5ª 2020

Pesquisa Nacional sobre Conscientização em Segurança da Informação

eskive

Flipside
SECURITY BEYOND TECHNOLOGY

SUMÁRIO

2020,
O ANO DA VERDADEIRA ODISSÉIA

Vivemos períodos de grandes desafios, nos últimos anos. Quem imaginaria que, em nossas vidas, teríamos uma mudança completa na sociedade, devido a um fator não bélico? A epidemia da Covid-19 mudou completamente a forma como encaramos as pessoas, o trabalho e as interações humanas. Mais do que nunca, a internet e a digitalização entraram em nossas vidas e nos aproximou - mesmo que virtualmente - enquanto precisávamos estar longe.

A pandemia elevou o número das ações dos cibercriminosos a patamares nunca antes imaginados. Número este que já vinha numa ascensão rápida de crescimento fez com que o assunto segurança da informação e privacidade de dados se tornasse um dos mais críticos para a Alta Direção das empresas.

Já não bastavam todos os desafios e dificuldades enfrentados, o ano de 2020 também ficará marcado pelo início da vigência da Lei Geral de Proteção de Dados (LGPD). Após meses de incertezas quanto à sua entrada em vigor, o mês de setembro consolidou a necessidade de adequação a lei numa realidade onde consumidores procuram, cada vez mais, produtos e serviços que agregam segurança e privacidade de dados na sua concepção, tornando componentes fundamentais nas ofertas de uma empresa.

E isso exige que as empresas não apenas gerenciem e protejam melhor os dados para evitar multas e penalidades significativas, mas garanta ao mercado transparência e eficiência nos seus controles de proteção como fator crucial para reputação de suas marcas. Entretanto, enquanto isso, o que vemos com frequência na imprensa são violações de dados expondo as informações pessoais de milhões de pessoas.

E um dos maiores riscos para a segurança das informações de uma organização não é uma fraqueza no ambiente de controle de tecnologia e sim a suscetibilidade que esse ambiente traz à ação ou omissão de colaboradores e outras pessoas que podem levar a incidentes de segurança.

A falta de consciência e conhecimento sobre segurança e privacidade das pessoas que manipulam estas informações em relação a até seus próprios dados pessoais, contribuem para os resultantes de invasões e perdas de dados. De acordo com a UK's Information Commissioner's Office (ICO), o erro humano causou 90% das violações de dados cibernéticos em 2019.

As empresas não podem mais depender exclusivamente de processos e tecnologia para redução de riscos de segurança e precisam de uma maior integração de pessoas com processos e tecnologia.

Nos últimos cinco anos, a Flipside vem realizando pesquisas de conscientização envolvendo centenas de empresas brasileiras. Nossas pesquisas demonstraram ao longo dos anos que as abordagens atuais de conscientização de segurança não atendem inteiramente a todos os requisitos para os desafios que os negócios exigem.

O objetivo desta pesquisa é aumentar a compreensão dessas lacunas e, por consequência, ajudar as organizações e os profissionais de segurança a desenvolverem políticas e treinamentos que ajudem a formar pessoas mais preparadas para prevenir ataques cibernéticos.

Priscila Meyer_
Sócia fundadora da Flipside e CEO do Eskive

O NASCIMENTO DA PESQUISA E SUA FERRAMENTA

Metodologia utilizada

Os dados deste relatório apresentam dados e comparativos da pesquisa anual realizada pela Flipside sobre Conscientização em Segurança da Informação. A análise desses dados identifica e avalia como as organizações gerenciam seu risco humano de acordo com o grau de maturidade do programa de conscientização de segurança, equipe e budget destinado ao programa fornecendo um cenário de tendências.

No seu 5º ano de pesquisa, que envolveu quase **300 profissionais** de segurança de **26 segmentos** distintos, exploramos ainda mais o impacto dos riscos ligados ao fator o humano e o crescimento da Área de Conscientização ou pessoas responsáveis pelo programa dentro das empresas. Além disso, avaliamos como as empresas estão estruturadas organizacionalmente e seu nível de preparo para atender a LGPD neste ano que a lei entrou em vigência.

O modelo da pesquisa é caracterizado pelas seguintes premissas:

1. As perguntas abordaram na sua maioria profissionais de segurança da informação com mais de 11 anos de experiência no mercado.
2. Os profissionais ocupavam principalmente os cargos de CISOs e CSOs que afirmaram estar familiarizados com os processos de conscientização em suas empresas.
3. Os entrevistados da pesquisa representam todos os principais setores e uma combinação de tamanhos de empresa.
4. As questões foram respondidas na sua grande maioria por pessoas que decidem ou influenciam na determinação do budget do programa de conscientização.
5. As empresas respondentes possuem em sua grande maioria uma Área de Segurança da Informação independente, com equipe própria e gestor dedicado.

Os resultados aqui apresentados tem como objetivo traçar um panorama do mercado de conscientização fornecendo às empresas a possibilidade de identificar como seus programas estão de acordo com este mercado e com isso, definir planos de melhoria.

ATO 1

A Aurora da conscientização

O SURGIMENTO DA ÁREA DE CONSCIENTIZAÇÃO NAS EMPRESAS

O ano de 2020 foi marcado pelo princípio de uma tendência que era observada apenas em empresas fora do Brasil: a criação de uma área e/ou de equipes dedicadas ao desenvolvimento e implementação de um programa de conscientização.

O aumento do número de golpes durante a pandemia do COVID-19, utilizando artifícios para enganar as vítimas, como campanhas mentirosas de solidariedade por exemplo, fez com que a importância do papel do usuário na proteção dos dados ficasse muito mais evidente.

Além disso, o princípio da "responsabilidade" como um tema fundamental na LGPD, onde as empresas devem ser responsáveis pela implementação de requisitos aplicáveis de privacidade e proteção de dados, mostrou que para estar em conformidade com a lei, os usuários precisam ser treinados e conscientizados quanto à importância da proteção e privacidade dos dados.

Estes fatores impulsionaram as empresas no entendimento acerca da necessidade de prover à seus usuários conhecimentos necessários para proteção das suas informações e investir em profissionais capacitados para desenvolver um programa de conscientização contínuo, no qual pudesse preparar as pessoas para saírem do papel de vítima e se tornarem barreira de proteção dos dados das empresas.

Para entender este crescimento, perguntamos aos entrevistados, qual o tempo dedicado da equipe nos programas de conscientização e qual empresa possui um área dedicada ao desenvolvimento e implementação deste programa. Nossa análise revelou que **66%** das empresas dedicam de **1%** a **25%** de todo o tempo do time de Segurança da Informação em programas de conscientização. E apenas **6%** das empresas possuem possuem 1 profissional dedicado como Gestor ou Analista de Conscientização

Possuem profissionais dedicados à Programas de Conscientização

No máximo 1/3 do tempo do time de segurança é dedicado ao programa de conscientização em 66% das Empresas

Apesar de uma perceptível tendência de crescimento **nestes números**, ainda vemos um baixo esforço para garantir o amadurecimento de um programa de conscientização. Assim como qualquer projeto que requer amadurecimento de longo prazo é necessário a alocação de equipes dedicadas em tempo integral para implantação de um programa robusto.

APOIO DA ALTA DIREÇÃO

Obter o apoio e patrocínio da alta administração é talvez o aspecto mais importante para o programa de conscientização. É vital construir um consenso entre os tomadores de decisão de que o programa de conscientização não é só importante para o negócio como também o tornará mais competitivo. Se os principais interessados não compreenderem o imperativo de um programa de conscientização de segurança da informação e não apoiarem os objetivos e metas, a iniciativa não seguirá em frente.

A pesquisa mostrou um aumento de **11%** no apoio da alta direção nos programas de conscientização, deixando evidente o quanto o papel do usuário na proteção das informações entrou na agenda dos executivos a partir de 2020.

Principalmente considerando que os números das pesquisas realizadas entre os anos de 2017 a 2019 não tiveram crescimento significativas. Conclui-se então, que cada vez mais, fatores humanos desempenham um papel significativo para proteger os negócios, a imagem da empresa e na estratégia dos negócios.

Aumento no apoio da alta direção nos programas de conscientização

Apesar do apoio da alta direção ter aumentado, espera-se uma liderança mais consciente quanto à priorização dos investimentos de treinamento de conscientização de segurança.

ATO 2

AMT-1

O QUE LEVA AS EMPRESAS A INVESTIREM EM UM PROGRAMA DE CONSCIENTIZAÇÃO

01 MINIMIZAR RISCOS DE INCIDENTES

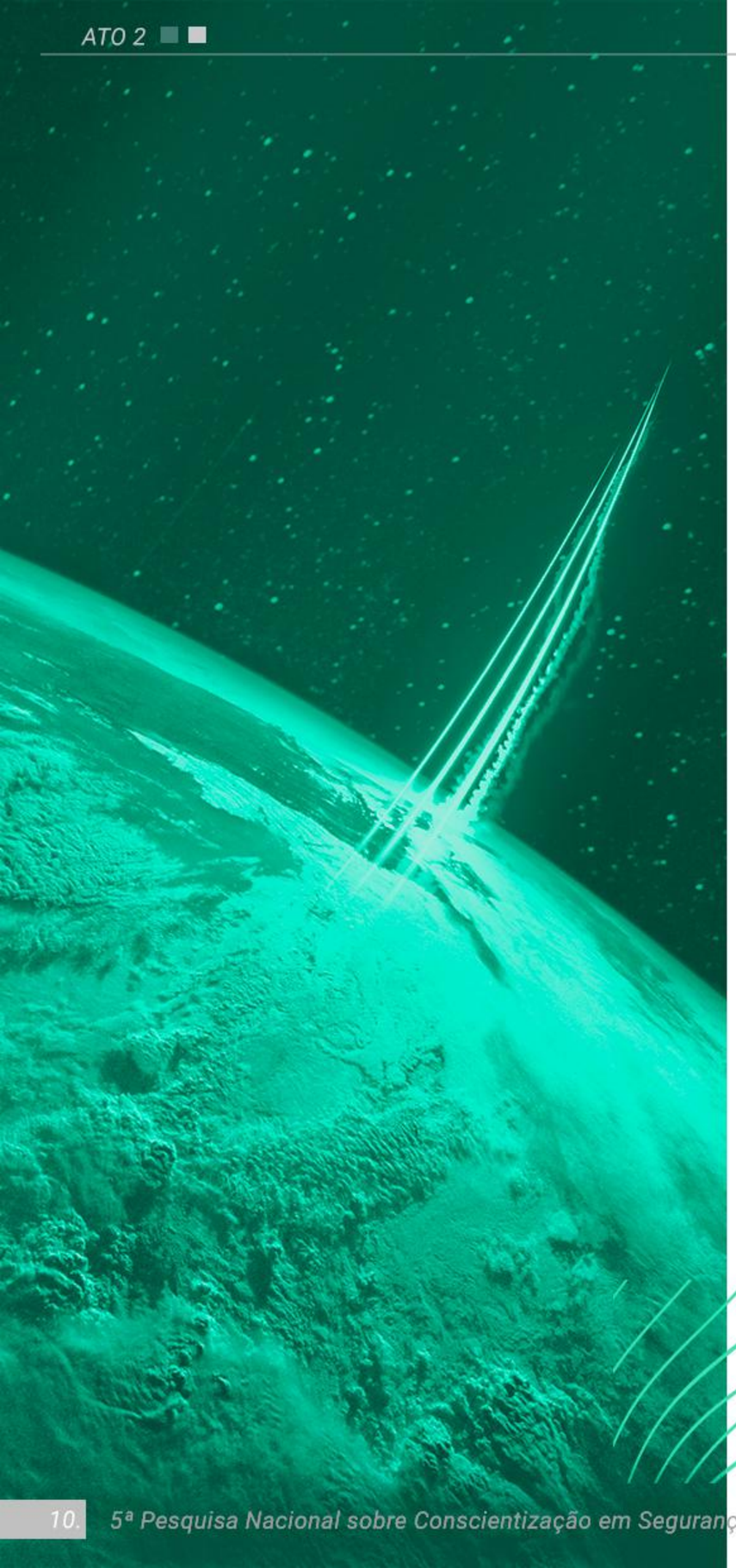
A possibilidade de sofrer um ataque cibernético ou uma violação de dados ainda é o fator **número um** no qual as empresas investem em programas de conscientização. Reconstruir a confiança do consumidor após uma violação pode frequentemente ser mais difícil do que a recuperação financeira, por isso minimizar incidentes de segurança envolvendo comportamento dos usuários é o motivador principal das empresas ao longos dos anos para treinar os usuários na proteção de dados.

02 LGPD, EXIGÊNCIAS REGULATÓRIAS E DE AUDITORIA

As penalidades trazidas pela LGPD e outras implicações financeiras associadas a multas de agências regulatórias e auditorias estão em **segundo lugar** no motivo dos quais as empresas investem em treinamento e conscientização. De uma perspectiva financeira, o investimento em treinamento e conscientização supera em muito as multas potenciais associadas a violação de dados. Além disso, ao longo dos anos, temos visto a adoção de uma postura firme em relação à segurança da informação também pode ter um impacto positivo na atração de novos negócios.

03 SEGURANÇA COMO ESTRATÉGIA DE NEGÓCIO

A adoção de segurança da informação como estratégia de negócio também pode ter um impacto positivo na imagem e nos produtos da empresa. A segurança de dados está crescendo rapidamente na agenda. Segurança da informação e privacidade de dados têm se tornando padrão nos questionários de due diligence. As empresas que podem demonstrar um forte foco na segurança da informação terão uma **vantagem competitiva**, especialmente quando visam clientes de primeira linha.



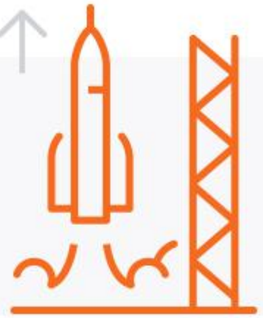
TENDÊNCIA DAS AMEAÇAS

Esta seção do relatório fornece uma visão geral das ameaças à segurança da informação que os entrevistados consideram ser mais relevantes para sua organização relacionadas aos comportamentos dos usuários. Por conta do cenário atual, pode-se perceber que os resultados foram impulsionadas por dois principais fatores: **o aumento no trabalho remoto** e aos **requisitos impostos pela LGPD**.

Considerando o aumento do número de usuários trabalhando remotamente notou-se um crescimento na ameaças ligadas à ataque de phishing e uma maior preocupação em relação ao uso inadequado do e-mail profissional, ao uso de grupos de trabalho em aplicativos de mensagens instantâneas, a visitas a sites maliciosos e à compartilhamento indevido em redes sociais.

Em contrapartida, tivemos uma diminuição em relação ao compartilhamento de senhas, uso de software não homologado e à utilização de senhas fracas.

A LGPD foi responsável pela necessidade de trazer respostas imediatas à problemas ligados à inconformidade com os tratamentos de dados e a práticas de controles de segurança inapropriados em fornecedores terceirizados.



+09% Phishing
+16% Uso inadequado do e-mail profissional,
+04% Grupos de trabalho no whatsapp
+11% Visitas a sites maliciosos
+03% Compartilhamento indevido em redes sociais
+ 20% Inconformidade com os tratamentos de dados
+ 08% Práticas de controles de segurança inapropriadas em fornecedores terceirizados ou subcontratados.

- 30% Compartilhamento de senhas
- 07% Uso de software não homologado
- 02% Uso de senhas fracas

ATO 3

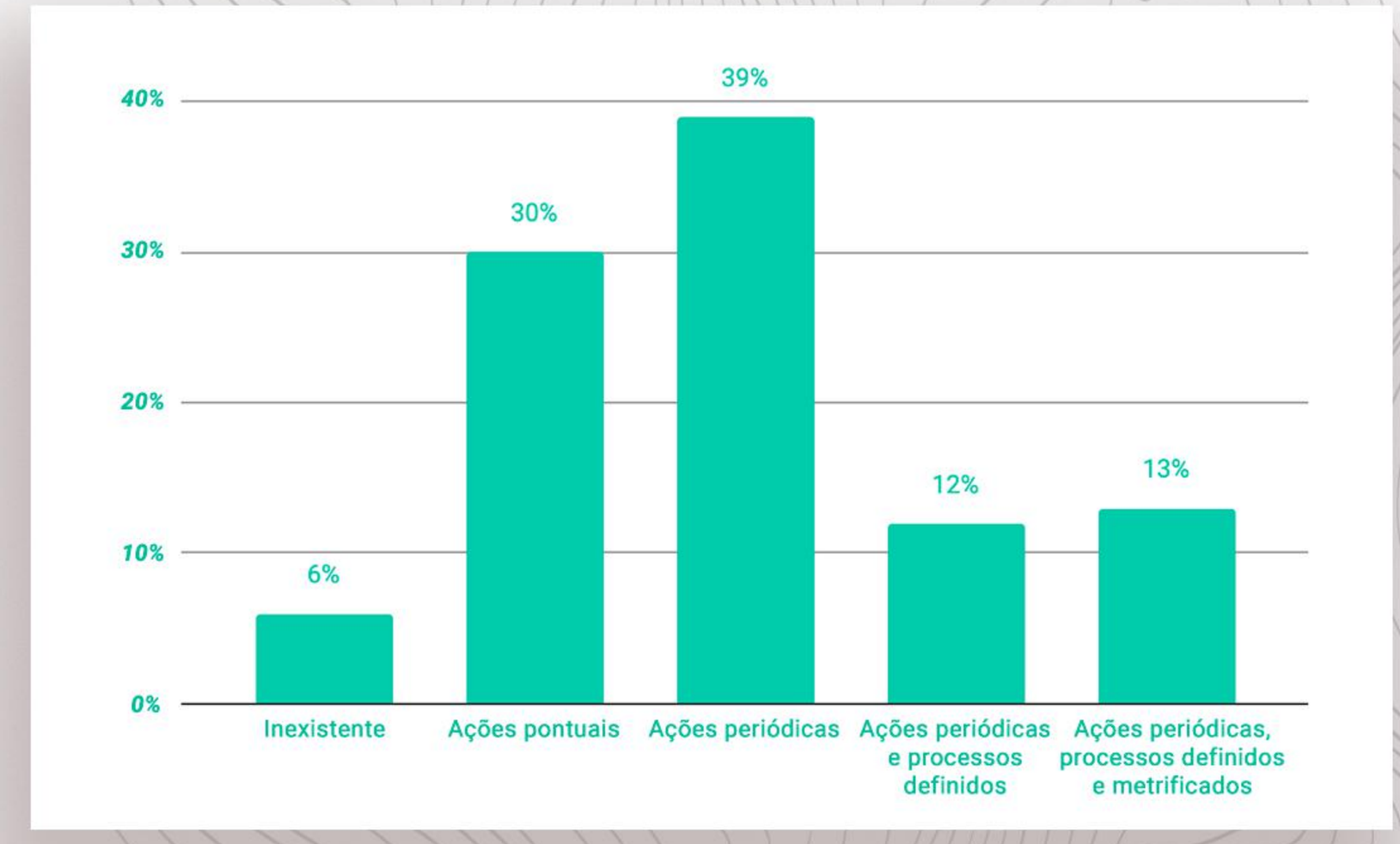
Missão Segurança

CAMINHO À MATURIDADE PERFEITA

Ao longo dos cinco anos de pesquisa foi possível observar um aumento gradativo na maturidade do programa de conscientização dentro das empresas.

O estágio que teve um resultado mais expressivo foi no que tange às empresas que não tinham nenhum tipo de ação de conscientização ou possuíam algumas ações pontuais, diminuindo uma média de **27%** nesses estágios. Com isso, houve um aumento de **21%** nas empresas que se encontram no estágio de execução de ações periódicas dentro de um programa de conscientização.

Porém, empresas que se encontram no estágio onde possuem ações periódicas com processos definidos e metrificados demonstrou um aumento de **7%**.



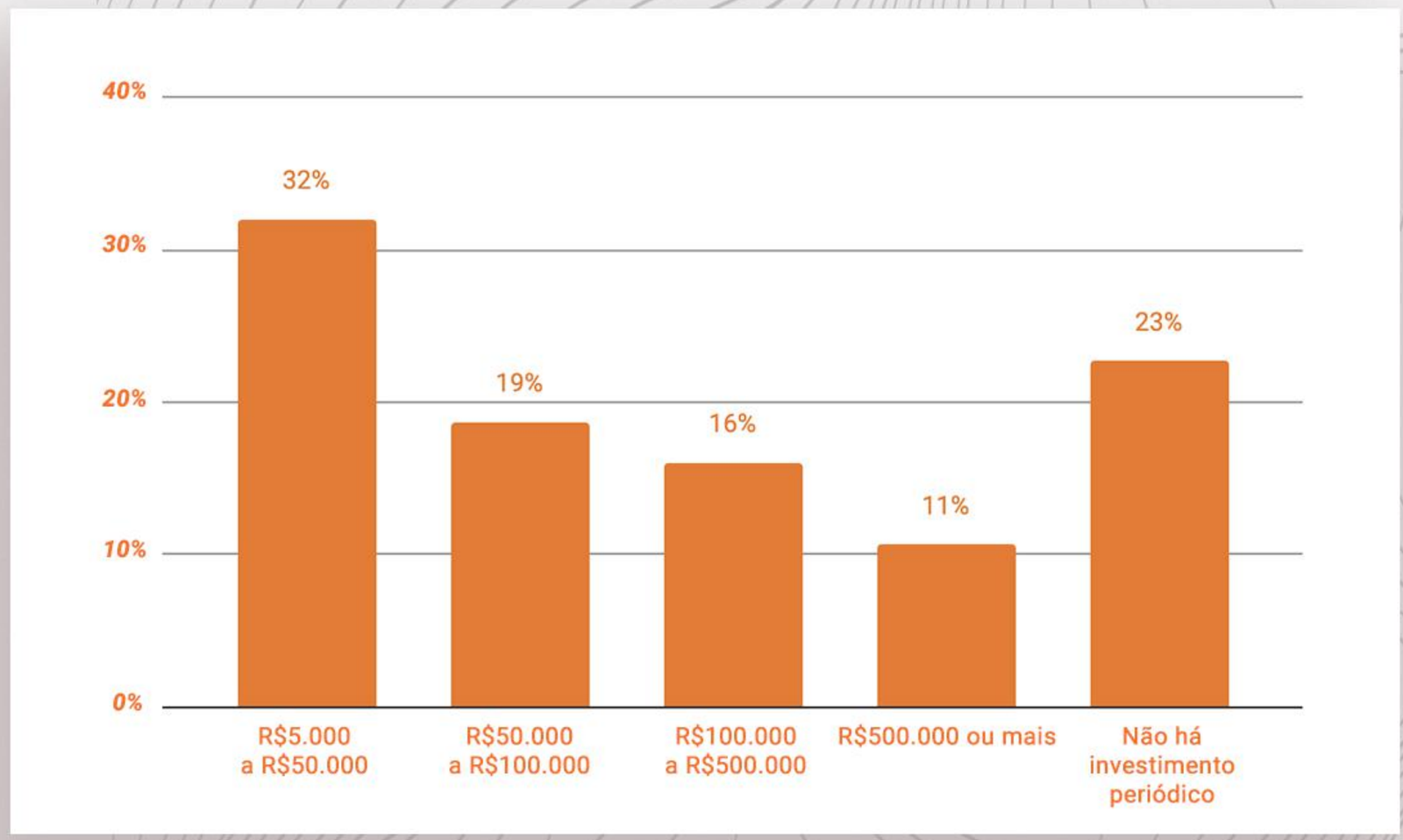
Isso demonstra que as empresas ainda estão num crescimento de maturidade lento e se encontram numa maturidade intermediária nos seus programas de conscientização. Isso é um sinal que necessitam buscar recursos para garantir que os esforços sejam integrados e a mudança alcance benefícios reais e duradouros.

INVESTIMENTOS VERSUS BUDGET SI

Considerando os cinco anos de pesquisa foi possível observar um aumento de mais de **10%** de empresas que começaram investindo em programas de conscientização. Entre os anos de 2016 e 2019, uma média de **33%** das empresas não possuíam nenhum tipo de investimento em ações de treinamento ou conscientização de usuários, face a **22%** em 2020.

Dentro das empresas que investem até R$ 100.000,00 o número se manteve estável na média de **50%** das empresas que adotam orçamentos para programas de conscientização. Orçamentos entre R$ 100.000,00 a R$ 500.000,00 tiveram um aumento de **6%**. Empresas que investem acima de R$ 500.000,00 se mantiveram na média de **10%**.

Com isso, é possível observar um aumento significativo nas empresas em adotar um budget exclusivo para o desenvolvimento de um programa de conscientização e um aumento gradativo no volume do orçamento nas empresas que já possuíam um budget reservado para treinar e conscientizar os usuários em segurança da informação.



ATO 4

Além do Infinito

LGPD: UMA LEI QUE MUDOU A PRIVACIDADE PARA SEMPRE

O ano de 2020 será marcado no Brasil, além do ano da pandemia, como o ano que a Lei Geral de Proteção de Dados (LGPD) entrou em vigor com a sanção da **Lei 14.058/2020** em 18 de setembro após sucessivos adiamentos e indefinições.

A LGPD teve sua concepção inspirada na regulamentação europeia (GDPR) foi aprovada em 2018, no governo Michel Temer, e modificada em 2019. A lei dispõe sobre o "tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural", conforme diz o texto da lei.

As empresas começaram a enfrentar dificuldades na implementação dos controles para adequação da lei por conta da ausência de consciência das pessoas em relação à importância da privacidade já que a proteção de dados pessoais diz respeito a todos e exige adesão da liderança e das equipes.

> Não é possível criar uma cultura em relação ao uso de dados pessoais nas empresas em que as pessoas entendam o valor comercial dos dados sem antes compreender a importância de valorizar os dados pessoais e aprender quais são as consequências de não lidar com eles adequadamente."
>
> ***Priscila Meyer**, Sócia Fundadora da Flipside e CEO do Eskive*

Existe uma grande desconexão entre a percepção das pessoas sobre a privacidade e o que elas devem fazer para garantir que seus dados pessoais estejam protegidos. Se forem questionadas se se importam com a privacidade de seus dados, certamente a grande maioria responderá de maneira afirmativa. Porém, o comportamento destas pessoas em relação a seus dados pessoais raramente estará compatível com suas afirmações.

Com isso, as empresas assumem a responsabilidade que vai muito além do que é simplesmente exigido por lei, desenvolvendo uma cultura que envolve ensinar às pessoas porque devem se preocupar com a proteção da privacidade e as implicações concretas que as violações de privacidade podem ter nos indivíduos, na organização e nos envolvidos em violações de dados. Ao promover uma cultura em que os funcionários recebem treinamento regular para evitar a divulgação de dados, reconhecer problemas e incidentes e responder de acordo com as necessidades de sua função de trabalho suas atitudes em relação à conformidade se torna parte das práticas cotidianas da vida profissional.

De acordo com a pesquisa, conscientizar os usuários sobre privacidade por conta da LGPD é o **segundo principal motivo de investimento em um programa de conscientização** e, comparado à pesquisa de 2019, teve um aumento de **6%**.

Porém, apenas **29%** das empresas pesquisadas possuem um programa de conscientização dedicado a desenvolver uma cultura de consciência sobre a importância dos dados pessoais e de capacitar seus usuários a como trabalhar em conformidade com a LGPD.

Para se alcançar a conformidade com a lei é necessário que todos estejam cientes de todos os impactos do novo regulamento e não só das multas em caso de violação. **46%** da empresas afirmaram ter efetuado alguma ação de conscientização pontual, onde se entende que a abrangência limitada muitas vezes pode deixar de fora partes interessadas importantes e a falta de periodicidade como parte de um programa contínuo de conscientização, dentro de um plano estratégico adequado, não permite uma real mudança de cultura. A privacidade intencional não é uma opção e sim uma obrigação na LGPD sendo responsabilidade de todos na empresa garantir que os dados sejam protegidos.

CONCLUSÃO

O ano de 2020 foi marcado por imensos desafios para quem tem a tarefa de proteger as informações das organizações. **O crescimento exponencial do número de ataques, o cenário de pandemia, o aumento de exigências regulatórias, o início da vigência da LGPD e as expectativas dos consumidores em relação ao nível de segurança e proteção dos dados** exigiram das organizações pessoas cada vez mais preparadas e com habilidades que impulsionam a excelência em privacidade, proteção de dados e segurança cibernética.

Com isso, nunca se ficou tão evidente a necessidade de um programa de conscientização para enfrentar estes desafios envolvendo todos os funcionários para que possam receber treinamentos apropriados e atualizações regulares em um esforço para proteger os dados que lhes foram confiados.

Porém, apesar do aumento do esforço dedicado em programas de conscientização e do aumento do apoio da alta administração conforme podemos observar como resultado desta pesquisa, sabemos que as iniciativas de conscientização dentro das organizações ainda estão muito distantes destes desafios que a Área de Segurança da Informação vêm enfrentando. A velocidade na qual os negócios estão se digitalizando e a interação dos clientes com as marcas por meio de uma variedade cada vez maior de pontos de contato, não refletem nas ações de conscientização e cada vez mais é possível observar um número preocupante de funcionários em empresas despreparados para lidar com a evolução das ameaças destes novos cenários.

Treinar os funcionários para que estejam preparados para lidar com os riscos inerentes às soluções de tecnologia que suas empresas estão adotando para ajudá-las a se recuperar e renovar na era pós-pandemia é um desafio crucial e deve ser encarado como estratégia de negócio para se criar vantagem competitiva, porém é visto principalmente como uma questão de TI ou segurança da informação.

Como especialistas em risco e segurança, você não pode mudar o curso das principais interrupções que afetam as empresas. Mas você pode treinar as pessoas para que entendam os riscos e ameaças cibernéticas em potencial para fazer o melhor para ajudar a prevenir ataques cibernéticos.

A Flipside

12 anos traduzindo nosso conhecimento em Segurança da Informação em soluções de conscientização. Desde as nossas Soluções de Conscientização até os nossos eventos, a educação está em tudo o que fazemos. Através do conhecimento queremos mudar comportamentos. *Segurança sozinha é um conceito, em conjunto é uma realidade!*

O Eskive

O Eskive é a plataforma brasileira de monitoramento de vulnerabilidade humana em segurança da informação. Muito mais que simulação de Phishing, o Eskive conta com diversos sensores de análise para que os gestores de Segurança da Informação consigam antever, treinar e preparar as empresas para os ataques de engenharia social.

Para obter mais informações sobre nossa organização, visite www.eskive.com

eskive

Flipside
SECURITY BEYOND TECHNOLOGY