Ano 2. Número 6.

Bridge

CISCO SECURE

Cibersegurança

Especial Trabalho híbrido

CX Danilo Pozo

Vice-presidente de Experiência do cliente da Cisco

Quem é quem: Luz María Murguía

OCP TECH

INGENIERÍA DE **IMPACTO**

EXPERTOS EN SOLUCIONES DE CIBERSEGURIDAD

¡CONOCE MÁS DE OCP TECH!

OCP TECH
OCP . TECH

CISCO Partner

ARGENTINA

Ing. Enrique Butty 240
piso 3 Capital Federal,
Buenos Aires, Argentina
T +54.11.2152.9600

COLOMBIA

Cra 9 N0. 115-06 Piso 7
Of 701, Edificio Tierra Firme,
Bogotá, Colombia
T +57 1 442 3209
T +57 313465.3030

USA

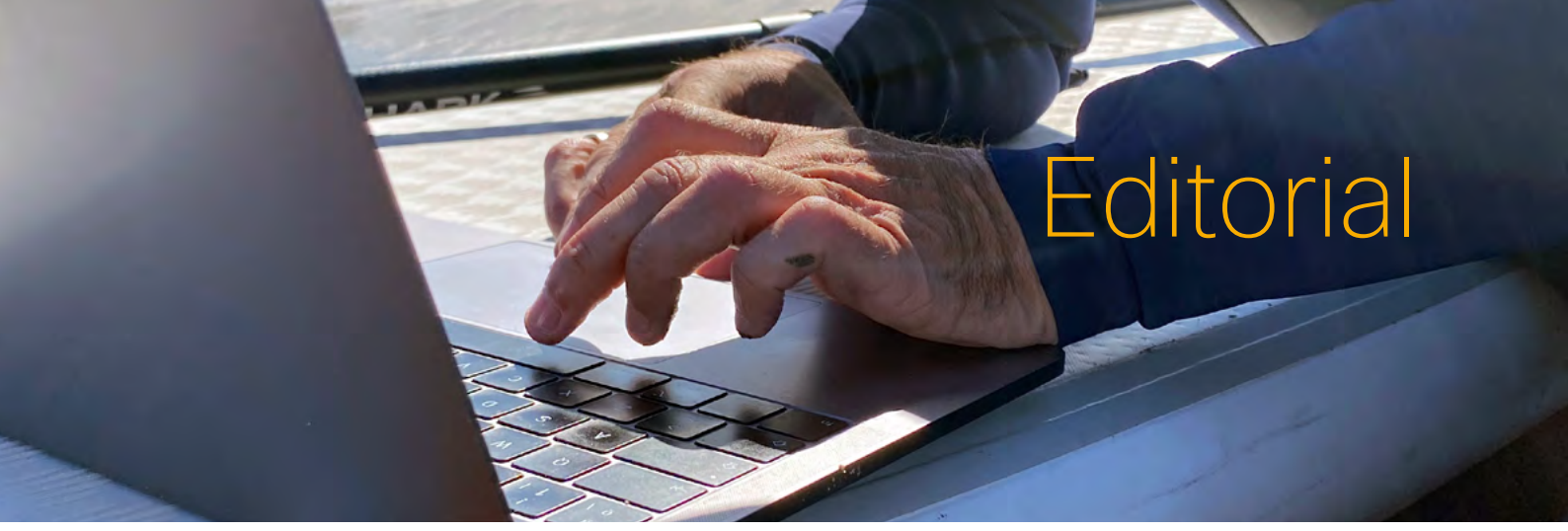
333 S.E. 2nd Avenue, Suite
2810, Miami, Fl 33131
United States of America
T +1.305.537.0800
T +1.305.537.0704

PANAMÁ

Oceania Business Plaza
Torre 2000 Piso 33 A,
Boulevard Pacífica - Punta
Pacífica, Panamá City -
República de Panamá
T +507 3877300

PERÚ

Calle Las Orquídeas 585,
Edificio Fibra, pisos 12 y
13, San Isidro, Lima.
T +511 712.5901



Editorial

Trabalhar na praia pode ser interpretado como a expressão máxima do trabalho remoto, da liberdade, do "work life balance". Também do ponto de vista negativo, pode-se pensar que a pessoa não pode deixar de trabalhar mesmo em férias. Da equipe editorial da Bridge, claro, ficamos com a primeira impressão.

Ao longo desta edição recolhemos perspetivas que sustentam o trabalho híbrido como modelo a ser seguido a partir da convicção de que é esta a resposta ao fato de que os trabalhadores procuram equilibrar o seu desempenho na vida, e também os empregadores, a partir de uma lógica de produtividade e retenção de colaboradores.

Estamos enfrentando uma mudança de época. A pandemia foi um catalisador para transformações que vinham se formando há muito tempo. Como aponta nosso colunista Pablo Marrone, "o padrão cultural flui, como se fosse um relógio Dalí". Esse relógio distorcido e maleável nos faz pensar em uma ruptura no tempo, nos horários, na sincronia, uma mudança fundamental na forma de interagir socialmente, de colaborar, de fazer tarefas.

Conseguir gerenciar essa mudança individual e coletivamente é um grande desafio. Há quase 10 anos, o filósofo Byung Chul Han nos alertou sobre um futuro distópico em seu livro "A sociedade do esgotamento", seguindo a convicção de que estamos nos realizando." Depois, em outra de suas obras, o mesmo autor nos falaria sobre o "Aroma do Tempo" e "O Desaparecimento dos Rituais". Parece que o filósofo vem entrelaçando os argumentos fundamentais de um chamado à reflexão sobre a necessidade de mudança em nosso modus vivendi.

Uma boa implementação do trabalho híbrido é certamente parte da resposta à necessidade de explorar nossas capacidades de produção de forma positiva, em vez de explorar a nós mesmos.

Pessoalmente, resisto a um olhar superficial sobre os benefícios do trabalho híbrido a partir de uma lógica de produtividade limitada à economia de tempo ou à preferência pelo conforto de trabalhar de pijama. Em vez disso, acredito que o panorama atual nos confronta com a possibilidade de projetar o trabalho desta nova era, criando os ambientes de produtividade mais eficazes para cada perfil de colaborador e entendendo a produtividade como deve ser: produzir os melhores resultados, a partir do melhor desempenho cognitivo, algo alcançado quando as pessoas estão motivadas, energizadas e em um fluxo mais harmonioso entre trabalho e vida pessoal, ou seja, em um "work life flow".

Juan Marino

Staff

Produção abrangente Basanta Contenidos

Diretora Editorial
Karina Basanta

Diretor de Arte
Nicolás Cuadros

Coordenadores
Marta Pizzini
Marta Assandri

Produção audiovisual
Salpufilms

Colaboradores neste número
Silvia Montenegro
Jorge Prinzo
Freddy Macho
Pablo Marrone

Fotografía e ilustração
Basanta Contenidos
Freepik
Pixabay
Unsplash

Agradecimentos
Nicolás Cacciabue
Isabella Cacciabue
Jorge Cuadros
Joaquín Cuadros
Santino Cuadros

Foto de Capa
Basanta Contenidos

Diretora Editorial
Karina Basanta

Diretor de Arte
Nicolás Cuadros

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

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

Ilustração: Freepik.

Revista Bridge **Impresso / Digital**
Ano 2. Número 6

Cisco Latinoamérica

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

Editor General
Juan Marino

Agradecimentos
Taiane Belotti
Luz María Murguía
Danilo Pozo
Jackeline Carvalho
Militza González

Marketing

Taiane Belotti
Líder de Marketing, Segurança Latam
Jimena Reyna Briseño
Gerente de Marketing de Contenidos, Segurança, Latam

Bridge Nº 6

Sumário

Editorial 3

4 **Staff**

6 **Sumário**

Pregunta aberta
Na visão de
Taiane Alves 8

10 Testemunhos de sucesso
Networking Academy
Rafael La Selva.
por Rodolfo Basanta

Entrevista 14
Danilo Pozo
VP Customer Experience, Cisco
por Karina Basanta y
Jorge Prinzo.

20 Quem é quem
Luz María Murguía
por Karina Basanta

Ad Content OCP Tech 26
Dionísio ou Dâmocles:
esta é a questão
por Fabio Sánchez

30 **Coluna**
Smart Supply chain
por Freddy Macho

Especial 42
Trabajo híbrido

Coluna
Pablo Marrone

44 Cumprir a promessa
do trabalho híbrido

48 Alinhamento C-level

50 Cinco dicas para mantê
lo seguro

Formação profissional 52
Programa neddux

56 Estudo de privacidade
de dados, Cisco 2022

OFFICIAL TECHNOLOGY PARTNER

Cisco e Real Madrid unidos para criar o estádio mais conectado da Europa.

Como Parceiro Tecnológico Oficial do Clube, a Cisco vai equipar o novo estádio Santiago Bernabéu com um destacamento integral de sua tecnologia líder na indústria, incluindo soluções de conectividade, segurança, centros de dados e sinalização digital, tudo concebido sobre uma única rede inteligente e convergente de Cisco.

O estádio multiuso de 85.000 lugares contará com a maior rede de conectividade sem fio baseada em tecnologia Wi-Fi 6 da Europa.

Mais de 1.200 pontos de acesso Wi-Fi 6 no Santiago Bernabéu oferecerão maior velocidade, confiabilidade e largura de banda do que o padrão anterior,para que os fãs desfrutem de experiências mais imersivas interagindo com seus dispositivos e aplicações, segurança, transmissão e repetição de vídeo.

Durante os próximos anos, a conectividade remodelará a indústria do esporte e redefinirá novas possibilidades. Acreditamos que a digitalização está mais importante que nunca.

Juntos, Cisco e Real Madrid já estão levando o setor do Esporte e Entretenimento para o futuro e além.

Na visão de

Taiane Alves
líder de marketing de segurança cibernética para a América Latina da Cisco

Nos últimos anos, o crescimento do SaaS como estratégia de negócios ficou evidente. Como o departamento de marketing acompanha esta tendência?

É um desafio muito grande, já que o setor de SaaS cresce a cada ano e é um mercado que deve movimentar cerca de US$ 85,1 bilhões apenas neste ano e atingir o total de US$ 113,1 bilhões em 2023 – um crescimento de 32,9% em apenas 1 ano, segundo relatório da consultoria Gartner.

Em um cenário de intensa competitividade e alta tecnologia, não há mais espaço para fazer tudo do jeito antigo. Ou seja, as soluções surgem em uma velocidade cada vez mais rápida e com funções específicas para resolver os problemas das corporações – logo, não é inteligente perder tempo (e dinheiro) tentando conectar estes sistemas de forma manual.

Dessa forma, para acompanhar este setor e se destacar no meio da multidão de concorrentes, abraçando este cenário de oportunidades, é imprescindível uma estratégia de marketing muito bem orquestrada, ou seja, o foco no digital não é apenas uma opção, ele é crucial e mandatório para o sucesso de uma campanha de marketing efetiva. Quando falamos de software como serviço, por não ser um produto físico e tangível, precisamos ir além das táticas de marketing convencionais. Existem alguns elementos, que devem acompanhar o mercado de SaaS, com o objetivo de atrair novos clientes e gerar negócios. Listo aqui alguns deles: campanhas 100% digitais, marketing de conteúdo, investir na otimização do SEO, ofertas de free trial, experiência do cliente, utilização de CTA's atraentes e claros e tudo isso aliado a um plano contínuo para a retenção de clientes a longo prazo.

Na Cisco, esta migração é acompanhada por uma forte estratégia de CX. Qual é a sua visão do marketing desta dupla corrente, ou seja, onde você vê o ponto de união?

Eu diria mais que ponto de união. É quase impossível pensar em uma estratégia de Marketing voltada para SaaS, sem pensar na experiência do cliente. A jornada de compra do cliente, desde a experimentação do produto até a efetiva compra, precisa ser diferenciada. O cliente precisa ter uma jornada sem percalços. O modelo SaaS só prosperará com o cliente satisfeito. Se por qualquer motivo o cliente tiver uma péssima experiência, ele simplesmente troca para a outra solução do concorrente. Resumidamente: a estratégia de CX é essencial para o marketing de SaaS.

Esta edição do Bridge é atravessada pela modalidade de trabalho híbrido a partir de diferentes pontos de vista. O que é o departamento de marketing da Cisco Latam Cybersecurity?

Para falarmos de trabalho híbrido acho importante pontuarmos qual é o seu significado. Na minha opinião, o trabalho híbrido é muito mais do que o simples fato do local de trabalho, seja em casa, no coworking ou na sede da empresa, mas na oportunidade de dar ao colaborador o poder de escolha. Você escolher o local onde irá trabalhar. Isto fala muito mais do que o trabalho em si, e traz a liberdade e a autonomia que geram benefícios positivos, não apenas na produtividade, mas na qualidade de vida e bem-estar das pessoas. É claro que o tema da segurança cibernética é importante quando trabalhamos remotamente, mas acredito sempre que o bom senso e soluções adequadas de proteção, juntamente com uma política de segurança da informação da empresa, ajudarão na tranquilidade de poder trabalhar em qualquer local.

Pergunta aberta

Essa seção é chamada de Pergunta Aberta porque convida o entrevistado a gerar sua autopergunta com um tópico livre. Qual é a tua? E sua resposta a ela?

Ainda sobre trabalho híbrido, gostaria de compartilhar alguns resultados do "Duo Security Report" da Cisco que revela o aumento do uso de soluções de MFA (duplo fator de autentificação) em empresas que adotaram o trabalho híbrido. Compartilho abaixo alguns números deste relatório:

- As autenticações multifatoriais aumentaram conforme as empresas deixam de usar as senhas para proteger os trabalhadores híbridos.

- A biometria aumentou significativamente, com um crescimento de 48% nas autenticações em relação ao ano anterior.

- Mais da metade dos tomadores de decisão de TI planejam implementar uma estratégia sem senha.

- Duo também teve um crescimento de cinco vezes no uso em Web Authentication (WebAuthn) desde abril de 2019.

- A América Latina teve um crescimento de 18% no uso de autenticação através de aplicações na nuvem. Europa e Oriente Médio tem o percentual mais alto, com 190%.

A autenticação sem senha do Duo faz parte da plataforma líder de mercado, Zero Trust da Cisco, que protege o acesso de qualquer usuário, a partir de qualquer dispositivo e em qualquer aplicação ou ambiente de TI. O produto é projetado para ser agnóstico em termos de infraestrutura, abrindo caminho para um futuro sem senhas ao mesmo tempo em que garante que as corporações possam proteger qualquer combinação de aplicações na nuvem e on-premises sem falhas, sem precisar de produtos de autenticação múltipla e sem abrir brechas graves de segurança.

Deixo aqui o convite para você baixar o Duo (free trial) hoje mesmo:: https://signup.duo.com/trial

Imagem: Gentileza Taiane Alves.

Testemunhos de sucesso

Networking Academy

Em primeira pessoa

Rafael La Selva,
Engenheiro em
Sistemas da Cisco,
Dynalogic

por **Rodolfo Basanta**

O que o motivou a se juntar ao programa de cibersegurança da NetAcademy?

Em agosto de 2017, eu me lembro de ler um artigo em um blog de notícias onde Cisco estaria oferecendo treinamento em Segurança Cibernética para aqueles que se inscreveram; o número foi limitado a 10.000 candidatos para uma das primeiras turmas. Este foi o primeiro contato que tive com o programa de NetAcademy. Nesta altura, eu já atuava como engenheiro de pós-venda de segurança e, como estava familiarizado com o portfólio do Cisco, decidi me candidatar. Fui aprovado com sucesso e, ao final, pude solicitar outra certificação técnica com um comprovante fornecido pela Cisco.

Como foi a tua experiência?

Foi uma viagem agradável, aproximadamente 6 meses de muita aprendizagem e prática. Não foi apenas um curso, mas uma verdadeira capacitação com todo o apoio da comunidade e dos colegas. Com o programa de bolsas de estudo e da NetAcademy da Cisco, pude continuar a desenvolver as minhas habilidades e a minha carreira em virtude de me tornar um profissional mais completo e apegado às exigências do mercado, especialmente em Cibersegurança.

Hoje você trabalha na Dynalogic. Como a sua formação contribuiu para isso?

A educação é sem dúvida um ponto fundamental na vida de qualquer pessoa, tenho uma carreira e algumas certificações que me deram uma boa base, além de uma amplitude sem fronteiras para o mercado de TI e Infraestrutura. Me lembro que já no primeiro semestre da universidade consegui meu primeiro trabalho como estagiário onde pude levar à prática tudo o que aprendi durante o curso. Possuir um segundo ou mesmo um terceiro idioma continua a ser essencial para ampliar horizontes.

No entanto, eu acho que muito mais importante do que o conhecimento é a viagem. O acesso a grandes líderes e mentores, colaborar em casos com equipes experientes que conhecem o tema foi o que realmente me ajudou a obter a direção e o enfoque necessários para meu desenvolvimento técnico e interpessoal.

O mercado indica que há uma grande procura de especialistas em cibersegurança. Qual é a sua recomendação para quem procura desenvolvimento profissional?

Posso dizer que este é um alerta que tem chamado a atenção e que ouço há anos, desde que tudo aponta para a aceleração da digitalização. Além disso, a demanda por cibersegurança se mostra ascendente desde que o acesso à internet passou a ser feito a partir de dispositivos pessoais.

Por exemplo, hoje é normal que os empregados trabalhem em casa com seus laptops pessoais ou da empresa, ou que eles acessem diretórios e arquivos sensíveis mesmo estando fora da organização, utilizando smartphones e tablets. Ao observar esses cenários, você pode imaginar o desafio de tornar todos estes dispositivos e acessos seguros. Por isto, a procura de profissionais especializados em cibersegurança se tornou tão importante. Vivemos um contexto ainda mais hostil do que no passado, dada esta mobilidade e descentralização dos dados.

Para todos aqueles que buscam se desenvolver profissionalmente em cibersegurança, há muitas oportunidades: se capacitar, aprender e evoluir no caminho; se expor a situações críticas; e trabalhar colaborativamente com grupos mais experientes. Tenho certeza de que, com o tempo, as respostas a muitas das perguntas virão naturalmente

Basanta
contenidos

Contenidos Multiplataforma

basantacontenidos.com

Produzimos textos originais

Entrevista

Danilo Pozo
VP Customer Experience,
Cisco.

CX

Imagem: Youssef Naddam, Unsplash.

Preservar e promover uma experiência de cliente ótima é um dos objetivos mais importantes das organizações de hoje. Em um contexto de alta competência onde qualquer falha pode desencadear a perda de um usuário, a área de CX assume um papel chave. Tanto que toda a cultura organizacional precisa se juntar a ela. Para aprofundar este tema, falamos com Danilo Pozo, VP de CX, Cisco.

por **Karina Basanta y Jorge Prinzo**

Do que falamos quando falamos de Customer Experience? Como nasce este conceito? É algo que deveria ter existido sempre, porém, na era digital, ganha uma relevância que antes ficava sobreposta.

A Cisco sempre esteve atenta ao negócio do cliente; uma das coisas mais bonitas da empresa é que ela vê as pessoas como uma prioridade. Acho que Customer Experience nasce da forma como definimos uma metodologia, um processo, como montamos uma equipe para garantir que este sentimento, esta percepção que o cliente tem de como ele pode crescer com a Cisco, tem uma forma de fazer. Além disto, entender como o cliente está crescendo em sua transformação digital. Estamos todos sob uma tremenda pressão para entregar valor de uma forma mais fácil, para chegar ao mercado mais rápido. Customer Experience tem o objetivo de preservar a experiência do cliente com a Cisco e acompanhá-lo até seus objetivos. Obviamente, trabalhando em conjunto com o parceiro para aumentar o valor de ambas as empresas e trazer uma única solução para os nossos usuários, para que eles estejam conectados de uma forma muito mais rápida, mais ágil, mais segura... trabalhar em conjunto para aumentar a automatização e o uso da inteligência artificial, para que a operação seja mais dinâmica e possa gerar resultados mais rápidos.

Como a experiência do cliente é medida? Existe alguma plataforma específica para isso? O que é o Rox?

Existe sim. Nós temos três coisas consideradas sumamente importantes, que são nosso norte, nossa visão. Primeiro, o que chamamos de CX Lifecycle, que é basicamente a metodologia de como nos alinhamos com o cliente e com o parceiro, para garantir que temos não só o melhor poritfólio, mas os especialistas e os processos adequados para que se implemente de forma rápida. Depois, adentrando-nos na fase de compra, procuramos assegurar que o caminho seja mais fácil, mais ágil. Isto nos leva a alcançar uma integração ótima que garanta a implementação no momento e no lugar mais adequados para as necessidades do cliente. E o que estamos começando a somar e desenvolver de uma maneira mais forte, é a parte de adoção de tecnologia. além disso, eventualmente, fazer com que o mesmo cliente comece a distribuir a notícia de que a Cisco tem uma solução robusta, rápida e segura. Por sua vez, na Cisco, a partir da vivência dos usuários, renovamos esta plataforma e a expandirmos para conseguir o Return of Investment ou Return of Experience.

A nossa segunda abordagem é que tudo vem em torno de insights em telemetria. Eu gosto de dizer que a CX está no negócio das pessoas (People Business), pois nossa equipe não cria um serviço ou um produto. Vemos como as pessoas trabalham com a Cisco, como percebem a empresa e as suas soluções. Isto é baseado em dados e telemetria, e tem a ver especificamente com a combinação de plataformas digitais. Hoje trabalhamos com o que chamamos de CX Cloud, que é um portal, que nos dá a oportunidade de ver onde está a plataforma do cliente, onde está a sua rede, quão vulnerável pode ser, quão segura está, quais são as versões de software que tem, e o que lhe convém. É muito dinâmico, e nos permite acelerar o cliente e levá-lo de um estágio para o próximo, através de sessões web que o ajudam a entender o que comprou, como usá-lo, como adotá-lo.

E a última coisa que medimos é o sucesso do portifólio da Cisco. O que a CX procura hoje não só criar o portólio e oferecê-lo, mas ouvir o cliente para entender a sua experiência. Especialmente em torno do que chamamos Success Tracks e Business Critical Services, que são combinações de serviços e de adoção que ajudam o cliente em arquiteturas específicas a acelerar o uso. E escutar, dentro de todos os níveis que temos nessas duas plataformas, qual é o nível adequado para o cliente, não só para serviços, mas também para o software, a combinação das soluções.

Ocorre-me que a Customer Experience está atravessando todas as verticais, porque você olha para a satisfação do cliente em todos: segurança, arquitetura, redes. Não que este departamento seja independente, mas transversal a todos.

Sim. Acredito que um dos valores mais importantes que temos como empresa é o multidomínio, a capacidade de ter um portifólio vasto e amplo. Se falarmos de colaboração, por exemplo, vamos lidar com a rapidez com que nossos clientes, parceiros ou nós mesmos podemos tê-la internamente, como a consumimos. Dentro desta plataforma de colaboração, também vamos focar em outros ingredientes muito importantes: segurança, estabilidade de rede, agilidade, velocidade e clareza que os serviços podem ter. Então, eu acho que um dos maiores valores da Cisco como empresa é sua capacidade de ter multidomínio, multiplataforma, e que eles se complementam. Parte do nosso valor agregado é garantir que nosso cliente tenha acesso a esse vasto portifólio e ajudá-lo em seu crescimento.

Como os insights são obtidos? Certamente uma parte se alimenta de métricas do CX Cloud, por exemplo. Mas, além disso, quando o cliente fala, além do que acontece com a plataforma, por quais meios ele se expressa? Através do seu executivo de contas? Através do Suporte?

Há uma combinação de tudo, e o que você acabou de dizer está correto. A primeira coisa que fazemos é colocar aparelhos e/ou produtos que nos dão esta telemetria. Um deles é o que chamamos de Compass, uma ferramenta totalmente dinâmica e proativa, dedicada a obter todos os dados do cliente. No entanto, uma vez que a informação é recebida, o que você faz? Se tivermos um relatório com informações e não pudermos traduzi-lo para o idioma do cliente, ele não tem o valor que queremos, ou que o próprio cliente gostaria que tivéssemos. Dentro de cada grande cliente, que são organizações que adotaram níveis significativos de software e serviços, temos o que chamamos de Executivos de Sucesso do Cliente, que se dedicam especificamente a um ou dois clientes, no máximo. Eles que traduzem as informações para que o cliente tenha noção de onde estamos, onde queremos estar, para onde vamos e com que rapidez podemos chegar ao objetivo juntos. Porque, lembre-se: trata-se de ver como otimizamos os desafios que temos hoje, quais são eles e como aceleramos os desafios que o cliente terá amanhã e, ao final, como inovamos com imagens que podemos definir junto com o cliente. Então nós temos essa combinação de telemetria através de relatórios específicos baseados na rede deles, com appliances e produtos que instalamos com nossos clientes e parceiros, e também geramos insights para discussões com nosso executivo. Quando não temos Executivos de Sucesso do Cliente, trabalhamos em estreita colaboração com nossos parceiros de negócios por meio do que chamamos de Gerentes de Programa de Sucesso, que já têm muitos clientes, mas também estão medindo a adoção do Ciclo de Vida.

Então é uma combinação, quando afirmamos que estamos no People Business, é com os dados, mas traduzindo para a linguagem que o cliente quer e para onde a gente quer chegar.

Estava pensando em estratégia de negócios. Você sempre pensa em vender e fidelizar. Parece-me que deve haver um equilíbrio, como se fossem dois pesos em uma balança, e o ponto de equilíbrio é a experiência do cliente, porque vender mais sem pensar em como reter o cliente, sem fazê-lo se sentir satisfeito, não há equilíbrio.

Concordo 100%. E eu te digo uma coisa. Pessoalmente, toda a minha carreira na Cisco foi baseada em vendas. Estou na empresa há 21 anos, sendo 18 anos em vendas. E esta é a primeira oportunidade que tenho de estar em uma organização onde a venda, que é sempre importante, não se dá por uma proposta, mas pelo valor que entregamos, e como ampliamos uma reforma. Nenhum cliente vai expandir uma reforma se não tiver uma excelente experiência com a solução, com as pessoas com quem trabalhou, com a metodologia e o processo. O cliente vai comprar e estender essa venda com base em como CX trabalhou com ele lado a lado. Então, hoje, o que nos leva ao sucesso é como o cliente percebe a Cisco como um todo, não apenas a área de Serviços ou Software. Na América Latina temos resultados muito bons e positivos. Uma de nossas métricas é dada pelo que chamamos de CX Sat, que proporciona a satisfação que o cliente tem com base no nosso trabalho na área de serviços ou a entrega de nossa renovação de expansão. São dados de métricas importantes para entender como vem o seguinte, que virá com a taxa de renovação: com que rapidez, com que pontualidade os clientes estão fazendo; e todo o ciclo de vida e processo de adoção que estamos criando. Então, eu diria a vocês que hoje a venda é importante, mas não é o que o fator de sucesso nos diz. Por isso Laércio Albuquerque (VP América Latina, Cisco) e eu trabalhamos coordenados e juntos, porque o resultado que ele tem impacta o nosso, e o nosso impacta nas Vendas. Agora, nossa discussão com o cliente não se baseia na pergunta da vida toda: como posso ajudá-lo? Já sabemos como podemos ajudá-lo. Hoje temos a informação, podemos dizer "isso é o que está acontecendo, estes são os comportamentos que estamos vendo, e este é o valor que podemos trazer para você com base em nossa arquitetura e nosso portifólio".

Eu ouço vocês falarem, e acho que vocês antecipam. Em geral, acontece o contrário com as empresas: o cliente primeiro reclama, ou pergunta primeiro. Na verdade, aqui está a possibilidade de antecipar a necessidade, de a propor primeiro.

Correto. Basicamente, nosso modelo é tentar antecipar eventos, entender quais estão por vir. Não estamos falando apenas do comportamento da rede, porque sempre foi uma de nossas prioridades, mas também do ponto de vista empresarial: como incubamos os negócios que são importantes, como nosso portifólio se encaixa no que é importante para eles. Porque não é simplesmente aquela filosofia de que você vai vender o que é, que não funciona mais;

Imagem: Diego ph, Unsplash.

você tem que ver o que está nessa plataforma, mas como combinar com as prioridades do cliente.

Também pensei na formação, porque imagino que toda a organização tem de estar alinhada com este objetivo em mente: não só fazer crescer o negócio com vendas, mas também sustentar a satisfação absoluta do cliente.

Sim, concordamos 100%. Iniciamos este projeto há 3,5 anos, e é muito bom construí-lo e vê-lo crescer, porque você começa a ver as capacidades que tem como empresa e como sua equipe incorpora novas pessoas que trazem uma filosofia diferente. Como você diz, neste crescimento é importante ter um esquema de treinamento bastante robusto. Hoje, temos treinamentos preparados para diferentes etapas: Faixa Azul, Verde e Preta, por exemplo. É um currículo bastante extenso, para que nosso pessoal, dependendo da função, adquira conhecimento com grande detalhamento. Hoje, em CX existem cinco funções específicas. A primeira é a equipe de Desenvolvimento de Negócios, que têm treinamento específico sobre desenvolvimento de portifólio. Em seguida, temos uma equipe de Delivery, que atende tudo relacionado à entrega, implementação, migração de nossa plataforma e otimização das plataformas através do portifólio de Business Critical Services. Além disso, temos três importantes equipes de Customer Success: o Customer Success Specialist, que são perfis técnicos, dedicados especificamente a facilitar a adoção de cada tecnologia; e os Customer Success Managers, que são os que ajudam o cliente a explorar todo o Ciclo de Vida dentro da arquitetura de tecnologias que temos. E, por último, mas não menos importante, a equipe de Partners, que se dedica a desenvolver nossos parceiros de negócios e ajudá-los a ter essa prática também. Cada um tem um currículo de formação muito específico.

Por fim, e no contexto de "usuários infiéis" em que vivemos, imagino que a cultura da organização também teve que se adaptar a esta nova modalidade, a esta visão, de olhar para o cliente e acompanhar todo o ciclo de vida da sua experiência com a Cisco.

Sim, acho isso extremamente importante, e aqui voltamos ao ponto de partida: "estamos no negócio das pessoas". E o People Business tem a ver com colaboração, comunicação, objetivos comuns, uma nova visão compartilhada. Acredito que estamos em um processo cultural muito importante na empresa, que não podemos mais ser silos, e que o sucesso deve ser comum a todos. Felizmente, acho que na América Latina, tanto Laércio quanto eu eos diferentes líderes, sabemos que o sucesso em comum é o único que conta. Hoje temos uma comunicação aberta, estamos criando diferentes grupos e fóruns para chegar a este entendimento do que é transformação. A transformação não passa pelo CX, mas este departamento tem que ser um veículo para alcançá-la, assim como o de Vendas. Laércio sempre nos lembra: se não podemos ser os maiores, podemos ser os primeiros, os que estão incubando e os mais admirados. Hoje temos a oportunidade de crescer juntos e alcançar bons resultados com uma cultura vencedora, onde podemos nos divertir, porque estamos fazendo coisas inovadoras. E ter a sensação de nos sentir bem em torno do que estamos fazendo. Acho que estamos no caminho.

Há uma palavra que sempre escuto nas entrevistas que tem a ver com isso, com se sentir bem com o papel desempenhado por cada um da equipe faz; e, por outro lado, aquele sentir-se verdadeiramente bem, faz o outro perceber a honestidade.

Sim, a energia positiva é contagiosa.

Exato; Vou levar isso como um aprendizado. Muito obrigado, Danilo.

Muito obrigado, Karina

Saber mais

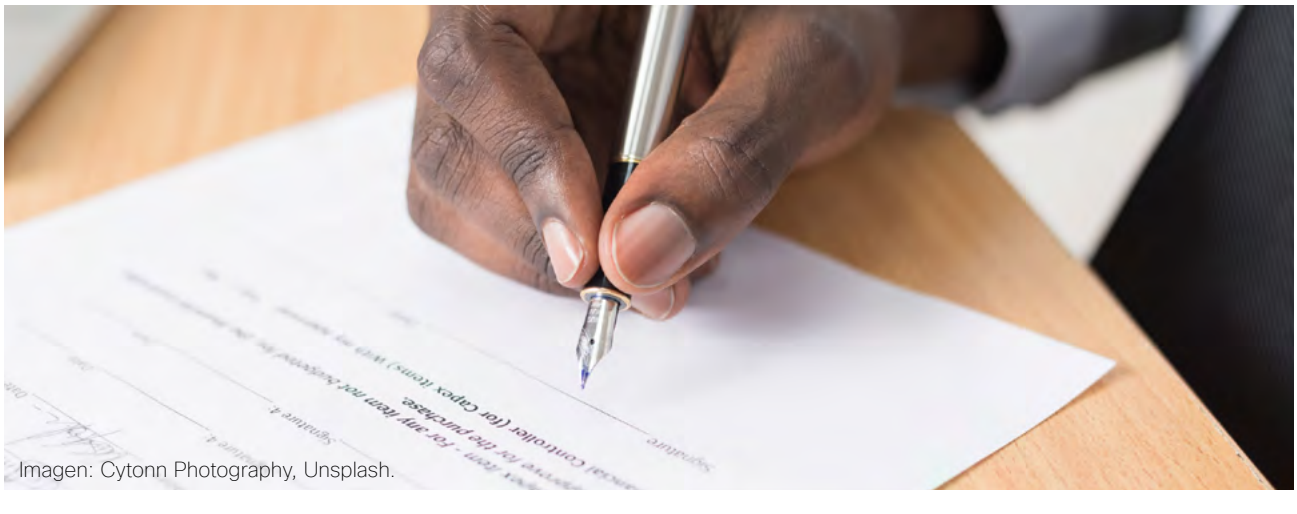


Imagen: Cytonn Photography, Unsplash.

É possível um mundo digital sem senhas?

Anualmente, entre 20% e 50% de o pedidos de assistência técnica de TI são para redefinir senhas, de acordo com o Gartner Group.

A fim de proporcionar ambientes seguros, o método de autenticação sem senhas ou passwordless é uma tendência que está crescendo no mundo do trabalho híbrido, em que os usuários interagem com smartphones, PC, laptops, tablets ou wearables, e que utiliza dados biométricos, chaves de segurança ou dispositivos móveis.

Soluções como a Duo Security brindam o usuário com uma verificação por múltiplos fatores e com diversas opções, que podem ser a notificação pelo smartphone, um token de hardware ou a biometría. Estas ferramentas liberam os usuários daqueles mecanismos que poderiam ser pesados ou pouco habilitados e também acompanham, por enquanto, os repositórios de senha, mas que também eventualmente vamos nos libertando deles.

Diga adeus às senhas sem comprometer a sua segurança, com a Duo!

> Saiba mais

Quem é quem

Luz María **Murguía**

por **Karina Basanta**

Encontramos Luz Ma – me permito aqui a abreviação – via Webex, apenas alguns dias antes dela deixar o cargo de Latin America Growth Marketing Director na Cisco para dar o salto desafiador rumo ao mercado de paytechs. Vinte e nove anos na indústria de tecnologia parecem ter fortalecido esta líder não só em seus conhecimentos e experiência, mas também em sua afirmação sobre quem é, o que busca e espera de suas equipes, dos ambientes e da vida.

Luz Ma iniciou em RR.PP., é comunicadora e está baseada na cidade do México. Durante quase 20 anos esteve na empresa Oracle, onde viveu 100% a evolução de uma empresa de tecnologia para software e depois para a nuvem.

Há quase seis anos, foi convidada a fazer parte da Cisco para liderar a equipe de Marketing do México e formar um time integrado por especialistas em conteúdos com foco em satisfazer as necessidades do país. Já na gestão, liderou a transição do conteúdo focado em tecnologia para o atual modelo de conteúdo produzido para audiências. Esta tarefa durou quase dois anos. A partir daí foi promovida com o objetivo de liderar a equipe da América Latina. Aqui se consolida a segmentação por audiências e se soma o segundo idioma: português. No entanto, o destaque da gestão de Luz é o que ela chama de "mestria em marketing e comunicação digital".

"Quando entrei na Cisco, eu dizia: não fazemos marketing digital, fazemos marketing em um mundo digital. São questões totalmente diferentes. Fazer marketing digital te insere no mundo digital, te leva a desenvolver agilidade e aprendizagem constante, visualização de dados e otimização de suas tarefas, e, assim, buscar a inovação. Este sim é um dos meus "Quotes": fazer marketing em um mundo digital. Nossa equipe viveu a transição do field marketing ao entendimento desta nova tendência e sua nomenclatura: o que é uma estratégia de programatic, de SEM (Search Engine Marketing), ou de SEO (Search Engine Optimization), e a forma podemos aperfeiçoá-las. Posso dizer que hoje, todos na equipe de marketing sabem como otimizar as estratégias em nível digital, e viver isto como uma grande conquista. Tive a sorte de ter uma equipe extraordinária de especialistas. Cada um deles, da sua área, fez a sua valiosa contribuição".

Imagem: Bisakha Datta, Unsplash.

O marketing B2B mudou muito nos últimos anos, não foi?

O marketing B2B (Business to Business) era conhecido como marketing de relacionamentos, onde tínhamos a etiqueta de "eventos". Um dos objetivos que me propus foi tirar-nos esta etiqueta. Marketing é muito mais do que isso: é contribuir com um conhecimento mais profundo do cliente através dos dados (data insights and analytics) para tomar decisões baseadas em informação e não por feeling. Além disso, estar perto do negócio nos permite colaborar com sua aceleração, promover novos negócios e dar contribuições para reter clientes. É o sinal do infinito: não basta com a venda, há que buscar a recompra, a renovação do software...

Quais foram as suas principais estratégias na Cisco?

As grandes estratégias em que me foquei foram:

- Uma comunicação certa sobre a necessidade do negócio.
- Como marketing pode trazer valor.
- De que forma o marketing pode chegar mais perto do cliente interno: Vendas.

Em relação a isso, algo muito importante para mim na Cisco foi gerenciar as audiências. Eu me concentrei em quatro:

- A audiência interna. Você pode investir milhões de dólares para posicionar uma mensagem, mas se seu vendedor não é consistente quanto ao momento de atender ao cliente, você definitivamente perde a oportunidade. Para mim, a primeira audiência partiu do colaborador, por isto escolhemos dar-lhe uma comunicação sobre a gestão do nosso departamento.
- Partners. Nosso negócio é 97% guiado e influenciado por eles, por isto a mensagem que a Cisco emite deve estar sempre alinhada com a do parceiro.
- O cliente final, senhor. Segmentamos esta audiencia depois da incorporação maciça do trabalho híbrido. Assim, nossa mensagem chega agora não só à pessoa de tecnología, para quem nos constituímos como mentores e guias, mas também à de capital humano, a de operações, a de logística.
- Os influenciadores. Embora esta audiência não reporta diretamente ao marketing é um grupo de grande importância. aqui, o alinhamento é dado com pessoas de relações públicas e analistas.

Migrar a venda de produtos de caixa para o modelo SaaS faz com que o foco se ponha sobre o conteúdo. Com isto, é possível prever tendências dentro junto aos clientes. O Marketing pode absorver estas tendências, que Vendas ainda não está vendo, porque é sobre o produto/serviço que você tem disponível para oferecer. Marketing através de sua leitura de tendências pode impulsionar o desenvolvimento de um novo negócio.

Absolutamente de acordo. No momento em que você entra em uma tendência de análise é onde o Account Base Marketing ajuda. Na Cisco podemos seguir a impressão digital do cliente do, por exemplo, nosso canal mais importante que é cisco.com, Você pode chegar a um vendedor e dizer: "Veja o percurso que este cliente fez: entrou por um podcast, depois foi a um pedido de demonstração, dali a ver um caso de sucesso e terminou em um click to chat para pedir mais informações".

Graças à tecnologia e aos dados, o marketing B2B se converteu em um business partner em vez de um executor, e é assim que me sinto dentro do negócio: Sinto-me como um parceiro empresarial que, com base em dados e informação, define em conjunto a estratégia em que nos devemos concentrar.

COVID-19: Como sua área reagiu?

A Cisco contava o grande benefício de ter o home office e tecnologias disponíveis. Todos tínhamos uma grande incerteza, mas sabíamos que era importante compartilhar o que estava acontecendo tanto com o cliente interno como externo.

Webex e Segurança foram os dois produtos que nos levaram a uma comunicação forte em espanhol e em inglês. Estas duas linhas de produtos se tornaram a ponta de lança em questão de ativação de conteúdo, de dados, de referências. Os casos de sucesso me marcaram muito. Sinto que a Cisco é outra desde que entrei: gosto de ouvir a Cisco como um influenciador, mas prefiro ouvir a voz do cliente, pois o seu impacto é maior.

Imagino que não tenha sido fácil se comunicar com todas as audiências de forma digital... Quais foram os principais desafios?

Claro que houve desafios. O principal foi a fadiga digital. Para nos ajustarmos a ela, fizemos duas grandes coisas:

- A primeira foi dar a oportunidade ao cliente de decidir quando quer nos ouvir ou participar de nossos eventos. A partir daí, disponibilizamos o material em nossa plataforma de conteúdos on demand. Tenhamos em mente que toda a atualização de conteúdo foi muito importante porque era preciso dar um alinhamento com o contexto da pandemia.

- A segunda foi a incorporação dos Podcast para que o usuário possa escutar temas que lhe interessem enquanto realiza outra atividade, como caminhar, por exemplo.

Em sua opinião, como se produz inovação?

A mudança constante nos leva à adaptação e à criação de novas opções de inovação, algo gerado através da visualização do comportamento do cliente. Sabemos que algo está em decadência quando acessamos a informação que retorna do usuário e a analisamos (precisamente as medições sobre cada ação realizada: open ratio e-mail, downloads, etc.). Saber como nossas ações de marketing foram recebidas na Cisco nos permitiu inovar. Por isto levamos adiante os podcasts, os eventos sob demanda e a interação virtual. Nossa nova proposta são as Masterclasses, das quais a primeira será sobre Hybrid Work. Neste sentido, também temos encarado uma mudança na forma de expor as informações no site da Cisco para priorizar a venda.

Além disto, acredito fortemente na geração comunidades que relacionam clientes com afinidades em comum, por exemplo algumas que levamos adiante na Cisco: Running Club, Meet & expert e Meet executive.

> *“Se estiver funcionando, replique. Se não estiver funcionando, pare.”*

Social Selling e Social Influencing como abordar na Cisco?

Durante a pandemia, percebemos que, embora tenhamos um crescimento exponencial nas redes sociais, tanto em espanhol como em português, nossos funcionários são uma grande fonte de informação e influência. Então começamos a trabalhar sob um programa chamado Digital Believer. Trata-se de um programa interno que se estendeu aos parceiros. Ele buscava conscientizar primeiro o funcionário sobre a relevância que têm as redes sociais, qual o objetivo de cada uma e quais são suas diferenças, e ao mesmo tempo convidá-los a publicar o conteúdo que cada um queira publicar. Trata-se de tomar consciência sobre como o social Influencing dos integrantes da Cisco é importante.

Imagen: Gentileza Luz María Murguía

> *“A equipe é quem faz as coisas acontecerem.”*

Para isto trouxemos especialistas que falaram de marca, de storytelling, da importância das redes sociais. Além disso, acabamos de finalizar uma estratégia chamada “Digital Adoption Academy”, que começou há quase três anos e que buscava repassar as diferentes formas de criar conteúdos digitais: de que forma fazer um e-mail, um post da LinkedIn, como você se converte em um influenciador... incluindo o básico de como o seu perfil está formado e que confiança você gera com ele. Na Cisco, já estávamos preparados para lidar com temas digitais antes da pandemia, tanto com a tecnologia que usávamos como com a comunicação interna e com o cliente.

Em sua experiência, quais são as principais redes sociais para fazer markerting B2B?

Acho que hoje as principais são LinkedIn, Twitter e Instagram. Agora o TikTok se juntou com muita força e influência, trazendo grande quantidade de seguidores e repercussão.

Por sua vez, o sucesso é potencializado já que hoje qualquer integrante da organização pode compartilhar as peças geradas em redes sociais, sobrecomunicar e ao mesmo tempo, escutar a voz do cliente. Uma campanha com forte intervenção dos empregados, que teve muita repercussão na Cisco, foi a que levamos adiante durante a semana da cibersegurança.

Por outro lado, um formato que está nos empurrando é o vídeo marketing. A mim dão-me muito resultado os vídeos espontâneos que me mostrem tal como sou, autêntica. Parte da nossa Digital Believer Academy em Q4 vai incluir a estratégia de como fazer vídeos de alto impacto.

Como você define seu tipo de liderança?

Considero-me uma líder por influência e não por hierarquia. Às vezes é necessário fazer a quebra da fronteira de reporte, porque o grande valor é ter uma estrutura que trabalhe em conjunto e orquestrando em busca de um objetivo claro, sem importar a quem se reporte.

“Respeito
Relações
Resultados
Reconhecimento
Resiliência”

Las 5 R de Luz Ma

Cisco é uma empresa comprometida com a diversidade e inclusão, você uma mulher com quase trinta anos no mundo da tecnologia. Meparece que a fantasia da Cisco e a sua coincidem.

Dentro da cultura Cisco, Diversidade e Inclusão são dois temas de grande importância. Nos últimos dois anos fui co-líder da Comunidade de Woman of Cisco LATAM e parte do Board Member do Woman of Cisco Americas, que me permitiu colaborar com a estrutura além de minhas tarefas tradicionais. Hoje sou membro do 30% Club.

Você está fazendo uma grande mudança ao passar para o mercado paytech. Qual é a sua última reflexão para esta entrevista, quando pensa na equipe de marketing da Cisco.

É verdade, acho que é uma boa altura para continuar a aprender e a construir o meu crescimento profissional com um novo desafio. A meu ver, hoje o marketing está muito mais ligado à valorização do negócio do que a uma execução isolada. Orgulhosamente, deixo uma equipe extremamente preparada com valores muito semeados de trabalhar em conjunto, de comunicar e sobrecomunicar, de concentrar-se na voz do cliente, de adotar a digitalização... Tenho sido a suaa líder nestes últimos três anos, aquela que teve o privilégio de guiá-los para a frente e estou grata pela vsua aceitação e companhia

#Teamwork Makes the dream work
#constantLearning

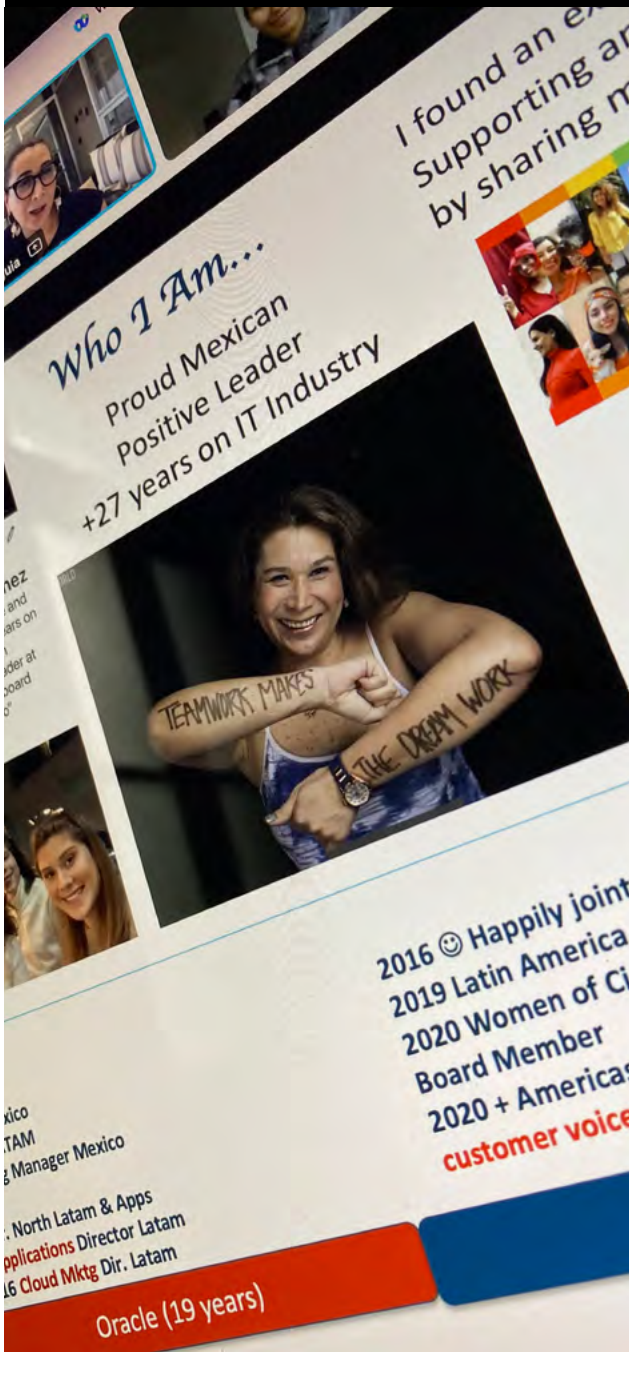
Nunca há uma segunda oportunidade para dar uma primeira boa impressão

Sellos de Luz Ma

Sempre comentei com minhas equipes que ter estrelas cadentes não funciona para mim. Brilhar por si só, não funciona para mim. O que procuro é ter uma constelação onde todas as estrelas brilhem em conjunto com um mesmo objetivo. Penso que esse é um dos grandes valores da minha equipe na Cisco: todos somam e a prioridade é estar perto para dar respostas ao negócio.

“Quando me conecto com as pessoas, dificilmente desligo com elas.”

Lado B



Sou a sétima de oito irmãos. Acho que o primeiro Teamwork Makes the dream work, ou seja, o primeiro círculo de respeito e admiração foi a minha família. Eu sou a pequena e a primeira geração feminina que tem uma carreira universitária... Em breve, a minha filha começa a carreira de engenharia biomédica. Sem querer e indo impactando as seguintes gerações com o modelo do estudo e o crescimento profissional.

Sou uma pessoa:
espiritual.

Se eu não tivesse sido marketera, teria sido:
psicóloga.

Para:
ouvir as pessoas.

O teu dom:
ajudar as pessoas.

Quando você se aposentar:
quando eu puder ser um Board Member, eu gostaria de viajar e ir pela Índia para testemunhar o que é o benefício da meditação.

Em que você confia:
Na energia e nos anjos.

Um amor:
os elefantes.

Por que:
porque eles têm orelhas grandes para ouvir melhor.

Instagram de LuzMa
@luzma_positiveimpact

Da editora:
A escuta define a Luz Ma, busca o dado para concretizá-la.

Dionísio ou Dâmocles: esta é a questão

O Rei Dionísio "O Velho" foi um tirano sanguinário que viveu em Siracusa por volta do século IV a.C. Em sua corte havia vários aduladores, como era habitual, mas entre eles se destacava um, Dâmocles, que invejava os luxos e comodidades do tirano. Um dia, Dâmocles, corroído pela inveja, falou com Dionísio e lhe disse: "Deves estar muito feliz! Tem tudo o que um homem pode desejar: fama, dinheiro, admiradores...". O Rei cansado das adulações invejosas planejou um castigo para Dâmocles, propôs uma troca de papéis para que pudesse desfrutar dos prazeres de ser Rei por um dia. Dâmocles aceitou imediatamente sem pensar e o Rei encomendou um banquete para essa mesma noite. Quando se encontrava sentado na cadeira do Rei, desfrutando dos deliciosos benefícios, percebeu-se que sobre sua cabeça pendia uma espada atada a um fino pêlo de crina de cavalo. Neste momento, esqueceu os privilégios e só se preocupava em morrer a qualquer momento. O Rei perguntou-lhe o que acontecia e quando Dâmocles lhe apontou a espada, Dionísio respondeu: "Sei que há uma espada ameaçando sua vida, porém por que deveria preocupar-se? Estou sempre exposto a perigos que podem fazer-me perder a vida a qualquer momento." Imediatamente Dâmocles rogou trocar o posto e abandonar todos os privilégios e benefícios que este trazia.

Não é claro se este fato aconteceu ou foi uma invenção do filósofo Cícero para mostrar realidades e expor os fundamentos da felicidade, mas esta história é muitas vezes utilizada para mostrar o pouco evidente que pode ser a responsabilidade e o peso de uma posição ou trabalho. Também representa uma situação que era pouco evidente e significativa há alguns anos.

Os aventureiros

Antes do início da pandemia, as áreas de segurança, dirigidas pelos mais ousados na matéria, eram equipes de trabalho subordinadas à gerência de Tecnologia ou à área de Governo, Risco e Cumprimento. Estas áreas eram formadas por poucas pessoas que entre muitas tarefas deviam repartir sua tarefa na definição e auditoria de políticas de segurança para o correto cumprimento de alguma norma ou regulamentação a que a companhia estivesse obrigada, e sublinho, estritamente obrigada a cumprir.

Em geral, quando convocados para participar nos projetos, foram incluídos nas reuniões sobre o trecho final do processo, antes de uma saída à produção, com o único objetivo de aprovar uma ferramenta que tem sido implementada por uma equipe de engenheiros nos últimos 12 meses ou mais.

Claro que todos nessa mesa esperavam uma aprovação rápida do projeto, e claro que isso não acontecia, porque neste momento eram advertidos quanto a todos os riscos, vulnerabilidades e princípios de arquitetura de segurança que tinham sido omitidos. Quando isto acontecia, as reuniões terminavam mal, com a metade da mesa apontando à área de segurança como um contraditor ao progresso do projeto, um Stopper que não entendia a urgência do negócio e a estratégia corporativa, que tinha ficado estagnado em suas políticas e seus controles extras, em sua caverna de eremita sem entender a realidade corporativa.

E chegou a pandemia

Neste contexto chegou 2020 e um vírus provenientecomeçou a mudar a realidade do mundo. Como em uma ficção, começou-se a falar de quarentenas e isolamento de cidades inteiras. Só quando nos aproximamos dele é que nos apercebemos da seriedade do assunto. Isolamo-nos e seguimos as nossas vidas, mas agora conectamo-nos a partir das nossas casas, ajudando os nossos filhos para que pudessem iniciar as suas aulas por videochamada, misturando o computador pessoal com o trabalho e as Webex familiares com as profissionais.

Neste contexto, todos os olhos se voltaram para a área de segurança. Era, de alguma forma, necessário flexibilizar as medidas e os controles que durante anos nortearam ações de escritórios e data centers, para permitir que todos pudessem se conectar, a partir de suas casas, a aplicações, servidores e bases de dados que por anos estiveram dentro

Ad Content

por **Fabio Sánchez**

Diretor de Prática de Cibersegurança,
OCP Tech

Imagen: Ricardo Cruz, Unsplash.

de uma espécie de zona militarizada, protegidos por 2 ou mais firewalls e com acessos restritos. De um momento para o outro estes equipamentos estavam novamente no centro do furacão, deviam agir rápido e entender a nova estratégia corporativa e urgência de negócio. Assim o fizeram... tudo se fez para que o negócio continuasse funcionando.

O peso da espada

Mas nesse momento a espada que se balançava sobre as nossas cabeças se fez mais pesada, e o fino pêlo de crina de cavalo, mais fraco. Poucos compreenderam a dimensão dos riscos assumidos e o nível de exposição a que as empresas foram expostas desde o início da pandemia, a ponto de se verem agora as consequências de anos de cortes orçamentais e de limitações do pessoal de segurança.

De acordo com o relatório sobre Cibercrime da Interpol[1], as principais ameaças para a pandemia de COVID19 em 2020 foram Phishing/Scam com 59%; e Malware e Ransomware com 36%. Isto porque a superfície de ataque aumentou como resultado da mudança para o teletrabalho, estilo ao qual as organizações tiveram que rapidamente adaptar os sistemas para acesso remoto, infraestrutura e aplicações que antes só eram acessadas a partir de escritórios centrais e sucursais. O mesmo relatório cita que, em abril de 2020, se registou um pico de ataques de ransomware por vários grupos de cibercriminosos que há meses se encontravam inativos, ação que pode implicitamente indicar que existe ramsomware implantado, mas ainda não ativo, esperando ser usado em momentos específicos para maximizar o seu impacto e preço para o resgate.

Depois de dois anos, o panorama das companhias segue muito similar, muitas delas não mudaram e voltaram à realidade da pré-pandemia; outras ainda afirmam que o trabalho das áreas de cibersegurança não é tão complexo e não requer mais investimento em pessoal e recursos tecnológicos, que devem se limitar à definição de políticas e à auditoria manual que sejam viáveis, sem prejudicar os processos empresariais. Nada está mais longe da realidade, e o risco aumenta a cada dia.

Para um novo paradigma

Urge, pois, uma mudança de paradigma. Um estudo realizado pelo Gartner prevê que, até 2023, 30% dos CISO (Chief Information Security Officer) não só deverão cumprir e ser responsáveis pela cibersegurança da companhia, mas também serão medidos diretamente por sua habilidade de trazer valor ao negócio [2]. À primeira vista, isto parece contraditório e mostra um futuro ainda mais incerto para as áreas de segurança:como se pode ser mais ativo e seguir a velocidade que os negócios requerem e ao mesmo tempo dar-lhe valor?

Para gerar valor ao negócio, a teoria geral menciona que existem três fatores a serem considerados: a imagem pública da empresa; a percepção que os consumidores têm da mesma; e a efetividade de seus produtos e serviços. A partir das áreas de segurança cibernética, existem muitas maneiras pelas quais devemos gerar valor, e nós, engenheiros especializados da OCP TECH, desenvolvemos projetos que garantem e valorizam as empresas.

Quando uma violação de segurança é exposta por atacantes filtrando dados privados de clientes, não há nada que se afete mais que a imagem da empresa, que terá que responder diretamente perante autoridades judiciais e clientes pela informação roubada.

Todas as medidas que se tomem para a prevenção destes fatos seja mitigando riscos conhecidos como conscientizando os empregados das organizações sobre os ataques aos que estão expostos, gera e preserva o valor das companhias a longo prazo. Devemos então ser mais assertivos na forma de apresentar os projetos, justificar os casos de negócio e o custo total de propriedade de soluções e projetos de segurança, pois já não podemos nos limitar a mostrar a economia de custos que uma ferramenta pode oferecer ou regulação e norma que a justifica, devemos ir mais longe e facilitar o alinhamento a médio e longo prazo com a estratégia da companhia.

O olhar do consumidor

Por muitos anos o consumidor se limitava a ver os benefícios que lhe dava o produto e/ou serviço e seu custo comparado com produtos similares ou substitutos, sempre guiado por sua intuição. Isto evoluiu e é cada vez mais complexo entender a mente dos usuários. Hoje, eles selecionam um produto influenciado por uma celebridade ou por um vídeo visto por milhões de pessoas na internet. Mas é a percepção de confiança de um produto ou serviço que realmente pode influenciar a compra. Na aquisição de um serviço, esta percepção pode ser afetada se o fornecedor não levar a sério os riscos de segurança a que os clientes estão expostos.

Métodos de autenticação, esquemas de prevenção contra fraude e fatores de autenticação biométricos já não são vistos pelos usuários como uma dor de cabeça e um impedimento no uso dos serviços, mas são percebidos como elementos que asseguram as suas compras. Na OCP TECH temos soluções focadas em gestão de acessos de clientes, com métodos de autenticação robustos e autenticação biométrica que se adaptam às ferramentas e soluções digitais já instaladas pelas empresas,sem deteriorar a experiência do cliente nos diferentes canais digitais

[1] COVID-19 Cybercrime Analysis Report- August 2020 - INTERPOL General Secretariat 200, quai Charles de Gaulle, 69006 Lyon, France.

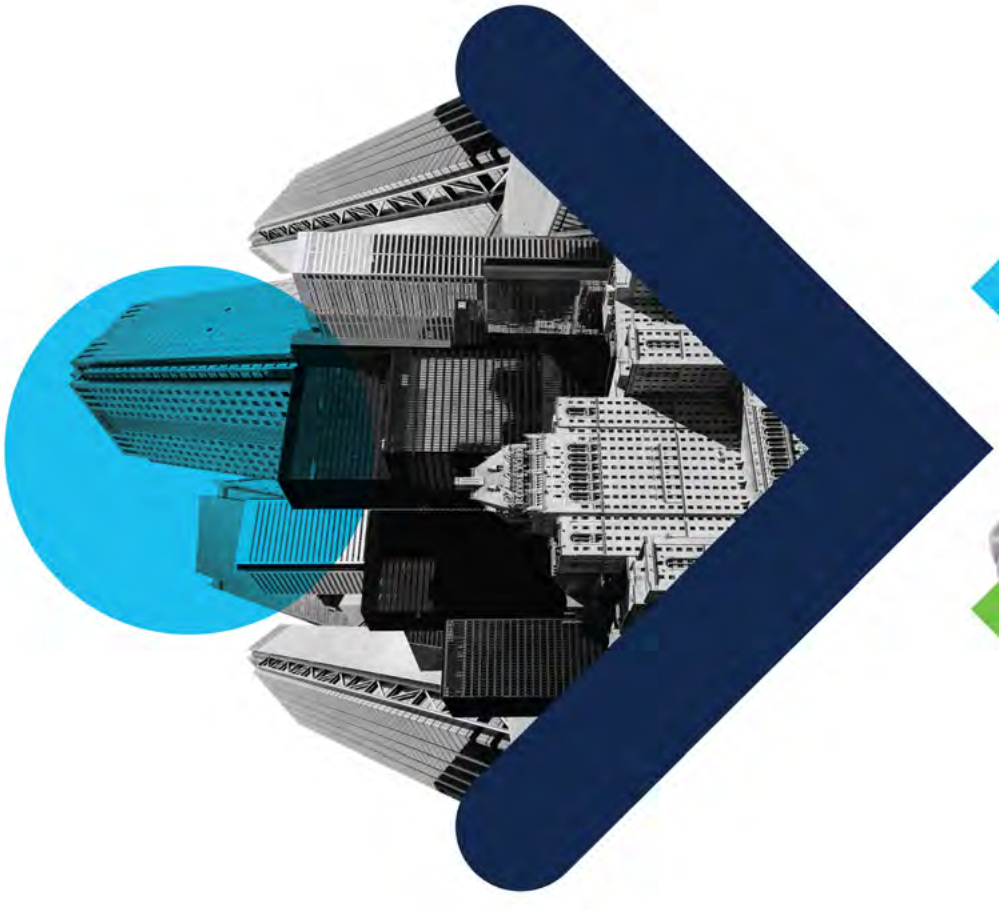
[2] Rethink the Security & Risk Strategy - Embrace modern cybersecurity practices while enabling digital business. EDITED BY Tom Scholtz Distinguished VP Analyst, Gartner © 2021 Gartner, Inc. and/or its affiliates. All rights reserved.ner © 2021 Gartner, Inc. and/or its affiliates. All rights reserved.

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

Columna

Smart Supply chain

“Cibersegurança baseada em Blockchain, ZKP e Zero Trust”

Conteúdo audiovisual

Imagen: Ryutaro Uozum, Unsplash.

por **Freddy Macho**

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

A transformação digital abriu uma nova forma de viver e trabalhar. À medida em que o desempenho e os novos níveis de conectividade permitem que as empresas aproveitem os benefícios das tecnologias inovadoras, o mundo se torna mais rápido, flexível e eficiente. Esta mudança cria um ecossistema global onde as coisas físicas e digitais estão cada vez mais conectadas, desde ativos de infraestrutura críticos até pessoas e dados.

É por isso que as empresas se veem obrigadas a investir tempo e recursos na reavaliação das suas cadeias de abastecimento, em busca de soluções para as suas fraquezas. A cadeia de abastecimento foi o setor que mais sofreu ataques após o surgimento da pandemia em 2020.

Antecedentes

Ao avançarmos para um mundo cada vez mais globalizado e complexo na sua dependência dos componentes de software, vemos o risco da cadeia de abastecimento evoluir e se expandir. Também vemos que embora problemas deste tipo em setores como o da energia tenham sido reconhecidos e estudados durante vários anos, eles ainda persistem.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

A Corporação de Confiabilidade Elétrica da América do Norte (NERC) está atualizando seus padrões de Proteção de Infraestrutura Crítica (CIP) para incluir proteções da cadeia de fornecimento, porém existem brechas: NERC-CIP aplica-se apenas a um subconjunto de sistemas e componentes que afetam a segurança e a confiabilidade em um subconjunto de serviços elétricos, e medir a segurança da internet é, na melhor das hipóteses, um indicador indireto da tecnologia utilizada nos sistemas de controle.

Em dezembro de 2015, centenas de milhares de casas ucranianas ficaram temporariamente às escuras no primeiro ciberataque confirmado contra uma rede elétrica. E em agosto de 2017, as senhas codificadas predefinidas (uma classe conhecida de vulnerabilidades da cadeia de abastecimento) num componente de sistemas instrumentalizados de segurança facilitaram o encerramento das operações da Saudi Aramco, sendo assim objeto de um novo ataque depois do sofrido em 2012.

Em dezembro de 2020, uma empresa de segurança cibernética descobriu uma campanha global de invasão cibernética que primeiro comprometeu o código fonte e depois atualizou a plataforma SolarWinds Orion, um produto de software de gerenciamento de TI amplamente implementado. A atualização corrompida foi baixada por milhares de clientes do SolarWinds e abrangeu agências governamentais dos EUA, entidades de infraestruturas críticas e organizações do setor privado. Este ataque cibernético sem precedentes em escala e sofisticação coincide com uma série de tendências persistentes no uso de vetores da cadeia de suprimentos.

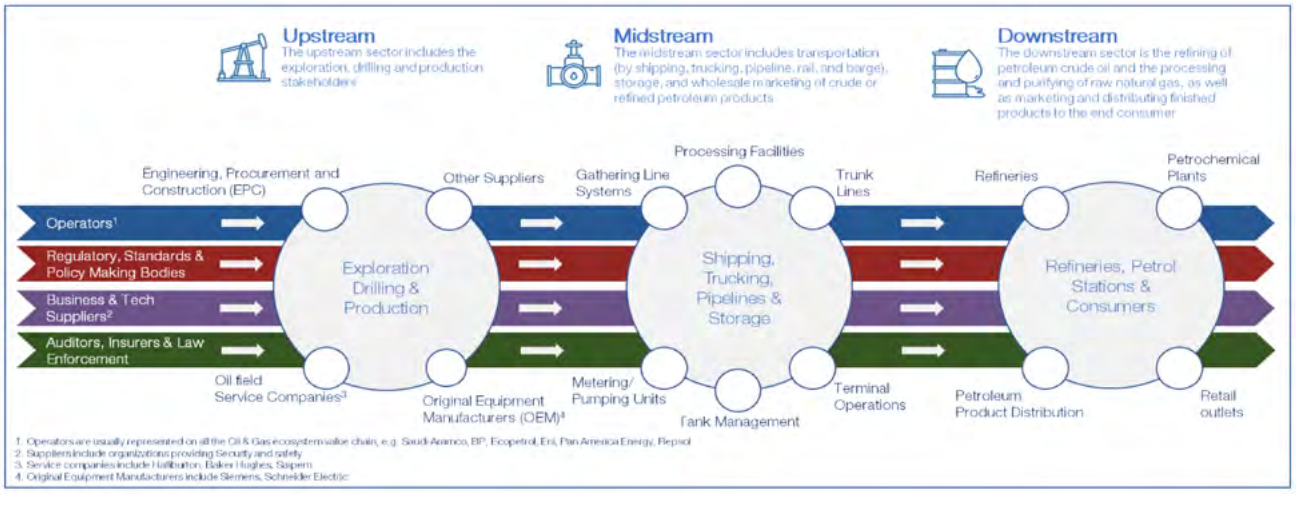
Durante o feriado de 4 de julho de 2021 nos EUA, uma quadrilha criminosa explorou uma vulnerabilidade do popular software de gestão de TI, Keseya VSA, utilizado por mais de 36.000 clientes em todo o mundo, para perpetrar um dos maiores ataques de ransomware na cadeia de fornecimento da história.

Imagem: Software Supply Chain Attacks – ASSESSMENT OF THE CRITICAL SUPPLY CHAINS SUPPORTING THE U.S.

Gestão de riscos de terceiros na cadeia de abastecimento

Os ataques à cadeia de abastecimento tiveram consequências dramáticas em termos operacionais, financeiros e de reputação. Estes acontecimentos não afetam apenas a vítima, mas todas as partes interessadas na cadeia de valor, e demonstram a importância de uma abordagem colaborativa e holística na gestão dos riscos de terceiros.

As empresas podem ter requisitos divergentes devido à singularidade e complexidade do modelo de negócio. Na indústria do petróleo e do gás, por exemplo, a digitalização vertiginosa das empresas transformadoras aumenta a complexidade de controlar o risco decorrente de terceiros na sua cadeia de abastecimento. A maioria das abordagens de gestão de risco de terceiros depende da configuração interna, cultura e prioridades da organização. Os processos e requisitos atuais da indústria permanecem conservadores.



Riesgos de terceros en la industria del petróleo y el gas - Cyber Resilience Oil and Gas of World Economic Forum's.

A cadeia de abastecimento é apoiada em todos os setores por um número representativo de pequenas e médias empresas que executam um orçamento operacional baixo e em sua maioria não investem adequadamente em cibersegurança. Por conseguinte, tornam-se alvos preferidos dos cibercriminosos, quer como alvos diretos ou como vetor de ataque para chegar às grandes corporações, agências governamentais ou infraestruturas críticas de serviços.

Durante uma investigação realizada pela Direção Nacional de Cibernética de Israel (INCD), muitas PMEs se queixaram de requisitos muito diversos de diferentes clientes e reguladores. As grandes empresas investem grandes quantias na definição de suas próprias necessidades para a gestão do risco cibernético de acordo com padrões como ISO 27036, 800-161 e outros. No entanto, muitas vezes se contentam com as declarações dos fornecedores em vez de insistirem em resultados de auditoria válidos.

Reconhecendo o risco em todos os domínios, o Centro Nacional de Segurança Cibernética (NCSC) do Reino Unido publicou um guia de segurança da cadeia de abastecimento para que as empresas tenham um maior controle de cibersegurança. As orientações são bastante completas e educam as empresas sobre como devem compreender e gerir o risco que se origina nos fornecedores, mas grande parte do trabalho exigido é deixado às próprias empresas. Uma auditoria recente da INCD mostra quantos dos controles de segurança cibernética individuais da organização cumprem com os padrões requeridos.

Existem diferentes abordagens para uma cibersegurança mais sólida, principalmente através da certificação de produtos e serviços. Para que o processo seja completo, precisamos melhorar o nível geral de higiene cibernética dos fornecedores e não apenas os seus produtos específicos.

Garantir que os produtos comprados através da cadeia de abastecimento sejam certificados e seguros é, naturalmente, uma camada importante. No entanto, a certificação do produto pode ser relevante para uma versão específica e pode perder relevância na seguinte. É imperativo complementar o esquema de segurança com um esquema de certificação de fornecedores do ponto de vista do cliente. As empresas devem assegurar que os fornecedores em que confiam mantêm um nível pré-determinado de segurança cibernética capaz de reduzir significativamente os riscos.

Visibilidade, pilar da cibersegurança

As transformações tecnológicas críticas nas quais se baseia a prosperidade futura (conectividade ubíqua, inteligência artificial, computação quântica e abordagens de próxima geração para a gestão de acesso e identidade) serão também desafios para a comunidade da cibersegurança, já que estas transformações têm o potencial de gerar riscos novos e sistêmicos para o ecossistema global. Duas tendências técnicas destacam o problema:

Aumento do uso de sensores/IoT:

pense no cenário em que um sensor de temperatura IoT de $5 habilitado para conexão sem fio e uma plataforma de gestão logística portuária de mais de $500.000 estão na mesma rede de comunicações. Estes não vêm com o mesmo investimento em cibersegurança, como código confiável, patches de segurança e uso de credenciais seguras. Como tal, serão necessárias ferramentas de visibilidade de rede inteligentes para ajudar a definir a segmentação, agrupar coisas que devem ser comunicadas entre si e aplicar controles de segurança alinhados com os riscos destes dispositivos reunidos.

Dados:

conectar coisas permite novas possibilidades e oportunidades comerciais ilimitadas. No entanto, leis de privacidade como GDPR e CCPA exigem frequentemente que as informações pessoais só possam ser compartilhadas dentro de certas condições, como consentimento e propósito. Para compartilhar dados pessoais legalmente dentro destes contextos, será necessário saber quais coisas em sua rede estão coletando dados pessoais e definir controles de intercâmbio aceitáveis, o que significa compreender as coisas e o tráfego que permite a comunicação.

Sobre a visibilidade dos dados, as cadeias de abastecimento são críticas e cada vez mais complexas. Isto, por sua vez, requer uma cadeia de infraestrutura que abrange tanto o software em todas as coisas conectadas, o hardware que cada um usa, os serviços de comunicações através dos quais se conectam e o hardware de comunicações sobre o qual se executam as comunicações.

Criar visibilidade em um mundo conectado

No domínio digital, a visibilidade é fundamental para habilitar novas capacidades. Em qualquer processo digitalizado, necessita de três pilares: (1) Dados que são processados (2) uma "coisa", por exemplo, um sistema IoT (dispositivo de borda); e (3) conectividade. Com efeito, a cibersegurança procura padrões de comportamento esperados ("normas") para tomar decisões. Mas à medida que fazemos mais conexões com coisas novas, este alcance se torna extremamente complexo.

Para gerar visibilidade, a comunidade de segurança deve priorizar três desafios:

Os padrões ainda são imaturos a nível mundial, e os dispositivos IoT muitas vezes usam suas próprias linguagens de comunicação e se comunicam de muitas maneiras. Alguns dispositivos usam criptografia, o que ajuda a proteger os dados, mas dificulta ainda mais a compreensão da comunicação em curso e a detecção de anomalias suspeitas. Como tal, precisa de cibersegurança que possa identificar tudo e definir normas de comportamento de forma contínua.

Ver todo o fluxo de tráfego para localizar qualquer problema. Um dispositivo ou coisa sempre se conecta à sua antena mais próxima, o que lhe dá um endereço de rede (um identificador). À medida que o dispositivo se move, esta identidade muda. Os protocolos asseguram que a comunicação seja fluida com o dispositivo final, com a segurança cibernética se movendo junto com o dispositivo. Por isto a importância de ferramentas de cibersegurança capazes de correlacionar este tráfico para encontrar o objeto real que está comprometido devido a um ataque cibernético ou vulnerável a um ataque futuro. Para gerenciar o risco, você deve monitorar os fluxos de comunicação em movimento (tanto em 4G e 5G), entender a comunicação entre os dispositivos e analisar se ele funciona de acordo com o planejado ou previsto, ou se existe alguma ameaça.

Por último, os controles de segurança devem conhecer a segmentação do tráfego e os controles de priorização. A segmentação de rede é uma abordagem arquitetônica que divide uma rede em vários segmentos ou sub-segmentos, com cada um atuando como sua própria rede. Isto permite aos administradores de rede controlar o fluxo de tráfego (e priorizar conforme necessário) entre sub-redes.

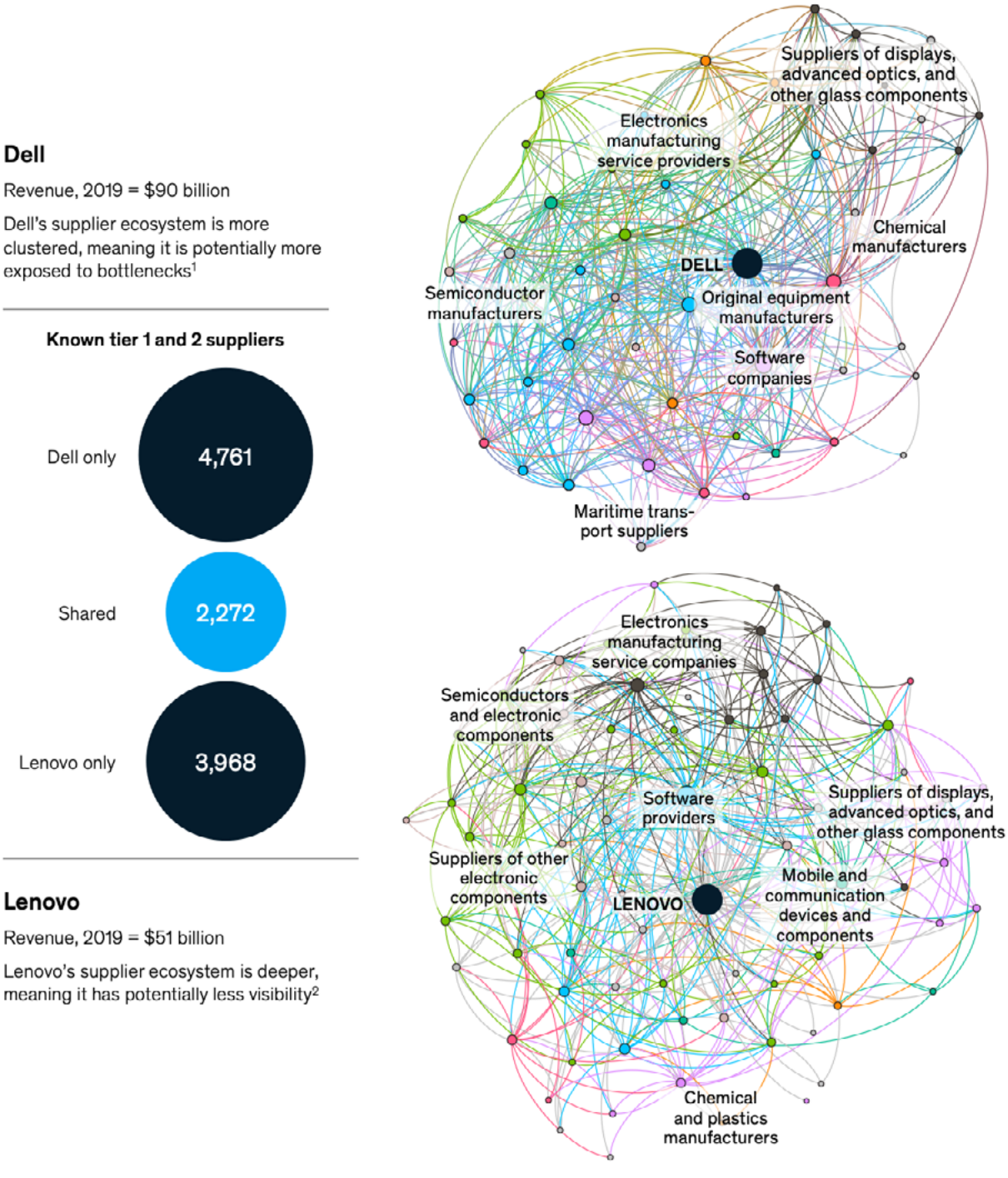


Imagem: ASSESSMENT OF THE CRITICAL SUPPLY CHAINS SUPPORTING THE U.S.

Modernização da cadeia de abastecimento

Desde a modernização das cadeias de abastecimento até a priorização da cibersegurança, as organizações devem agir para acompanhar o ritmo da transformação digital. Uma melhor visibilidade da cadeia de abastecimento pode impulsionar os métodos de produção sustentáveis e aumentar a confiança das empresas na origem dos seus materiais. O site de gerenciamento de dados do Statista cita uma pesquisa de 2018 que "descobriu que o maior desafio (21,8%) para os executivos da cadeia de suprimentos global era a visibilidade".

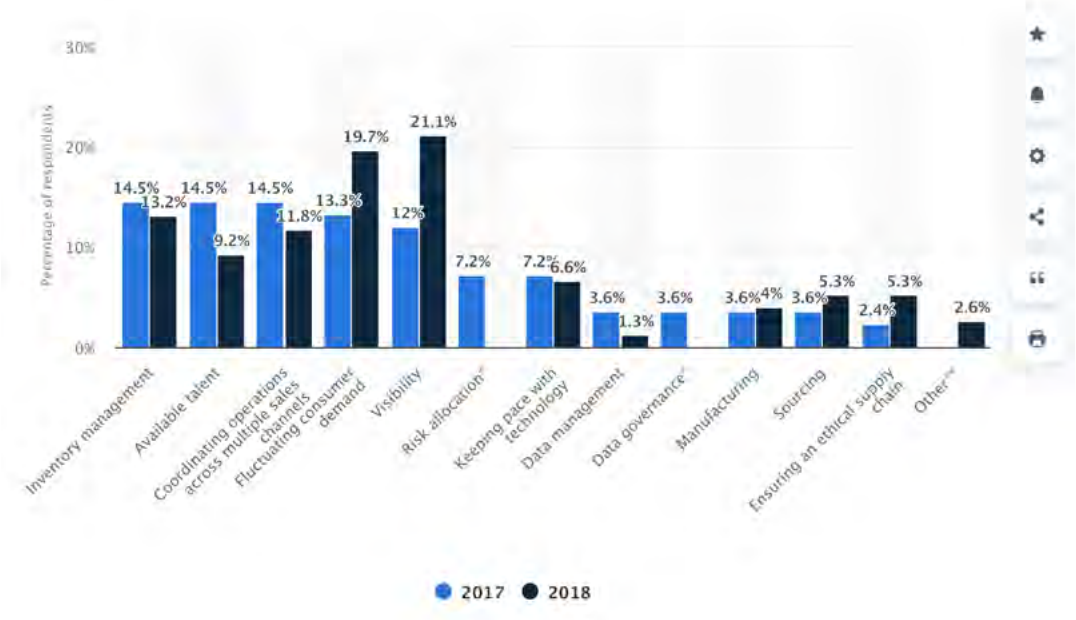
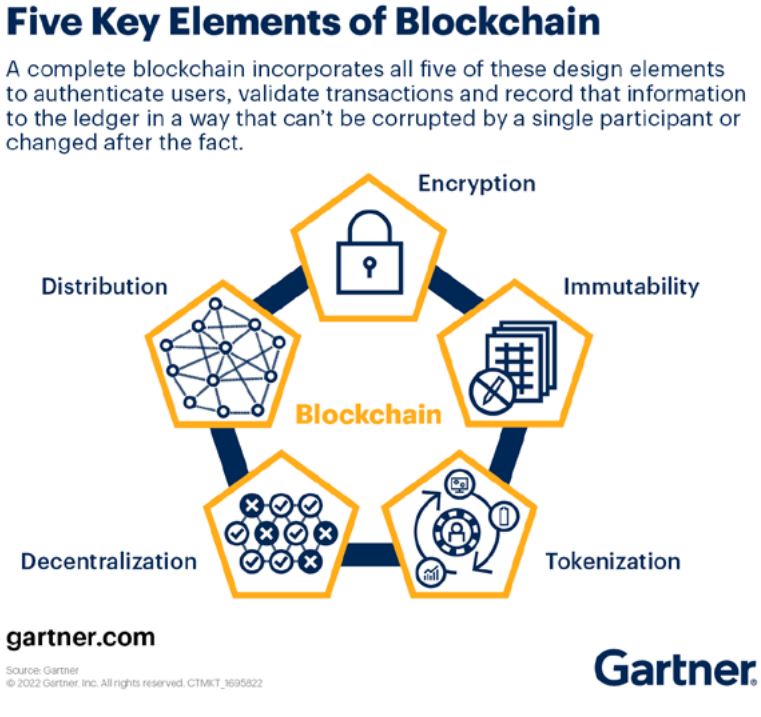


Imagem: Statista--Desafios da cadeia de fornecimento.

Blockchain na cadeia de abastecimento digital

As cadeias de abastecimento cada vez mais globalizadas e complexas estão wxercendo um grande impacto nas empresas internacionais. As partes interessadas nas cadeias de fornecimento precisam lidar com uma maior quantidade de informações enquanto rastreiam mais transações, registram o desempenho e planejam atividades futuras. A logística está se tornando cada vez mais complexa, com mais partes envolvidas direta ou indiretamente nas cadeias de suprimentos. Esta complexidade cria desafios relacionados com a comunicação e a visibilidade de extremo a extremo, o que torna os processos logísticos ineficazes.

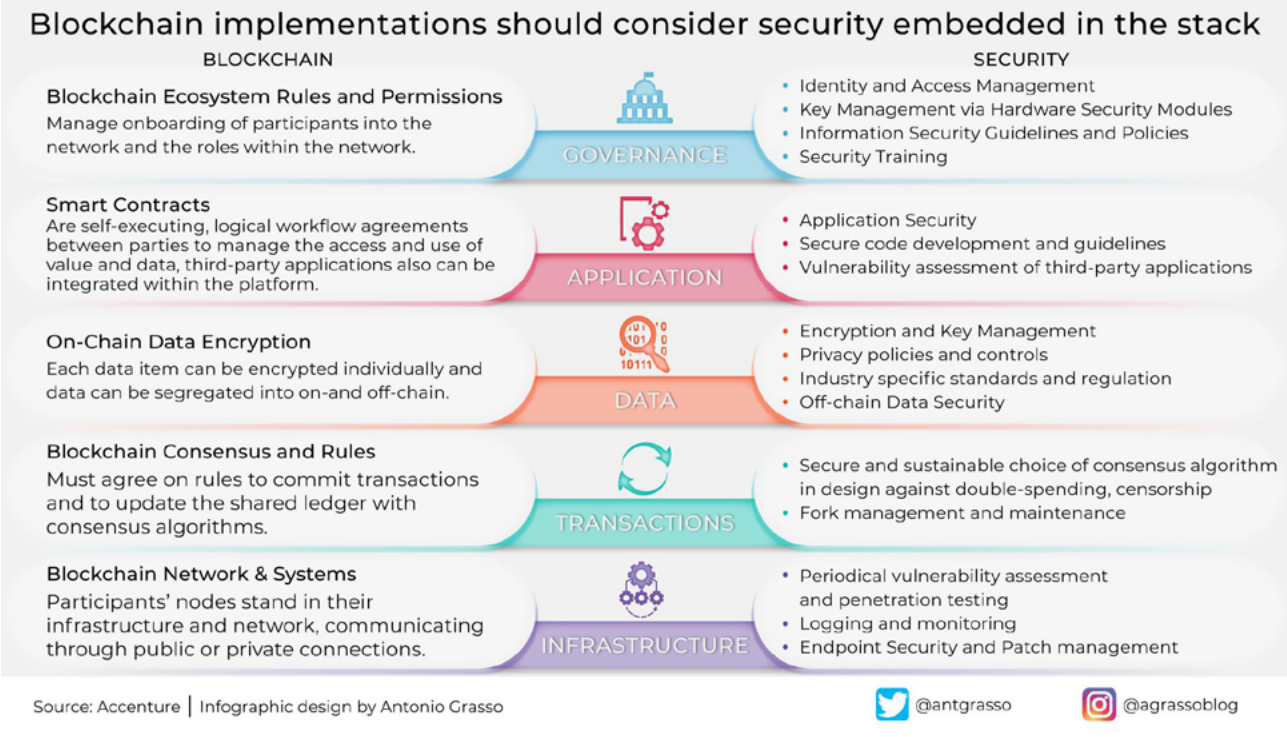
A Blockchain é uma tecnologia baseada na internet que é apreciada por sua capacidade de validar, registrar e distribuir publicamente transações em livros de contabilidade criptografados e imutáveis por meio de uma cadeia de blocos.



Essencialmente, trata-se de uma base de dados partilhada. Especificamente, o termo blockchain se refere a um registo de dados seguro e descentralizado que não pode ser alterado e que se forma através de uma rede de igual para igual.

O termo "cadeia de blocos" é derivado dos "blocos" de transações validadas e imutáveis e de como eles são ligados em ordem cronológica para formar uma string (documento). Por isso o termo.

Em última análise, a blockchain permite que diferentes organizações partilhem dados de forma segura e alcancem objetivos comuns de forma mais eficiente. Permite às partes interessadas interagirem sem necessidade de uma organização de controle central. E pode abrir oportunidades para desenvolver modelos de negócio completamente novos.



Benefícios de blockchain na cadeia de abastecimento

A tecnologia pode resolver desafios-chaves ao criar um registro digital criptografado que rastreia os produtos em cada etapa da cadeia de abastecimento. Faz com que qualquer irregularidade que possa interromper um envio seja claramente visível, o que permite às empresas resolverem os problemas rapidamente. Pode automatizar processos ao mesmo tempo em que facilita a verificação de mercadorias, reduzindo a burocracia e apoiando a rastreabilidade de extremo a extremo.

Melhorar a transparência e a rastreabilidade da cadeia de abastecimento

- Proporcionar transparência de extremo a extremo.
- Monitorar o desempenho.
- Confirmar a proveniência.
- Aumentar a visibilidade em tempo real.

Garantir a segurança, a imutabilidade e a autenticidade

- Autenticar dados e documentos.
- Detecção de fraude.
- Evitar roubos.

Reduzir a complexidade do processo

- Eliminar os intermediários.
- Melhorar a garantia de qualidade.
- Aumentar o nível de automação.

Melhorar a eficiência operacional

- Melhorar a conformidade.
- Reduzir o custo de transação.
- Reduzir o erro humano.

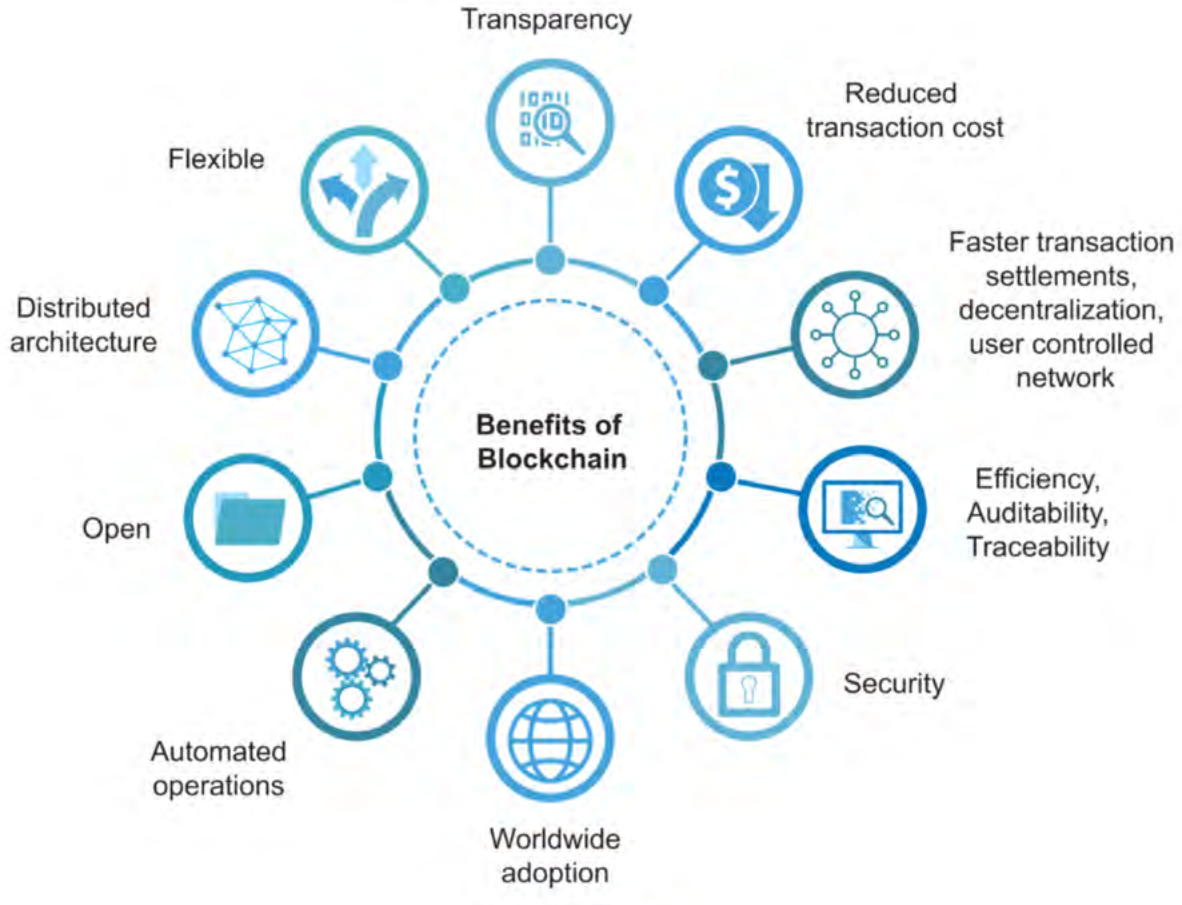


Imagen: Gartner

Casos de uso de blockchain em logística

Existe um grande potencial para as aplicações de blockchain dentro das funções logísticas. A tecnologia pode resolver desafios-chaves ao criar um registro digital criptografado que rastreia os produtos em cada etapa da cadeia de abastecimento. Os possíveis casos em que podem ser utilizados incluem:

Proveniência

Em logística, a origem se refere a uma linha temporal de mudanças na propriedade, custódia ou localização de um objeto. Poderia ser descrito como uma pista de auditoria e tem como objetivo garantir que cada produto enviado tenha um "passaporte" digital que demonstre a sua autenticidade. Estes passaportes incluem dados sobre onde e quando o produto foi fabricado, bem como a rota percorrida.

Pagamentos e faturamento

O faturamento e os pagamentos relacionados à logística implicam frequentemente processos manuais e em papel porque cada uma das empresas envolvidas mantém registros separados. Consolidar as faturas com os pagamentos vencidos ou creditados é uma tarefa que requer muito tempo para as empresas. A blockchain pode armazenar e compartilhar registros digitalizados, ao mesmo tempo em que cria contratos inteligentes que manipulam automaticamente faturas e pagamentos para encurtar os tempos de processamento e garantir a precisão.

Documentação digital

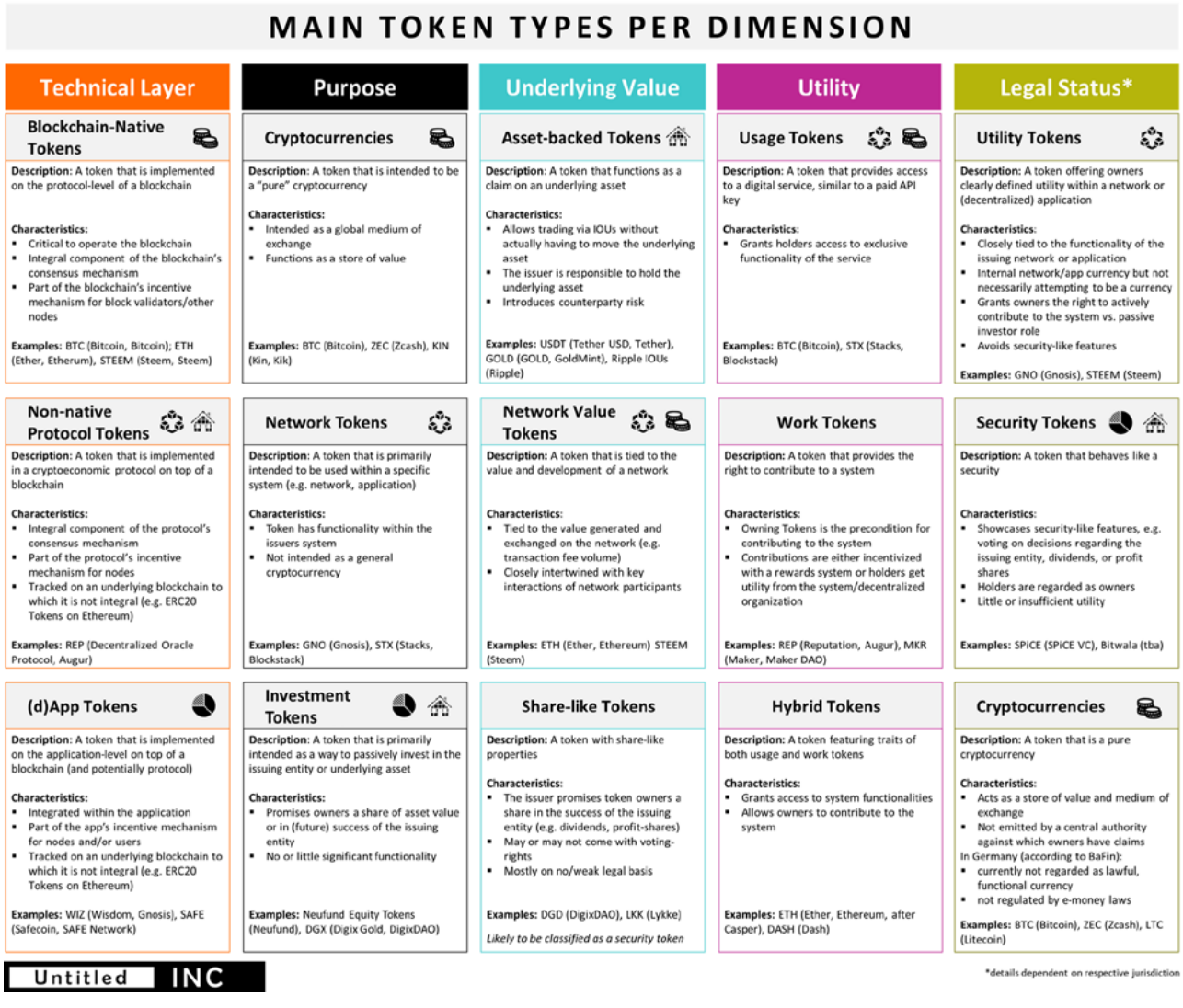
A combinação de blockchain com Internet of Things (IoT) pode resultar em contratos de logística inteligentes. Isto é possível quando os documentos digitalizados (por exemplo, registro de embarque, certificados, faturas, avisos prévios) e os dados de envio em tempo real estão integrados em sistemas baseados em cadeias de blocos. A documentação digital e os contratos inteligentes que utilizam blockchain já estão disponíveis nos portos de Antuérpia, Roterdão e Singapura.

Gestão de identidade

Blockchain Identity Management é uma solução segura que protege as identidades das pessoas contra fraudes ou roubos. Utiliza um modelo de confiança distribuído para garantir a privacidade, no qual os participantes autorizados asseguram, verificam e validam os documentos de identidade.

Mercado logístico

A blockchain permite uma comunicação fluida e integrada através de cadeias de fornecimento complexas. Desta forma, melhora a confiança, a segurança e a rapidez. Você pode até mesmo usá-la para criar plataformas onde os prestadores de serviços de logística ofereçam capacidade gratuita em caminhões ou barcos em tempo real.



Zero-Knowledge Proofs (ZKP)
ZKP é um método criptográfico no qual um testador pode convencer um verificador de que conhece um código secreto, sem revelar qualquer informação além do fato de que possui a informação. Embora isso exija alguma entrada do verificador (por exemplo, desafiar uma resposta), há também uma forma deste modelo chamado ZKP não interativo, não requer tal interação entre as duas partes.

As aplicações que se beneficiam da ZKP são aquelas que exigem uma medida de privacidade de dados. Algumas destas aplicações são:

- **Os sistemas de autenticação**. O desenvolvimento da ZKP foi inspirado por sistemas de autenticação, em que uma parte precisava provar a sua identidade a uma segunda parte através de informações secretas, mas sem revelar o segredo por completo.
- **Sistemas anônimos**. A ZKP pode permitir que as transações de blockchain sejam validadas sem a necessidade de revelar a identidade dos usuários que realizam uma transação.
- **Sistemas confidenciais.** Assim como os sistemas anônimos, o ZKP pode ser usado para validar transações de blockchain sem revelar informações relevantes, tais como detalhes financeiros.

O Zero-Knowledge Proofs (ZKP) permite a troca de informações entre os participantes das cadeias de valor, mantendo a capacidade de ajustar a quantidade de informações divulgadas. Dessa forma, as cadeias de blocos podem ser usadas para fornecer um registro ultra-resistente da proveniência de qualquer coisa que se possa registrar em uma base de dados, o que permite conhecer o nome da granja que cultivou os alimentos, por exemplo. Ou, no caso dos processos industriais, se o alumínio reciclado de uma encomenda provém efetivamente de uma fonte de alumínio reciclado.

A ZKP mantém a informação oculta indefinidamente, permitindo que os usuários da cadeia de blocos a interroguem. Em vez de listar todos os materiais de um componente, o ZKP funciona como um portal de perguntas e respostas.

O modelo Zero-Trust de Cibersegurança

O modelo Zero-Trust tem sido amplamente reconhecido como uma abordagem eficaz para evitar vazamentos de dados e reduzir o risco de ataques à ca-

deia de suprimentos. Embora este modelo tenha sido amplamente reconhecido, a sua adopção nos sectores público e privado tem sido lenta e inconsistente.

O Zero-Trust tem como princípio básico que não devemos confiar em ninguém nem em nada só porque está dentro do perímetro da organização. A Forrester estabeleceu o modelo Zero-Trust que se centrou no princípio orientador "Nunca confiar, sempre verificar" e o reconhecimento de que os firewalls perimetrais já não são suficientes para proteger segredos comerciais e ativos.

Imagem: Tecnologia mundial

É importante reconhecer que não existe um produto milagroso nem uma forma única de implementar Zero-Trust. Requer uma abordagem de segurança em camadas que cubra toda a infraestrutura digital, os sistemas antigos e modernos, com foco em ter os controles adequados onde o usuário acessa os recursos digitais e uma menor dependência da segurança do perímetro.

Embora não existam definições comummente aceitas, estes princípios são reconhecidos como essenciais para a implementação de um roteiro estratégico do Zero-Trust:

Princípio 1: Coerência na forma como autentica e autoriza os utilizadores e recursos digitais.
Princípio 2: Assegurar todas as comunicações, in-

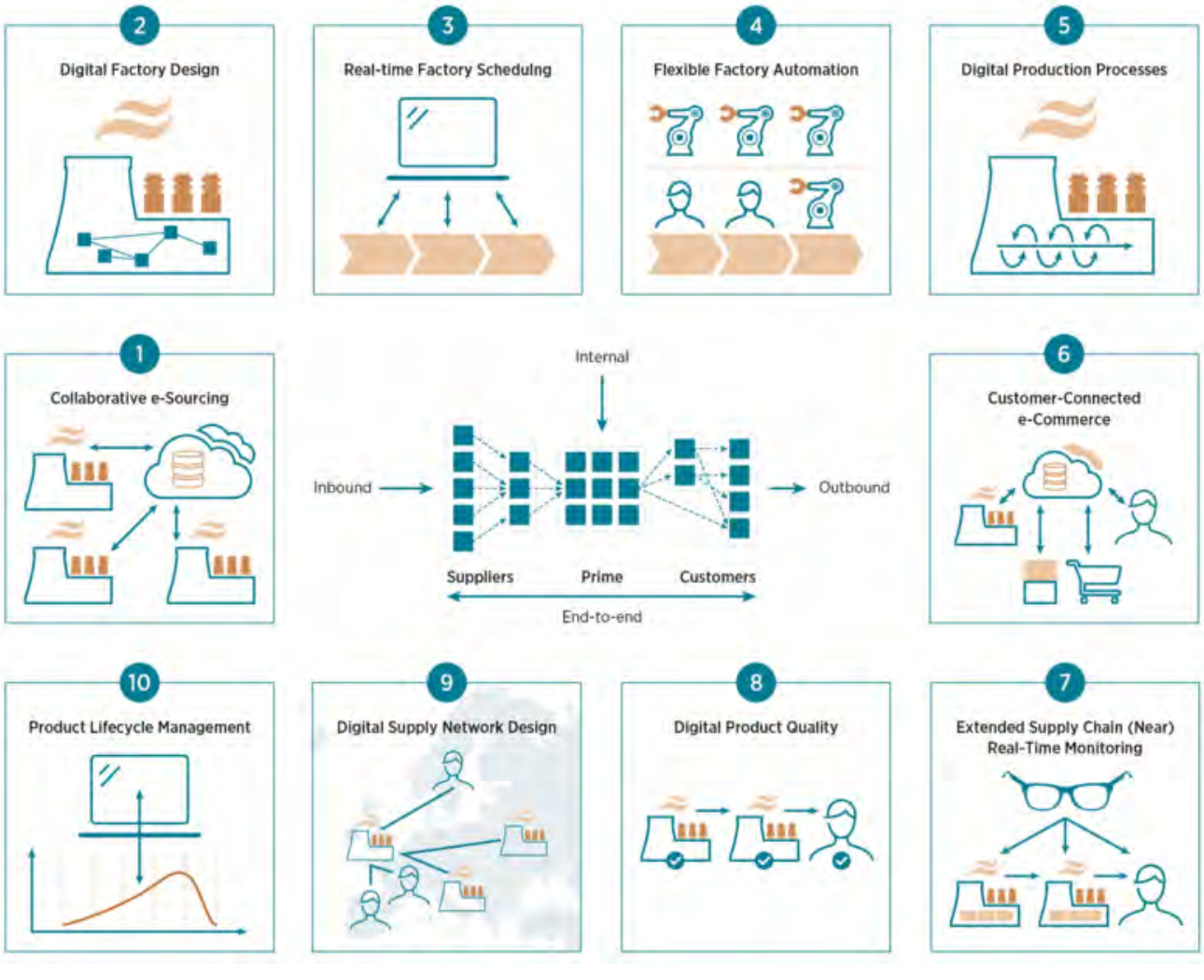


Imagem: Universidade de Cambridge - As cadeias de fornecimento digitais são cada vez mais complexas.

dependentemente da localização da rede.
Princípio 3: Aplicar o acesso baseado no princípio do privilégio mínimo.
Princípio 4: Monitorar e verificar explicitamente a postura de segurança e a integridade de todos os recursos digitais.
Princípio 5: Consultar sempre os princípios orientadores "Nunca confie, sempre verifique" e "suponha uma infração".

O componente de maior valor da cadeia de abastecimento.

A implementação de tecnologias como a Blockchain, o ZKP e o Zero-Trust, entre outras, nos convida a pensar que as soluções para os novos desafios que se apresentam com o desenvolvimento da transformação digital e a indústria 4.0 poderão ter um bom ponto de equilíbrio em relação à segurança digital proporcionada por estas tecnologias. Como ponto relevante deste equilíbrio se apresenta o componente humano, o elo mais importante dentro da proteção e resguardo da cadeia de fornecimento, e ao mesmo tempo o mais fraco.

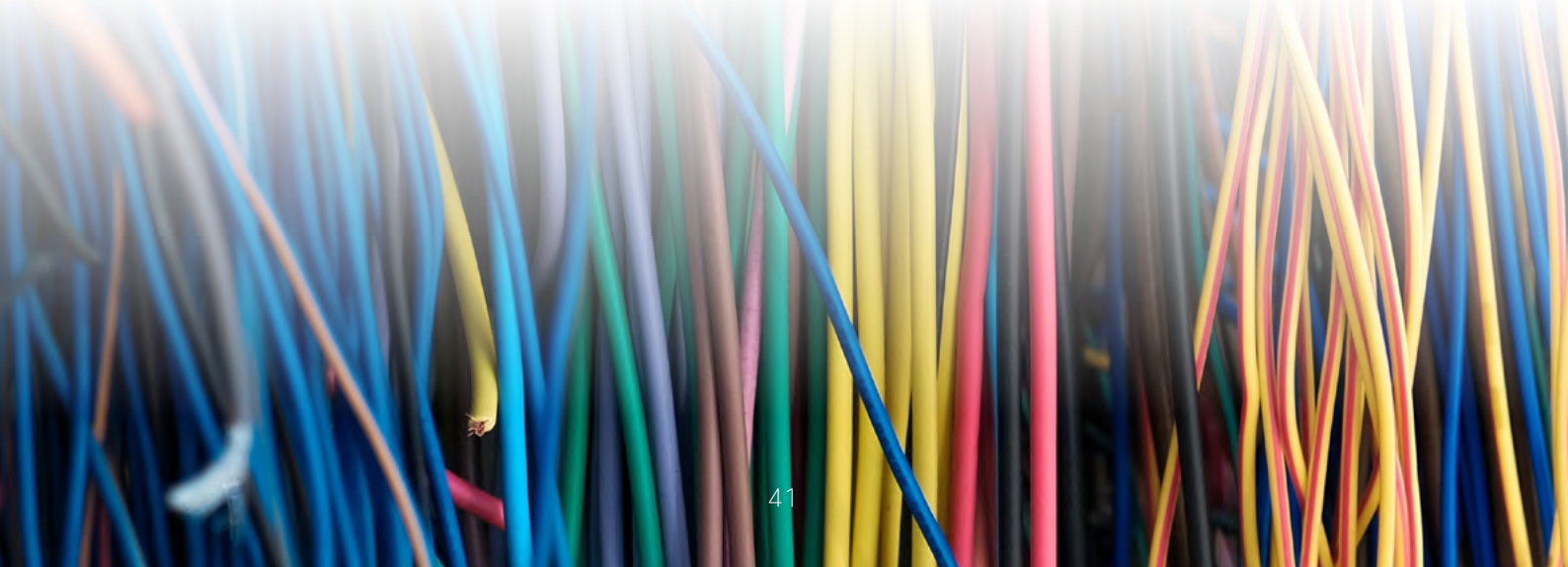
A carência na América Latina e no Caribe de formação acadêmica em cibersegurança é alta em termos regionais, e muito dispar entre os diversos países de compreendem as sub-regiões do continente e assim o demonstra o Relatório de Cibersegurança 2020 elaborado pela OEA e o BID. Segundo o relatório, dois terços dos países da América Latina e do Caribe apresentam poucas ou nenhuma melhorias quanto ao nível de maturidade em matéria de educação, capacitação e desenvolvimento de habilidades em cibersegurança. Além disso, a oferta de formação especializada em segurança digital na maioria destes países é inexistente ou tem caráter de incipiente, e usualmente considera apenas a dimensão técnica da cibersegurança.

Na busca de uma métrica que indique quais poderiam ser os níveis de avanço nos diversos países da região, descobrimos que em poucos países se conta com algum tipo de levantamento de informação que demonstre o uso dos ambientes IoT - IIoT dentro da cadeia de fornecimento em nível operacional. Além disso, se identifica que em nenhum dos países da região se conta com um estudo que possa demonstrar o nível de cibersegurança dos ambientes hiperconvergentes na cadeia de fornecimento. Ou seja, o trabalho neste sentido está apenas no início.

Aprender é uma virtude dos seres humanos, de forma a mantermos sempre presentes as lições aprendidas e evitemos repetir experiências como a adesão definida em diversos países de LATAM de uma normativa como a NERC-CIP que é aplicada como uma solução para resguardar a Proteção de Infraestrutura Crítica - CIP e não como uma normativa de cibersegurança para o setor elétrico (o mesmo país criador desta normativa reconhece que este não é o objetivo para o qual foi concebida, e por essa razão atualmente desenvolve diferentes iniciativas que são impulsionadas tanto pelo Departamento de Energia – DOE dos Estados Unidos - como pela CISA, e têm por objetivo desenvolver diversas leis e normativas técnicas focadas na segurança digital deste setor).

A definição de regulamentos que fortaleçam o quadro jurídico da cadeia de abastecimento no âmbito da cibersegurança é uma necessidade que será altamente valorizada na região sempre que esta envolva planos de desenvolvimento de profissionais de cibersegurança para os ambientes IoT - IIoT. Desta forma, se evitará o vazio de capacidades humanas que gerou a incorporação de regulações que não integravam o desenvolvimento destas habilidades e que agora sofrem as diferentes equipes de recursos humanos de mais de 1000 empresas do setor elétrico na LATAM, que procuram pessoal em cibersegurança sem encontrá-lo. Neste contexto, é muito baixa a oferta de crescimento profissional ou acadêmico que ajude a cobrir a demanda de pessoal criada na região, assim como também não pessoal com conhecimento empírico que acredite implementações de cibersegurança como casos de sucesso.

A criação de Estratégias de Cibersegurança para as Infraestruturas Críticas dos países da LATAM é o primeiro grande passo na região



Especial
Trabalho Híbrido

Abundância e confusão, medo e infidelidade

Imagem: Sharon Mccutcheon, Unsplash.

Coluna

por **Pablo Marrone**
Assessor em CX e Comunicação

Trabalhar em tempos de “quase pós-pandemia” e “quase terceira guerra mundial”. É disso que se trata.

Ou ser líder de equipe, nesse mesmo contexto: sustentar objetivos, inspirar horizontes, cativar talentos.

Em tempos de medo e confusão crescentes, a abundância de tecnologias permite gerar cenários de trabalho diversos a fim de atrair empregados cada vez mais infiéis às suas próprias organizações. A “grande renúncia” gerou um desafio nunca visto.

A oferta do empregador deve gerar uma “experiência do colaborador”, tendo a infraestrutura de hardware e software como plataforma habilitante. Muito semelhante ao que acontece quando navegamos na web, ou vamos a um negócio e nos envolvem com a “experiência do cliente”.

Com essa plataforma, dar opções: alguns precisam da segurança e previsibilidade do escritório; outros da flexibilidade de escolha sobre que dia estar aqui ou lá. Todos precisam se convencer de que são donos das suas escolhas.

O padrão cultural flui, como se fosse um relógio de Dali e desafia os líderes, que devem encontrar nessa fluidez sua nova zona de conforto. Ao mesmo tempo, manejar as novas ferramentas, e implementar métricas imprescindíveis para o negócio. Mas sem ser intrusivos.

O trabalho é híbrido, mas também a gestão e as interações. Estou presente sem estar. Lidero sem ver. Cumpro sem me gabar. Estou disponível sem “micro gestão”. Inspiro. Deixo-me inspirar. Acredito e ajudo a criar.

Em tempos de “pós-pandemia” e “quase terceira guerra mundial”, a fidelidade à organização deriva de uma experiência humana e emocionalmente alinhada com os colaboradores. O trabalho híbrido é uma resposta possível a esta necessidade de limitar a confusão e o medo.

O escritório como espaço alternativo, a virtualidade colaborativa como valor, a tecnologia como aliado invisível, amigável e transformador.
É sobre isto que estamos falando

Especial
Trabalho Híbrido

Imagem: Sincerely Media, Unsplash.

Cumprir a promessa do trabalho híbrido

O trabalho híbrido é uma abordagem que projeta a experiência de trabalho em torno e para o trabalhador onde quer que ele esteja, permitindo que as pessoas trabalhem a partir de casa, no escritório ou em qualquer lugar. É uma evolução natural do trabalho remoto e representa uma grande transformação da cultura laboral. Além disso, permite às organizações de hoje acentuar os pontos fortes da sua força de trabalho e alinhar-se com os seus estilos de trabalho preferidos, resultando em empregados mais felizes e produtivos. Este documento examina como a convergência de pessoas, tecnologias e lugares está impulsionando o trabalho híbrido e os passos a seguir para que esta modalidade funcione.

Imagem: Cristian Tarzi, Unsplash

O futuro de um trabalho ainda mais híbrido

Embora a implementação prática das políticas de trabalho híbrido possa variar de organização para organização e de indústria para indústria, a maioria dos trabalhadores concordaria em manter a flexibilidade como política no futuro. Isto é ilustrado pelo estudo feito pela Cisco, segundo o qual apenas 9% dos trabalhadores querem regressar ao escritório a tempo inteiro. A implicação é clara: o trabalho híbrido está aqui para ficar e as organizações devem evoluir seus modos tradicionais de operar para sobreviver e prosperar nesta nova era de trabalho.

A vantagem do trabalho híbrido

A boa notícia para as empresas é que muitos líderes ouviram e planejam atender ao chamado do trabalho híbrido. A pesquisa mostra que 9 em cada 10 executivos esperam 38% de trabalho híbrido como modelo de fato para suas empresas no futuro.

Visão clara de futuro

O mandato para um futuro do trabalho mais híbrido é claro. Muitas empresas e seus líderes já o reconhece. O que ainda está nebuloso é a visão, o alinhamento e a experiência necessários para avançar.

O que segue no trabalho híbrido

Recursos para ajudá-lo a avançar mais e mais rápido na evolução do trabalho híbrido.

Existem vários recursos úteis disponíveis para empresas interessadas em desenvolver e implementar sua própria estratégia de trabalho híbrido.

A Cisco tem uma ferramenta simples de preparação para o trabalho híbrido que fornece uma avaliação da posição de uma empresa para a viabilidade do trabalho híbrido em comparação com os seus pares. A ferramenta de avaliação também irá gerar um guia detalhado sobre temas como:

- Como otimizar o trabalho remoto.
- Como garantir e gerenciar uma infraestrutura de trabalho híbrida.
- Como criar uma cultura de trabalho inclusiva e solidária.
- Como trazer os empregados de volta ao escritório em segurança.

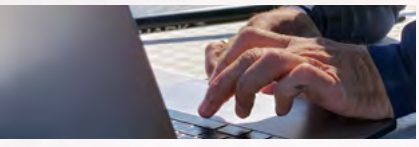
O índice global de trabalho híbrido da Cisco identificou tendências de trabalho emergentes, mostrando como as organizações podem dar vazão à criatividade e inovação, e melhorar o bem-estar de seus trabalhadores.

Você já se perguntou como as empresas bem sucedidas estão fazendo a transição para novas formas de trabalhar e como sua organização é comparada com os líderes da indústria? Em junho de 2022, a Cisco apresentará o Modelo de Maturidade do Trabalho Híbrido para ajudar as organizações a avaliar onde estão em suas jornadas rumo ao trabalho híbrido e o que devem fazer para alcançar seus objetivos. O modelo se baseia nos resultados de inquéritos de organizações de todas as dimensões e de uma variedade de indústrias em todo o mundo. Examinará o espectro de maturidade do trabalho híbrido através das etapas, começando com organizações que ainda não percorreram seu caminho, outras que começaram a implementá-lo e a aprender, até aquelas que realmente adotaram um modelo de trabalho híbrido e, através de sua liderança, estão impulsionando os limites do que se pode alcançar.

Dos desafios do trabalho híbrido às oportunidades para a inovação

A mudança para o trabalho híbrido marca um momento verdadeiramente único para organizações de todo o mundo que podem redefinir todos os aspectos do trabalho para criar ambientes de trabalho mais flexíveis, incluindo apoio, administração e segurança. Esta tendência geracional é impulsionada pela convergência de pessoas, tecnologia e locais e está constantemente remodelando as expectativas tanto dos empregadores como dos empregados.

Embora a mudança para o trabalho híbrido apresente vários desafios, as organizações que tomam medidas significativas têm agora a oportunidade de promover a inclusão, melhorar a produtividade e permitir a interactividade a níveis sem precedentes. Isso resultará em empregados mais felizes e produtivos, o que pode criar organizações mais fortes que liderem nesta próxima era de trabalho



Alinhamento C-level

Como jogar luz sobre o trabalho híbrido

O mandato d o trabalho híbrido está em vigor e muitas organizações e líderes já o reconheceram. O que não está claro são os passos que estas empresas devem dar para avançar. Um relatório recente (1) ilustra isto quando nove em cada dez executivos afirmam que visualizam um modelo de trabalho híbrido no futuro e só têm um plano básico de alto nível para seguir em frente. De fato, um terço das empresas dizem que a ideia do trabalho remoto "não recebe o apoio da alta gestão" e "apenas uma em cada dez organizações começou a comunicar e provar essa visão".

Isto apresenta uma oportunidade para os líderes e suas equipes em funções-chave como estratégia tecnológica, gestão de pessoas e operações para ajudar a impulsionar a visão de trabalho híbrido em suas organizações. Aqui apresentamos um resumo dessas oportunidades por função:

CIO:

O trabalho híbrido está criando uma convergência de tecnologias de colaboração, redes e segurança. Nossos funcionários precisam de acesso fácil a aplicativos e experiências colaborativas de alta qualidade, o que torna fundamental proteger as ferramentas de trabalho remoto para proteger os dados dos clientes e funcionários em todos os momentos. Os CIOs podem desempenhar um papel central ajudando suas empresas a navegar em estratégias digitais de colaboração, redes, segurança e outras. Isso resultará em organizações mais ágeis e com conhecimentos digitais que podem satisfazer melhor às necessidades de funcionários, clientes e parceiros.

CHRO:

Compreender as necessidades e expectativas de nossos funcionários é fundamental para reter os melhores talentos e expandir o grupo. Os empregados de hoje querem mais flexibilidade e mais voz sobre onde, quando e como trabalham. Mas não há um tamanho único para todos. As experiências de trabalho, os estilos de trabalho e as preferências profissionais são tão variados e pessoais como as pessoas que compõem a força de trabalho de uma organização. Ao ouvir os funcionários e permitir que as equipes determinem as configurações de trabalho híbridas que funcionam melhor para eles, as empresas podem treinar seus funcionários e equipes para aproveitar seus pontos fortes e se concentrar em fazer o trabalho funcionar para eles.

COO:

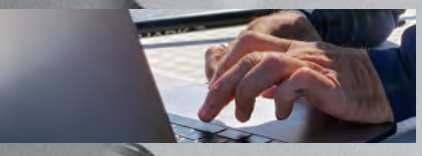
O trabalho híbrido redefinirá significativamente a gestão de operações e instalações, especialmente quando os funcionários voltarem a trabalhar em larga escala. Garantir a segurança e a produtividade dos funcionários são as principais prioridades, o que requer redesenhar nossos locais de trabalho para que se concentrem mais no ser humano e menos no escritório. Isto incluirá a construção de espaços de colaboração dedicados e "inteligentes" para conferências mais fáceis e menos espaços de trabalho atribuídos ou menores. Portanto, o diretor de operações pode desempenhar um papel integral para ajudar a criar um local de trabalho "centrado no ser humano" que seja fundamental para o desempenho híbrido.

À medida que desenvolve a estratégia de trabalho híbrido para cada organização, a Cisco sugere utilizar as seguintes cinco características (2) que podem servir como um quadro útil ou uma lista de verificação para criar soluções para este tipo de trabalho:

Inclusivo: igualdade de experiências para todos.
Flexível: adaptando-se a qualquer estilo de trabalho, papel, ambiente.
Apoio: centrando-se na segurança, na empatia e no bem-estar.
Seguro: ser seguro por design, privado por padrão.
Gestão: fornecimento de infraestruturas modernas, gestão sem atritos

(1) McKinsey & Company: o que os executivos dizem sobre o futuro do trabalho híbrido, maio de 2021.
(2) Cisco: O que é o trabalho híbrido? Características do Trabalho Híbrido, 2021.

Imagem: Marten Bjork, Unsplash.



Especial
Trabalho Híbrido

Cinco dicas
para mantê-lo seguro

À medida que o mundo faz a transição para uma força de trabalho híbrida permanente, a flexibilidade traz novos benefícios e desafios para empregadores e trabalhadores. Quer a equipe esteja a trabalhar no escritório, de forma remota ou sob um esquema intermédio, é preciso não comprometer a segurança. Aqui dividimos uma lista de cinco conselhos simples para manter a cultura de força de trabalho híbrida, enquanto os trabalhadores e os ativos da empresa são protegidos.

Imagem: Charlesdeluvio, Unsplash.

01

Educar a força de trabalho para que adote práticas de trabalho seguras

Os trabalhadores esperam que a tecnologia os siga onde quer que vão, mas ter locais flexíveis os expõe (e à sua organização) a ameaças de novas formas. É por isto que as equipes de TI e segurança devem garantir que a experiência híbrida seja segura em todos os pontos finais ao educar os usuários sobre práticas seguras e perigos potenciais.

02

Verificar se a pessoa é quem diz ser

A autenticação multifator (MFA) é uma primeira camada de segurança simples que todas as empresas necessitam antes de conceder acesso aos seus ativos. Trata-se de um método de controle de acesso digital em que a um usuário é concedido acesso ao sistema apenas depois de apresentar duas ou mais provas diferentes de que ele é quem diz ser, com o objectivo de verificar a sua identidade e o estado do dispositivo.

03

Habilitar acesso seguro de qualquer lugar

A VPN (Virtual Private Network) fornece um túnel seguro entre os usuários e aplicativos para que os trabalhadores possam se manter produtivos e conectados quando estão viajando ou trabalhando em casa. Ajuda a garantir que apenas os usuários aprovados acessem os sistemas, fornecendo um nível adequado de segurança sem comprometer a experiência do usuário.

04

Adotar a defesa contra ameaças de segurança em qualquer ponto de entrada

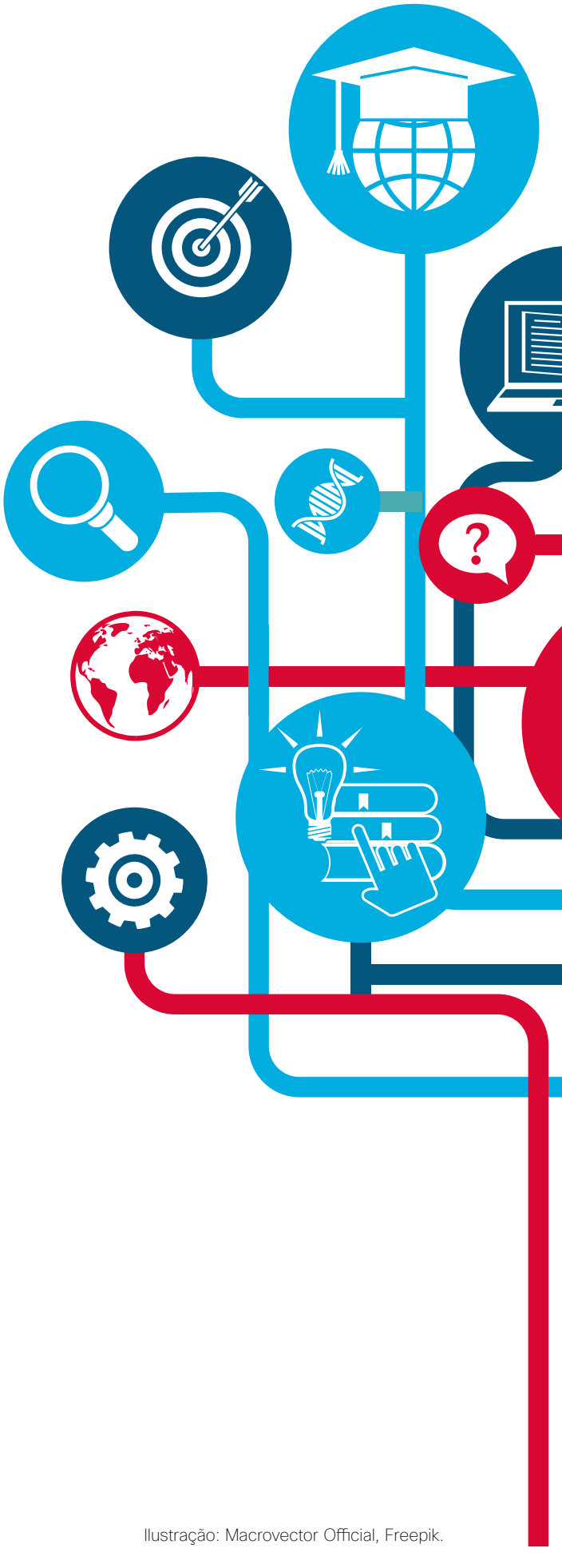
A maioria das violações de segurança têm como alvo os usuários finais, o que requer uma primeira linha de defesa na camada de DNS e uma última linha para as ameaças que são filtradas. A primeira camada bloqueia os domínios associados ao comportamento malicioso antes de entrar em sua rede ou conter malwares se já estiver dentro, enquanto a última camada protege contra ameaças mais avançadas.

05

Unificar a segurança através de uma plataforma simples e integrada

Fazer da segurança algo fácil e efetivo é uma via que colabora na gestão integral. Através da plataforma Securex, os produtos Cisco Secure e a infraestrutura se unem e contribuem para uma administração de segurança simples e eficaz.

Com o Cisco Secure Hybrid Work é possível manter os dados seguros independente de onde estejam trabalhando as pessoas que fazem parte da organização, já que se trata de uma solução simples e unificadora para habilitar a segurança em toda parte e potencializar o trabalho a partir de qualquer lugar



Por que um programa de formação online sobre cibersegurança?

A Cibersegurança é uma especialidade que ganhou ainda mais importância em função da transformação tecnológica experimentada por instituições e empresas e cuja finalidade última consiste em proteger os ativos digitais - equipamentos de trabalho, informação, serviços na internet, redes de comunicações etc.- de ameaças que comprometam a sua confidencialidade, integridade e disponibilidade. Hoje em dia, as empresas não se questionam se serão vítimas ou não de um ciberataque, simplesmente têm que estar preparadas para quando lhes tocar.

Qual é o objetivo do programa?

O objetivo do Programa neddux online em Cibersegurança é duplo:

1. Transmitir os conhecimentos necessários para compreender o alcance e a relevância desta matéria e

2. Aplicar esse conhecimento na gestão das situações e na resolução dos problemas que se colocam.

Para o efeito, foram concebidas duas modalidades, tendo em conta os diferentes perfis de empregados que existem numa organização e que, por conseguinte, requerem uma formação diferenciada:

Ilustração: Macrovector Official, Freepik.

Seção

Formação profissional

A Cisco Secure, através da empresa neddux, irá oferecer um programa de formação em cibersegurança para líderes da região. Em uma conversa agradável, Eduardo Gómez, CEO da neddux, compartilha com a Bridge as diretrizes deste treinamento.

1.- Programa de Gestão: dirigido aos responsáveis pela área de Sistemas, Cibersegurança e ao primeiro nível gerencial, que está à frente nas decisões. É composto por seis módulos que abrangem todas as fases chave para gerir a Cibersegurança, seguindo a metodologia do caso. Tem duração aproximada de 45 horas, distribuídas de forma autônoma ao longo de três meses.

2.- Programa de Sensibilização, dirigido a todas as pessoas que manuseiam bens, equipamentos, informações, serviços, redes de comunicação etc., e cujo objetivo é consciencializar sobre a importância de uma gestão adequada e evitar a entrada de cibercriminosos por desconhecimento. Dura uma hora.

Quais são os benefícios que diferenciam este programa de treinamento dos demais?

O programa da Universidade Neddux e Francisco de Vitoria tem características próprias e desenvolve uma metodologia que não existe atualmente na área da formação online:

Use o cinema acadêmico:
A produção cinematográfica personalizada, baseada em experiências reais e casos de ciberataques, permite ao aluno viver a experiência como mais um protagonista do filme, despertando uma parte do cérebro que normalmente está adormecida nos processos tradicionais de aprendizagem. O cinema também é aplicado em cada uma das fases da metodologia neddux: trabalho em equipe, diagnóstico e tomada de decisão. O aluno mantém o interesse e ingressa na disciplina progressivamente, quase sem perceber, consolidando os conceitos de forma natural e simples e aplicando-os a uma realidade concreta.

O cinema acadêmico é apenas o primeiro passo, embora muito importante, dentro da metodologia neddux.

O rigor acadêmico do método de casos:
O programa é baseado no método de casos, que é aplicado nas melhores escolas de negócios do mundo. O aluno tem a oportunidade de percorrer todas as fases desta metodologia, aprimorando sua capacidade de análise, síntese, diagnóstico, gerando alternativas de ação, avaliando-as e, por fim, tomando decisões. Isto melhora seu processo de tomada de decisão e o prepara para enfrentar problemas futuros com maior competência.

Autoestudo: todo o conteúdo acadêmico foi encapsulado em um formato flexível, que pode ser adaptado à disponibilidade de tempo dos alunos para estudar. Essa flexibilidade é alcançada porque incorporamos o cinema a outros elementos-chave do método de caso, como o trabalho em equipe, a aula do professor e a tomada de decisões, por exemplo. Aumentamos o valor da formação online através do cinema acadêmico.

Conteúdo do programa de gerenciamento

O *"Programa de Gerenciamento de Cibersegurança"* é uma especialidade que consiste em seis módulos independentes apresentados progressivamente na seguinte ordem:

Gerenciamento de riscos em segurança cibernética. São identificados os principais conceitos de risco que permitem compreender uma disciplina como a cibersegurança, que gira em torno do conhecimento de ativos, vulnerabilidades, ameaças, riscos potenciais, controles etc.

Centro de Operações de Segurança (SOC). Este módulo detecta atividades hostis contra infraestruturas tecnológicas e seus serviços e a gestão de alertas associados.

Vulnerabilidades e patches de segurança cibernética. O programa avança analisando vulnerabilidades, que são fragilidades de controle ou erros do sistema que colocam em risco a segurança das informações e dos serviços.

Plano de Resposta a Incidentes. Este módulo aprofunda o plano de resposta a incidentes, que é um conjunto ordenado de ações focadas em responder a um incidente com altos níveis de criticidade e impacto nas operações e funções de negócios.

Plano Diretor de Cibersegurança. O quinto módulo analisa a importância de ter um plano elaborado, explica como prepará-lo e os principais elementos que devem estar presentes para reduzir ou mitigar riscos.

Estruturas de segurança cibernética. Por fim, é apresentada a necessidade de se ter um quadro de referência, que contenha o conjunto de boas práticas, atividades estruturadas, controles, avaliações e medições, de modo que haja uma cultura transversal em segurança cibernética.

Conteúdo do Programa de Conscientização

O *"Programa de Conscientização sobre Cibersegurança"* é um curso apoiado principalmente pelo filme no qual são resolvidas questões básicas para entender a importância de ser prudente na gestão dos ativos da empresa.

O valor fornecido pelo grupo, chave para se manter atualizado.

Além de ser um programa baseado na autoformação, os participantes fazem parte de uma promoção de 25 alunos em que poderão partilhar as suas experiências em dois momentos ao longo de cada um dos seis módulos: em trabalho em equipa, composto por cinco alunos cada, e nas sessões plenárias dadas pelo docente no final do estudo de cada módulo.

Os cibercriminosos estão continuamente inovando como fazer o mal e estão sempre à frente. Este programa visa contrariar esta vantagem através da troca de experiências, apoiadas no conhecimento e no vasto conhecimento da equipe docente

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

Imagem: Timon Studler, Unsplash.

A privacidade torna-se uma missão crítica

Estudo comparativo de privacidade de dados, Cisco 2022

Introdução

Nos últimos anos, a privacidade se tornou missão crítica para organizações em todo o mundo. Mais de dois terços dos países promulgaram leis de privacidade, os clientes não compram de organizações que não protegem seus dados e as métricas de privacidade ganharam espaço na alta direção das corporações. Adicionalmente, as competências em matéria de privacidade são cada vez mais importantes também entre os profissionais de segurança digital, e as organizações se beneficiam financeiramente dos investimentos nesta área. Este relatório, nossa quinta revisão anual de questões-chave de privacidade para as organizações, analisa o impacto da privacidade nas empresas em todo o mundo.

Pontos-chave do relatório

1. A privacidade se tornou essencial para a cultura e as práticas comerciais das organizações, incluindo os seus processos de compra, métricas de gestão e áreas de responsabilidade dos empregados.
2. O retorno do investimento (ROI) da privacidade continua elevado pelo terceiro ano consecutivo, com maiores benefícios especialmente para as pequenas e médias organizações e ainda mais elevado para as organizações maduras no tema.
3. A maior parte das organizações reconhece a sua responsabilidade de tratar os dados de forma ética, mas muitos clientes querem mais transparência e estão preocupados com a utilização dos dados, em particular na Inteligência Artificial (IA) e em decisões automatizadas.
4. Os requisitos de localização dos dados são considerados importantes, mas onerosos.
5. Alinhar a privacidade com a segurança parece criar vantagens financeiras e de maturidade em comparação com outros modelos organizacionais.

Metodologia

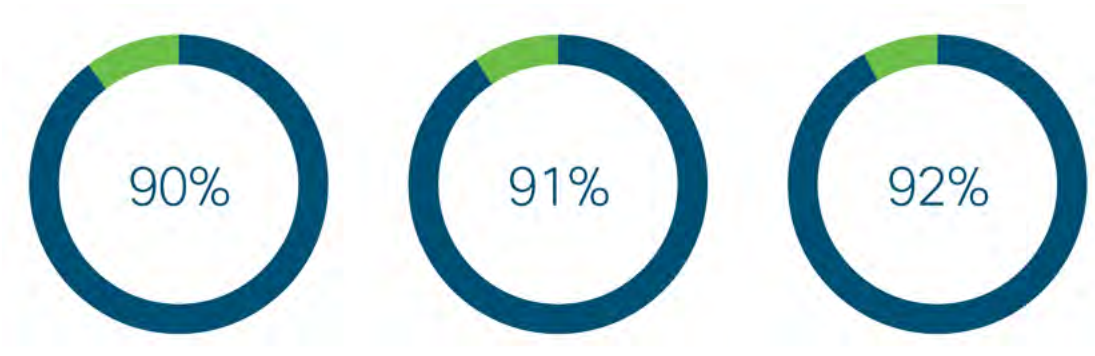
Os dados desse estudo são derivados da pesquisa Cisco Security Outcomes, na qual os entrevistados eram anônimos para os pesquisadores e não foram informados quem estava realizando o levantamento. Usando a mesma metodologia dos anos anteriores, mais de 5.300 profissionais de segurança de 27 localidades completaram a pesquisa no verão de 2021. Os inquiridos representam todas as principais indústrias e uma combinação de dimensões de empresas (ver Apêndice 1). Dirigimos perguntas específicas sobre privacidade aos mais de 4.900 entrevistados que indicaram estar familiarizados com os processos de privacidade em suas organizações. Neste relatório, também incluímos resultados relevantes da Pesquisa de Privacidade do Consumidor da Cisco 2021, que foi completada no verão de 2021 por 2600 adultos em 12 países.

1. A privacidade se torna uma missão crítica

A privacidade se tornou um imperativo comercial e um componente crítico da confiança do cliente para organizações em todo o mundo. Pelo segundo ano consecutivo, 90% dos entrevistados em nossa pesquisa global disseram que não comprariam de uma organização que não protege adequadamente seus dados, e 91% disseram que certificações externas de privacidade são relevantes no processo de compra.

A pandemia de COVID-19 fortaleceu ainda mais o papel da privacidade, já que 91% das organizações

disseram que suas equipes de privacidade as ajudaram a lidar com muitos problemas complexos de dados pessoais da força de trabalho que surgiram nos últimos anos. Talvez não seja surpreendente que 92% das organizações disseram que respeitar a privacidade é parte integrante de sua cultura.



Nossos clientes não nos comprariam se não protegessemos adequadamente seus dados
90 %

Certificações de privacidade externas são um fator em nosso processo de compra
91 %

A privacidade é parte integrante da nossa cultura
92 %

Visão fortemente favorável das leis de privacidade

A legislação em matéria de privacidade continua a ser muito bem-vinda em todo o mundo. Estas leis desempenham um papel importante na garantia de que os governos e as organizações são responsáveis pela forma como tratam os dados pessoais, e mais de dois terços (128 de 194) dos países já possuem leis de privacidade. Embora cumprir estas leis muitas vezes envolva esforço e custo significativos (por exemplo, catalogar dados, manter registros de atividades de processamento, implementar controles - privacidade por projeto, responder aos pedidos dos usuários), as organizações reconhecem o impacto positivo. Dos entrevistados corporativos, 83% disseram que as leis de privacidade tiveram impacto positivo; 14% foram neutras; e apenas 3% indicaram que as leis tiveram um impacto negativo. Apesar da complexidade adicional provocada por mais legislação no ano passado, este resultado é ainda mais positivo do que no estudo feito no ano passado (onde os inquiridos foram 79% positivos, 7%

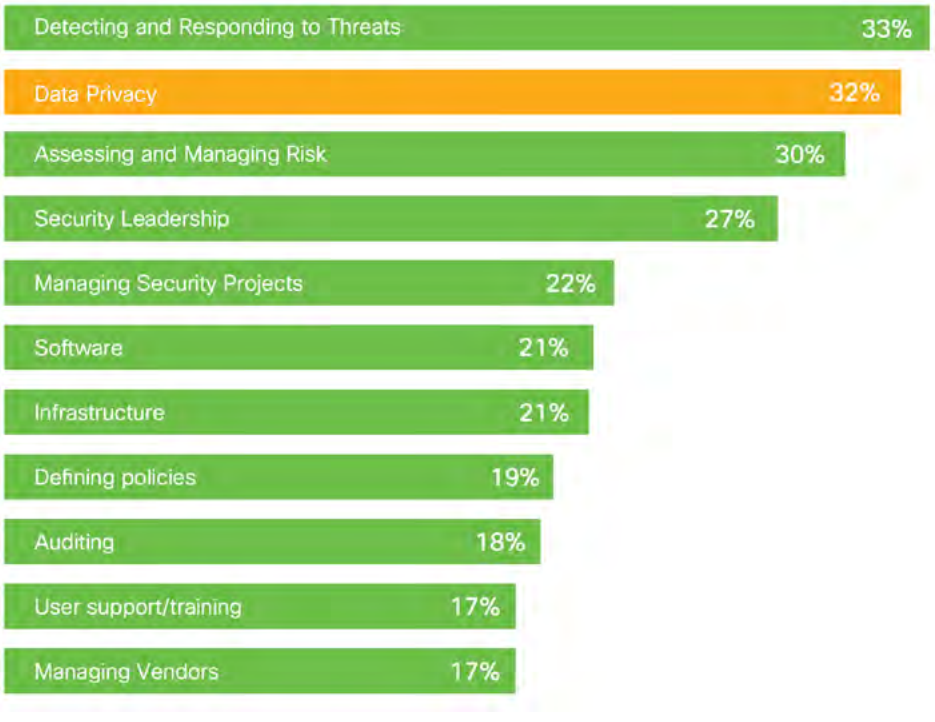
negativos). Também é preciso salientar a força que isto tem em todo o mundo. Em muitas geografias, incluindo as Filipinas, o México, a Tailândia, a Indonésia, a China e o Vietnã Vietnã, 90% ou mais dos inquiridos disseram que a regulamentação da privacidade teve um impacto positivo, e em cada geografia da nossa sondagem, pelo menos dois terços dos inquiridos afirmaram o mesmo. Veja a Figura 2. Como discutido em nossos relatórios anteriores, tanto os consumidores quanto as organizações esperam e valorizam um forte papel governamental na proteção da privacidade. Os regulamentos podem proporcionar padrões de atendimento mais consistentes, maior clareza sobre os direitos e recursos dos proprietários de dados e orientações sobre quais atividades de processamento de dados são permitidas e aquelas que são proibidas.

A grande maioria está informando as métricas de privacidade a seu Conselho de Administração

Uma indicação importante da relevanância da privacidade para uma organização é o uso de métricas, especialmente quando elas observadas pelas gerência executiva e o corpo diretivo. Entre as organizações ouvidas para aa pesquisa deste ano, 94% relatam reportar uma ou mais métricas relacionadas à privacidade Conselho de Administração. Enquanto alguns relatam até 10 métricas de privacidade, a maioria diz ter algo entre 1 e 3, com uma média geral de 2,6. As métricas mais informadas incluem os resultados da auditoria do programa de privacidade (34%), as violações de dados pessoais (33%) e os resultados das avaliações de impacto na privacidade (32%).

A privacidade é uma área central dentre as responsabilidades dos profissionais de cibersegurança

As habilidades de privacidade se tornaram cada vez mais críticas, especialmente entre aqueles que são diretamente responsáveis pela manutenção da segurança dos dados. Os profissionais de segurança que completaram nossa pesquisa foram convidados a definir as suas três principais áreas de responsabilidade. "Privacidade e governança de dados" foi selecionado por 32% destes entrevistados, o que o coloca em segundo lugar depois de "Detectar e responder a ameaças" e logo à frente de "Avaliação e gestão de riscos". Consulte a Figura 4. A privacidade dos dados também se tornou uma competência central aos



equipamentos de segurança digital, e a integração das capacidades de privacidade pode ajudar a evitar que pessoas sem autorização para acessar os dados os manuseiem de forma inadequada.

Curiosamente, várias geografias da Ásia-Pacífico apresentaram percentual elevado dos inquiridos em que a privacidade foi identificada como uma área de responsabilidade, ou seja, a Indonésia (45%), o Vietnã (43%), a Índia (43%) e a Malásia (42%). Os números mais baixos foram observados no Chile (19%), na França (22%), Colômbia (23%) e no Reino Unido (24%). Veja a Figura 5. As diferenças podem refletir uma maior integração entre segurança e privacidade em muitos países da Ásia-Pacífico. Também pode ser devido a organizações em países com regimes de privacidade mais antigos atribuirem responsabilidades de privacidade a áreas diferentes de cibersegurança, mas será necessária mais investigação sobre este assunto.

2. Investimento e benefícios em matéria de privacidade

À medida em que a privacidade se integra às prioridades organizacionais, o investimento continua aumentando. O orçamento médio em privacidade aumentou 13%, de US$ 2,4 milhões no ano passado para US$ 2,7 milhões este ano. O gasto de organizações menores de 50 a 249 empregados aumentou de US$1,1 milhões para US$1,7 milhões, e aquelas com 250 a 499 empregados aumentaram de US$1,6 milhões a US$2,1 milhões. Enquanto isso, as maiores organizações (mais de 10.000 funcionários) viram uma ligeira diminuição nos gastos de US$ 3,7 milhões para US$ 3,5 milhões este ano, após um forte aumento no ano passado. Veja a Figura 6. Em pesquisas futuras, vamos explorar de onde vem o crescimento dos gastos, seja o número de empregados, a tecnologia ou o aconselhamento externo.

O valor comercial associado a estes investimentos continua a ser elevado. De todos os entrevistados, 90% disseram que consideram a privacidade um imperativo empresarial. Mais especificamente, perguntamos aos entrevistados sobre os benefícios potenciais em 6 áreas: reduzir os atrasos nas vendas, mitigar as perdas por vazamentos de dados, permitir a inovação, alcançar a eficiência operacional, criar confiança com os clientes e tornar a sua empresa mais atraente. Para cada uma destas seis áreas, mais de 60% dos inquiridos sentiram que estavam a obter benefícios significativos ou muito significativos, e esta medida foi amplamente consistente nos últimos dois anos. Ver a figura 7.

Os entrevistados também foram convidados a estimar o valor financeiro dos benefícios de seus investimentos em privacidade, e a estimativa média aumentou 3%, de US$ 2,9 milhões no ano passado para US$ 3,0 milhões este ano. Curiosamente, as organizações menores viram os maiores aumentos percentuais este ano. Aqueles com 50-249 empregados aumentaram de US$ 1,1 milhões para US$ 2,0 milhões, e aqueles com 250-499 empregados aumentaram de US$ 1,9 milhões para US$ 2,5 milhões. Os lucros em organizações com 1000-9999 empregados se mantiveram constantes em US$ 3,4 milhões e nas maiores organizações com mais de 10.000 empregados, eles caíram ligeiramente de US$ 4,0 milhões para $3,8 milhões.

O ROI diminui ligeiramente, mas se mantém forte

De uma perspectiva de retorno sobre o investimento, a organização média estimou os lucros em 1,8 vezes a despesa, que é inferior a 1,9 da pesquisa do ano passado. Pensamos que isto se deve às necessidades contínuas de resposta à pandemia, à adaptação à nova legislação, à incerteza sobre as transferências internacionais de dados e ao aumento dos requisitos para a localização de dados (ver abaixo). No entanto, a maioria das organizações continua a obter um retorno muito atrativo dos investimentos em privacidade. 32% das organizações obtêm lucros de pelo menos o dobro do que gastam, e apenas 19% estimam que não atinge o ponto de equilíbrio dos seus investimentos em privacidade.

Rendimentos mais altos para organizações mais maduras e onde a privacidade se integra com a segurança

Também é interessante observar as correlações entre o desempenho e outros fatores como a maturidade da privacidade. Os entrevistados que sentiram que o seu programa de privacidade estava abaixo de seus pares recebiam um retorno menor do que aqueles que sentiam que estavam do mesmo modo ou à frente de seus pares. Em particular, os menos maduros tinham uma rentabilidade média de 1,53, em comparação com uma rentabilidade média de 1,97 dos mais maduros. Isto demonstra ainda mais o valor do investimento na privacidade, já que as organizações mais maduras também obtêm os maiores lucros. Ver a figura 10.

Outra correlação relevante foi entre o desempenho da privacidade e ela como responsabilidade central das atividades dos profissionais de segurança. As organizações onde o entrevistado identificou a privacidade como uma responsabilidade tiveram um desempenho médio de quase 2x em comparação com 1,71x naquelas em que o entrevistado não identificou a privacidade. Este resultado sugere que há um valor comercial em ter privacidade e segurança trabalhando de mãos dadas.

3. Ética dos dados e tomada de decisões automatizada

A inteligência artificial (IA) e a tomada de decisões automatizada impõem desafios específicos às organizações e aos consumidores no que diz respeito à utilização de dados pessoais. Noventa e dois por cento dos entrevistados reconhecem que sua organização tem a responsabilidade de usar os dados apenas de forma ética. E quase a mesma quantidade (87%) acredita que já tem processos implementados para garantir que decisões automatizadas se realize de acordo com as expectativas do cliente. Os consumidores não concordam. Com base nos resultados da Pesquisa de Privacidade do Consumidor da Cisco 2021, quase metade (46%) dos consumidores sentem que não podem proteger adequadamente seus dados, e a principal razão é que eles não entendem exatamente o que as organizações coletam e fazem com as suas informações. Ver a figura 11.

Os consumidores valorizam a transparência quando se trata da forma como os seus dados são utilizados, e a tomada de decisões com AI pode ser particularmente difícil de explicar. Com efeito, 56% dos inquiridos manifestaram preocupação quanto à forma como as empresas utilizam atualmente a IA. Além disso, quando perguntada sobre a utilização de dados pessoais em vários casos típicos de utilização de IA (por exemplo, selecção de um representante de vendas, fixação de preços, determinação da solvência), uma percentagem elevada, que varia entre 37% a 55%, disse que confia menos numa empresa que utiliza IA para tomada de decisões. Consulte a Figura 12. As organizações devem fazer mais para garantir que os clientes compreendam como seus dados são utilizados e para gerar confiança. Este será provavelmente um desafio importante no que diz respeito às decisões baseadas em IA.

4. Localização dos dados

Quanto mais governos e as organizações continuam a exigir proteções e compromissos para os dados transferidos para fora de suas fronteiras nacionais, mais eles estão implementando requisitos de localização de dados. Em uma nova área da pesquisa deste ano, 92% dos entrevistados disse-

ram que isto se tornou um assunto importante para suas organizações, e a mesma porcentagem disse que acredita ser necessário para ajudar a proteger os dados pessoais. Mas tem um preço. Oitenta e oito por cento disse que os requisitos de localização estão adicionando um custo significativo a sua operação.

Embora este requisito seja muitas vezes impulsionado por leis e atitudes nacionais, não houve uma variação substancial entre os entrevistados em diferentes geografias. A percentagem de inquiridos- que disse que a localização de dados estava adicionando custos a sua operação esteve entre 77% e 94% em todas as geografias.

5. Opções organizacionais em matéria de privacidade

Nos exercícios de avaliação comparativa, os profissionais da privacidade estão particularmente interessados em compreender onde se encontra a função de privacidade dentro de outras organizações e onde poderia ser melhor encaixar-se. Entre os entrevistados, não parecia haver um modelo dominante. A privacidade foi mais frequentemente colocada em TI (37% dos entrevistados), seguida de Segurança, Conformidade, Legal e Operações. Ver a figura 15.

Quanto à área em que poderia se encaixar melhor, o retorno médio mais alto ocorre em organizações nas quais a Privacidade está em Segurança, com um retorno de 1,91. As localizações em TI tiveram uma rentabilidade média de 1,87 e aquelas em que privacidade é parte das atribuições de Legal 1,77.

Do ponto de vista da maturidade da privacidade, era mais provável (43%) para aqueles em que a Privacidade está localizada em Segurança afirmarem que estavam à frente da concorrência, em comparação com aqueles em que a Privacidade está localizada em TI (37%), Legal (37%), Compliance ou Operações. Consulte a Figura 17. Estas correlações sugerem novamente que existe um valor comercial significativo a partir de uma integração mais estreita entre privacidade e segurança.

Recomendações

A privacidade continua a se integrar às prioridades organizacionais, e as conclusões desta investigação apontam para recomendações específicas sobre como demonstrar confiança e maximizar os benefícios dos investimentos em privacidade, incluindo:

1. Continue a desenvolver capacidades de privacidade em toda a sua organização, especialmente entre os profissionais de segurança e de TI e aqueles que estão diretamente envolvidos com processamento e protecção de dados pessoais.

2. Seja transparente sobre a forma como os produtos e serviços oferecidos pela sua organização utilizam dados pessoais. Os clientes querem saber, e ter certeza, que os seus dados não estão sendo abusados ou utilizados da forma como não esperam, conhecem ou compreendem.

3. Proceder com cuidado e consideração ao utilizar dados pessoais no IA e tomar decisões automatizadas que afetem materialmente os clientes. Conceber e construir com um quadro ético, estabelecer a governança e a supervisão do programa de IA e proporcionar transparência sobre quando e como está utilizando a tomada automatizada de decisões , são todos os passos positivos que as organizações podem tomar.

4. Investir na privacidade: vale a pena!

A Cisco manterá o monitoramento destas tendências e problemas e compartilhará suas descobertas. Para informações adicionais sobre a investigação de privacidade da Cisco, entre em contato com Robert Waitman, diretor de pesquisa e economia de privacidade da Cisco, rwaitman@cisco.com
Acesse o estudo completo com as figuras e o apêndice. aquí.


CISCO
SECURE