Proteção de dados e LGPD

Sua opinião é muito importante!

Sua opinião é muito importante para o Distrito. Por isso, queremos saber quais foram as suas impressões, críticas e sugestões sobre este relatório. Além disso, gostaríamos de saber quais outros estudos você gostaria que o Distrito Dataminer realizasse.

Quer falar com a gente? É só encaminhar um e-mail para: inside@distrito.me

Sumário

Para navegar pelos capítulos deste estudo, **clique nos botões na margem superior**. A qualquer momento, **clique no logo do Distrito no canto inferior direito para voltar a esta página.**

Metodologia

As startups delineadas no report foram selecionadas a partir de um trabalho minucioso de pesquisa e consulta ao banco de dados de startups proprietário do Distrito. Também foram realizadas consultas a bancos abertos e informações públicas do governo.

As startups foram examinadas individualmente para verificar adequação ao tema do report e aos critérios de seleção estabelecidos. São eles:

- **Ter a inovação no centro do negócio, seja na base tecnológica, no modelo de negócios ou na proposta de valor;**
- **Estar em atividade no momento da realização do estudo, medida pelo status do site e atividade em redes sociais;**
- **Desempenhar atividade diretamente relacionada ao setor estudado;**
- **Ter nacionalidade brasileira e operar atualmente no Brasil.**

O trabalho de definição das categorias foi baseado em análise da literatura relevante e das classificações utilizadas amplamente no mercado, no Brasil e no mundo.

A definição da categoria a que pertence cada startup foi feita por nossa equipe, e, quando uma startup opera em mais de uma categoria, a situamos na que interpretamos como sua atividade principal ou de maior visibilidade.

Também temos uma preocupação em incluir somente aquilo que consideramos startups—e, por mais que nosso critério para defini-las seja bastante amplo, excluímos alguns tipos de negócio que, embora muitas vezes se autodenominam startups, acabam fugindo do conceito. Isso inclui empresas que têm como característica principal serem:

- **Software Houses (desenvolvimento de software sob demanda);**
- **Consultorias;**
- **Agências de marketing, publicidade e design.**

Enfatizamos aqui que os números expostos podem sofrer alterações conforme a evolução da acurácia das informações e maior capacidade de interação com as próprias startups ao longo do tempo.

Entrevistados

Henrique Vaz
CEO
Clean Cloud

Aline
CEO
Privacy tools

Claúdio
DPO
ANP/CNPD

Introdução

Introdução

No Inside Cybertech #3, focamos em trazer alguns dos principais pontos sobre a Lei Geral de Proteção de Dados (LGPD), que vem impulsionando o setor de Cibersegurança. O Brasil agora possui uma legislação séria e robusta sobre esse tema, que deve auxiliar ainda mais um desenvolvimento tecnológico sustentável e ético para com os dados de colaboradores, consumidores e investidores.

A LGPD também iniciou um movimento que destaca a importância de investimento das empresas no setor, principalmente em um momento da economia digital em que dados se tornaram um dos ativos mais valiosos dentro das organizações.

Além de atualizar o ecossistema das Cybertechs, destacamos duas soluções que receberam aporte dentro da nossa base de startups de cybersecurity, trazendo entrevistas exclusivas com empreendedores experts do tema e buscando entender como as empresas de inovação são afetadas pela nova legislação. Ademais, comparamos o status brasileiro frente ao cenário internacional dentro de proteção e privacidade dados, buscando startups referência no exterior.

Por fim, nosso relatório busca faz apostas em tendências para o setor, com o intuito de entender qual o caminho as empresas de inovação irão seguir nos próximos anos.

Agradecemos o apoio e o patrocínio da Cisco na confecção do report, que pretende alimentar cada vez mais conteúdos sobre cibersegurança, tema que se torna cada vez mais relevante dentro das corporações.

Boa leitura!

Ecossistemas Cybertechs

Highlights

205
Startups

13
Categorias

6.358
Funcionários empregados

40
Startups com investimento recebido

US$ 388M
Investimento recebido desde 2013

US$ 282M
Investimento recebido nos últimos 2 anos

11
M&A's desde 2012

RADAR: CYBERTECHS

DISTRITO

Identity Access Management

DAITAN
acert
AIKNOW
akiyama
Assine Online
autentique
AutoSeg
BeCloudx
BRy Tecnologia
CH tecnologia
Chico
Computer ID
contraktor
CRED DEFENSE
D4S
GO! FIVE
Formalizar e-signature
FULLFace
w3lcome
griaule big data biometrics
GrupoCloud
GRYFO
hq
contract
ID ESSENTIALS
idwall
inloco
INOVACODE
JURIDOC
PONTO marcação móvel
Let's Work
.ai
mavie
MEERKAT
MULTIFACE BIOMETRIA
NATOSAFE BORN TO BE UNIQUE
nexti
nTokens
payface
qriar
QualiSign
SHIELDER
SimpleID IDENTIDADE CONFIRMADA!
VSOFT
SVA TECH
T-SHIELD
acesso digital
unike
UNISEC Segurança, tecnologia e conforto

Network _ Infrastructure Security

CONNECT
ISH
lumiun CLOUD MANAGED NETWORK
munic SECURITY
ProFUSION
StartLink
TI Safe
Virti

Web Security

apura
AuditSafe
CromiWAF cyber defense
KRYLSEC
SITE BLINDADO
Gatefy
XLabs ON SECURITY
XLabs security
<unxpose>
UPX TECHNOLOGIES

Cloud Security

ADTsys
baxtru | cloud backup
BrasilCloud Nuvem Corporativa
DDMX
nuvic cloud solutions
RedeHost
skalena

Application Security

Berghem
BugHunt
CONVISO
OGASEC

RADAR: CYBERTECHS

DISTRITO

Data protection

a2f · ADDERE SOLUTIONS · beAnalytic · CIAware · CLAVIS segurança da informação · Privacy tools · DADOS LEGAIS · dogma · ethquo ETHICAL QUOTIENT · GLOBAL DATA BANK · guardSI Cybersecurity · ID ESSENTIALS · Intelivix · leadcomm trusted digital security · LOGS360 · MODULO · NETTIME SISTEMAS · CleanCloud · PRIVALLY · riskex · [SAFE WAY] · senhasegura · SENSR. · Simply. · ST3TAILOR

Fraud Transaction Security

akaer · B2e Group · bankSe · bigdatacorp. · BLOCO1 · BrScan · COMBATE A FRAUDE · CQuantt · datarisk.io · EXATO DIGITAL BETA · deepen · HUPDATA · inlocomedia · infodatos · konduto · legiti · MaChiron · MOST · Neoway · NeuralMind · NeuroBanco · NEXTCODE · REFINARIA DE DADOS · Owli · TRANSFERO SWISS AG · certo · VIVALISTO · ZAIG

Security Consulting and Services

ANDRADESOTO · BLAZE INFORMATION SECURITY · CECyber · Collision INTELLIGENCE LABS · CROMISOFT · Deep.bbl · DESEC · ESTUARIO.TI · HACK3R_RANGERS · IBLISS DIGITAL SECURITY · InfoSafe · SOLVIMM · nova8 Cybersecurity · OPTRA SECURITY · PHISHX · REDBELT · RUSTCON · STRONG SECURITY · TEMPEST · Unbroken Cyber Security

IoT Security

GAVB · LATOS · Ochain · POLSEC · PREVISIOWN · ROBBIOT · TrackerThings

GRC

ECOIT SEGURANÇA DIGITAL · GAT InfoSec

Mobile Security

BluePex.

Security Operations Incident Response

AXUR · gocache next-gen CDN

LGPD e proteção de dados

Panorama Nacional

Proteção de dados: debate inicial

Quando em 2018 foi revelado pelo The Guardian e pelo New York Times que a empresa Cambridge Analytica tinha obtido dados ilegalmente de 50 milhões de perfis de usuários do Facebook, o debate de proteção de dados se tornou ponto focal nos Estados Unidos e ligou um alerta em nações que ainda não tinham prestado atenção no assunto. O caso remete à utilização de dados dos perfis para direcionar propagandas com o intuito de influenciar em campanhas eleitorais e processos de consulta da população como o Brexit, sendo as informações coletadas por um aplicativo chamado *thisisyourdigitallife*.

O aplicativo conseguiu coletar uma série de informações que eram armazenados pelo Facebook, que não tinha uma política de segurança adequada com a grande quantidade de dados que eram obtidos. Entretanto, sabe-se que o debate sobre proteção de dados é bastante antigo, sendo a primeira lei sobre o tema registrada na Alemanha na década de 70. No mesmo ano nações como França, Noruega, Suécia e Áustria também implementaram regulações.

Em 2016, a GDPR (atual regulação de dados na união européia) teve sua primeira publicação, e foi utilizada como inspiração da Lei Geral de Proteção de Dados, regulação brasileira que marca um avanço do país extremamente importante no tema. Destaca-se que no Brasil algumas regulações no tema já existiam como alguns pontos na constituição, mas a parte vital da regulamentação veio com o marco Civil da internet em 2013.

É essencial destacar que o debate com proteção de dados foi muito acentuado na era digital, principalmente com a popularização das redes sociais. O Brasil conta com mais de 130 milhões de usuários de internet, que disponibilizam seus dados abertamente em diversas situações.

Por aqui, privacidade de dados é um tema que ganha cada vez mais relevância, como apontado em um levantamento da Febraban em julho de 2021, que capta algumas da principais percepções das pessoas sobre o tema. Levantamos aqui os pontos de maior importância:

- **86% dos entrevistados afirmam ter medo de ser vítima de fraudes ou de violações de seus dados pessoais;**
- **75% dos entrevistados afirmam ter medo do que as organizações que coletam dados fazem com essas informações;**
- **83% dos entrevistados afirmam ter interesse em acompanhar notícias a respeito de privacidade de dados;**

LGPD e proteção de dados no Brasil

A Lei 13.709, de 14 de agosto de 2018, mais conhecida como Lei Geral de Proteção de Dados (LGPD), foi baseada na lei vigente na União Européia (GDPR) e visa regulamentar a proteção de dados no Brasil. A LGPD teve um grande impacto no meio empresarial por exigir uma série de requisitos das corporações no que se refere a proteção e tratamento de dados, e contém, previstas em lei, multas e sanções relevantes para corporações que não estejam em conformidade, podendo chegar até R$ 50 milhões.

Abrange todo o território nacional, a lei conta com mais de 60 artigos, e o segundo deles tange um ponto fundamental: aumentar a proteção à privacidade e à autodeterminação informativa sem inviabilizar o desenvolvimento tecnológico e social. Ou seja, embora a LGPD gere custos adicionais às empresas, esses gastos são necessários para a continuidade de um mercado inovador que vem sendo observado no Brasil, mas que ao mesmo tempo respeite requisitos básicos de segurança e tratamento de informações.

É essencial destacar que a LGPD é de fato uma demanda da sociedade. No observatório da Febraban, foi apontado que 62% dos entrevistados acreditam que o número de golpes e fraudes vai diminuir com as leis de proteção em vigor (sendo a principal a LGPD).

Todas as Violações da LGPD podem ser observadas no link

Como a LGPD beneficia o mercado de cibersegurança no Brasil?

De todo o orçamento das corporações para Tecnologia e Informação, apenas 4% é destinado para cibersegurança, no entanto, essa realidade já está mudando com a LGPD em vigor. As empresas naturalmente precisam se adequar às novas leis para não sofrer sanções descritas pela Autoridade Nacional de Proteção de Dados (ANPD). Além disso, o constante crescimento de ataques cibernéticos de diferentes esferas ligam um alerta necessário para todas as empresas de não só estarem de acordo com a lei, mas também garantir que de fato estejam em um ambiente seguro.

Cibersegurança está se tornando mais do que simples políticas de segurança, uma vez que o setor está se tornando parte essencial da estratégia por fazer parte transformação digital de qualquer empreendimento. Nos artigos 46 e 52 da lei, são destacados as exigências que as empresas devem ter para prevenir acidentes de segurança da informação, o que naturalmente aumenta os investimentos no setor e impacta positivamente soluções de cyber em todo o Brasil.

Destacar a importância dos protocolos de segurança das informação é um passo fundamental da LGPD, que está mudando todos os dias a mentalidade das companhias, e , [pr consequência, cada vez mais investem em formas formas de proteção. Ataques de hackers, spams, vírus, malware, tentativas de phishing e e-mails corrompidos se tornaram parte do dia a dia nas empresas, e a legislação entra como mais um enforce da responsabilidade que as corporações devem ter.

Nesse contexto de maior investimento em cibersegurança e preocupação com a LGPD, surgem algumas figuras de colaboradores importantes dentro das corporações, como o Chief Security Officer (CSO) e o Data Protection Officer (DPO). A figura do DPO vem sendo cada vez mais demandada desde que a LGPD foi implantada, por ser um profissional especializado em proteção de dados que monitora a empresa para garantir que as regras de compliance sejam cumpridas, além de intermediar as relações do titular dos dados com a organização e, no pior dos casos, cooperar com as autoridades com qualquer assunto relacionado a proteção de dados.

Dessa forma, a LGPD beneficia o mercado de cibersegurança em diversos aspectos, e espera-se que cada vez mais soluções robustas com grandes possibilidades de atrair a atenção dos investidores apareçam dentro do mercado brasileiro, que está em processo de consolidação.

Segurança e conformidade com a LGPD na Nuvem

Henrique Vaz
CEO
Clean Cloud

A CleanCloud se apresenta como uma empresa de produto, auxiliando outras companhias na conformidade com a LGPD para Nuvem. Qual a importância da solução de vocês para o mercado?
A LGPD tem três grandes pilares:

1) Pilar legal: parte de contratos, documentos, etc.

2) Processamento de dados: fazer todo o mapeamento, onde será o dado e treinamento do time.

3) Tecnologia.

A CleanCloud atua neste pilar, especificamente em computação em nuvem. Trabalhamos com base no modelo de responsabilidade compartilhada, que é a limitação do dever do provedor de nuvem. Em termos práticos, o provedor de nuvem, AWS, Azure, Google Cloud ou qualquer outro, é o único responsável pela camada de infraestrutura — por exemplo, as certificações do data center.

Enquanto isso, o usuário é o responsável pela configuração — o que usa da nuvem, os serviços e políticas, como senhas, acessos e encriptação. Desta forma, ele tem menos atribuições do que se tivesse um data center privado, mas precisa se atentar à segurança e conformidade de sua nuvem para estar de acordo com as regulações, como a LGPD.

O CleanCloud Score verifica se as configurações da nuvem estão em conformidade com algumas das principais regulações do mercado, com destaque para LGPD, com mais de 300 verificações para as nuvens AWS, Azure e Google Cloud. O detalhamento do produto vai ao ponto de trazer o artigo da LGPD que cada verificação faz referência, sempre usando benchmarks como o CIS ou ISO 27001 como referência.

O artigo 2º da LGPD, da legislação presente, visa aumentar a proteção à privacidade, à autodeterminação informativa sem inviabilizar o desenvolvimento tecnológico e social. Qual é o impacto que pode ser observado da LGPD nas empresas de inovação? Existem prós e contras?
Sem dúvida existem os prós e contras.

A lei brasileira adquiriu uma maturidade de dados muito grande nos últimos anos, como, por exemplo, a atenção que hoje se dá a um vazamento de informações. Então, vejo a LGPD como uma legislação que atende a uma demanda social: →

→ uma regulação para que as empresas tratem os dados de forma adequada. A maior vantagem é que, com os parâmetros do tratamento de informações adequados bem definidos, podemos separar os casos de vazamento causados por imprudência falta de treinamento, investimento em produtos e pessoas — e fatalidade, pois mesmo que com todos controles a companhia pode sofrer um ataque cibernético e ter um vazamento.

Por outro lado, há a questão do custo que a LGPD acarreta, especialmente para pequenas empresas. Existem algumas propostas de lei que estabelecem um faturamento mínimo para a aplicação da LGPD de forma completa, em linha com o CCPA — a legislação de proteção de dados do Estado da Califórnia, EUA. Vejo essa proposta com bons olhos, mas vale destacar que, pelo menos na CCPA, esse benefício não se aplica a startups que usam os dados para a geração da maior parte de sua receita.

Conhecendo o mercado e os clientes que você já tem, a LGPD mudou a visão das empresas sobre cibersegurança? Existe uma preocupação maior sobre o tema após a entrada em vigor?
Vale destacar que a LGPD não é uma lei de cibersegurança — em nenhum momento fala de segurança cibernética, mas sim de tratamento adequado das informações digitais. Dito isso, é inegável que em 2020 nossas vidas ficaram muito mais virtuais, e, consequentemente, passamos a ter dados sensíveis também on-line.

Isso é um dos motivos do aumento do número de ataques cibernéticos. Aliado ao aumento da importância dos dados que comentei anteriormente, vejo como movimentos paralelos, mas não necessariamente relacionados. Em outras palavras: ainda que não houvesse uma LGPD as empresas estariam mais preocupadas com a cibersegurança.

Como vocês avaliam o tema de proteção de dados no Brasil comparado a outros países? Quão importante a LGPD foi e está sendo na mudança de concepção de dados no país?
O Europeu é, de modo geral, mais preocupado com o tema, inclusive as primeiras regulações nesse sentido são da década de 1950. Por outro lado, vejo o brasileiro mais preocupado com o assunto que o norte-americano, que ainda está engatinhando com algumas legislações estaduais e, sem dúvida, muito à frente do asiático.

A promulgação da LGPD foi muito importante para trazer esse tema para a população e empresas, para que hoje tenha esse alcance. Há três anos seria muito raro ver um usuário pedir que uma empresa deletasse seus dados. Hoje se tornou algo comum e a expectativa é que a lei evolua conforme a sociedade se torne mais consciente quanto a este tema.

As startups nascentes vão se adequar mais rápido? Como você vê isso?
Tem o lado positivo e negativo. O lado bom: é muito mais fácil criar políticas e controles no início do que com centenas de funcionários e milhões em faturamento. →

Segurança e conformidade com a LGPD na Nuvem

Henrique Vaz
CEO
Clean Cloud

→Por outro lado, isso gera um custo adicional. Uma startup que está nascendo terá que contratar um bom advogado para definir política de dados, processos relacionados ao uso de informações, softwares para tratar dados de forma adequada, entre outros. Mas, o mercado exige isso. Então é importante abraçar a legislação e usar como uma vantagem competitiva, pois os incumbentes terão ainda mais gastos e dificuldades para se adequar.

Segurança e conformidade com a LGPD na Nuvem

Henrique Vaz
CEO
Clean Cloud

O que minha empresa precisa fazer para se adequar à LGPD?

Além da boa prática para mitigar ataques cibernéticos, as empresas precisam se adequar à nova legislação para evitar multas elevadas. Embora haja empresas especializadas na adequação à LGPD e melhora nas políticas de privacidade e proteção de dados, existem boas práticas que devem ser seguidas em qualquer organização para facilitar o processo de adequação.

Em um primeiro momento, os principais passos dentro da organização são:

- **Conhecimento dos seus próprios dados**
- **Avaliação e gerenciamento das informações**
- **Proteção (Cibersegurança)**
- **Documentação do progresso.**

Dentro de da etapa de segurança, é essencial que sejam adotadas medidas técnicas e administrativas na organização para garantir de fato a proteção e privacidade das informações que são sensíveis. É importante destacar que todas as medidas adotadas pela empresa precisam ser devidamente testadas e avaliadas em processos rígidos de segurança, para de fato não sofrer sanções dos órgãos responsáveis por garantir o cumprimento da legislação.

Nesse cenário, existem ferramentas no mercado que auxiliam as empresas a estarem adequadas a LGPD e na garantia da segurança dos dados das organizações. Além de empresas que prestam um serviço completo de segurança em diferentes camadas, como o sistema Talos da CISCO, ferramentas de segurança fornecidas por startups como a Clean Cloud e a Privacy Tools já estão se destacando no mercado por suprirem essas necessidades.

É claro que existe um custo necessário para se adequar à nova legislação, entretanto, é essencial que as empresas compreendam que em um cenário que ataques cibernéticos e vazamentos de dados são cada vez mais frequentes, é necessário para a segurança de todos um investimento em ferramentas de cibersegurança.

Privacy tools

Categoria
Data Protection

Local
Porto Alegre, Rio Grande do Sul

Ano de Fundação
2019

Público
B2B

Investimento Recebido
US$ 200 k

Investidores
OBr.Global

Sobre

A Privacy Tools é uma plataforma que visa apoiar a conformidade regulatória em proteção de dados das organizações com forte dependência de dados pessoais.

Plataformas do tipo são ferramentas poderosas quando se fala em privacidade de dados, pois conseguem fazer uma gestão efetiva de possíveis incidentes, armazenam em bancos os principais dados da empresa, mapeiam a operação da empresa e são necessárias em diversas frentes. Ademais, a possibilidade de gerenciar os dados da corporação garantindo sua proteção em uma única plataforma é uma demanda cada vez mais presente no mercado, frente a necessidade das corporações se adequarem a regulação.

A Privacy Tools se diferencia dentro do mercado com uma produção extensa de conteúdo em privacidade de dados, Lei Geral de Proteção de dados e políticas de compliance, em formatos de texto, blog, podcasts e e-books.

Com preços a partir de R$ 239,00/mês , já contam com grandes clientes como Pague Menos e Rede D'Or.

CleanCloud

Categoria
Data Protection

Local
São Paulo, São Paulo

Ano de Fundação
2016

Público
B2B

Investimento Recebido
US$ 1,8 M

Investidores
GV Angels, Anjos do Brasil, Bossa Nova Investimentos

Sobre

A CleanCloud é uma plataforma de gerenciamento de infraestrutura em nuvem pública, que destaca a conformidade com a LGPD para nuvem AWS, Azure e Google Cloud.

A plataforma proporciona uma redução da superfície de ataque, garante uma visão Multi Cloud para CISO e DPO e se apresenta como única no segmento com verificação para LGPD e Banco Central. A CleanCloud oferece, além de seu produto de compliance e conformidade, um outro de otimização de custos com dashboards e relatórios, sendo uma solução completa em diversas frentes.

A CleanCloud já conta com grandes investidores estratégicos que auxiliam na expansão da operação e com grandes clientes que utlizam do sofware, como Cogna Educação e Sicredi.

Em um mundo em que diversas empresas já nascem na nuvem e precisam se adequar às legislações de proteção de dados, soluções como a CleanCloud estão ganhando uma notoriedade conhecida no mercado.

Como plataformas especializadas ajudam na adequação à LGPD?

Aline DeParis
CEO
Privacy Tools

A Privacy Tools se apresenta como uma plataforma de gerenciamento de privacidade e adequação das empresas à LGPD . Qual a importância da solução de vocês para o mercado?
Com todo este movimento global em busca de mais privacidade, uma plataforma de gerenciamento da privacidade se torna fundamental e porque não dizer, obrigatória para a grande maioria dos negócios. É praticamente impossível imaginar uma empresa que trate dados pessoais ficar na mão de planilhas e procedimentos manuais para automação dos direitos dos titulares. Por exemplo, imagine que você receba 100 pedidos de acesso a dados que estão espalhados em dezenas de bancos de dados, fornecedores e plataformas - como automatizar esta busca, classificação e entrega? Ou imagine que a autoridade nacional de proteção de dados exija a entrega de um relatório de impacto de um determinado processo da sua empresa, como fazer esta entrega rapidamente, com evidências e controles? São para necessidades como esta, além de vários outros recursos, que plataformas de gestão da proteção de dados e privacidade se tornam fundamentais para os negócios.

A Privacy Tools produz uma série de conteúdos para o mercado relacionados a LGPD e proteção de dados. Como isso fortalece a marca de vocês e quais são os principais pontos que você gostaria de destacar nos conteúdos que vocês produzem?
Quando começamos um negócio com foco em privacidade para um mercado tão nascente nesta disciplina como é o mercado brasileiro a gente compreendeu que parte do sucesso do negócio se dá pela educação e disseminação de uma cultura de privacidade e importância da proteção de dados nas empresas e também para as pessoas de modo geral. Ao mesmo tempo que a lei traz oportunidades e obrigações para as empresas, também traz direitos e oportunidades para as pessoas e isso precisa ser disseminado. A gente vislumbra a LGPD tendo a mesma popularidade que é o código de defesa do consumidor hoje, mas é uma construção coletiva que depende de muito apoio de todos os agentes envolvidos.

Nós criamos uma websérie em 2021 chamada "Privacidade acima de tudo" onde buscamos especialistas em suas áreas para trazer a discussão da LGPD em uma linguagem de fácil acesso e também passamos a criar ebooks, podcasts, cards em redes sociais populares, campanhas patrocinadas, tudo em pró de uma disseminação massiva do assunto. →

Também apoiamos financeiramente ou com permuta e conteúdo portais de conteúdo como o PrivacyTech.com.br e eventos da área de outras iniciativas e associações que possuem o mesmo propósito. Entendemos que o branding é importante, mas no nosso mercado não é o principal objetivo, pois não adianta nada termos uma marca forte se as empresas não deram credibilidade para a aplicação da lei e se as pessoas não conhecerem seus direitos, seria como reinar no deserto.

Aline, você já conta com uma trajetória na área de tecnologia. Como você avalia o crescimento da área de cibersegurança dentro do investimento em T.I nas empresas depois da implantação da LGPD no país? Você acredita que isso terá impactos positivos no curto e no longo prazo?
Cibersegurança é uma disciplina ampla que conta com muitas subdisciplinas como criptografia, privacidade, riscos e várias outras.

Analisando o mercado de privacidade, só em 2020 mais de US 1.2 bilhão de dólares foram gastos em todo o mundo com tecnologia para privacidade e a previsão é chegar até U$ 18 bilhões de dólares até 2028, números da Globe Newswire. A LGPD possui um papel fundamental nos orçamentos de Ti e segurança das empresas e a tendência é ampliar muito em 2022, mas não podemos também deixar de dar "créditos" aos eventos recentes de vazamentos de dados e sequestro de dados que empresas populares como Lojas Renner e JBS que causaram um verdadeiro pânico no mercado e fazendo com que concorrentes sintam diretamente que o problema está mais perto do que parece e que ninguém está totalmente protegido. Acho que uma coisa leva a outra pois a adequação com a LGPD não é apenas ajustes em contratos e adequação de websites mas sim uma mudança cultural em processos e métodos de trabalho que passam essencialmente, em sua maior parte, por tecnologia e segurança da informação.

Quais são os pontos que você gostaria de destacar, dentro da LGPD, que são benéficos para os consumidores de serviços? De fato podemos nos sentir mais seguros?
A LGPD brinda os titulares ou consumidores com novos direitos que eles podem, desde agosto de 2020, exercer perante a qualquer empresa com a qual a pessoa teve uma relação de troca de dados. Por exemplo, se você foi funcionário de uma empresa, se você comprou um produto, se você forneceu alguma autorização fornecendo dados pessoais, se você preencheu algum formulário de cadastro, todas as ações realizadas pelas empresas acabaram fazendo um tratamento e/ou compartilhamento dos dados com sistemas, terceiros, parceiros e demais cadeias de distribuição para cada negócio em cada contexto. Você como pessoa, dona dos seus dados, pode exercer seu direito sobre estes dados, eles não são de propriedade das empresas, eles estão temporariamente com as empresas para que elas cumpram com o propósito do tratamento de dados original, respeitando a LGPD e demais normas. Isso representa um benefício enorme para as pessoas que antes entregavam seus dados de maneira indiscriminada e não tinham nenhum direito sobre o que cada empresa poderia fazer com estes dados.

Como plataformas especializadas ajudam na adequação à LGPD?

Aline DeParis
CEO
Privacy Tools

Como você avalia o cenário brasileiro com a LGPD, frente à outras regulações de dados que existem no mundo, como a GDPR na Europa e a CCPA na Califórnia?
A LGPD segue uma teoria expansionista de privacidade e proteção de dados, com foco maior no opt-in do titular em respeito à metodologias como Privacy by design e seus princípios. Existe mais semelhança da LGPD com a GDPR do que se comparado com as leis setoriais dos EUA como COPPA ou mesmo leis regionais como a CCPA. Contudo, vejo que a atuação da ANPD vem sendo primordial para elucidar diversos pontos da lei que foram muito criticados como o tratamento diferente para pequenas empresas, meios para notificar um incidente ou mesmo critérios para transferência internacional e tratamento de dados de menores. Vejo a LGPD como bem avançada e esperamos que no futuro a comissão europeia coloque o Brasil como adequado para proteção de dados junto com os outros 13 países fora do bloco europeu.

A Privacy Tools já recebeu aportes relevantes que reafirmam a qualidade da plataforma frente a um mercado que necessita de adequação em proteção de dados. Como vocês avaliam a trajetória de vocês até aqui e quais são os próximos passos?
A Privacy Tools nasceu como uma startup em um mercado ainda nascente e correndo risco da lei nem mesmo ser aprovada. Mas acreditávamos que o Brasil não iria ficar fora desta corrida global pela privacidade, então investimos muito no desenvolvimento da melhor e mais completa plataforma brasileira para gerenciamento da privacidade que já vem sendo utilizada por +400 empresas sendo a maior parte delas grandes corporações de capital aberto. Para poder entregar esta qualidade de software e serviços buscamos investimentos em 2020 e realizamos um processo de aceleração com uma das principais aceleradoras brasileiras que aplica metodologia do Vale do Silício no mercado nacional visando uma expansão internacional.

A Obr.global nos ajudou como aceleradora também para a captação de investimento anjo que fizemos no último ano e neste momento estamos estruturando o negócio para o próximo tiro de crescimento no final deste ano pois entendemos que 2022 o mercado estará muito aquecido não apenas no mercado de empresas privadas mas também no governo.

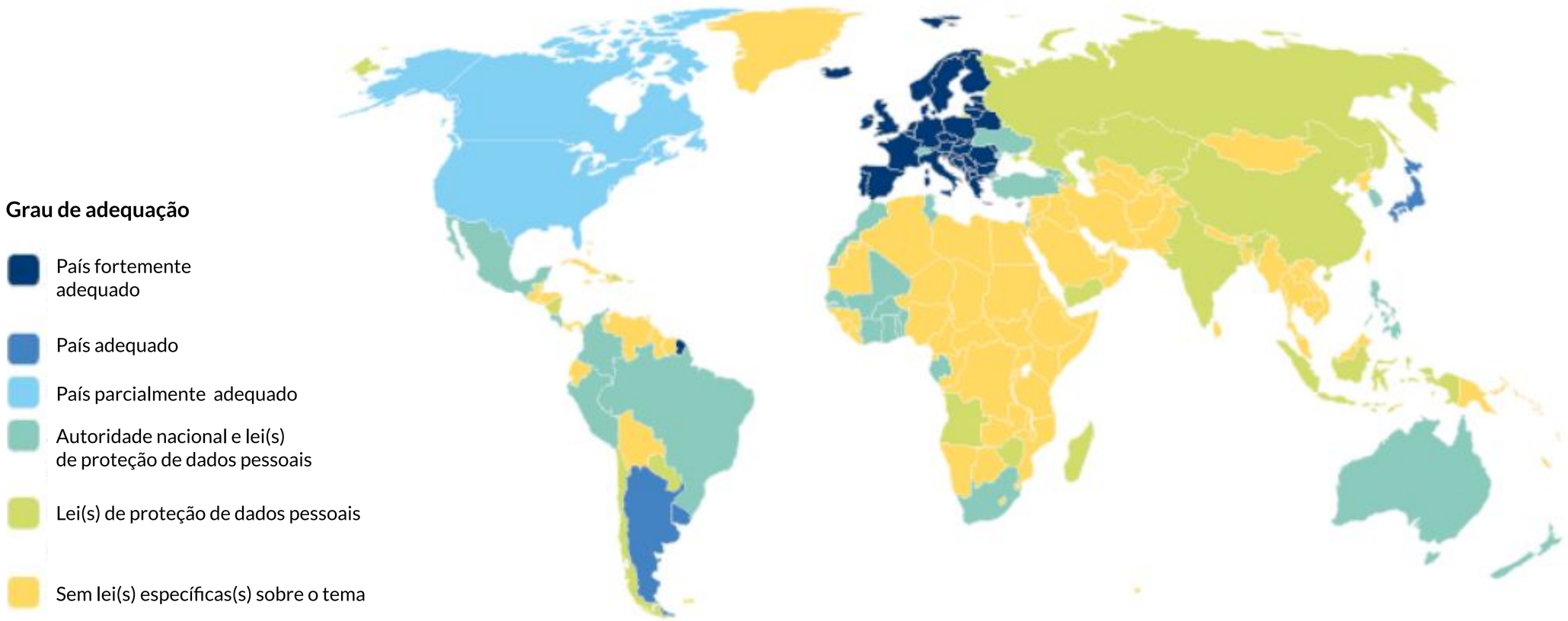
Como plataformas especializadas ajudam na adequação à LGPD?

Aline DeParis
CEO
Privacy Tools

Proteção de dados no mundo

Panorama Internacional

Adequação de proteção de dados ao redor do mundo



©CNIL/FRANÇA

Regulação de dados ao redor do mundo

No cenário internacional, vemos diferentes cenários em desenvolvimento, uns mais maduros do que outros. Os países europeus são pioneiros na questão de proteção de dados, e alguns países como a Alemanha, por exemplo, já possuíam leis de proteção de dados muito antes do assunto virar pauta internacional. Já outros países dos continentes africano, asiático e da oceania não possuem ainda leis específicas para a proteção de dados e segurança virtual dos usuários, mas sim uma série de leis fragmentadas relativas ao direito do consumidor e segurança pessoal. Os países das Américas se encontram em um meio termo, em uma fase de transição onde alguns países como Argentina, Uruguai, Brasil e Estados Unidos já possuem encaminhamentos para políticas mais maduras de proteção, enquanto outros, como Bolívia e Venezuela, não possuem alinhamento claro sobre o tema.

A União Européia foi pioneira em criar a *General Data Protection Regulation* (GDPR) em 2016, sendo base de exemplo para as legislações posteriores de outros locais como o *California Consumer Privacy Act* (CCPA), regulamentação do estado da Califórnia, nos Estados Unidos, a Lei Geral de Proteção de Dados (LGPD), aqui no Brasil, e o *Protection of Personal Information Act* (POPIA), na África do Sul.

É importante salientar que, apesar de todas terem um cunho favorável à proteção de dados dos usuários, cada lei tem suas peculiaridades, que envolvem desde o tempo de resposta para incidentes, até a obrigatoriedade da existência de uma figura central dentro das empresas, que será responsabilizada caso ocorra algum caso de vazamento de dados, ou mesmo a abrangência regional por onde a lei pode ser aplicada. Essas peculiaridades acabam levando em conta a cultura de cada país e as adaptações necessárias para a efetividade da regulamentação.

Confira a seguir um comparativo entre a LGPD e as duas regulamentações mais avançadas, GDPR e CCPA.

Comparativo entre a LGPD, GDPR e CCPA

Lei reguladora	Data de criação	Data de vigência das sanções	Abrangência	Tempo máximo de resposta ao dono do dado	Data Protection Officer (DPO)	Prazo para comunicar violação de dados	Valor da penalidade em caso de violação
Lei geral de proteção de dados (LGPD)	Agosto de 2018	Agosto de 2021	Geral para pessoas localizadas no Brasil, ou de origem brasileira, pelo mundo	Até no máximo 15 dias	Obrigatoriedade de pessoa dedicada e indicada especificamente para a função	Em um prazo razoável (tendo sido regulado pela ANPD o prazo de até 2 dias úteis do conhecimento do incidente)	2% do faturamento anual da empresa, limitado a R$ 50 milhões
General Data Protection Regulation (GDPR)	Abril de 2016	Maio de 2018	Global	Até um mês	Obrigatório para órgãos governamentais e/ou públicos e companhias que processam dados pessoais em larga escala	Em até 72h	Máximo de 4% do faturamento anual, ou US$ 20 milhões. O que for maior
California Consumer Privacy Act (CCPA)	Junho de 2018	Janeiro de 2020	Na Califórnia e globalmente para moradores dos Estados Unidos	Dentro de uma janela de 45 dias, podendo ser estendido para até 90 dias	Não é exigido	Não há um prazo geral, mas o Estado da Califórnia exige respostas a demandas de consumidores em um prazo máximo de 72 horas	US$ 7,500 por violação individual e reivindicações pessoais de $750 por incidente

OneTrust
PRIVACY, SECURITY & GOVERNANCE

Categoria
Data Protection

Local
Atlanta, Geórgia, Estados Unidos

Ano de Fundação
2016

Público
B2B

Investimento Recebido
US$ 920M

Investidores
Insight Partners, Coatue, TCV, SoftBank Vision Fund 2 e Franklin Templeton

Sobre

Mais de 10.000 clientes, incluindo metade da Fortune Global 500, usam o OneTrust, implementando fluxos de trabalho ágeis centrados em privacidade, segurança, governança de dados, GRC, risco de terceiros, ética e conformidade e programas ESG.

A plataforma OneTrust é apoiada por 150 patentes e alimentada por seu mecanismo de automação robótica através de inteligência artificial. Suas soluções incluem softwares de gerenciamento de privacidade, inteligência de dados, intercâmbio de risco de terceiros, gerenciamento de risco integrado, conformidade e ética e o software de consentimento e gerenciamento de preferências.

ENSIGHTEN

Categoria
Data Protection

Local
Menlo Park, Califórnia, Estados Unidos

Ano de Fundação
2009

Público
B2B

Investimento Recebido
US$ 108,5M

Investidores
Volition Capital, Insight Partners, Mack Capital

Sobre

A Ensighten é uma das líderes globais em governança e segurança de dados de websites, permitindo privacidade e proteção de dados de última geração.

Com a tecnologia da startup, as organizações podem avaliar seus riscos de segurança e privacidade e impedir o vazamento ou roubo não autorizado de dados, bem como cumprir com o CCPA, GDPR e outros regulamentos de privacidade de dados.

TrustArc

Categoria
Data Protection

Local
São Francisco, Califórnia, Estados Unidos

Ano de Fundação
1997

Público
B2B

Investimento Recebido
US$ 107M

Investidores
Baseline Ventures, Bregal Sagemount

Sobre

A TrustArc é utilizada principalmente por líderes em privacidade que buscam simplificar e automatizar seus programas de privacidade.

Essa experiência de plataforma é fornecida por meio de sua combinação de estruturas de privacidade, percepções, inteligência, conhecimento e operações. A TrustArc fornece inteligência de privacidade contínua, juntamente com uma plataforma totalmente automatizada para gerenciamento de privacidade de ponta a ponta.

VERY GOOD SECURITY

Categoria
Data Protection

Local
São Francisco, Califórnia, Estados Unidos

Ano de Fundação
2015

Público
B2B

Investimento Recebido
US$ 104,9M

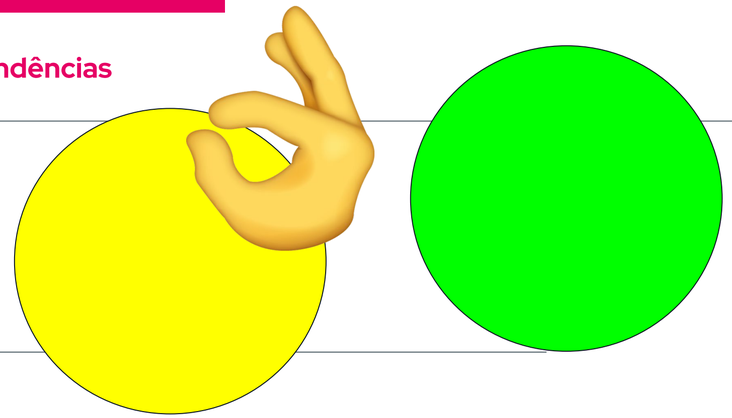
Investidores
Andreessen Horowitz, Goldman Sachs, Visa Ventures, Vertex Ventures.

Sobre

Fornecendo segurança essencial e infraestrutura de conformidade, a Very Good Security (VGS) permite que startups e empresas se concentrem em seus negócios principais, em vez de conformidade e sobrecarga regulamentar.

Através da integração da plataforma, a VGS fornece vários métodos para coletar dados confidenciais com segurança, evitando que os clientes sequer os tenham em seus sistemas, ao mesmo tempo em que aceleram as conformidades como PCI, SOC 2, GDPR, entre outras normas regulatórias.

Tendências



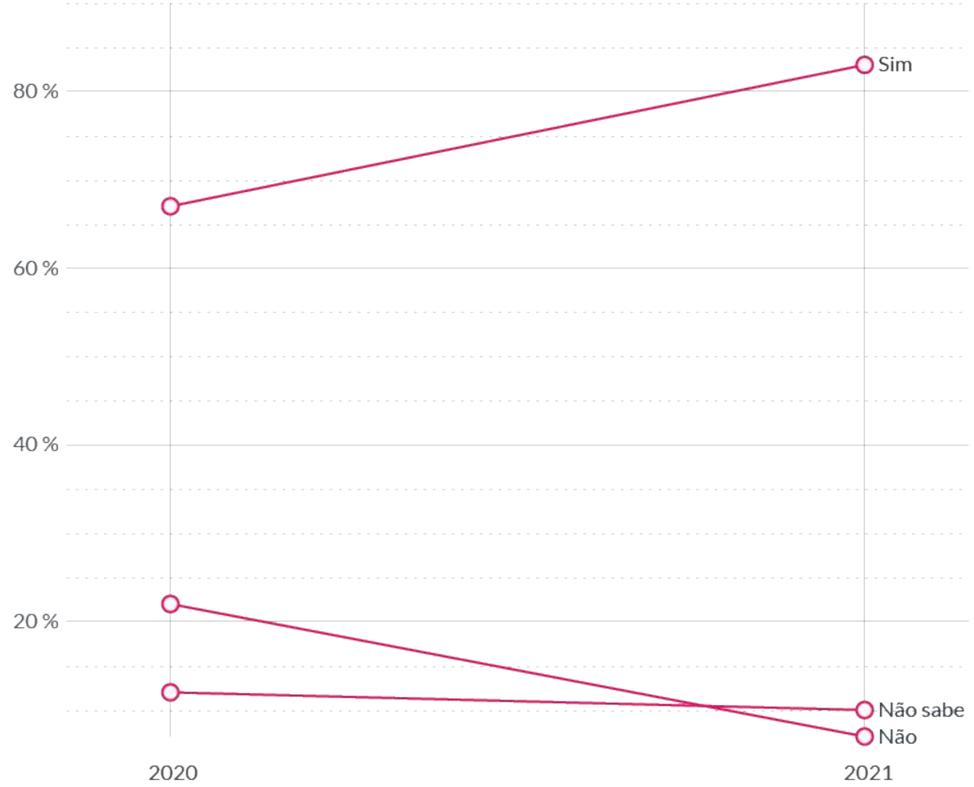
Privacidade de dados será cada vez mais importante dentro das empresas

Como foi abordado anteriormente, cada vez mais empresas estão dedicando recursos importantes para cuidar das áreas de privacidade e segurança, seja por regulações cada vez mais presentes dentro de diferentes nações ou pelo medo de ataques cibernéticos cada vez mais crescentes. Fato é que existente uma tendência crescente de investimento direcionado à cibersegurança e proteção de informações sensíveis.

Apesar dos avanços, um levantamento realizado pela TrustARC mostra que ainda há muitos objetivos que ainda precisam ser alcançados. Em 2021, dentre diversas entrevistadas, foi constatado que 86% das empresas concordam que políticas de privacidade são essenciais nas estratégias de longo prazo do negócio, um aumento de 3 pontos percentuais em relação à 2021. Entretanto, 73% dos entrevistados concordam que ainda há muito a ser feito para garantir políticas efetivas de privacidade de dados.

Embora haja uma clareza de que o tema deve ser tratado com mais seriedade, as transformações dentro das empresas precisam ser imediatas, pois cada vez mais existem ameaças cibernéticas que podem causar danos incalculáveis às organizações. Privacidade e Segurança, embora sejam conceitos diferentes, caminham juntos em busca de um objetivo maior.

Empresas que possuem um escritório dedicado a privacidade de dados



Presente e futuro em privacidade de dados

Claúdio Rocha
DPO
ANP/CNPD

Destaque: Para essa entrevista, Cláudio Rocha deixou claro que fala apenas em seu próprio nome e não do CNPD.

Como membro do Conselho Nacional de Proteção de Dados e da Privacidade (CNPD), o que você espera nos próximos em relação à proteção de dados?

Espero um aumento significativo da cultura da privacidade e proteção de dados no país. E acredito que o CNPD deverá ter um papel relevante nesse ponto. Pois, além de propor diretrizes estratégicas e fornecer subsídios para a Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a própria ANPD, compete ao Conselho realizar debates e audiências públicas sobre a proteção de dados e também disseminar conhecimento sobre o tema à população.

Podemos dizer que a proteção de dados veio para ficar?
Sem dúvida nenhuma. Não tem "ctrl+z". Cada vez mais o tema vai se tornando vital, tanto para o titular de dados, que está descobrindo que tem direitos sobre seus próprios dados pessoais, quanto para as organizações, que são custodiantes desses dados, e devem fazer o que for possível para protegê-los, além de serem transparentes com o titular sobre a finalidade do tratamento de seus dados.

Quando você fala que as organizações devem fazer o que for possível para proteger os dados pessoais, isso se reflete em um aumento na segurança da informação?
Perfeitamente. Não existe privacidade sem segurança da informação.

A chegada da pandemia e o repentino teletrabalho escancararam para todos as nossas deficiências em TI e segurança da informação. Notícias recentes sobre megavazamentos de dados pessoais e ataques a bancos de dados de grandes organizações públicas e privadas só corroboram a importância de uma política de segurança da informação robusta e de uma capacitação contínua de todos os colaboradores.

O trabalho de casa também catalisou uma tendência: a utilização da nuvem para aplicações empresariais, intensificando a necessidade de segurança dos dados da mesma forma nesses ambientes.

Hoje usamos nuvem para tudo, seja ela pública, particular ou híbrida. E a acessamos de todo lugar, por inúmeros equipamentos e redes, e isso requer uma segurança maior, uma verificação de identidade e de permissões mais robustas. Talvez seja por isso que o conceito Zero Trust (never trust, always verify) começou a ser difundido mais rapidamente. →

Algum conselho para as organizações?
Preparem-se e capacitem seus colaboradores. Por lei, as organizações são responsáveis por adotar medidas de segurança, técnicas e administrativas, para proteger os dados pessoais dos titulares, inclusive por situações acidentais de destruição, perda, alteração, comunicação ou difusão.

Uma organização tem que se defender de inúmeros ataques todos os dias enquanto o atacante só precisa ser bem-sucedido uma única vez para causar um estrago grande. É uma batalha árdua. E também não adianta ter os melhores sistemas e ferramentas, se uma das maiores vulnerabilidades está entre o monitor e a cadeira. Kevin Mitnick que o diga!

Presente e futuro em privacidade de dados

Claúdio Rocha
DPO
ANP/CNPD

Cybertechs

Glossário de categorias

Categorias

NETWORK & INFRASTRUCTURE SECURITY
Companhias que apliquem processos de proteção da infraestrutura de rede, instalando medidas preventivas para negar acesso não autorizado, modificações, exclusões e roubo de recursos e dados. Essas medidas de segurança podem incluir controle de acesso, segurança de aplicativos , firewalls, redes virtuais privadas (VPN), análise comportamental, sistemas de prevenção de intrusão e segurança sem fio. Se relaciona com a camada física de transmissão e conexão. Também englobamos soluções de endpoint e messaging security nesta categoria.

WEB SECURITY
Medidas e protocolos de proteção que empresas utilizam para proteger suas organizações de cyber criminosos e ameaças que usam a web como canal. Se relaciona com a camada não física de segurança, o que engloba internet e segurança de sites.

APPLICATION SECURITY
Medidas de segurança que impedem roubo/sequestro de dados e códigos dentro de dentro de aplicativos e plataformas.

DATA PROTECTION
Data protection engloba empresas responsáveis pela proteção de informações sensíveis à empresa (Banco de Dados, Informações de Corporações) e enquadram às corporações na LGPD.

MOBILE SECURITY
Empresas que atuam com produtos e serviços voltados a garantir a segurança do device (dispositivo móvel), IoS, Android. Via de regra, são companhias que visam a proteção contra ameaças associadas à conexões wireless.

SECURITY OPERATIONS & INCIDENT RESPONSE
Empresas que desenvolvem soluções estruturadas para responder a vazamentos de dados ou ciberataques. A solução visa minimizar os impactos de ataques cibernéticos já realizados, possibilitando um controle da situação com o menor tempo e custo.

IOT SECURITY
Empresas que atuam com segurança relacionada a internet das coisas, aparelhos e networks que estão conectados entre si.

IDENTITY & ACCESS MANAGEMENT
Empresas que desenvolvem soluções que garantem a veracidade das informações e identidades de todas as partes envolvidas em um processo. Aqui se encontram empresas de Identidade as a Service, que capturam, armazenam e asseguram a veracidade do usuário, e companhias de assinatura digital, que trazem inovação e segurança para todo o ciclo de documentos.

Categorias

BLOCKCHAIN
Blockchain as a Service (BaaS) são empresas que possibilitam o desenvolvimento de produtos digitais com a tecnologia blockchain, instalando, hospedando e/ou mantendo redes desse tipo em nome de outras organizações.

FRAUD & TRANSACTION SECURITY
Empresas que aplicam tecnologias de análise de dados para gerar avaliações e insights sobre clientes, permitindo mapear riscos, analisar a conformidade com leis e regulamentações e se prevenir contra perdas, desvio, fraude e ataques cibernéticos.

CLOUD SECURITY
Cloud Secutiry refere-se às startups que atuam com políticas, tecnologias, aplicativos e outros mecanismos de controle utilizados para proteger IP virtualizado, dados, aplicativos, serviços e a infraestrutura associada de computação em nuvem.

SECURITY CONSULTING & SERVICES
Security Consulting and Services refere-se a startups que prestam serviços para testar ou aprimorar serviços de cibersegurança. Um exemplo aqui são empresas que atuam com simulações de ataques cibernéticos como forma de identificar possíveis falhas nos sistemas.

GOVERNANCE, RISK AND COMPLIANCE
Soluções GRC (Governança, Risco e Cokmpliance) são compostas por ferramentas que abrangem a gestão de riscos, governança corporativa e práticas de auditoria e controle, com o objetivo de garantir a conformidade com leis, regulamentos, frameworks e padrões de boas práticas.

Corporates members

APOIO

Cybertechs

Glossário de termos

Blockchain em diferentes setores

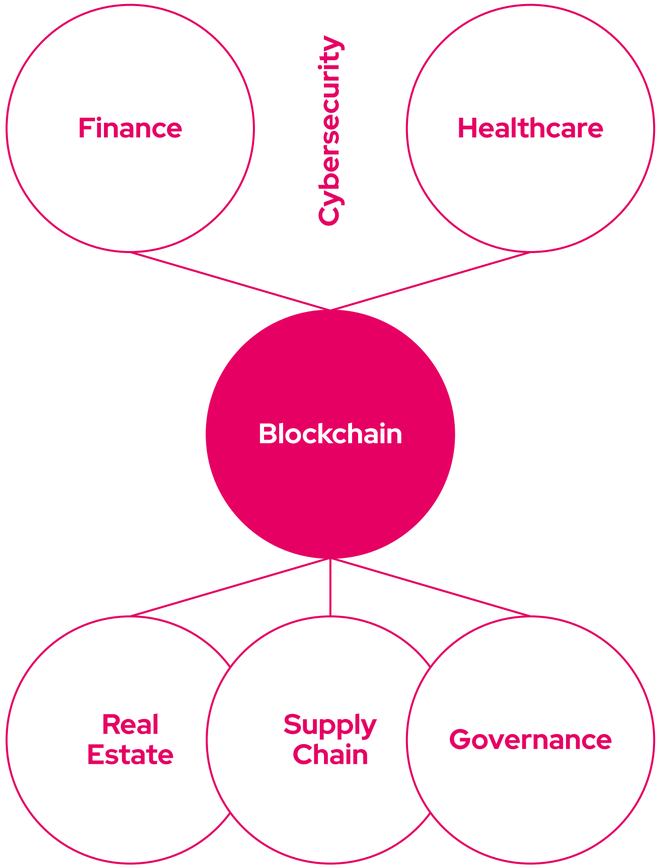
Finanças: No setor de finanças, o maior valor da tecnologia blockchain está na transparência das transações e da não adulteração dos dados transacionados. Armazenar tudo que é realizado na blockchain é mais transparente e seguro, se comparado às formas de tecnologia tradicional ou em papel. Grandes bancos já se utilizam da tecnologia para deixar seus dados mais seguros.

Saúde: O ataque a dados médicos tem sido uma preocupação crescente nos últimos anos, e organizações de saúde podem se beneficiar guardando essas informações dentro da blockchain. A BurstIQ é uma plataforma americana que auxilia empresas no setor de saúde a armazenar e proteger dados de diferentes departamentos e instituições em tempo real.

Setor imobiliário: Validação de propriedade e transferência e transferência de fundos podem ser solucionados utilizando da tecnologia blockchain, garantindo a veracidade e segurança das informações.

Supply chain: Gigantes presentes no mercado de abastecimento como Walmart e BMW se utilizam da blockchain para melhor a segurança de seus dados e a transparência da operação. A rastreabilidade dos produtos se destaca como principal solução da tecnologia.

Governança: A blockchain pode ser uma ferramenta poderosa nos processos de governança e compliance, melhorando a segurança e transparência das organizações. Confira melhor o tema no nosso Inside ESG #4, que explora as aplicações e as soluções da tecnologia voltadas para governança corporativa.



Glossário – Cybersecurity

Ameaça: Causa potencial de um incidente.

Ativo: Tudo aquilo que possui valor.

Ativo de Informação: Patrimônio intangível da corporação, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, mercadológico, de recursos humanos, legal natureza, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas a organização por parceiros, clientes, empregados e terceiros, em formato escrito, verbal, físico ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional da organização ou por infraestrutura externa, além dos documentos em suporte físico, ou mídia eletrônica transitados dentro e fora de sua estrutura física.

Confidencialidade: Propriedade dos ativos da informação da corporação, de não serem disponibilizados ou divulgados para indivíduos, processos ou entidades não autorizadas.

Controle: Medida de segurança adotada pela corporação para o tratamento de um risco específico.

Gestor da Informação: Usuário da informação que ocupe cargo específico, ao qual foi atribuída responsabilidade sob um ou mais ativos de informação criados, adquiridos, manipulados ou colocados sob a responsabilidade de sua área de atuação.

Incidente de segurança da informação: Um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações da corporação.

Integridade: Propriedade dos ativos da informação da corporação, de serem exatos e completos.

Risco de Segurança da Informação: Efeito da incerteza sobre os objetivos de segurança da informação da corporação.

Segurança da Informação: A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações da corporação.

Vulnerabilidade: Causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações da corporação.

Engenharia Social: Manipulação psicológica de pessoas para a execução de ações ou divulgar informações confidenciais.

Acha que faltou algum termo? Manda pra gente!

Principais riscos da Blockchain em Cybersecurity

Embora existam vantagens claras na utilização da tecnologia, é essencial destacar que existem riscos associados à implantação de soluções que utilizam blockchain dentro de cibersegurança.

DESAFIOS DE ESCALA

Redes de blockchain tem limites distintos, relacionados ao volume dos blocos e transações processadas por segundo, que podem impedir a escalabilidade de algumas soluções.

NECESSIDADE DE CHAVES PRIVADAS

Apesar de representar uma grande vantagem no âmbito da segurança e da autenticidade das informações, as longas sequências de números que dão origem às chaves privadas da blockchain, caso forem perdidas, não conseguem ser recuperadas. Dessa forma, é preciso ter muito cuidado com o armazenamento dessas chaves.

PROBLEMAS DE ADAPTABILIDADE

Apesar de tecnologias em blockchain puderem ser aplicadas em quase todos os modelos de negócio, muitas empresas enfrentam dificuldade na implantação. Soluções de Blockchain podem precisar substituir completamente os sistemas existentes para funcionar da melhor forma. Assim, antes de implantar soluções que utilizem esse tipo de tecnologia, é importante considerar todos os trâmites necessários.

CUSTOS DE IMPLANTAÇÃO

Uma rede blockchain precisa de um poder computacional substancial e necessita de uma grande quantidade de espaço para ser armazenada. Todos esses fatores podem aumentar os custos marginais da operação em comparação à outros sistemas de segurança.

GOVERNANÇA E REGULAÇÃO

As operações realizadas na blockchain não são necessariamente regularizadas ao redor do mundo, e algumas nações estão mais avançadas que outras. Entretanto, as regulações ameaçam mais soluções ligadas às criptomoedas, que são vistas como risco financeiro para alguns países, por não ter o estado como produtor e detentor do monopólio.

ESPECIALISTAS

Apesar do número crescente de soluções em blockchain no mercado, ainda existe uma falta de profissionais qualificados que consigam manter a rede funcionando da melhor forma. Desenvolvimento de soluções em blockchain requerem uma grande quantidade de habilidades, conhecimento em diferentes linguagens de programação e ferramentas.

Highlights

26
Startups

220
Funcionários empregados

3
Startups com investimento recebido

US$ 538 Mil
Investimento recebido desde 2016

Startups de Blockchain em Cybersecurity

Blockchain as a Service (BaaS) são empresas que possibilitam o desenvolvimento de produtos digitais com a tecnologia blockchain, instalando, hospedando e/ou mantendo redes de blockchain em nome de outras organizações.

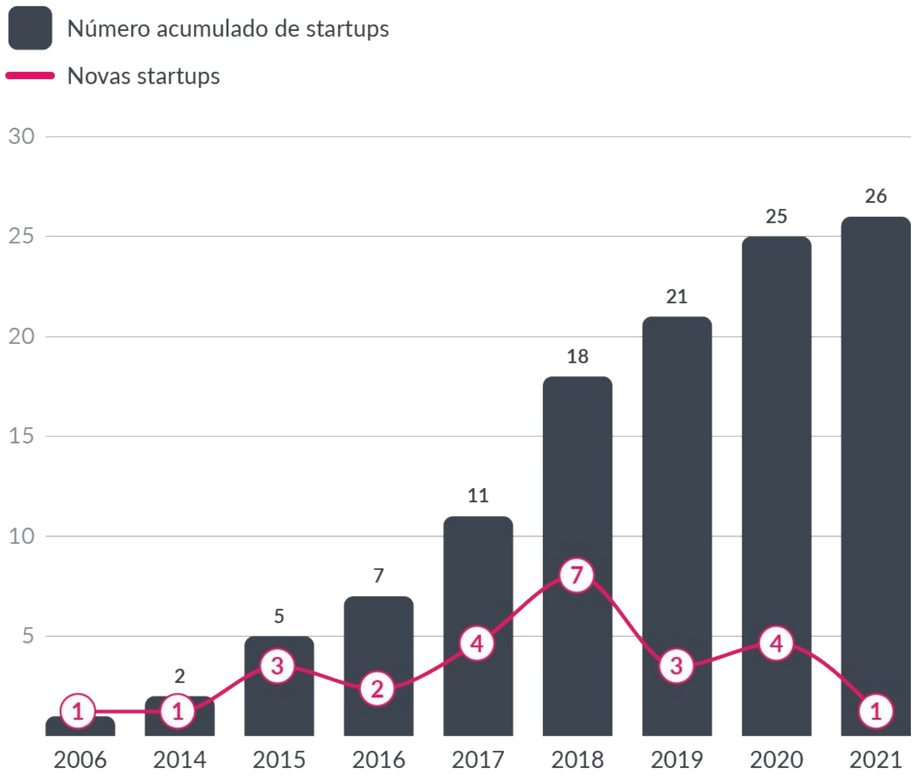
OriginalMy blockchain

Growth Tech

rhizom
IN AUTONOMY WE TRUST

Soluções de blockchain em cybersecurity

Ano de fundação startups



As soluções brasileiras de blockchain relacionadas a cybersecurity, tal como o restante do ecossistema, estão em desenvolvimento e em busca de se firmarem em um mercado que ainda não apresenta um grande número de empresas consolidadas. O segmento ainda está muito conectado com o mercado de criptoativos, oferecendo possibilidade de transações, compras e armazenagem, entretanto é esperado que mais soluções de blockchain que não estão associadas à sua origem apareçam com o passar dos anos, espelhando o mercado internacional.

Em um relatório publicado pelo Bradesco em parceria com a inovabra, dentre as startups que trabalham com blockchain no Brasil atualmente, 12,7% estão dentro do segmento de segurança digital. A categoria que mais se destaca é a de serviços financeiros, que compreende 49,7% das soluções.

GoLedger

Categoria Blockchain

Ano de Fundação 2017

Público B2B e B2G

Investimento Recebido XXX

Investidores XXX

Sobre

Com a missão de unificar e instanciar projetos compartilhados entre várias entidades ou instituições públicas, a GoLedger é pioneira no desenvolvimento de soluções em blockchains permissionados para governo. Situada na capital federal, a empresa é uma fabricante nacional de soluções focadas para atender os reguladores e tem grande vocação para atuação na administração pública e empresas privadas.

A empresa possui diversas soluções em blockchain, entre elas: Contratos inteligentes, Compartilhamento de dados e Orquestração de rede (GoFrabric), ID digital (GoBio), gestão de documentos e assinaturas digitais (GoProcess), Rastreamento de produtos (GoTrace), Portal de consentimentos LGPD (GoPrivacy) e Votação eletrônica (GoVote).

A startup tem ganhado destaque nas mídias por se posicionar como uma das empresas preparadas para implementar o voto eleitoral através de blockchain. A tecnologia foi incluída no programa de transformação digital do Governo Federal.

Já estabelecida no mercado, a GoLedger tem parceria com grandes provedores mundiais de Nuvem como AWS, IBM, Microsoft e Huawei, e já possuímos uma rede de canais e parceiros com escritórios nos estados de São Paulo, Rrio de Janeiro, Ceará, Paraná e Distrito Federal com empresas de grande porte como Capgemini e Golden Tecnologia.

Atualmente compõem o marketplace da ETICE sendo a única empresa privada capaz de realizar a venda de soluções, infraestrutura e serviços em blockchain através de Dispensa de Licitação.

OriginalMy blockchain

Categoria Blockchain

Ano de Fundação 2015

Público B2B e B2G

Investimento Recebido Não divulgado

Investidores 3xBit

Sobre

Iniciada em 2015 no Brasil, mas mudando sua sede para a Estônia em 2018, a OriginalMy Blockchain nasceu com o propósito de desburocratizar o mundo. A startup utiliza a tecnologia blockchain dentro de sua plataforma para fornecer serviços como: Coleta de evidências para processo judicial (PACWeb), Consentimento do usuário em relação a LGPD (OMyPass), Proteção de direitos autorais sobre arquivos digitais (PACDigital), assinatura eletrônica e certificação de documentos digitais (OMySign) e relatório de dados sobre possíveis parceiros e fornecedores (KYC).

Eles são uma das primeiras empresas no Brasil a fornecer soluções reais baseadas em blockchain e uma das únicas com parceria com cartório para oferecer a autenticação de documentos de forma 100% digital.

Em 2018 ganhou o prêmio de empresa mais inovadora, no CriptoAwards, e em 2020 a startup ganhou o prêmio de campeã mundial na categoria Privacy, Data Protection and Compliance, em cibersegurança, realizado em um dos eventos de investimento mais importantes do mundo, organizado pelo Ministério da economia dos Emirados Árabes Unidos.

Growth Tech

Categoria Blockchain

Ano de Fundação 2015

Público B2B e B2C

Investimento Recebido XXX

Investidores XXX

Sobre

A Growth Tech é uma startup que desenvolve soluções para automação inteligente e desintermediação de processos, através de Smart Contracts e da tecnologia Blockchain. Ela usa tecnologias disruptivas como pilar fundamental em seus projetos.

A startup é uma das primeiras a trazer soluções de problemas usando blockchain no Brasil. Possui produtos para assinatura eletrônica ou digital, com certificado digital (PropLedgers), gestão condominial inteligente (Digi), rede virtual de cartórios (Notary Ledgers), além de seus projetos em consultoria em blockchain.

A Growth Tech foi responsável pela primeira oficialização de união estável homoafetiva através de blockchain no Brasil, assim como o primeiro registro de nascimento com a tecnologia em território nacional.

Blockchain: uma nova forma de pensar em cybersecurity

Conforme exposto no Inside Cybertechs #1, o prejuízo causado globalmente em decorrência de ataques cibernéticos chegou em US$ 945 bilhões, beirando a marca de US$ 1 trilhão, com grandes sinais que esse número se torne cada vez maior. Esses ataques cibernéticos usualmente perpassam as barreiras tradicionais impostas por políticas internas de cybersecurity dentro das corporações, como autenticação de identidade dos usuários na rede, manutenção de senhas, criptografia e privacidade de dados.

Com a pandemia e o aumento do número de casos de *cyber attacks* dentro das empresas, principalmente causados por uma nova dinâmica de trabalho e desafios de segurança impostos pelo trabalho remoto, muitas corporações estão repensando os sistemas implantados para garantir menos vulnerabilidades no âmbito da segurança da informação. Nesse contexto, a blockchain aparece como uma possibilidade de maior segurança, principalmente pelo *ledger* distribuído que oferece, e também por ser um ambiente menos familiar para criminosos cibernéticos que elimina as vulnerabilidades menos óbvias de um sistema de segurança.

A blockchain possibilita uma criptografia melhor, pois consegue verificar a integridade e o pertencimento dos dados mais rapidamente e eliminar a necessidade de senhas — usualmente um dos links mais fracos dentro de um sistema de segurança, por ser de responsabilidade do usuário. Uma outra vantagem importante que a blockchain possui, justamente pela sua natureza de ser uma rede compartilhada, é a possibilidade de sempre estar vigiando à ameaças, anomalias e "organismos" não familiares sem a necessidade de um controle central. Basicamente o *ledger* distribuído consegue utilizar uma infraestrutura de chaves públicas para garantir uma comunicação segura, validar mudanças de configuração do sistema, autenticar dispositivos móveis e garantir de fato uma segurança e transparência em todas as partes do sistema. Ainda, a blockchain pode ser uma forma de prevenção de ataques DDoS (ataques de negação de serviço), um DNS (Domain name systemn) baseado em blockchain elimina o ponto único de falha no sistema que possibilita crimes cibernéticos acontecerem com mais facilidade.

Dessa forma, é natural que diversas organizações, de multinacionais até instituições governamentais, estejam procurando soluções em segurança da informação que se utilizem da tecnologia blockchain. Entretanto, é necessário salientar que a intersecção entre blockchain e cybersecurity está em constante desenvolvimento e aprimoramento. Soluções que envolvem identidades digitais, sistemas descentralizados de armazenamento de dados, contratos inteligentes e outras, nem sempre estão alinhadas com as necessidades reais e imediatas do mercado, por isso considera-se que há um espaço para encontrar aquelas que seriam ideais para a maior parte das organizações.

Pilares da blockchain em cybersecurity

CONFIDENCIALIDADE

As chaves dos integrantes da rede blockchain são o único link entre os dados presentes na rede e o próprio usuário, mas essas chaves são fáceis de serem deixadas anônimas. Algumas redes também utilizam "non-interactive zero-knowledge proofs", basicamente uma forma de limitar a interação entre os indivíduos, com o objetivo de maximizar a confidencialidade e o anonimato dos próprios. Como consequência, enquanto soluções em blockchain tem a traceabilidade como um dos seus principais ativos, o anonimato dos usuários é mantido.

INTEGRIDADE DOS DADOS

Redes de blockchain são compostas por blocos que utilizam criptografia baseada nas funções dos *hashs*, que são guardadas no *ledger*. Dessa forma, quando uma transação é realizada na blockchain, ela não pode ser deletada nem alterada. Quaisquer novas alterações serão gravadas em cima do que já foi processado, gerando uma nova informação. Dessa forma, as soluções em blockchain garantem a integridade de todos os dados, inalteráveis e gravados no livro razão.

DISPONIBILIDADE

Ter um grande número de nós (agrupamento de participantes que tem o mesmo interesse, para exempo, no caso do bitcoin seria a transferência de dinheiro) garante que a blockchain seja resiliente mesmo quando alguns não estão disponíveis. Como cada nó na network tem uma cópia do *ledger* distribuído, a informação correta permanece disponível para os usuários em caso da falha em um nó.

Vantagens da Blockchain em Cybersecurity

PROTEÇÃO E PROCESSAMENTO DE DADOS

Dados gravados na blockchain são imutáveis e qualquer mudança feita gravada e transparente, além de não removível. Dessa forma, dados guardados na blockchain são mais íntegros e seguros se comparados à outros métodos tradicionais.

TRANSFERÊNCIAS SEGURAS DE INFORMAÇÃO

A blockchain permite transações rápidas e seguros de dados ou produtos financeiros. Adendos como contratos inteligentes registrados na própria rede garantem que o negócio seja feito da forma mais transparente e efetiva possível.

ELIMINAÇÃO DE UM PONTO VULNERÁVEL

Redes blockchain que não precisam de senha para serem acessadas são descentralizadas e portanto, como já exposto, se tornam mais resilientes. O comprometimento de um único nó não afeta todo o resto da operação de segurança, isso significa que mesmo em caso de ataques DDoS, o sistema será operável normalmente, graças às várias cópias do ledger distribuído em cada um dos nós.

TRANSPARÊNCIA E RASTREABILIDADE DOS DADOS

Todas as transações na blockchain são digitalmente assinadas e com o horário gravado, logo qualquer informação é facilmente rastreável a qualquer momento

CONFIDENCIALIDADE DO USUÁRIO

A confidencialidade dos usuários da rede é extremamente alta devido à uma chave pública criptografada que autentica os usuários. Entretanto, algumas startups conseguem ir um passo além, desenvolvendo soluções que permitem a autenticação do usuário sem a utilização dessas chaves

AUMENTO DA CONFIANÇA

A principal vantagem da blockchain é o conjunto de todas as vantagens já citadas, que garante que os usuários e consumidores do produto se sintam seguros em utilizar soluções de blockchain

Blockchain reduz o risco de fator humano

Com empresas que geram grandes quantidades de dados todos os dias, o armazenamento deles de maneira centralizada sempre é um fator de vulnerabilidade que pode ser explorado por criminosos. Ademais, o número de dispositivos conectados à internet está projetado para chegar em 13,8 bilhões em 2021, que naturalmente são alvos de ataques de segurança da informação. É imprescindível que um protocolo uniforme de cibersegurança dentro das empresas seja consolidado. Entretanto, mesmo que eles existam, erros humanos geralmente são a principal porta de entrada para vazamento dados.

Dito isso, além de um protocolo estabilizado e medidas de conscientização constantes para manter a segurança da empresa, todas as medidas necessárias para reduzir o risco do fator humano precisam ser estabelecidas.

A natureza descentralizada da tecnologia blockchain provém os melhores padrões de transparência e integridade de dados, diminuindo abruptamente as chances de vazamentos de dados causados por erro humano. Dados na blockchain, como já foi exposto anteriormente, não podem ser adulterados, porque todas as informações são cruzadas entre os nós. No combate às ameaças cibernéticas que permeiam as empresas diariamente, a blockchain pode pode se aliar aos sistemas de defesa e agregar valor, criando um protocolo de segurança padrão, verificando todas as atividades que podem trazer riscos à corporação.

95%
Dos vazamentos de dados são causados por erros humanos

90%
Dos malwares são entregues e acessados via e-mail

34%
Das empresas demoram mais de uma semana para recuperar acesso aos dados invadidos

US$ 6 Trilhões
Deve ser o custo de crimes cibernéticos no fim de 2021

Em que casos a blockchain pode ser utilizada em cybersecurity?

Apesar de não ser impenetrável, a tecnologia blockchain evoluiu para ser uma das formas menos fraudulentas e mais seguras de transação dentro de uma rede. Dentro de cybersecurity, algumas utilidades se destacam:

IOT SECURITY

Observa-se um aumento da quantidade de ataques cibernéticos voltados para dispositivos de ponta, como roteadores e termostatos, que possibilitam uma porta de entrada para a rede toda. Nesse caso, a blockchain pode ser uma possibilidade de descentralizar a administração da rede, fazendo com que os dispositivos consigam ter uma segurança própria mais efetiva, sem depender de um controle central.

PROTEÇÃO CONTRA ATAQUES DDoS e DATA HACKING

Um ataque DDoS ocorre quando uma rede fica inutilizável após um ataque cibernético, geralmente criminosos pedem resgate em criptomoedas para permitir o acesso dos usuários novamente. A blockchain consegue diminuir esse tipo de ataque por descentralizar as entradas de Sistemas DNS (Domain Name System). Dessa forma, pontos únicos e vulneráveis são eliminados. Essas soluções de descentralização também são utilizadas em sistemas de armazenamento de dados, visto que grande parte desses sistemas também são explorados por hackers por terem um ponto de acesso vulnerável, e criminosos conseguem acesso à informações sensíveis que podem prejudicar de inúmeras formas uma corporação caso vazadas.

VERIFICAÇÃO DA INFRAESTRUTURA DE CIBERSEGURANÇA

As capacidades de verificação e autenticação que existem na tecnologia blockchain são capazes de auferir falhas de sistema, adulteração de dados e problemas simples de integridade da informação que potencializam sistemas de cybersecurity dentro das corporações. Todas as informações geradas em uma estrutura com o intermédio da blockchain tem uma garantia maior de assertividade.

PROTEÇÃO EM TRANSMISSÃO DE DADOS E MENSAGENS

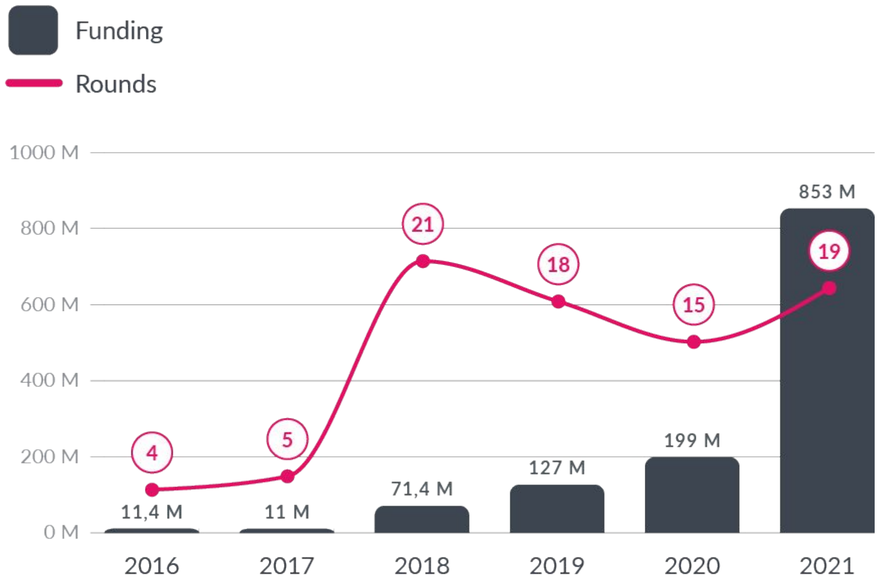
A blockchain consegue impedir acessos não autorizados a qualquer tipo de dado em trânsito, utilizando de uma criptografia própria da tecnologia. Destaca-se que um dos pontos de ataque mais visados por hackers no roubo ou adulteração de informações é enquanto existem dados em trânsito.

CHECAR A PROVENIÊNCIA DE UM SOFTWARE

A blockchain pode ser utilizada para avaliar a integridade de um software ou de qualquer download para prevenir possíveis invasões de ameaças externas. Quaisquer atualizações, instalações e consertos podem ter suas atividades verificadas com a tecnologia blockchain . É importante destacar que podem existir falhas, pois os *hashs* providos pela plataforma podem já estar comprometidos, mas a integridade do que é inserido no sistema é mais garantido quando se usa a blockchain.

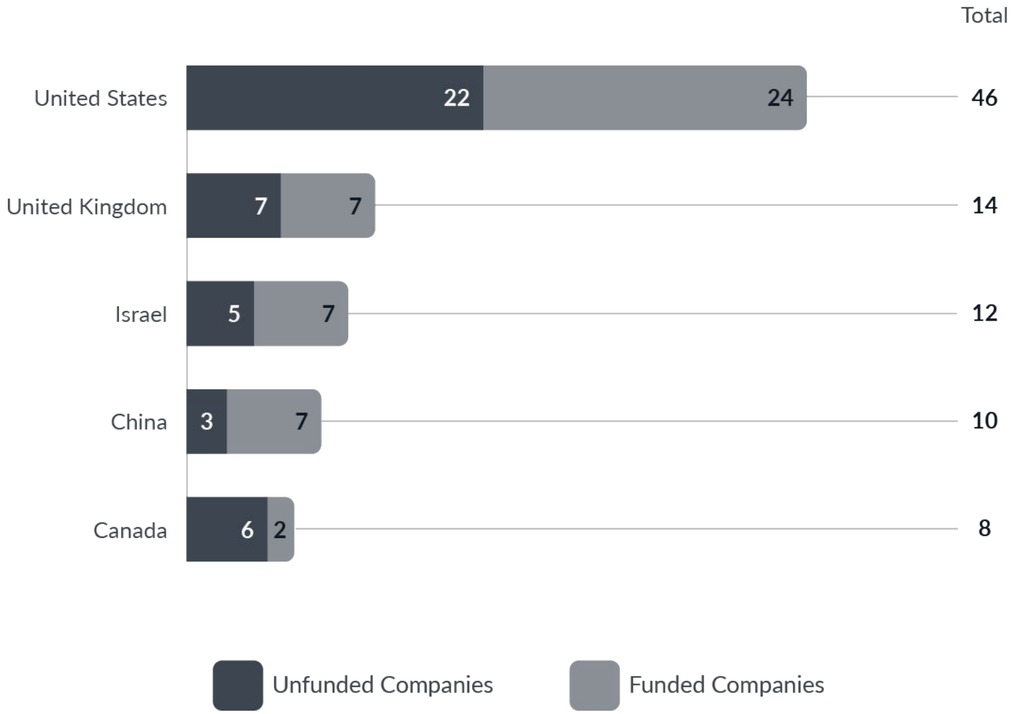
Soluções de blockchain em cybersecurity

Financiamento e número de rodadas ano a ano no mundo



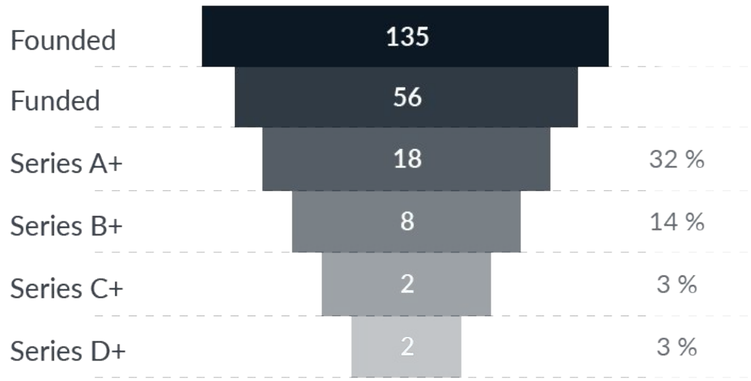
1,3 B
Total Funding

Países com mais soluções



Soluções de blockchain em cybersecurity

Empresas por estágio



Top Companies Mundo

Top Companies	Ano Fundação	País	Total Funding
Fireblocks	2018	Estados Unidos	489,0 M
Chainalysis	2014	Estados Unidos	367,0 M
StartkWare	2018	Israel	118,0 M
Elliptic	2014	Reino Unido	44,3 M
Casa	2016	Estados Unidos	10,0 M

Top 5 investidores internacionais

Blockchain 1.0

Criptomoedas

- Fundação das tecnologias blockchain.
- Redes blockchain para transação entre criptomoedas
- Transações descentralizadas
- Protocolo Proof of work (PoW)

Blockchain 2.0

Contratos inteligentes

- Mais funcionalidades além de simplesmente uma rede de transações
- Aplicações de descentralização baseados em linguagens de programação
- Execução anônima de algoritmos
- Protocolo Proof of work (PoW)

Blockchain 3.0

Novas funcionalidades

- Aplicações de larga escala que se distanciam da origem da blockchain focadas em criptomoedas. Focadas no Ledger distribuído e rastreabilidade de informações.
- Melhora de performance com mais escalabilidade.
- Protocolo Proof of Work (PoW)

Porém, existe uma tendência pequena, mas crescente, de empresas privadas brasileiras que estão iniciando estudos e projetos em Blockchain para melhorar seus processos e aumentar o valor dos seus produtos, além de oferecer uma imagem positiva para os clientes com a utilização de uma tecnologia confiável.

Empresas integradoras de sistemas e desenvolvedoras também têm oferecido ao mercado serviços de qualidade com base em frameworks Blockchain, tais como o CPqD, a GoLedger e a IASIS Tech. No evento promovido pelo consórcio Hyperledger (que oferece plataformas open-source de Blockchain e DLTs), o Hyperledger Global Forum 2021, diversos casos e palestras foram apresentados, mostrando que o Brasil está se destacando na tecnologia Blockchain para o resto do mundo.

Os próximos anos devem levar o Brasil a um patamar maior que estamos hoje, com mais projetos, cases e profissionais capacitados na tecnologia Blockchain.

Como o panorama das soluções de blockchain no Brasil se compara ao internacional?

Marcos Sarres
CEO
Go Ledger

Chainalysis

A Chainalysis oferece soluções de investigação de criptomoedas e de conformidade às agências globais de aplicação da lei, reguladores e empresas que trabalham em conjunto para combater a atividades ilegais com moedas digitais.

Ela busca gerar transparência para uma economia global construída sobre blockchain, permitindo que bancos, empresas e governos tenham uma compreensão de como as pessoas usam a criptomoeda.

A empresa também fornece iformações, software, serviços e pesquisas em mais de 60 países. Sua plataforma de dados fornece ferramentas de investigação, conformidade e gerenciamento de risco que têm sido usadas para resolver alguns dos casos de ciber-criminosos mais importantes do mundo e aumentar o acesso dos consumidores à criptomoedas com segurança.

Só neste ano a startup já levantou duas rodadas de investimento, uma em março e outra em junho, alcançando assim um valuation de 4.2 bilhões de dólares.

Chainalysis

FUNDAÇÃO	LOCALIZAÇÃO	TOTAL FUNDING	PRINCIPAIS INVESTIDORES
2014	Nova Iorque, Estados Unidos	US$ 366.6 M	Coatue, Paradigm, Addition, Ribbit Capital, Sound Ventures, MUFG Innovation Partners, Sozo Ventures, Accel, Benchmark

Fireblocks

Feita para instituições que precisam armazenar e mover ativos digitais sem a dor de cabeça operacional ou de segurança, a Fireblocks é uma plataforma tudo em um para armazenar, transferir e emitir ativos digitais em todo o seu ecossistema.

A startup simplifica as operações trazendo todas as suas trocas, OTCs (Mercado de balcão), contrapartes, carteiras e custódias em uma única plataforma. Carteiras, endereços de depósito e credenciais API são assegurados usando a tecnologia de isolamento de chip com patente pendente e o mais novo avanço em criptografia (MPC). As instituições estão usando Fireblocks para movimentar fundos com segurança em segundos, ao invés de horas.

Com a API da Fireblocks, as instituições passam a ter acesso seguro a toda a gama de protocolos DeFi para estratégias como comércio de câmbio descentralizado e ativos como o token nativo da Cardano, ativos da Plygon, ou Dogecoin.

A startup entrou na lista *The 50 Fintech 2021*, feita pela Forbes e neste ano já levantou duas rodadas de investimento, uma em março e outra em julho, alcançando assim um valuation de US$ 2,2 bilhões.

Fireblocks

FUNDAÇÃO	LOCALIZAÇÃO	TOTAL FUNDING	PRINCIPAIS INVESTIDORES
2018	Nova Iorque, Estados Unidos	US$ 489 M	Coatue, DRW Venture Capital, SCB 10X, Sequoia Capital, Spark Capital, Stripes, Ribbit Capital, Paradigm, Cyberstarts, Eight Roads Ventures, MState, Tenaya Capital

StarkWare

A StarkWare resolve os problemas inerentes ao blockchain como escalabilidade e privacidade. Ela permite que o blockchain seja escalado em massa, confiando em provas criptográficas produzidas por um provérbio fora da cadeia que corre na nuvem, e depois verificadas por um contrato inteligente na cadeia. A solução em desenvolvimento pode reduzir o custo de cada transação baseada em blockchain em até 20.000 vezes.

Seus produtos são a StarkNet, uma Zero Knowledge -Rollup descentralizada sobre o Ethereum; o StarkEx, um motor de escalabilidade de segunda camada, que está em produção na Mainnet para escalonar múltiplas trocas e plataformas; e o Cairo, uma linguagem de produção para escalonar dApps usando a tecnologia STARKs.

O gasto energético por cada transição em blockchain ainda é alto, o que limita o número de aplicações. A tecnologia da StarkWare promete acelerar a adoção de blockchain para registrar e assegurar as transações não só de criptomoedas, mas de qualquer coisa que seja transferível digitalmente.

STARKWARE

FUNDAÇÃO	LOCALIZAÇÃO	TOTAL FUNDING	PRINCIPAIS INVESTIDORES
2018	Netanya, Hasharon, Israel	US$ 111 M	Paradigm, Sequoia Capital

DefenseArk

Inicialmente conhecida como OpenAVN, a norte-americana DefenseArk atua na proteção de dados e ameaças digitais por meio da coleta de um alto volume de *malwares* disponíveis na internet movida à utilização de tecnologias como Blockchain e Machine Learning. Com isso, a empresa desenvolve soluções para cada uma dessas ameaças com o objetivo de proteger os sistemas de seus usuários em uma velocidade superior à de antivírus tradicionais por meio de plataformas de escaneamento de *malwares* em tempo real (Brightscan) e extensões de cibersegurança a navegadores (Torus). Desse modo, o público-alvo de seus produtos vai desde usuários domésticos, empresas e "*home officers*" até instituições de ensino.

Posto isso, a DefenseArk recebeu seu último investimento em 2019, no qual captou um seed de US$ 1,5 M da plataforma de *equity crowdfunding* SeedInvest.

FUNDAÇÃO	LOCALIZAÇÃO	TOTAL FUNDING	PRINCIPAIS INVESTIDORES
2019	Nova Iorque **Estados Unidos**	US$ 2,2 M	MetaSquare Holdings, SeedInvest.

Blockchain no Brasil

Hugo
Co-Founder
Growth Tech

Como a blockchain revoluciona processos de segurança da informação?

Antes de qualquer ponto, destaco que a Blockchain é descentralizada e isso permite uma espécie de "governança coletiva" entre seus atores. Por si só, me parece que esta é uma característica que contribui bastante para segurança da informação.

Criptografia de ponta, rastreamento sofisticado (considerando dentre outros, a descentralização proporcionada), e a imutabilidade dos dados são outras características que podem ampliar a contribuição e sinergia para com os processos de segurança da informação.

Comparado ao mercado internacional, como o Brasil se posiciona quanto ao desenvolvimento de soluções que envolvam blockchain?

Penso que novas soluções em Blockchain tem surgido em todo ecossistema mundial, incluindo a parte brasileira. Por aqui temos avançado bem. Hoje, por exemplo, temos um "unicórnio cripto" na América Latina (Mercado Bitcoin), e este já é um fato muito considerável e de orgulho para quem 'milita' na indústria Blockchain brasileira. Porém, certamente, precisamos dar saltos maiores, fomentar mais o uso da tecnologia, educar nossa comunidade, investir em pesquisa e desenvolvimento, além de melhorar o ambiente competitivo que temos.

A Growth Tech é uma das startups pioneiras no Brasil, no segmento Blockchain. Como está sendo a trajetória de vocês?

Sim, iniciamos nossas operações em 2016. De lá pra cá vimos estudando bastante esta fabulosa tecnologia, e desenvolvendo projetos diversos. Nossa primeira solução foi uma rede de cartórios em Blockchain. Nela, realizamos alguns serviços pioneiros no Brasil, em parceria com grandes incorporadoras. Apesar de todo êxito, o ambiente cartorial brasileiro é bastante complexo e percebemos que várias questões regulatórias precisariam ser transpostas para o devido avanço desse movimento. Então, decidimos focar nossa energia em novas oportunidades, e aí desenvolvemos novas soluções. Criamos a Digi, uma plataforma para gestão de condomínios — que utiliza Blockchain para maior transparência de processos fundamentais para este mercado. Desenvolvemos também 'PropLedgers', uma plataforma para assinatura e registro de documentos em Blockchain permissionada. →

Desde o ano passado, “colocamos o pé” na Blockchain pública, e duas novas soluções foram desenvolvidas. “Registra Fácil” — plataforma para registro de documentos na Blockchain Ethereum e “PropToken” — solução para suportar novas modalidades de negócios imobiliários, através da tokenizacao. Definitivamente, percebemos que nosso mercado-alvo é o Imobiliário e estamos muito animados com as oportunidades que vimos amadurecendo nesta temática de tokenizacao. Vale destacar que essas duas últimas soluções estão em fase final de testes e devem estar disponíveis ao público final em no máximo 2 meses.

Blockchain em cybersecurity

Hugo
Co-Founder
Growth Tech