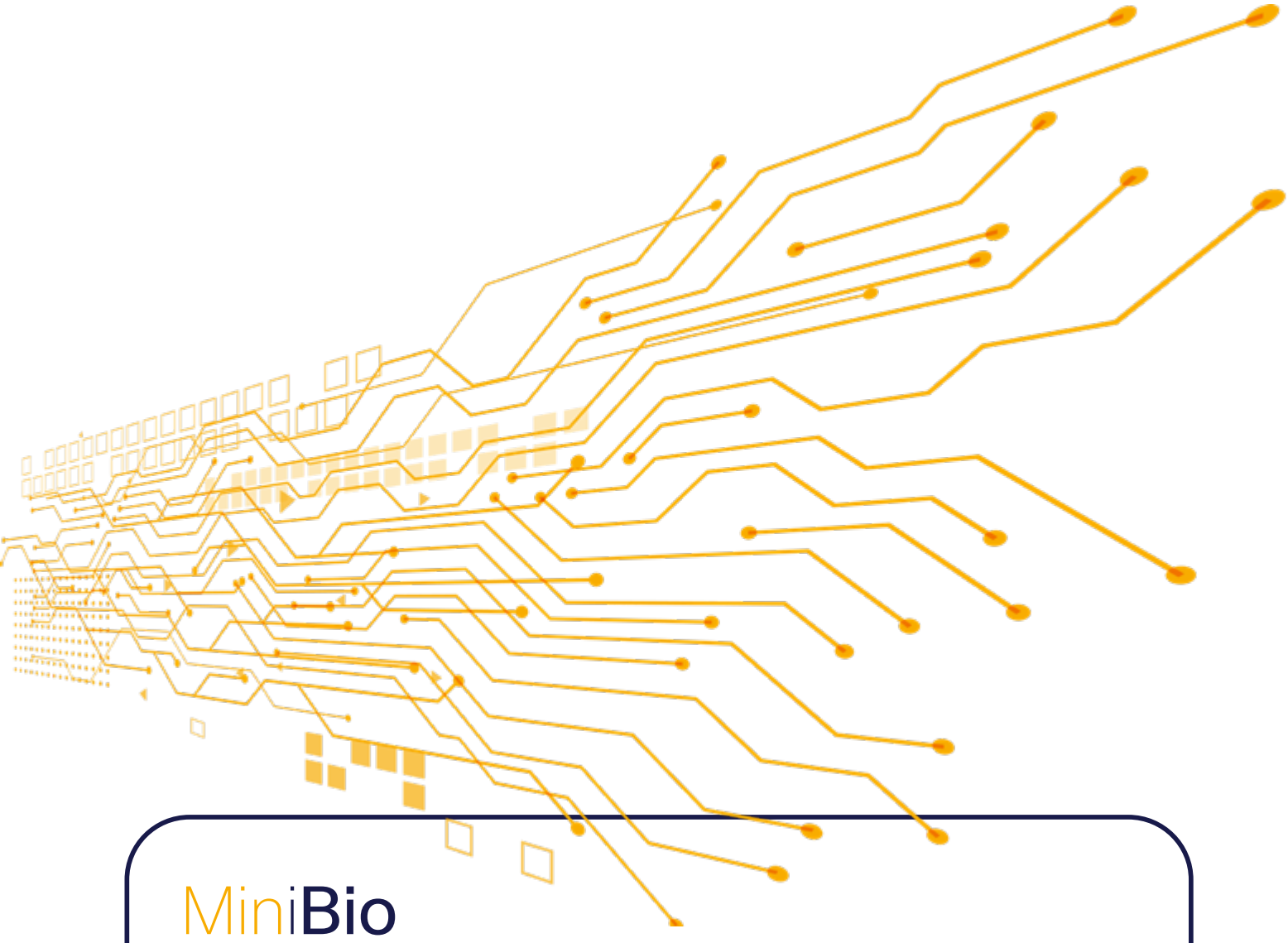
Descreva um dia típico em sua função.

É um dia que começa muito cedo, às cinco da manhã. Gosto de praticar esportes, é a primeira coisa que faço pela manhã. Também cuido dos meus filhos, no meu papel de mãe, antes de ir para o trabalho. E já entrando na área de cibersegurança, atendo aos meus alunos no Mestrado. Também leio e me atualizo em tecnologia. Este momento que a humanidade vive em decorrência da pandemia obrigou grande parte das empresas a incorporar processos digitais; depois os usuários, os clientes, as informações, os bancos de dados... todos os requisitos desses usuários estão conectados à internet, mesmo aqueles que não existiam antes. Estamos fazendo uso de muitos sistemas que exigem segurança. Por isto, temos que treinar, ler, ser autodidatas. Há muitos documentos e estudos importantes publicados na internet, à disposição de todos. É simplesmente querer fazer, ter paixão por fazer, e o resto flui. Esta é a minha rotina na Escola Superior de Guerra. Quando podemos, fazemos fisicamente, é fisicamente, ou de casa, resolvendo problemas e aconselhando sobre questões de segurança cibernética para os diferentes sistemas, apoiando os alunos em questões de pesquisa e escrevendo também. Gosto de escrever, gerar novos conhecimentos e compartilhá-los. Meu dia a dia também é complementado pelos papéis de mãe, esposa, filha, irmã, todos os papéis que, como mulheres, também temos que frequentar e nunca negligenciar. Muito pelo contrário, são estes suportes que nos levam para frente, que nos dão força... é a família que nos apoia no papel profissional.

No seu entendimento, quais são as habilidades necessárias para se destacar em segurança cibernética?

Seja persistente. Às vezes, as coisas não acontecem do jeito que queremos da primeira vez. Então: insista, insista e insista no que quer, porque no final a gente consegue. E paixão: ser apaixonado pelo que fazemos, gostar do que fazemos é fator essencial para progredir e ser feliz. No final, é isso que nos deixa felizes: trabalhar no que gostamos, estudar o que gostamos, investigar o que queremos.

Parece que você conseguiu encontrar espaço em diferentes instituições que são um tanto rígidas quanto à diversidade de gênero e profissão. O que isso significa para você e que impacto teve em sua vida pessoal?



MiniBio

Engenheira de Sistemas com 18 anos de experiência profissional em Segurança da Informação, gestão de tecnologia da informação e comunicação, análise de vulnerabilidade Cibersegurança, Defesa cibernética, governança de segurança da informação, análise de vulnerabilidade, gestão de incidentes, criação de CSIRT, CERT e SOC. Conselheira e professora militar e universitária. Palestrante Nacional e Internacional. Participou da formulação do documento CONPES 3701 "Diretrizes da Política de Segurança Cibernética e Defesa Cibernética para a Colômbia" e do CONPES 3858 "Política de Segurança Digital"; co-fundadora do Comando Cibernético Conjunto das Forças Militares Colombianas. Diretora de diversos projetos de segurança informática e telecomunicações, com elevadas condições humanas e éticas. Magister in Information Security (Universidad de los Andes), Magister in Cybersecurity and Cyberdefense (Escuela Superior de Guerra), Specialist in Network Security, Physical Security and Information Security. Atualmente trabalha como Chefe do Mestrado em Cibersegurança e Ciberdefesa da Escola Superior de Guerra da Colômbia e Assessora em Cibersegurança e Ciberdefesa do Ministério da Defesa Nacional da Colômbia.

As forças militares estão se transformando. Há vários anos oferecemos a participação das mulheres, trabalhamos com questões de inclusão. Então não foi mais tão difícil para mim. Acho que para se destacar na área de cibersegurança, e em qualquer área, é preciso apresentar resultados nos projetos apresentados à instituição. É isto que nos orienta. É o que mostra que atingimos a meta. Foi o que tentei fazer: mostrar a eles como os militares foram obrigados a assumir a responsabilidade pela segurança e defesa cibernéticas. Isto foi o que me destacou um pouco neste tema: mostrar resultados, inovar, pensar prospecti-

vamente para onde vão a segurança cibernética e a defesa cibernética e antecipar o que pode acontecer.

O que é fragilidade para a Major Milena Realpe? Você pode responder de qualquer ponto de vista.

Acho que temos que nos concentrar em nosso tópico. A fragilidade dos nossos sistemas permite que sejamos violados, que corramos riscos de segurança cibernética. Se tivermos computadores frágeis, que não foram configurados para entregar bons controles de segurança, ficamos frágeis contra qualquer ataque, e nossas informações podem ser afetadas: confidencialidade, integridade, disponibilidade... Se não quisermos ser frágeis, se quisermos ser fortes contra possíveis invasores que queiram acessar nossos sistemas, temos que proteger nossos equipamentos, fazer uma configuração forte.

Uma palavra para descrever seu amor pela segurança cibernética.

Paixão: a paixão de fazer essas coisas. Para mim é empolgante trabalhar com cibersegurança e, em meu caso particular, com ciberdefesa. Inovar, propor, levantar questões militares em perspectiva de meu país, a Colômbia, não tem comparação. Ver como podemos crescer, como seguir em frente a partir de experiências de outros países, propor algo novo para o nosso país, é espetacular para mim, é uma paixão.

Quais são os próximos passos para 2021 em termos de cibersegurança?

A maioria das empresas migrou para o domínio digital, era obrigatório nos reinventar e fazer. Em termos de oportunidades de trabalho, para especialistas em segurança cibernética, o campo é enorme. Os profissionais, e aqueles que querem começar, têm muitas oportunidades de trabalho e também uma remuneração muito boa. Todos os sistemas precisam garantir sua segurança, que as informações sejam protegidas com bons controles. E é isso que a cibersegurança nos oferece. A tecnologia continuará crescendo. A cada dia teremos novas tecnologias disruptivas que precisarão ser estudadas. A educação é essencial. E buscar novos projetos que nos permitam continuar crescendo. Isso nos levará a fazer nosso país e nossa região progredirem, e nosso campo de ação se expandir

Imagem: Kobby Mendez-Unsplash

Macrina Pérez Bermúdez

Entrevista com o Presidente do grupo de cibersegurança do setor de seguros no México e colaborador na sensibilização sobre este assunto da WOMCY México.

por: **Marta Pizzini**

O que significa "segurança" para Macrina Pérez Bermúdez?

Trabalhar online com a certeza de que as informações são confidenciais, completas e sempre disponíveis.

Sua trajetória mostra uma vasta experiência em termos de segurança cibernética. Atualizar e buscar soluções para novos problemas exige estar sempre atento a novos conhecimentos. Como você equilibra a continuidade na carreira e a atualização constante?

A aprendizagem contínua é um processo que dura a vida toda. O desenvolvimento tecnológico, novas metodologias, processos de trabalho, novas ameaças, ataques etc., geram habilidades e lacunas de conhecimento que só podem ser superadas com a atualização constante de conhecimentos. Caso contrário você perde a oportunidade de combinar sua experiência com novas formas de fazer / ver as coisas e limitando o valor que você pode entregar.

A julgar pela transformação digital acelerada que foi desencadeada em 2020, a segurança cibernética está se moldando para ser um trabalho do presente e do futuro, com ampla promessa sobre fontes de trabalho. Como a força de trabalho é atraída para este setor de destaque?

De acordo com o estudo ISC2 de 2020, o déficit global de pessoal de segurança cibernética é de 3,1 milhões: 17% corresponde à América Latina. 12% para a América do Norte, 5% para a Europa e 66% para a região Ásia-Pacífico. No México, o tamanho da lacuna da força de trabalho é de 195.594 profissionais.
No meu entendimento, para atrair força de trabalho, algumas decisões podem ser tomadas, tais como:

- O setor empresarial deve se aproximar do setor acadêmico e expressar suas necessidades e tendências em segurança cibernética.
- Treinar especialistas em segurança cibernética por meio de programas técnicos e habilidades sociais.
- Promover modelos de trabalho alternativos (local, remoto, combinado).
- Dar oportunidade a jovens sem experiência, com alto potencial.
- A segurança cibernética é principalmente para pessoas técnicas, mas também para pessoas não técnicas.

No seu entendimento, quais são as habilidades necessárias para se destacar em segurança cibernética?

Eu diria que os três "As" são a chave:

- **Antecipação:** seja proativo, esteja um passo à frente, prepare-se e esteja pronto para o que está por vir.
- **Alinhamento:** adaptar o nosso papel, seja o que for que desempenhemos, para ser um "facilitador" de valor na transformação.
- **Adaptabilidade:** redesenhar os programas de segurança cibernética com base nas necessidades do negócio, ambiente, situação específica ou imprevista etc.

Como você vê a segurança cibernética no México e como está o posicionamento do país em relação à América Latina?

Acredito que o México tem muitas áreas de oportunidade em termos de segurança cibernética, embora não tenha uma legislação de segurança da informação e uma estratégia de segurança cibernética em nível de país. No entanto, desde 2018 (como resultado dos ataques de SPEI, Pemex, CFE), vi que a abordagem está mudando, passou a ser uma prioridade para empresas privadas dispostas a se envolver, investir e aumentar a conscientização em segurança. O México e a América Latina continuarão a enfrentar ransomware e, principalmente, ataques direcionados.

Uma palavra para descrever seu amor pela segurança cibernética.

Paixão.

Quais são as próximas etapas em 2021 em termos de cibersegurança?

- Segurança no trabalho remoto: é prioridade no "Novo Normal" proteger e proteger a informação em qualquer lugar.
- Maior confiança nos serviços e segurança na nuvem.
- Maior colaboração entre empresas do mesmo setor, compartilhando inteligência de cibersegurança.
- Inteligência artificial e ciência de dados aplicadas às tecnologias de cibersegurança.

Compartilhe conosco uma breve mensagem final sobre seu desejo por questões de segurança cibernética.

O elo mais fraco no mundo da cibersegurança ainda é o ser humano, por isso é importante desenvolver e promover as competências digitais: seja inteligente e prudente online como no mundo real

Funções mais exigidas em segurança cibernética

Segurança na operação: é a primeira linha de defesa, os engenheiros especializados em tecnologia.
Administração de segurança: são eles que definem a estratégia e as diretrizes de segurança.
Gestão de riscos: identificar, analisar e priorizar os riscos de segurança para o negócio.
Cumprimento regulamentar: conhecem e interpretam as leis e normas a cumprir.
Desenvolvedores de software seguros: aqueles que se concentram em incluir a segurança em aplicativos.
Especialistas em análise de vulnerabilidade e testes de penetração: são responsáveis por avaliar, por exemplo, infraestrutura, aplicações.
Perícia informática, ou seja, quem investiga e resolve casos de violação da segurança da informação.

MiniBio

Macrina Pérez Bermúdez tem mais de 20 anos de experiência em tecnologia da informação e segurança, gestão de riscos, compliance, gestão de SOCs, implementação de DRPs, gestão de identidade, programas de conscientização docente. Já trabalhou em empresas especializadas em Cibersegurança, na ONU em Viena, Áustria, e atualmente trabalha no setor de Seguros, onde contribui para o fortalecimento da segurança tecnológica. Ela é presidente do grupo de segurança cibernética do setor de seguros no México. Colabora na criação de consciência em segurança cibernética de WOMCY México.

Um dos ativos mais valiosos e subestimados na era digital são as informações contidas em nossos computadores, e-mails e repositórios em nuvem. São essas informações que ficam expostas a inúmeras ameaças na rede. Apenas um clique aliado a controles de segurança inadequados é suficiente para deixá-las à mercê de criminosos inescrupulosos que podem leiloar, extorquir ou abusar delas em territórios estrangeiros, fora da legal jurisdição de nossos países.

É com um único clique que qualquer um de nós pode cair nas armadilhas mais elaboradas e imagináveis, expondo informações pessoais ou da empresa sem perceber que foram objeto de um ataque cibernético avançado e colocando em risco seu prestígio e ativos, o que levará anos para se recuperar depois de muito esforço e dinheiro. É por isso que hoje existe uma necessidade urgente de consciência individual e empresarial sobre o risco latente a que estamos expostos e pelo qual somos responsáveis independentemente da área da organização e função que desempenhamos. Cada um de nós é dono e responsável pelas informações que manejamos, enviamos, guardamos, pelo uso adequado das mesmas e pelos cuidados que tomamos.

Os números dos últimos anos mostram um aumento nos ataques de malware e phishing devido à digitalização acelerada diretamente alavancada pela pandemia de 2020. Os números fornecidos à INTERPOL por parceiros privados mostram que, de fevereiro a março de 2020, houve um crescimento de 569% nos registros maliciosos, incluindo malware e phishing e um aumento de 788% nos registros de alto risco.1

Esse apetite voraz de cibercriminosos por usuários neófitos em questões digitais foi compensado no início da pandemia, quando em fevereiro de 2020 muitos tiveram que se isolar em casa e foram forçados a participar digitalmente de diferentes atividades, acessar serviços e realizar transações remotamente. Tudo que antes o faziam de forma presencial. E naqueles primórdios de navegação pelo mar da grande rede, ficaram expostos a criminosos e vulneráveis a uma miríade de vetores de risco totalmente desconhecida até então e ignorada hoje.

Mas não estamos sozinhos nessa luta. Os grandes fabricantes de software e hardware e seus aliados vêm desenvolvendo um portfólio de soluções que estão à disposição de todos e que, a partir de diferentes abordagens, buscam proteger, prevenir ou remediar os diversos pontos de acesso de risco aos quais os indivíduos e as empresas estão expostos nesta nova era digital.

Atualmente, a segurança da informação pode se concentrar em controles que sejam transparentes para os usuários, protegendo-os das ameaças mais avançadas sem que eles percebam, ou em controles mais persistentes e ativos nos dispositivos do dia-a-dia, como laptops e telefones celulares. Os antivírus e antimalware tradicionais requerem atenção mais assídua da nova população digital inexperiente.

Um exemplo de controle transparente e ativo para usuários de negócios é o monitoramento de IPs e domínios inseguros, que são constantemente alimentados em um repositório global. Uma solução como o Cisco UMBRELLA, que atende a solicitações DNS tradicionais, pode validar o acesso em tempo real para determinar ameaças potenciais e bloquear essas solicitações sem a intervenção do usuário: apenas apontar o DNS para Cisco UMBRELLA pode iniciar a proteção efetiva e ativa dos usuários, fora e dentro a empresa, de suas casas e até os dispositivos mais sensíveis, proporcionando aos analistas de segurança a visibilidade de possíveis ataques em andamento e dos sistemas comprometidos em um ataque.

Outro exemplo é a análise do comportamento do usuário por meio do monitoramento constante de suas atividades habituais. Com esta atividade, é possível determinar se um usuário foi objeto de um ataque e se seus acessos e contas estão sendo mal utilizados. O estudo é realizado por meio de uma análise preditiva dos padrões de comportamento de um usuário conhecido ou sob análise de pares, e permite visualizar se certas ações e atividades específicas ou consistentes estão fora da média ou do comportamento comum de um indivíduo ou grupo. Com essas informações, o analista de segurança pode detectar e agir rapidamente contra um possível ataque que está perpetuando a organização.

A OCP TECH oferece aos seus clientes uma abordagem de consultoria avançada que lhe permite fornecer, de forma abrangente, soluções e serviços que respondam aos novos riscos da era digital, criando um caminho de adoção ágil, eficiente e alinhado com os objetivos do negócio.

A OCP TECH é uma empresa americana que processa mais de 150 milhões de dólares por ano com operações em todas as partes do mundo. O núcleo possui diversas empresas e escritórios na América Latina

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

Imagem: Ijeab, freepik

Sequestro e extorsão na era digital

por **Fabio Sánchez**

Diretor de Prática de Cibersegurança
fabio@ocp.tech

Transformação digital segura em **saúde**

Entrevista com o Dr. Jairo Pérez Cely, diretor do Departamento de Cuidados Críticos do Hospital Universitário Nacional da Colômbia e Professor da Universidade Nacional da Colômbia.

texto: **Javier Castro**
vídeo: **Basanta Contenidos**

Na Saúde, o processo de cuidar e a presença sempre estiveram intimamente ligados. Como o isolamento produzido pela pandemia impactou este modelo?

Como você mencionou, viemos de um formato tradicional de prestação de serviços, marcado pelo contato pessoal. No momento em que surge a pandemia, este tipo de contato se torna um risco. Ao mesmo tempo, o isolamento social é inserido como medida preventiva, o que nos levou a dois cenários de oportunidade para gerar novas estratégias. O primeiro era ter uma abordagem diferenciada tanto com pessoas com doenças crônicas e que não podiam continuar com seus tratamentos ou controles em hospitais ou centros de alta complexidade quanto com aquelas que vivem em áreas rurais. Diante da inviabilidade de circulação de pessoas, pudemos realizar os controles remotamente, por meio de tecnologia digital.

Conteúdo audiovisual

CDA / Segurança
Colombiana

Por outro lado, também pudemos dar continuidade à prestação de serviços de alta complexidade em patologias relacionadas ou não à COVID-19. Isto se refere ao fato de muitas instituições terem passado a prestar serviços de cuidados críticos sem poder contar o talento humano, com experiencia e formação nestas áreas. Tínhamos que encontrar uma maneira de ajudar estes centros e regiões a fornecer serviços de cuidados intensivos remotamente. Entramos como Hospital Universitário e como Universidade Nacional para fornecer suporte por meio do nosso programa de telessuporte em cuidados intensivos.

Como a transformação digital apoiou o programa de telessaúde e quais os novos desafios que ele apresenta?

A transformação digital passou a ser a nossa principal alternativa de prestação de serviços de saúde. Primeiro, do ponto de vista da disponibilidade de alguns serviços que não puderam ser acessados em algumas regiões. Por exemplo, habilitamos serviços de infectologia e nefrologia em regiões que não os tinham. Em segundo lugar, do ponto de vista do atendimento. Terceiro, do ponto de vista do treinamento. Quarto, do acompanhamento, durante e depois da pandemia. Esse suporte ocorre em três sentidos: no manejo dos pacientes, nos equipamentos biomédicos e no manejo geral do espaço de terapia intensiva. Se pensarmos que alguns profissionais tiveram contato com um ventilador mecânico pela primeira vez, nosso auxílio foi treiná-los remotamente e em tempo real, com um passo a passo de como operar o sistema. Do ponto de vista de gestão, também ajudamos as regiões no controle de surtos em pessoal de saúde, por isto tivemos que nos envolver em todas as etapas do processo de atendimento aos pacientes de COVID-19.
A transformação digital também nos trouxe outras oportunidades, como aquelas relacionadas a programas de prevenção e promoção da saúde.

À primeira vista, parece que um dos benefícios do Telessaúde é facilitar o acesso ao sistema de saúde. Na sua opinião, quais são os outros benefícios e qual é o seu principal ponto fraco na Colômbia?

O principal ponto fraco é algo muito importante a se levar em consideração, que é a conectividade. No programa de telessuporte de cuidados intensivos, revisamos a condição dos pacientes em vários horários do dia, porque não podemos esperar o dia seguinte ou a semana seguinte para avaliar a eficacia da estratégia de tratamento adotada para que eles melhorem. Quando vamos nos comunicar, infelizmente não há conexão. Às vezes a ligação cai, às vezes não podemos ver as imagens. Um desafio para o Ministério de TIC (Tecnologia da Informação e Comunicação) do país é como melhorar a conectividade.
Outro ponto fraco é o fato de que os programas de remédios aumentaram muito no país, então temos que ter certeza de que são seguros. Muitas vezes queremos oferecer tudo o que temos à disposição, porém pode não ser o que a região precisa. Devemos olhar para as necessidades de cada um e depois disponibilizar o que eles precisam.
Outra fragilidade é a cultura da transformação digital, não só na saúde, mas em outras áreas também. Devemos fazer desta nova forma de trabalho e educação, que aprendemos com tanta urgência, algo normal para continuarmos implementando, pois facilita a prestação do serviço. Sempre digo que a telemedicina veio para ficar.

Pelo que falamos, parece que a pandemia trouxe e promete novos avanços na telessaúde da Colômbia. Qual foi o impacto da doação da Cisco por meio do programa Country Digital Acceleration (CDA) da Colômbia?

Vou falar especificamente sobre o nosso programa de telessuporte para cuidados intensivos. Nós definitivamente não tínhamos isto antes. Quando começamos a analisar em março o comportamento da pandemia na Europa, Ásia e, principalmente, na Espanha e Itália, aonde a capacidade hospitalar e, especificamente, as unidades de terapia intensiva estavam sobrecarregadas, na Universidade e no Hospital surgiu a preocupação sobre o que aconteceria se fosse possível conseguir os ventiladores que o governo federal havia planejado - que era chegar a mais de 10.000 leitos de terapia intensiva – e é uma realidade hoje. Ficamos imaginando quem iria manusear este tipo de equipamento biomédico, uma vez que não tínhamos esta experiência e era necessário talento humano da equipe de terapia intensiva básica. Não só o médico intensivista, mas os enfermeiros e todo o pessoal precisam de especialização e experiência.
Diante desta constatação, decidimos entrar em contato com as regiões para oferecer a nossa principal força ao seu principal ponto fraco: o talento humano. Mas surgiu o problema de como se conectar. E aí apareceu a Cisco. Um tinha a necessidade e o outro como satisfazê-la, a Cisco colocou o canal para que pudéssemos nos comunicar. A Cisco nos ajudou de duas maneiras: levando equipes para diferentes regiões como Amazonas, Tumaco, Quibdó, que são áreas com muitas limitações de atendimento. A empresa também nos doou os equipamentos e suas licenças em determinadas regiões e nos 22 hospitais que, atualmente, ajudamos com o telessuporte de talento humano em cuidados críticos. Com a Cisco teríamos, inclusive, conseguido chegar a mais lugares, a outras áreas ainda mais remotas, o que só não

Imagem: Gerd Altmann, Pixabay

foi possível devido a problemas de conectividade. Infelizmente, a falta de conectividade em alguns lugares ainda é uma realidade e hoje mostra as consequências. Esta é a grande contribuição que a Cisco nos deu: ter conseguido implementar um plano e ser capaz de mantê-lo no futuro. Como sempre digo, não se trata apenas da pandemia e como nos unimos para responder a estas necessidades urgentes que nos levaram a acelerar muitos processos, mas também de como os manteremos, porque o problema do talento humano nas regiões continuará com e sem pandemia. Em tudo isto, a Cisco está nos ajudando.

> “O desafio agora é manter o que nós ganhamos e transformamos o pandemia para melhorar todos os serviços de saúde no país.”

Houve avanços na formação de pessoal especializado em saúde sob a metodologia digital remota nesta época em que todos fomos lançados na vida digital?

Sim, claro, muito. Hoje temos 22 hospitais que atendemos. Não estivemos presentes em nenhum deles e ajudamos a todos. Os avanços no treinamento e na educação sobre cuidados intensivos têm sido muito importantes.
Outro tópico altamente relevante é o treinamento em tempo real. Você está vendo o paciente, o monitor, o ventilador, e pode ajudar a interpretar os gráficos, os exames, pode indicar como fazer o cuidado. A comunicação síncrona nos permite ter esta interação com o outro profissional. Ele me pergunta e eu pergunto a ele, como especialista e também como acadêmico. O treinamento continua o tempo todo.
Por outro lado, da academia, na graduação e pós-graduação formal, também estamos levando toda a formação graças à transformação digital.

Do que falamos quando abordamos Cibersegurança em Saúde?

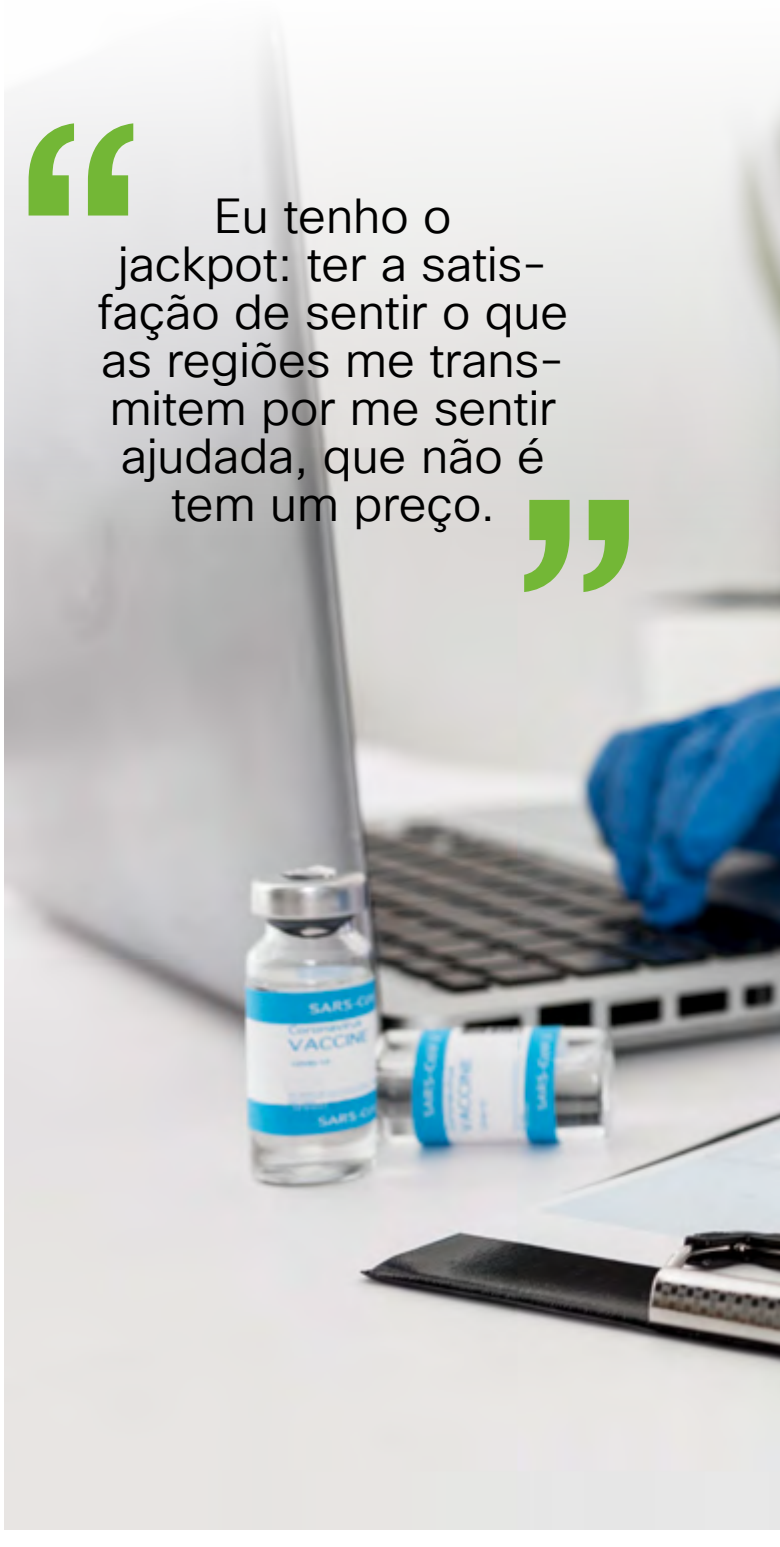
Isso é importante para nós. Nosso principal ator a proteger são os dados que mais tarde formam o histórico médico de uma pessoa. São sempre informações sobre pessoas e devem ser totalmente confidenciais. Quando falamos em cibersegurança em saúde, significa que os dados devem ser conhecidos apenas pelo profissional e pelo paciente, e devemos ter certeza de que assim o será. Muitos países já foram vítimas de crimes cibernéticos na área da saúde, o que é muito estressante para nós como profissionais de saúde. Se vamos tratar um paciente em qualquer região, precisamos garantir, antes de mais nada, que a comunicação será segura.

Definitivamente, o principal ativo a ser protegido durante a digitalização de sistemas é a informação. Em termos médicos, tanto as informações dos pacientes, como os tratamentos e a continuidade do perfeito funcionamento dos sistemas são cruciais e altamente críticas, então quais você acha que são as características que uma plataforma de telessaúde deve ter para ser considerada altamente cibersegura?

Exatamente, o principal ativo a proteger são as informações. Como mencionei, a primeira coisa a garantir é que ninguém mais terá acesso à comunicação entre o profissional e o paciente, a menos que a gente queira compartilhar voluntariamente. As informações devem ser estritamente confidenciais. Por outro lado, pelo menos em cuidados críticos, debe-se permitir conectividade em tempo real, uma vez que as decisões que devemos tomar são imediatas. O terceiro aspecto é que nos permita guardar os dados e que possamos ter a sua rastreabilidade para que possamos acessá-los sempre que necessário, claro, de forma altamente confidencial e sob todas as medidas de segurança, como acontece em todos os registos médicos.

Com base em toda essa experiência, qual é o futuro de médio e longo prazo do Telessaúde?

Desafios muito importantes estão chegando. Assim como assumimos o desafio de enfrentar a pandemia, devemos também assumir o desafio de manter



estes laços que estabelecemos entre os diversos atores para melhorar a prestação de serviços nas regiões. Os governos locais, o governo nacional e os próprios hospitais fizeram investimentos significativos em infraestrutura, principalmente na expansão e fornecimento de novos serviços de cuidados intensivos. Porém, quando a pandemia acabar, continuaremos com os mesmos problemas enfrentados nas regiões, que é a falta de pessoal altamente qualificado para prestar serviços de alta complexidade. O desafio é como manter estes laços e como continuar somando ao que temos feito até hoje. Como manter estas pontes entre o hospital municipal, o hospital de alta complexidade e o hospital regional, mas com tudo coordenado. E como manter a ponte por meio destas plataformas, como se

Imagem: Freepik

comunicar permanentemente para melhorar ainda mais a prestação dos serviços. Acredito que este seja o desafio mais importante que nos chega agora, porque o problema de não ter pessoal altamente qualificado vai continuar nos hospitais regionais. Então, deve-se garantir que, por meio destas tecnologias, possamos fornecer este serviço remotamente para estas regiões. Acredito que existe o desafio de manter o que conquistamos e fazer da pandemia uma oportunidade de melhorar todos os serviços de saúde do país.

São estes laços que nós estabelecemos, por exemplo, com as regiões, com outras disciplinas ou profissões, como engenheiros, os laços de coordenação com os ministérios. O desafio é continuar adicionando.

Dr. Pérez, muito obrigado por esta conversa e por suas valiosas contribuições para a saúde da Colômbia.

Muito obrigado Javier, muito gentil. Obrigado também a você por toda a colaboração e por nos permitir chegar às diferentes regiões. Ganhei o maior prêmio: ter a satisfação de sentir o que as regiões me transmitem, sentindo-me ajudado, o que não tem preço. Agradeço pessoalmente a cada um de vocês por ter feito a sua parte para que isto acontecesse. Muito obrigado Javier, de verdade

Ad content

O papel da **identidade digital** no processo de vacinação contra a **Covid-19**

Entrevista com **Kennedy Roman**, diretor Comercial Regional para o Caribe e América Central da VU Security.

Conteúdo audiovisual

A irrupção no mundo da imprevista pandemia da Covid-19 acelerou o processo de transformação digital em todas as áreas. Em tempos de distanciamento e isolamento social, a tecnologia tornou-se uma aliada de governos, empresas e cidadãos. Soube trazer soluções, ferramentas e métodos, que ofereceram uma importante cota de segurança à humanidade em xeque e ajudaram a superar desafios até recentemente difíceis de imaginar.

Nesse sentido, a experiência do Acordo sobre "Identidade Digital no Processo de Vacinação Covid-19", que uniu os Governos da América Central à VU Security, empresa multinacional especializada em prevenção à fraude e proteção de identidade, é muito interessante e motivadora, pois mostra como a segurança cibernética oferece respostas estratégicas, seguras e simples para alguns dos principais problemas que a sociedade enfrenta hoje.

Kennedy Roman, diretor regional para o Caribe e América Central da VU Security, explica como foram adotadas soluções presentes em um dos negócios mais regulamentados do mundo, o setor bancário, para acompanhar o cidadão no processo de vacinação, atestando a segurança desde o momento da identificação das pessoas até "Farmacovigilância", um elemento muito significativo que as empresas farmacêuticas já colocaram na mesa. Ao mesmo tempo, foi possível fortalecer o vínculo entre os governos e a indústria de tecnologia.

Na segurança de sua casa, o cidadão foi convidado a concluir o processo de registro para vacinação, aceitando os termos e condições, entre outras etapas, e acessando uma plataforma de registro:

por **Néstor Serravalle**

Diretor de Vendas Global,
VU Security.

Ilustración: kotkoa/Freepik

"Contamos com nossos aplicativos biométricos. Basta o cidadão digitar o número de identidade, tirar uma selfie e preencher um questionário de perguntas, validado por instituições médicas em todo o mundo. Ele também precisa informar se sofre de alguma doença crônica ou alergia, onde mora, data estimada para se vacinar, entre outras informações". A partir destas informações, são estabelecidas a segmentação, ordem de prioridade, grupos de interesse e condições de saúde dos cidadãos; é gerada a marcação da vacinação. Posteriormente, a evolução e os possíveis efeitos colaterais de cada pessoa são monitorados.

Kennedy Roman acrescenta: "A identidade digital é a base para a construção deste processo. Além de validar o cidadão, a plataforma registra o lote da vacina aplicada e permite o desenvolvimento da estratégia de farmacovigilância e monitoramento de efeitos colaterais. O processo nasce digital e permanece digital. Isto mudou todo o sistema de programas de vacinação, que era manual".

Ele destaca que foi possível gerar fluxos para todos os segmentos: "Muitos governos duvidaram do processo digital em locais com lacunas tecnológicas e problemas de conectividade. Porém, por meio de diferentes plataformas, o cidadão pode se autenticar e se inscrever. Com um dispositivo móvel básico, qualquer pessoa pode se tornar um multiplicador de inscrições, ajudando familiares, vizinhos e colegas de trabalho. A comunidade está unida nesta pandemia".

O foco da cibersegurança é tornar o mundo mais seguro, simples e, principalmente, permitir que os benefícios gerados pelo universo digital cheguem a toda a comunidade

Proteção de dados: Como colocar a Cibersegurança a serviço da LGPD

Ilustração: pch.vector, freepik

por: **Fernando Zamai**

A Lei Geral de Proteção de Dados (LGPD), uma espécie de versão brasileira do Regulamento Geral de Proteção de Dados (GPDR) europeu, entrou em vigor no dia 18/09/2020. A Lei considera dados sigilosos qualquer informação que permita identificar, direta ou indiretamente, um indivíduo que esteja vivo, e considera como dado pessoal: nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial, localização via GPS, retrato em fotografia, prontuário de saúde, cartão bancário renda etc.

Isto faz das organizações com operação em solo brasileiro guardiãs destas informações sigilosas e as coloca na mira de uma multa que pode chegar a R$ 50 milhões. Em outubro de 2020, praticamente dois meses após o início da vigência da lei, as primeiras decisões relativas à LGPD já ganhavam publicidade. A Justiça vem considerando, principalmente, o indevido compartilhamento de dados e, consequentemente, a falta de proteção de dados pessoais.

A LGPD pegou um mercado praticamente despreparado para esta nova realidade. Em meio à pandemia e com a crença de que a data seria mais uma vez adiada, as empresas ainda estão adaptando processos administrativos, operacionais e jurídicos. Também passou a ser urgente uma análise aprofundada da infraestrutura de cibersegurança, para emprego efetivo da tecnologia na proteção da base de dados dos clientes.

Falando em infraestrutura tecnológica, a pandemia da Covid-19 obrigou as empresas a colocarem boa parte dos seus colaboradores trabalhando em casa, com acesso remoto aos servidores corporativos e sem as tradicionais proteções empregadas no ambiente corporativo. Isto aumentou a taxa de vulnerabilidade fazendo com que, em 2020, fossem registrados recordes de crescimento anual de ataques de phishing, ransomware e outros riscos cibernéticos.

A vida digital ficou mais intensa e o anúncio de ataque de ransomware pode ser, inclusive, uma cortina de fumaça para desviar a atenção de algo que já ocorreu e aguarda o momento certo para uma barganha inescrupulosa de pagamento do "sequestro" contra a divulgação parcial ou total dos dados do seu cliente em ambientes obscuros.

Então como a tecnologia pode ajudar as organizações a se adequarem à LGPD? Como preservar a sua imagem frente aos clientes, já que, ao mesmo tempo em que são guardiãs das informações estão vulneráveis aos ataques cibernéticos?

A resposta está na infraestrutura de cibersegurança. Passou da hora de uma revisão generalizada e aprofundada dos recursos disponíveis internamente. É preciso saber quanto da infraestrutura de cibersegurança está efetivamente em uso e qual é a eficiência em relação à proteção a ataques. Controle hoje é igual a custo, número que pode ser alto dependendo da pena aplicada pelos juízes nos julgamentos que consideram a LGPD.

Faça um Helth Check, sem custo, da sua infraestrutura de segurança cibernética. Nosso time de especialistas acessa remotamente, por Webex, a sua base e realiza um laudo em horas. Sua rede virtual (VPN) não pode ficar exposta. Por isto, recomendamos controles avançados integrados com o serviço internacional de inteligência Talos, para que você não apenas tenha domínio do ambiente de TI que suporta os dados protegidos pela LGPD como tenha um canal seguro para contar em caso de problemas.
Contate a um especialista da Cisco

Resiliência da força de trabalho: estenda a segurança para os funcionários remotos

por **Juan Pablo Mongini**

Alguns eventos são tão prejudiciais que nos obrigam a repensar tudo. Mas muitas vezes são uma bênção disfarçada. Todos os tipos de inovações surgem de questões como "Existe uma maneira melhor de fazer isso?" e "Devemos realmente fazer isso?"

Por exemplo: muitas empresas acreditavam que era impossível para toda a sua força de trabalho atingir seus objetivos sem trabalhar no escritório. Mas, vejamos o que aconteceu. Em face das grandes mudanças, nossos funcionários prosperaram. Muitos descobriram que são mais produtivos em casa do que no escritório. Eles se beneficiaram por passar mais tempo com suas famílias e menos tempo em viagens longas e estressantes para o escritório. Um estudo recente concluiu que "quase 90% dos funcionários prefeririam continuar trabalhando em casa em alguma função e quase metade gostaria de trabalhar em casa com mais frequência ou o tempo todo".

As empresas também se beneficiaram com funcionários mais produtivos, despesas operacionais reduzidas (com escritórios vazios, sem reuniões de trabalho e sem viagens) e reavaliaram o acesso a pessoal qualificado distribuído.

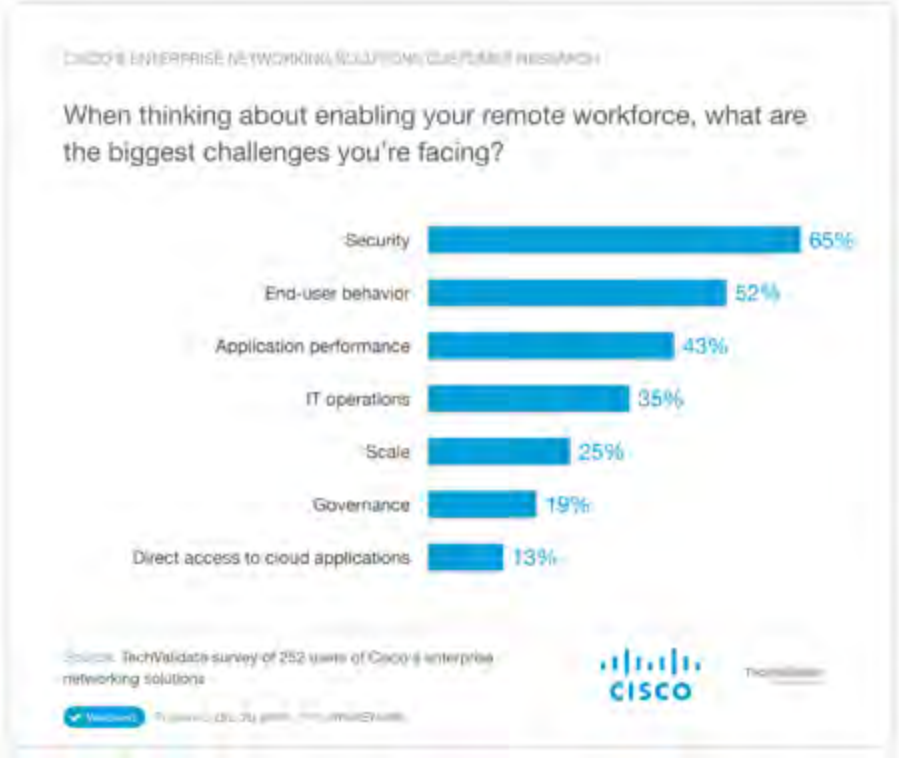
Isso levanta a questão: é hora de redesenhar a rede de negócios? Quer sua empresa exija ou não que seus funcionários trabalhem no local, às vezes eles precisam trabalhar remotamente. Mesmo sob uma perspectiva de resiliência de negócios, diante de um evento perturbador, a sua organização deve ser capaz de estender a rede, com segurança, a todos os usuários, independentemente de onde eles estejam.

Parece fácil, parece apenas uma questão de expansão da VPN, com a adição de alguns aplicativos em nuvem, para que os funcionários tenham acesso e trabalhem a partir de qualquer lugar.

Infelizmente, habilitar o trabalho remoto apresenta novos desafios. O funcionário remoto nem sempre tem a largura de banda que os aplicativos de negócios de alta qualidade consomem. Além disso, eles nem sempre (como posso dizer isso sutilmente...) têm as melhores práticas de segurança. Eles en-

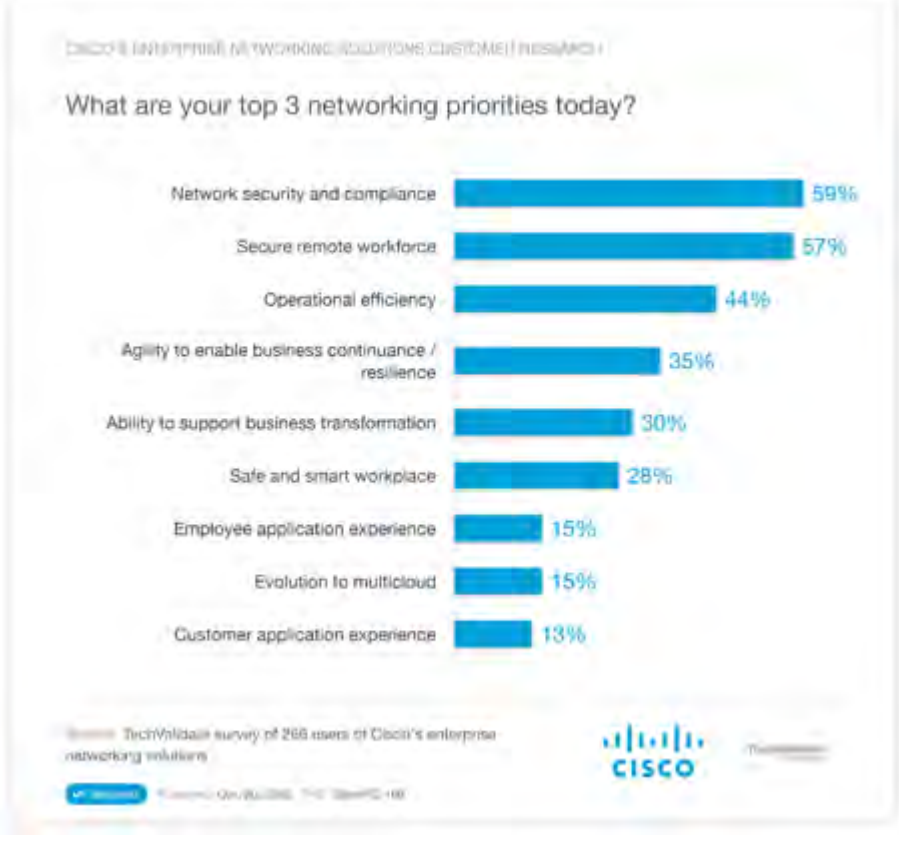
Imagen: Bella H., Pixabay

tram em redes não confiáveis, clicam em links de phishing, usam seus dispositivos pessoais e baixam aplicativos maliciosos (TI paralela?).Não vamos nem pensar em casos como o usual “Senha1”. E só porque usam uma VPN, os funcionários podem, nem mesmo, perceber quanto tráfego geram na rede corporativa ao executar aplicativos não comerciais como YouTube, Netflix, FaceTime ou Spotify.



Em uma pesquisa recente com clientes da Cisco, os comportamentos do usuário final aparecem como o segundo maior desafio que a equipe de TI tem que enfrentar com relação à força de trabalho remota. (A segurança sempre vence neste concurso.)

Gráfico de desafios para força de trabalho remota



Esta mesma pesquisa, realizada em setembro, descobriu que para 57% das organizações a segurança da força de trabalho remota era uma alta prioridade, um aumento de 23% em relação ao período anterior à pandemia. Ou seja, apenas cinco meses antes do êxodo dos escritorios, em março.

Gráfico das 3 principais prioridades da rede

O que podemos fazer? A área de TI deve implementar estratégias para estender a conectividade à rede de funcionários remotos que trabalham em casa ou em micro-escritórios de forma segura, proporcionando-lhes uma experiência ideal com aplicações, por meio de soluções gerenciadas de forma centralizada. A TI deve fornecer aos funcionários remotos o mesmo nível de proteção, go-

vernança e desempenho que eles desfrutam no escritório.

Aqui estão alguns requisitos de rede para que funcionários remotos tenham segurança de nível empresarial:

Dimensione VPNs para proteger funcionários remotos

VPNs são definitivamente uma opção para expandir o controle de nível empresarial e proteger funcionários remotos. Os túneis divididos também podem ajudar a reconectar aplicativos comerciais críticos à rede corporativa e desviar aplicativos não comerciais da Internet.

Melhor conectividade: pontos de acesso corporativos em casa

Você quer levar a experiência a um nível totalmente novo? Os funcionários que usam um ponto de acesso corporativo atrás de seu roteador pessoal não precisam usar uma VPN. Essa opção também otimiza os aplicativos de voz e vídeo e permite que os usuários se conectem com eficiência a partir de vários dispositivos, como telefones IP e terminais de vídeo.

O modelo Secure Access Services Edge (SASE) protege aplicativos multi-nuvem

A segurança baseada em nuvem e o modelo SASE ajudam na defesa contra ameaças na Internet, independentemente da conexão, dispositivo ou ambiente de nuvem que o usuário usa.

Conclusão

Ao repensar quais medidas serão necessárias para se recuperar de qualquer interrupção, os funcionários estão no epicentro. Estender a rede para onde os usuários estiverem, embora não seja fácil, é o futuro. Afinal, a rede dá aos nossos funcionários acesso seguro aos aplicativos e os dados de que precisam com o alto desempenho que esperam, estejam trabalhando em casa ou no escritório

- Leia as cinco principais tendências de rede para 2021 em relação à resiliência de negócios.
- Aprenda como você pode conectar seus funcionários que trabalham em casa com segurança.
- Aprenda sobre as soluções de rede da Cisco para garantir a continuidade dos negócios.

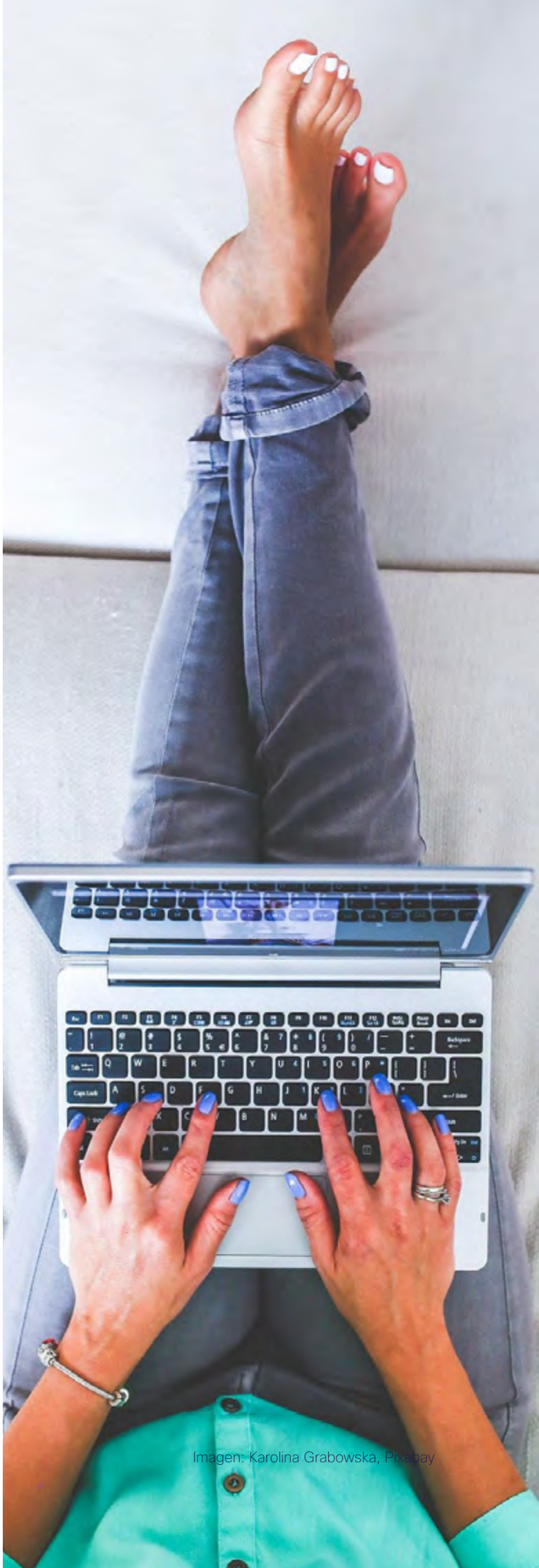


Imagen: Karolina Grabowska, Pixabay

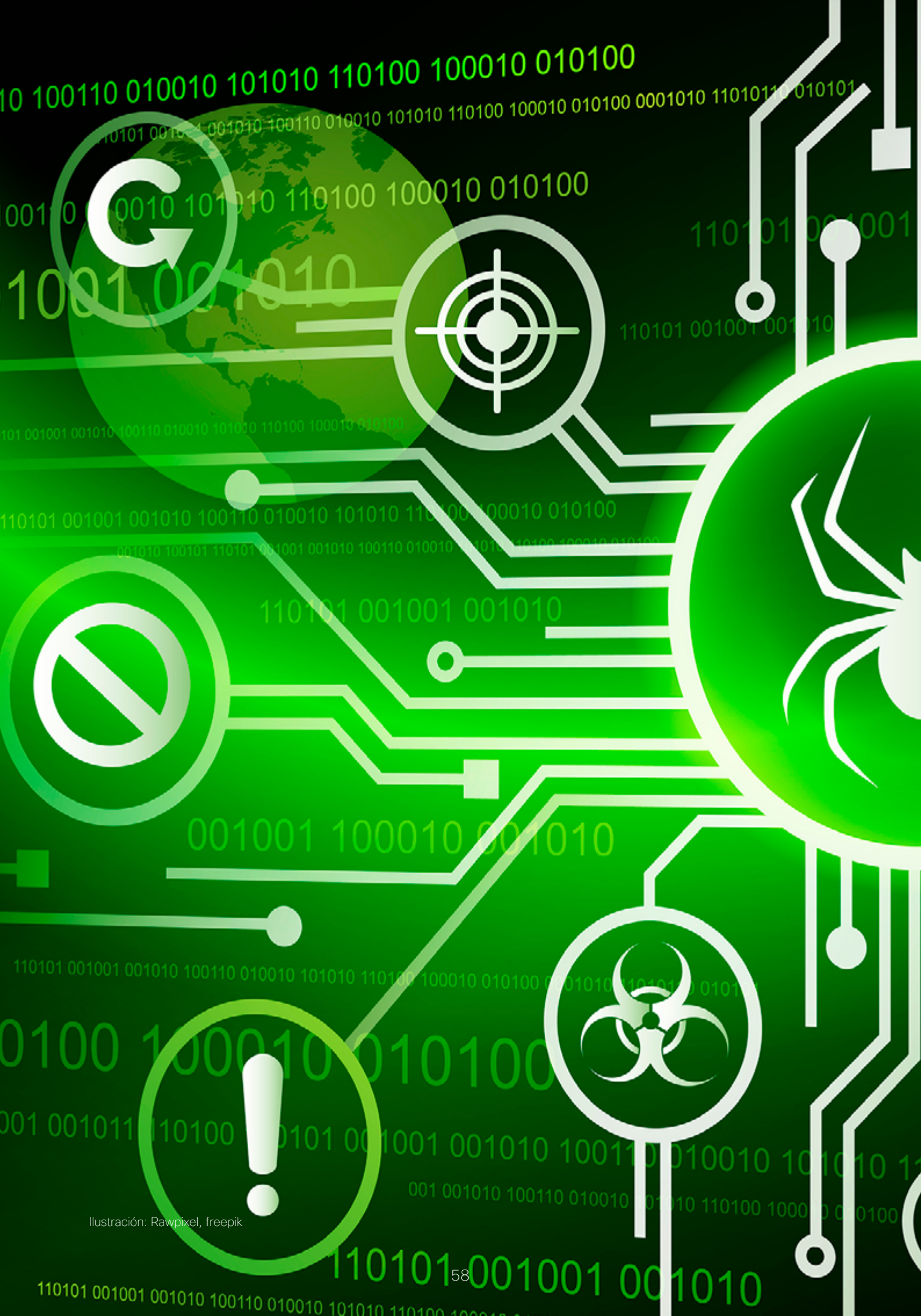


Ilustración: Rawpixel, freepik

Guerra Cibernética

por **Marcelo Bezerra**

Em 2015, o presidente da China Xi Jinping e o então presidente dos Estados Unidos, Barak Obama, assinaram o que é considerado o primeiro acordo entre nações para o controle de ações de ataque cibernético da história. No documento, os países concordaram em não patrocinar ações de espionagem industrial e roubo de atividade intelectual. O acordo, histórico indubitavelmente, nos leva a pensar no que convencionamos chamar de guerra cibernética.

Travar uma guerra através da internet faz parte do nosso imaginário há bastante tempo, graças aos filmes de Hollywood e a alguns eventos marcantes como o famoso caso do vírus Stuxnet, criado em 2010 especialmente para atacar os sistemas de controle das centrífugas iranianas de enriquecimento de urânio.

Embora não tratando literalmente de guerra cibernética, o acordo entre Estados Unidos e China confirmou o que naquele ano, 2015, ainda não era publicamente admitido: que países patrocinam ações ofensivas contra outras nações, inimigas ou não, através da internet. Hoje, a situação está bem diferente. Não só sabemos que as ações existem, como temos conhecimento de que elas fazem parte publicamente da estratégia militar de vários países. Em setembro de 2019, o Departamento de Defesa dos Estados Unidos publicou no seu plano estratégico o propósito do uso de armas cibernéticas ("cyber weapons"), para promover os interesses e a defesa dos EUA. Já no Reino Unido, um general confirmou que o país possui armas para "degradar, interromper e destruir" infraestrutura crítica no momento necessário, em caso de guerra.

O tema, entretanto, não é consensual. Há muita discussão sobre o que significa arma e guerra cibernética, principalmente se consideramos que as armas mais sofisticadas atualmente embutem um sem-número de sistemas e componentes eletrônicos.

Para o ex-conselheiro do governo dos Estados Unidos, Richard A. Clarke, autor do best-seller sobre o tema –Cyber War– publicado em 2010, guerra cibernética se define como as ações patrocinadas por um Estado nacional para penetrar em redes ou computadores de outras nações, com o objetivo de causar dano ou sabotagem. À luz do mundo interconectado globalmente, a definição não deixa dúvidas de que muitas ações empreendidas ou patrocinadas por um Estado poderiam ser consideradas um ato de guerra.

Inteligência de ameaças para monitorar de perto o problema

Bem recentemente, duas ações tornaram-se públicas e foram atribuídas a países, embora não admitidas. A primeira delas foi a invasão da empresa de segurança FireEye e o roubo do software criado por seus especialistas para uso em seus contratos de consultoria. O fato de a empresa ter noticiado que não havia nenhuma técnica ou malware para exploração de vulnerabilidades desconhecidas entre o material roubado não reduz sua importância. O segundo foi a descoberta do comprometimento de um software de gerência amplamente usado por empresas e organizações estatais do fabricante SolarWinds. Novamente atribuído à um país, e novamente não admitido.
Dois artigos no blog do Talos, em https://blog.talosintelligence.com, ajuda a entender os ataques e seus potenciais efeitos. O Talos, atualmente a maior organização privada de inteligência de ameaças, parte da Cisco Secure, vem acompanhando com atenção o tema. Uma ação de espionagem contra diplomatas baseados no Chipre foi analisada pela equipe, que identificou uma campanha ainda mais ampla, que atingiu 40 diferentes organizações.
Os ataques realizados por países costumam ser altamente sofisticados e trazem riscos diversos caso vazem e ataquem computadores além do alvo inicial. O grupo também analisa continuamente a segurança de sistemas de infraestrutura crítica, provavelmente o maior alvo em caso de uma ação de guerra real.

Armas cibernéticas: com foco em vulnerabilidades

A tecnologia empregada na guerra cibernética possui características únicas. Diferente das armas tradicionais, uma arma cibernética não possui potencial destrutivo. O seu impacto irá depender do sistema atacado e não dela propriamente.
Imaginem um programa de ataque capaz de invadir um computador permitindo que este seja controlado remotamente. Qual o efeito? Se for o computador das nossas casas, iremos perder algumas centenas de fotos, mas e se for o computador que controla a operação de uma indústria? E se for uma central nuclear? O efeito de um ataque cibernético é também desconhecido até que ele ocorra, e mesmo assim é possível que a vítima consiga acobertar parte dos impactos. Deste ponto de vista, parece uma arma pouco eficaz, mas aí temos o que faz dela algo tão atrativo. Ela é totalmente fria. Não há explosões ou mortes aparentes. Não há cenas emotivas ou soldados mortos. Ela é invisível e pode penetrar em bunkers totalmente a prova de ataques, até mesmo nucleares, por meio de um simples pendrive de um funcionário desatento. E, muito importante, pode ser facilmente negada. Dificilmente uma nação poderá retaliar outra tendo como base apenas um ataque a seus sistemas de computador, já que ataques bem feitos dificilmente são rastreáveis. Como retaliar se não há certeza absoluta?
Armas cibernéticas também não são estocáveis. Em uma guerra tradicional leva clara vantagem o adversário que possui maior quantidade de armas e maior poder de destruição. Na guerra cibernética não há quantidade de armas e, como já comentado, seu potencial de destruição depende do seu alvo. Um arsenal cibernético é também diferente, pois é composto de técnicas e conhecimento. As técnicas são as vulnerabilidades existentes em sistemas e os programas de invasão capazes de explorá-las. Quanto mais desconhecidas maior o valor destas vulnerabilidades chamadas de dia zero.
Os programas são geralmente porções de códigos de programação intercambiáveis que podem ser usados em diferentes situações para explorar vulnerabilidades. Há também programas específicos para burlar sistemas de defesa digital, como firewalls. Estas diferentes porções de código são então combinadas em kits de ataque, sistemas de invasão complexos como o Stuxnet.
Para tudo isto, vulnerabilidades dia zero, programas e kits, há a necessidade do conhecimento de especialistas e gênios da computação, os hackers. Este patrimônio intelectual é a base do "estoque" da guerra cibernética. Sem ele, não há ataque nem defesa. Em uma guerra totalmente científica conta-se cérebros e não ogivas

Spoiler Bridge №4

Hackeando previsões

Passado pisado. Futuro, hackeado? Quando as previsões não são boas, podemos interferir para desviar seu curso. Como podemos colaborar, unindo forças entre os setores público e privado, provedores de tecnologias e serviços de segurança cibernética? Que contribuição empresas como a Cisco estão dando ao mundo para permitir vida e economia digitais resilientes?

Nesta produção audiovisual e escrita, **Juan Marino**, gerente regional de segurança cibernética da Cisco, revisita as principais previsões dos analistas de mercado e dá dicas para "hackeá-las" ou cumpri-las conforme apropriado.

Entrevista

Ángel Thomas Paulino C., CISO do Banco Caribe e Presidente do Comitê de Segurança Cibernética da Associação de Bancos Comerciais da República Dominicana (ABA).

Juanita Rodríguez Kattah, Vice-reitora de Inovação Acadêmica, EAN University, Colômbia.

Ping-pong - perguntas e respostas com Gary Becklund

Nesta reunião, o líder que mais recentemente atuou como diretor de Operações e diretor de Vendas, Segurança Cibernética das Américas na Cisco, analisa sua carreira de 20 anos na companhia e compartilha experiências e aprendizados.

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*