Relatório de Resultados de Pesquisa Setorial em Cibersegurança - ABRASCA e SDL

Cristiano Iop Kruger„ Alexandre Vasconcelos„ Rafael Sasso„ Paulo Moura


The
Security
Design Lab
abrasca
Resultados
Pesquisa Setorial
em Cibersegurança
2023
Cyber
Score

Introdução

Ficha Técnica

Este relatório é fruto da “Pesquisa Setorial em Ciber Segurança 2023”.

O projeto é uma iniciativa da ABRASCA – Associação Brasileira das Empresas de Capital Aberto e do SDL – The Security Design Lab.

Realização

ABRASCA – Associação Brasileira das Empresas de Capital Aberto

Idealização

SDL – The Security Design Lab

Capital Markets Lab – Comissão de Inovação Corporativa CINC ABRASCA

Coordenação

Cristiano Kruger Iop, Fernanda Camargo, Alexandre Vasconcelos e Rafael de Campos Sasso

Financiadores

- Alvarez & Marsal
- Akamai
- Bidweb
- Elytron
- Howden
- Urbano Vitalino Advogados

Apoiadores

- ABCIS – Associação Brasileira dos CIOs de Saúde
- ABES – Associação Brasileira das Empresas de Software
- Centro de Tecnologia e Sociedade da FGV Direito Rio (CTS-FGV)
- Cesar Schooll
- DATAPREV
- FIT - Instituto de Tecnologia
- FIPECAFI – USP
- IMREDD - Université Côte d'Azur
- Inatel – Instituto Nacional de Telecomunicações
- INSPER
- Instituto Eldorado
- MID – Movimento de Inovação Digital
- Ryto Public Affairs
- Woman's Club

Design e diagramação

Marcelo Caldeira

Como citar este relatório

Pesquisadores a serem citados: IOP KRUGER, Cristiano; VASCONCELOS, Alexandre; SASSO, Rafael; MOURA, Paulo e Pesquisa Setorial em Cibersegurança 2023 - ABRASCA - Associação Brasileira das Empresas de Capital Aberto e SDL - The Security Design Lab.

Disclaimer

As opiniões expressas neste documento são um retrato das conclusões da presente pesquisa, não refletindo, necessariamente, a opinião institucional da ABRASCA e/ou das organizações apoiadoras. O presente relatório consiste em material meramente informativo e não substitui a necessidade de aconselhamento técnico.

Apresentação

Este relatório é resultado da "Pesquisa Setorial em Ciber Segurança 2023", uma uma iniciativa da ABRASCA – Associação Brasileira das Empresas de Capital Aberto na sua Comissão de Inovação Corporativa por meio do Capital Markets Lab e do SDL – The Security Design Lab.

Esta pesquisa visa medir o nível de maturidade em cibersegurança das empresas de capital aberto, trazendo entendimento da situação e gerando *awareness* sobre a importância deste tema dentro do Mercado de Capitais.

A relevância e preocupação que o tema têm gerado junto a investidores, conselheiros e executivos, face aos inúmeros casos ocorridos nos últimos anos, que estão afetando desde a reputação das empresas até a própria continuidade dos negócios, começou a chamar a atenção de reguladores e autoridades, preocupados em entender e reagir e essa nova camada de complexidade, que se tornou parte inerente do ambiente de negócios e da sociedade.

O resultado da pesquisa visa subsidiar, com dados, o debate e formação do advocacy da entidade em uma futura Política ou Legislação de Cibersegurança para empresas de Capital Aberto e/ ou formação de um framework de autorregulação da entidade, permitindo a criação de um Programa de Governança e Gestão em Cibersegurança. Desse modo, a pesquisa também direcionou a criação do "Guia de Segurança da Informação", lançado em conjunto com este relatório.

Organização

O relatório está organizado em 2 partes, visando dar ao leitor instrumentos de compreensão do significado dos resultados do ponto de vista comparativo com outras empresas e países.

A Parte 1 contextualiza a pesquisa dentro do cenário atual de cibersegurança para as empresas e no mercado de capitais, elencando seus desafios e discutindo pontos de partida.

A Parte 2 analisa e expõe os resultados do questionário aplicado às companhias e à metodologia aplicada, o Cyber Score.

Agradecimentos

Este estudo foi realizado a partir da metodologia do CyberScore, criada e patenteada pelo SDL, e pelas discussões, materiais e suporte intelectual dos apoiadores e patrocinadores. Além disso, agradecemos a todos os participantes e as empresas respondentes e suas equipes que participaram da pesquisa.

Painelistas e debatedores no evento de lançamento

Painel 1 - Regulação, Legislação, Política e Melhores Práticas em Cibersegurança no Mercado de Capitais

- Pablo Cesário – Presidente-Executivo ABRASCA
- João Pedro Nascimento – Presidente CVM
- Luiz Fernando Moraes da Silva – Secretário GSI
- Eduardo Gomes – Senador
- Marcello Junqueira – Urbano Vitallino

Painel 2 - Mercado de Capitais: Impactos de um Ciberataque em Empresas de Capital Aberto

- Prof. Edgard Bruno Cornacchione Junior - Phd (FIPECAFI/ USP)
- Marta Schuh - Cyber Insurance Director – Howden
- Helder Ferrão - Industry Strategy Manager LATAM Akamai
- Nycholas Szucko - MID

Painel 3 - Análise dos Resultados da Pesquisa Setorial em Cibersegurança

- Flávia Brito - CEO Bidweb
- Eduardo Magalhães - Senior Director DI Alvarez & Marsal
- Paulo Moura - Deputy Director IMREDD
- Victor de Queiroz - Offensive Security Engineer Elytron
- Alexandre Vasconcelos – The Security Design Lab

Financiadores e Apoiadores

ABRASCA

Sasso, Rafael

Alvarez & Marsal

Cavina, Alexandre

Bidweb Security

Brito, Flavia

Centro de Tecnologia e Sociedade da FGV Direito Rio (CTS-FGV)

Belli, Luca

Gaspar, Walter Britto

Bakonyi, Erica Brito

Elytron

Garcia, Pedro

FIPECAFI & USP

Cornacchione, Edgard

FIT

Savoy, Alexandre Mancin

de Souza, Rodrigo Costa

Pittorri, Flávio Antônio

Howden

Schuh, Marta Helena

IMREDD

de Moura, Paulo Carvalho Basílio

INSPER

Batista, Andre Filipe de Moraes

Instituto Eldorado

Sanz, Igor Jochem

Moia, Vitor Hugo Galhardo

Rebello, Gabriel Antonio Fontes

Junior, João Claudio Capelari

MID – Movimento de Inovação Digital

Szucko, Nycholas

Security Design Lab

Vasconcelos, Alexandre

Sikur

Iop, Cristiano Kruger

Urbano Vitalino Advogados

Junqueira, Marcello

Assis, Hermes

Backes, Ingrid

Barakat, Nagib

Melo, Silvana

Henrique, Paulo

Sumário

Capítulo 1 - Snapshot Global – Como estamos em 2023 10

Capítulo 2 - Impactos Financeiro e Valor de Mercado de Companhias Abertas após um ciberataque – Como estamos em 2023 16

Capítulo 3 - Custos de Curto e Médio Prazos x Longo Prazo e o impacto nos negócios 21

Capítulo 4 - Entendimento e Prevenção 24

Capítulo 5 - A Pesquisa 27

Metodologia Cyber Score 27

Fase 1 – Definição do Escopo e Pesquisa das Fontes 28

Fase 2 – Definição das Fontes que serão utilizadas no Assessment 28

Fase 3 – Extração do conteúdo de cada fonte 28

Fase 4 – Inserções de perguntas adicionais 28

Fase 5 – Definição das questões pontuáveis 29

Fase 6 – Definição do nível de Criticidade de cada controle 29

Fase 7 – Definição do nível de Complexidade para Implementação de cada Controle 30

A Pesquisa 31

Resultados 31

Respostas ao questionário 32

Seção Introdutória 32

Seção 1 - Identificação, Autenticação, e Provedores de Identidade 32

Seção 2 - Nuvem, On-premises e Controle de Acessos 35

Seção 3 - Mecanismos de Auditoria 39

Seção 4 - Continuidade de Negócios, Backup e Disaster Recovery 41

Seção 5 - Criptografia e Gerenciamento de Chaves 43

Seção 6 - Chat Corporativo e Mensagens 45

Seção 7 - Conformidade com os Regulamentos de Proteção de Dados 47

Seção 8 - Resposta a Incidentes 49

Seção 9 - Proteção de Mídias Digitais 51

Seção 10 - Governança e Segurança da Informação 52

Seção 11 - Gerenciamento de Risco da Cadeia de Suprimentos (Supply Chain) 54

Seção 12 - Dispositivos Conectados 56

Conclusão 57

Termos técnicos chave para o entendimento 58

Capítulo 1

Snapshot Global – Como estamos em 2023

Introdução

Neste capítulo, destacamos uma visão geral dos incidentes cibernéticos, comparativamente, entre 2022 e 2023. O foco são as incidências de ataques de ransomware, as principais maneiras que os invasores acessam uma corporação, detalhes dos incidentes do ponto de vista macrorregional, incidência de ataques em infraestruturas críticas, valores médios dos pagamentos de resgates e os riscos mais significativos na visão dos executivos.

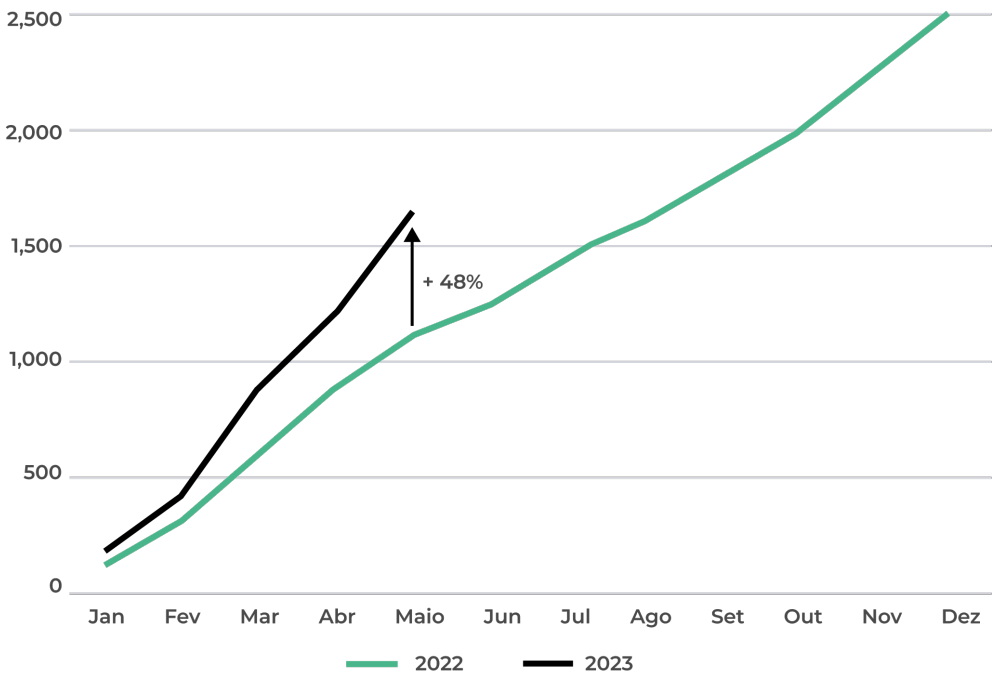
O cenário geral é de crescimento de eventos de cibersegurança e grande envolvimento do elemento humano nos casos. O crime organizado continua liderando os ataques externos e as principais motivações são financeiras. Para a America Latina, o cenário é muito parecido com o global. O ponto mais preocupante, além dos ataques à infraestrutura crítica que preocupa os governos, é o fato de o tíquete médio dos resgates estar aumentando consideravelmente.

A seguir destacamos uma visão macro de dados recentes de incidentes cibernéticos globais

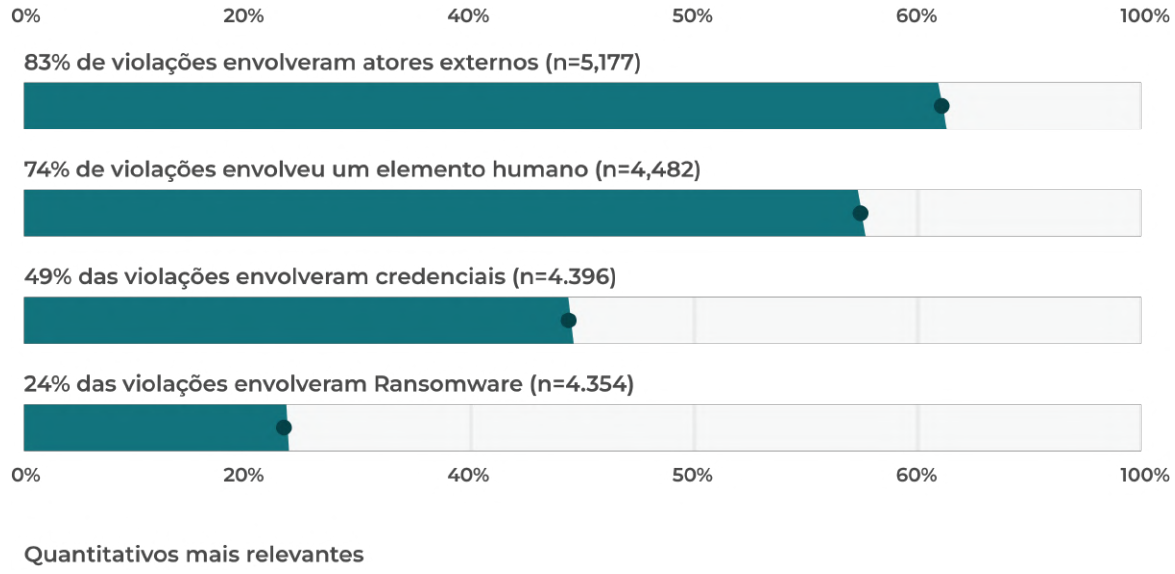
O gráfico abaixo mostra dados dos primeiros 5 meses do ano de 2023. O ransomware continua dominando o cenário de ataques cibernéticos. Comparando a atividade cumulativa de ransomware em 2022 e 2023 com os dados mais recentes do NCC Group até maio vimos um crescimento superior a 48% em comparação ao período correspondente do ano passado.

Atividade cumulativa global de ransomware por mês - 2022 vs 20223

(Fonte: Howden analysis based on data from NCC Group)



O gráfico abaixo mostra que 74% de todas as violações incluem o elemento humano, com pessoas sendo envolvidas através de erros, usos indevidos de credenciais privilegiadas, roubo de credenciais ou engenharia social.



Fonte: Verizon, 2023

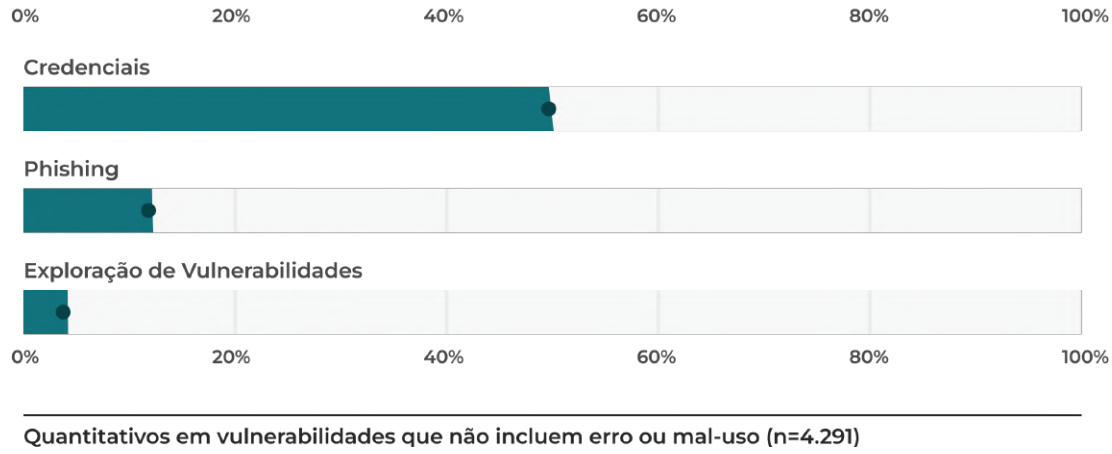
As três principais maneiras pelas quais invasores acessam uma organização são:

I. Credenciais roubadas;

II. Phishing; e

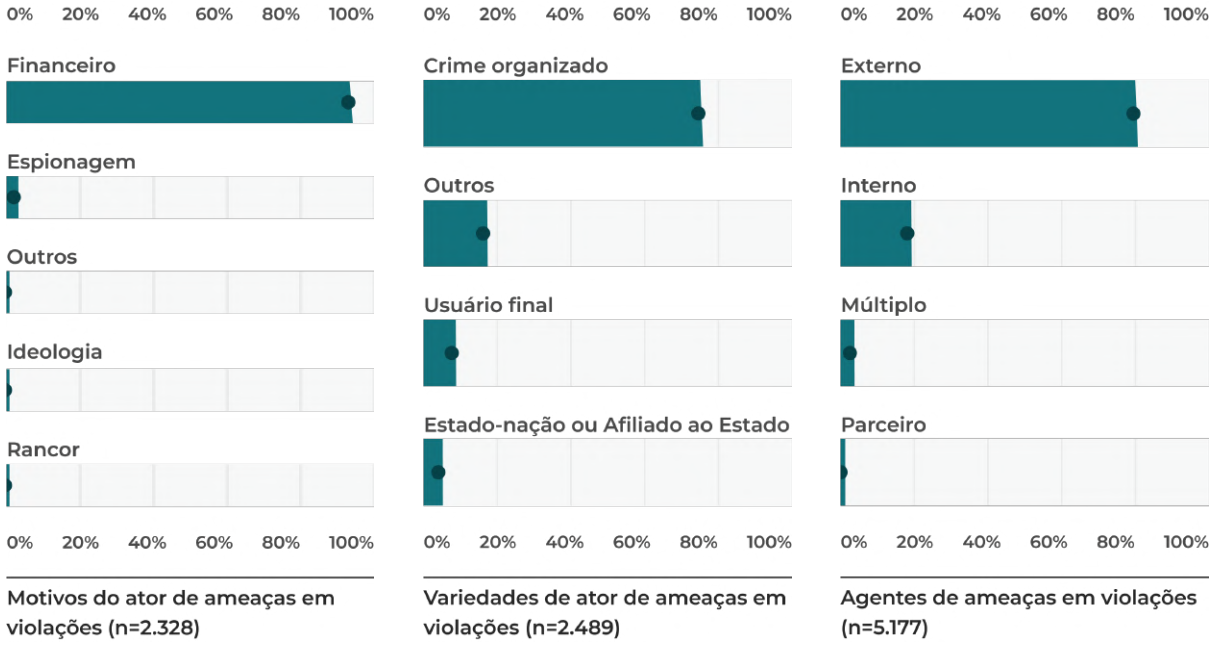
III. Exploração de vulnerabilidades.

Os funcionários das organizações são os alvos prediletos, o que sugere que as empresas deveriam prestar mais atenção no gerenciamento adequado de credenciais.



Fonte: Verizon, 2023

Cerca de 83% das violações envolvem atores externos às Companhias, com 95% dos ataques sendo motivados por questões financeiras e o maior índice de ataques externos é o crime organizado.



Fonte: Verizon, 2023

A figura abaixo mostra detalhes dos incidentes de cibercrime do ponto de vista macrorregional, considerando a região LAC (Latin America and Caribbean).

América Latina e Caribe (LAC)

Frequência	535 incidentes, 65 com divulgação de dados confirmada
Principais padrões	Intrusão do sistema, engenharia social e ataques básicos de aplicativos da Web representam 94% das violações
Atores de ameaças	Externo (95%), Interno (5%), Parceiro (2%), Múltiplos (2%) (violações)
Motivos do ator	Financeiro (93), Espionagem (11%), Ideologia (2%) (violações)
Dados comprometidos	Sistema (55%), Interno (32%), Classificado (23%), Credenciais (23%), Outros (19%) (violações)

Fonte: Verizon, 2023

Os governos continuam alertando sobre a ameaça à infraestrutura crítica de agentes afiliados a estados. O gráfico abaixo mostra a evolução dos ataques cibernéticos às infraestruturas críticas nos últimos 10 anos.

Número de ataques de ransomware em infraestrutura crítica em todo o mundo - 2013 a 2023

(Fonte: Howden analysis based on data from Temple University)

(2022).“Critical Infrastructure Ransomware Attacks (CIRA) Dataset”. Version 11.9. Temple University. Online at https://sites.temple.edu/care/ci-rw-attacks/. Funded by National Science Foundation CAREER Award #1453040. ORCID: 0000-0002-6396-1066.

Os pagamentos médios de resgate no início de 2023 foram quase o dobro dos pagos em 2022. 40% das empresas pesquisadas relataram pagamentos de mais de US$ 1 milhão, um aumento significativo se comparado com apenas 11% no ano passado, conforme mostra a figura abaixo. Alguns pedidos extremos de resgate neste ano ultrapassaram a marca de US$ 100 milhões.

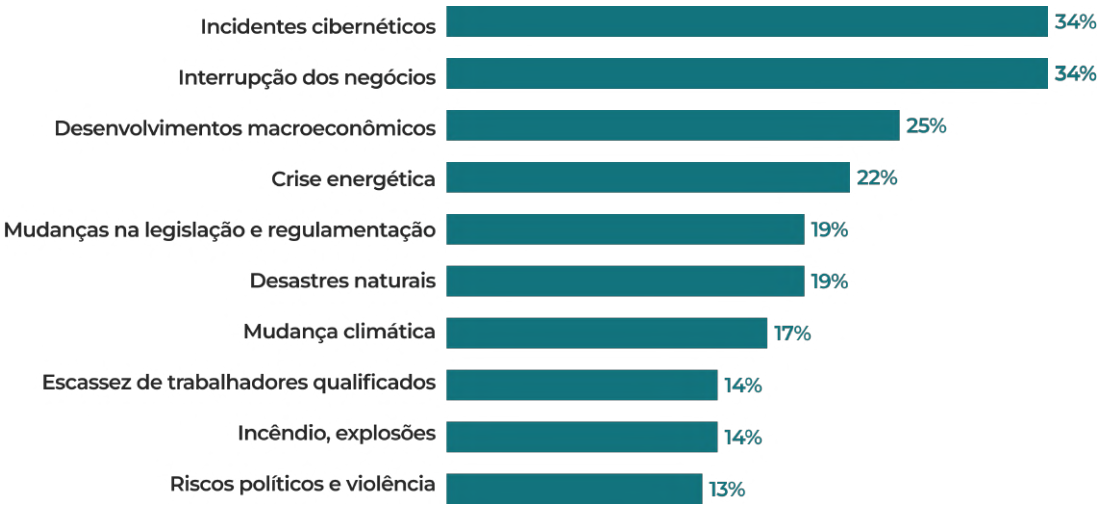
Distribuição dos valores de pagamento de resgate - 2023 vs 2022

(Fonte: Sophos)

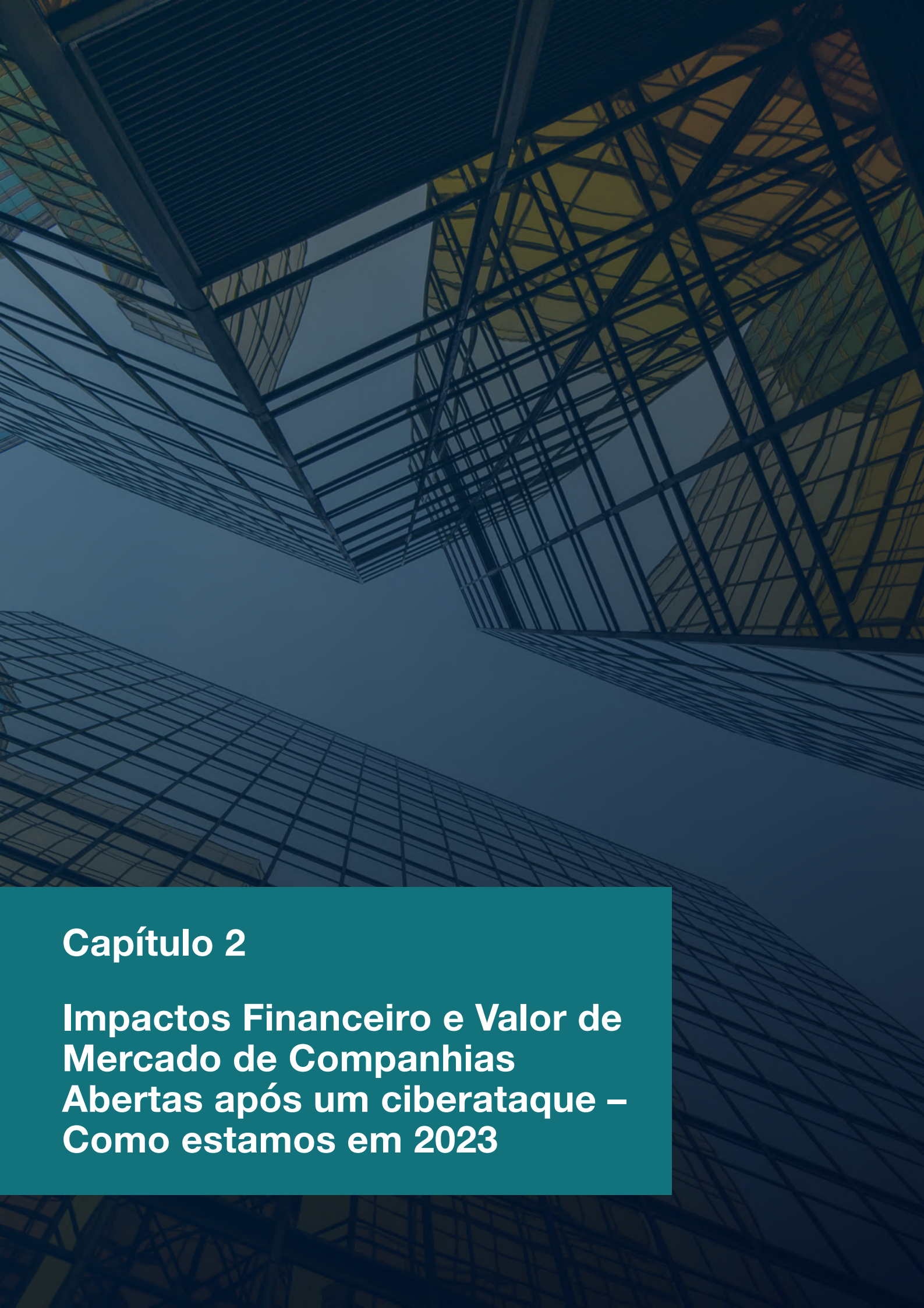
Os executivos continuam classificando os ataques cibernéticos e interrupção dos negócios como dois dos riscos mais significativos enfrentados pelas empresas hoje.

Allianz Risk Barometer 2023

Os números representam a frequência com que um risco foi selecionado como uma porcentagem de todas as respostas da pesquisa de 2.712 entrevistados. Os números não somam 100%, pois todos os entrevistados puderam selecionar até três riscos por setor.



(Fonte: Allianz Global Corporate & Specialty)



Capítulo 2

Impactos Financeiro e Valor de Mercado de Companhias Abertas após um ciberataque – Como estamos em 2023

“Existe aqui uma grande fonte de preocupação com Insider trading em ataques” (Rafael Sasso, Abrasca)

O Security Design Lab (SDL) analisou dois importantes estudos - da Morningstar Sustainalytics[1] e Harvard Business Review[2] - que avaliam o impacto dos incidentes cibernéticos nos preços das ações das empresas de capital aberto ao longo do tempo, comparando o status pré e pós ataque, bem como a projeção do mercado, se não houvesse ocorrido o incidente.

A análise buscou entender e medir 3 grandes pontos, sendo eles: i) o impacto imediato de um incidente nos preços das ações; ii) a influência nos retornos prováveis; e iii) o período que a empresa experimenta sentimento negativo por parte dos investidores.

A primeira conclusão vinda de ambos os estudos é de extrema importância para o Mercado de Capitais: Um incidente cibernético tem grande potencial de afetar o preço das ações de uma organização, especialmente no curto e médio prazos. Segundo o levantamento da Harvard Business Review, as empresas de capital aberto sofreram uma queda média de 7,5% no valor de suas ações após um ataque cibernético, juntamente com uma perda média de capitalização de mercado de US$ 5,4 bilhões.

Outro fato relevante levantado pelo estudo é que esse impacto pode repercutir em toda a cadeia de suprimentos, criando um efeito cascata que pode causar uma perda de até 26 vezes no ecossistema de negócios de uma empresa. Um exemplo, foi o ataque de ransomware à ION Trading Technologies em 31 de janeiro deste ano que fez com que diversas as instituições financeiras, que dependiam da tecnologia para operar, tivessem que realizar as negociações manualmente durante a indisponibilidade, impactando assim, nos resultados. Outro caso de grande repercussão ocorreu em 2020, quando um ataque cibernético, atribuído a hackers militares russos, atingiu a SolarWinds e se espalhou para 18.000 redes de computadores governamentais e privadas, atingindo departamentos de Justiça, Estado, Tesouro, Energia e Comércio dos EUA por nove meses. No Brasil, destacamos o Fleury, um dos maiores laboratórios de exames do país, que foi alvo de dois ataques, sendo o primeiro em 2021 e o segundo em 2023, afetando não apenas os serviços da Companhia, mas a sua cadeia de suprimentos, em especial diversos hospitais que utilizam, prioritariamente, seus serviços. Ou seja, a operação e,

“impacto pode repercutir em toda a cadeia de suprimentos, criando um efeito cascata que pode causar uma perda de até 26 vezes no ecossistema de negócios de uma empresa”

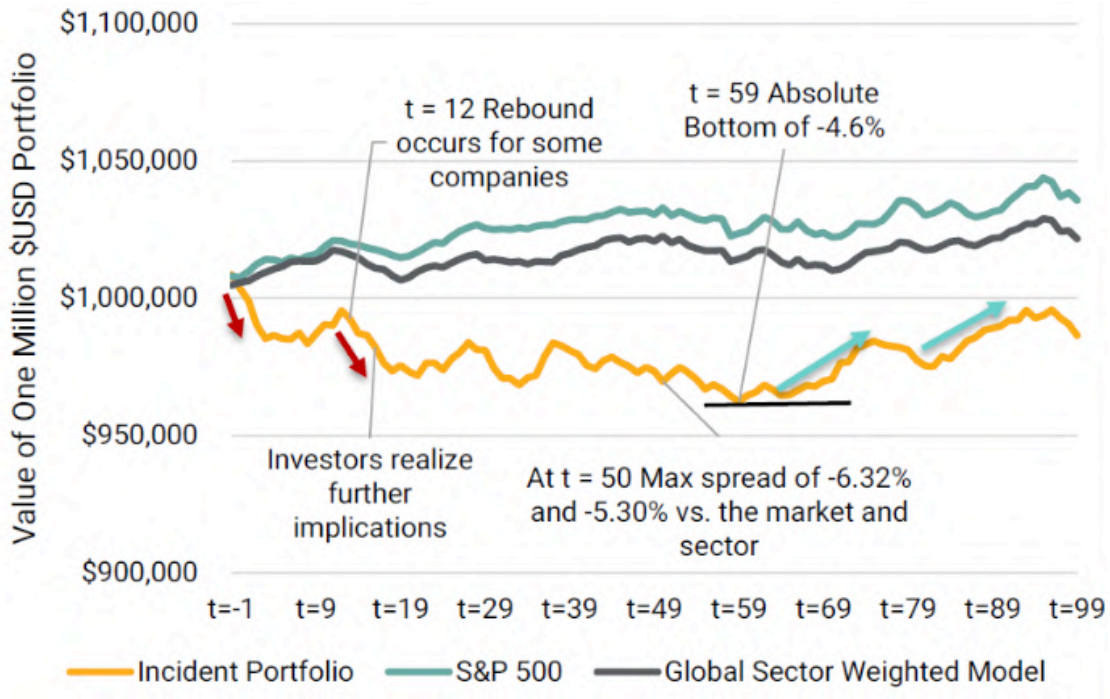
[1] Morningstar Sustainalytics

[2] Harvard Business Review

consequentemente, o valor das ações de uma empresa podem ser afetados, sem que ela seja o alvo direto do ataque cibernético.

No estudo do Morningstar Sustainalytics, foram analisados 69 incidentes de alto impacto em uma escala de tempo. Visando garantir que não houvesse nenhuma interferência de vazamento de informações que pudesse alterar o cenário do estudo. Foi utilizado como base o preço das ações destas empresas em t=-20, ou seja, 20 pregões antes do incidente se tornar público, sendo t=0 a data do comunicado do incidente ao mercado.

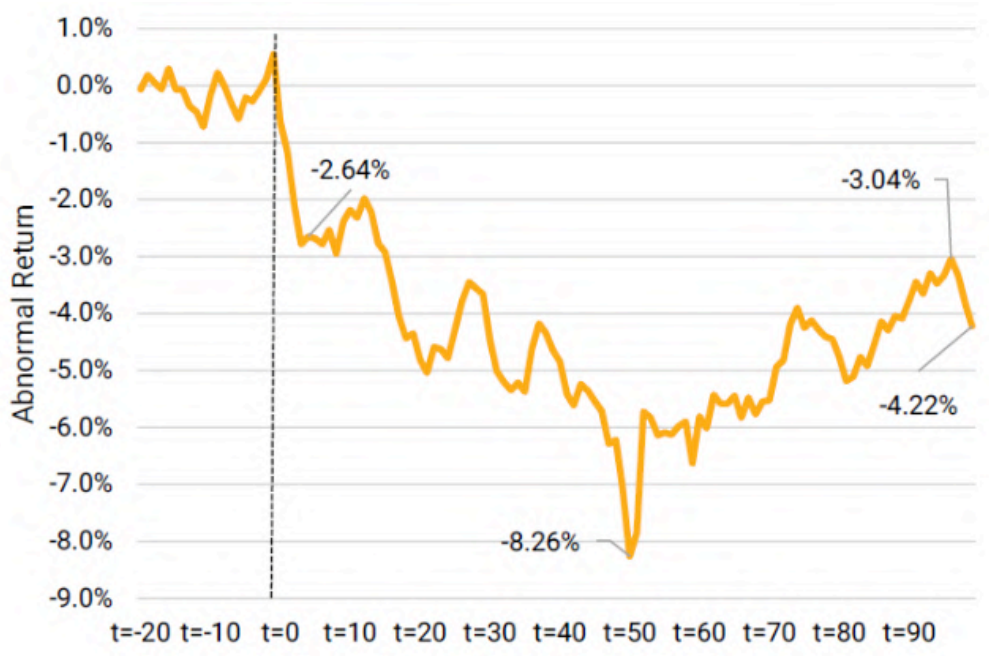
Foi examinada a reação média das ações ao longo de 100 dias de negociação com base em uma análise de série temporal de comunicados de imprensa. O declínio inicial dos preços das ações foi de -2,3% no quarto dia após a data do incidente, chegando ao menor valor no 59° dia após o incidente com -4,6% de queda, conforme mostra o gráfico abaixo.



Série temporal (médio prazo) - Reação do preço das ações a ataques cibernéticos

Fonte: Morningstar Sustainalytics

Verificou-se, ainda, no 51° dia de negociação após o incidente, o maior *spread* entre o preço das ações entre as empresas que sofreram o incidente, sendo -6,32% comparado ao S&P 500 e -5,3% em relação ao portfólio de empresas do mesmo setor, não atingidas por um incidente cibernético.



Retorno Anormal Cumulativo - Igual Ponderação

Fonte: Morningstar Sustainalytics

O gráfico acima mostra que a partir do 51° dia após o incidente marcou o início de um ponto de retomada. Deste ponto em diante - nos próximos 49 dias de negociação até o 100^{0} dia - o retorno médio da empresa foi de 4,9% e os retornos anormais foram de 4,04%, com 54% das empresas experimentando um aumento no preço das ações, com metade das empresas tendo retornos anormais positivos.

Um ano pós ataques, vemos que as empresas que tiveram incidentes ainda estão com movimentos ascendentes tímidos. Notamos os investidores cautelosos para investimentos de longo prazo nestas empresas, já que menos de um terço delas conseguiu acompanhar seus respectivos benchmarks do setor, após este prazo, conclui o estudo.

“menos de um terço delas conseguiu acompanhar seus respectivos benchmarks do setor, após este prazo.”

Devido a relevância e preocupação sobre o tema, a SEC (Securities and Exchange Commission) propôs vários novos regulamentos divididos em 3 regras separadas para entidades de mercado, visando “padronizar” a divulgação do risco de cibersegurança e “melhorar a estabilidade financeira” segundo o presidente da instituição, Gary Gensler. De acordo com as propostas, corretores, empresas de investimento, consultores e outras entidades de mercado seriam obrigados a notificar os clientes cujas informações confidenciais tiveram vazamento, mesmo que tenham (ou provavelmente) sido usadas sem autorização. As notificações teriam que ser no máximo 30 dias após as empresas identificarem o incidente e a SEC deveria ser

notificada por escrito imediatamente, seguido de um relatório mais detalhado em 48 horas.

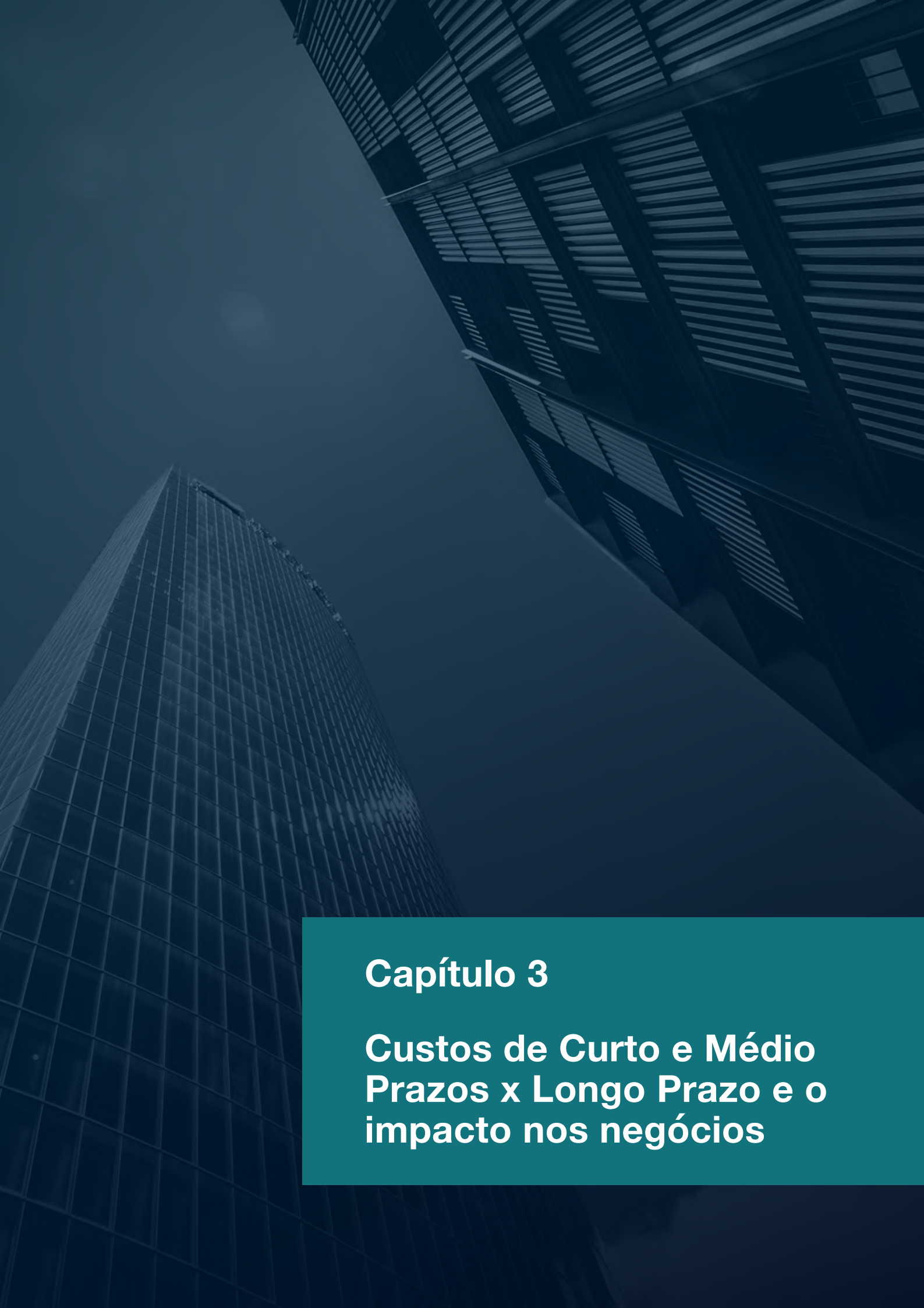
O Jornal Internacional de Contabilidade e Gestão da Informação observa que as intenções dos investidores em investir são maiores quando uma estrutura de risco de segurança cibernética está em vigor, juntamente com boa qualidade da informação e conscientização sobre o tema. Algumas organizações também superam violações de segurança cibernética mostrando sua transparência e confiabilidade. Eles discutem o que fizeram de certo para se preparar para essa eventualidade e depois falam sobre seus planos para melhorá-lo ainda mais.

“as intenções dos investidores em investir são maiores quando uma estrutura de risco de segurança cibernética está em vigor, juntamente com boa qualidade da informação e conscientização sobre o tema.”

Analisando dados específicos em diferentes mercados, vimos que as empresas que sofrem um incidente significativo de violação de dados apresentam desempenho inferior ao índice NASDAQ em 8,6% após um ano do incidente, sendo que essa diferença pode aumentar para 11,9% após dois anos. Quando a Capital One (NYSE:COF) divulgou que sofreu um incidente cibernético, o preço de suas ações, imediatamente, caiu quase 6% nas negociações após o expediente. Nas duas semanas seguintes, o preço das ações despencou quase 14%. Um outro exemplo foi o ataque cibernético sofrido pela Medibank (ASX:MPL) em outubro de 2022 na Austrália. Como resultado, a venda das ações foi suspensa por uma semana. Quando as ações finalmente retornaram ao mercado, o preço despencou 15% e permanece bem abaixo do preço pré-ataque até hoje.

“Analisando dados específicos em diferentes mercados, vimos que as empresas que sofrem um incidente significativo de violação de dados apresentam desempenho inferior ao índice NASDAQ em 8,6% após um ano do incidente, sendo que essa diferença pode aumentar para 11,9% após dois anos.”

No Brasil analisamos casos semelhantes em 2021, onde empresas como Lojas Renner (BVMF:LREN3) e Fleury (BVMF:FLRY3) foram alvos de ataques cibernéticos, afetando, fortemente, os serviços das Companhias. Horas após o incidente os papéis LREN3 apresentavam queda de 1,5% e FLRY3 queda de 2,34%. Recentemente, o Fleury divulgou o seu balanço do primeiro trimestre de 2023, com uma queda de 15% no lucro. Apesar dos números seguidos dos fatos, não podemos afirmar se o segundo ataque cibernético sofrido pela Companhia teve influência neste resultado. Outro caso emblemático foi o ataque ocorrido contra a JBS (BVMF:JBSS3), paralisando diversas plantas da Companhia em vários continentes. Em comunicado, o CEO da JBS USA, Andre Nogueira, confirmou o pagamento de USD 11 milhões aos hackers para retomar as operações.



Capítulo 3

Custos de Curto e Médio Prazos x Longo Prazo e o impacto nos negócios

Além de grande potencial em afetar a competitividade das companhias, a cibersegurança está abrindo um novo capítulo em financiamento e custo de capital, já sendo agregada como parâmetro em processos de Rating e em operações de crédito. Ou seja, diretamente afetando o Mercado de Capitais e os processos de financiamento das companhias.

Impactos de curto, médio e longo prazos

Embora os impactos de curto e médio prazo no valor de mercado de uma empresa sejam expressivos, não podemos desprezar os impactos de longo prazo que podem ser ainda mais importantes, como perda de vantagem competitiva, redução de crédito, aumento no preço dos produtos, entre outros.

"os impactos de longo prazo que podem ser ainda mais importantes, como perda de vantagem competitiva, redução de crédito, aumento no preço dos produtos, entre outros."

Um incidente cibernético consumirá, diretamente, os recursos de uma empresa, levando a um aumento no custo de fazer negócios. Em 2022, o custo médio global de uma violação atingiu US$4,35 milhões. Essas despesas podem incluir, desde pagamentos de resgate e perda de receitas até tempo de inatividade da empresa, remediação, honorários advocatícios e de auditoria, sem considerar os custos intangíveis, como reputação, por exemplo. Os custos de auditoria para as empresas, após um incidente cibernético, podem ser cerca de 13,5% mais altas do que aqueles para empresas que não sofreram violações. Enquanto perdas de milhões de dólares podem levar à falência uma pequena empresa, mas não ter muito efeito sobre uma empresa listada, os invasores geralmente são "inteligentes" o suficiente para causar mais problemas para as empresas maiores.

"Os custos de auditoria para as empresas, após um incidente cibernético, podem ser cerca de 13,5% mais altas do que aqueles para empresas que não sofreram violações."

Segundo dados globais da carteira da corretora de seguros cibernéticos Howden, foram pagos em reinvindicações de incidentes cyber relacionados a Ransomware cerca de £40M nos últimos três anos – R$247M, tendo o setor de saúde como o mais afetado, seguido por empresas de varejo, finanças e serviços.

Em 2020, considerando os eventos acumulados, além de ransomware a relação sinistralidade/prêmios literalmente explodiu para atingir os 190%, o que resultou em pagamento de €201,5M em compensação a clientes, enquanto foram coletados apenas €105,9M em prêmio. No Brasil, os incidentes em que foram acionadas apólices de seguros, tiveram o pagamento de despesas entre R$2M e R$65M, frente as reinvindicações junto ao mercado local. Embora seja sabido que houve incidentes em que valores superaram os segurados pelas apólices – já que, diferente de ativos físicos, o limite estabelecido vai de acordo com apetite de risco da empresa tomadora. O mercado declarou perdas de US$63.941.060 segundo a SUSEP em 2022.

Essas perdas podem ser repassadas aos clientes e investidores, limitando a capacidade da empresa de manter sua posição no mercado. Por exemplo, 60% das organizações que sofreram violações de dados aumentaram os preços de seus produtos e serviços.

“60% das organizações que sofreram violações de dados aumentaram os preços de seus produtos e serviços.”

Os fatores citados anteriormente precisam ser considerados pela alta gestão e conselho das companhias, segundo a regra publicada pela SEC recentemente, que vigorará a partir de setembro de 2023 para todos os registrantes. A implementação de gestão de risco de segurança cibernética, juntamente com estratégias e práticas de governança, divulgação de incidentes, podem afetar sua reputação e preço das ações; e ainda, exercer uma análise de materialidade que não deve ser apenas com base estimativas "mecânicas" e nem deve ser baseada apenas em uma análise quantitativa de um incidente de segurança cibernética, mas sim do conjunto de fatores.

Riscos cibernéticos podem resultar em um rebaixamento da classificação de crédito, afetando a capacidade e o custo de uma empresa para garantir financiamento. Por exemplo, empresas com baixa maturidade de segurança cibernética e carentes de boas práticas, tendem a enfrentar custos de empréstimos mais altos e maior risco

"Riscos cibernéticos podem resultar em um rebaixamento da classificação de crédito, afetando a capacidade e o custo de uma empresa para garantir financiamento."

financeiro, já que a Moody's anunciou em 2018 que avaliaria as práticas de segurança cibernética das empresas ao atribuir classificações de crédito. De fato, a Moody's reduziu a classificação de crédito da Equifax em 2019 após o incidente cibernético que a Equifax sofreu em 2017.

Capítulo 4

Entendimento e Prevenção

Entre as empresas de Capital Aberto afetadas pelos incidentes cibernéticos, notamos que as que implementaram iniciativas de proteção estavam mais bem preparadas para resistir. Em média, as empresas que apresentavam maior conformidade com as

> “notamos que as que implementaram iniciativas de proteção contra os ataques cibernéticos, estavam mais bem preparadas para resistir. Em média, as empresas que estavam em melhor conformidade com as melhores práticas, políticas de segurança e Lei Geral de Proteção de Dados, mantiveram o ritmo de seu benchmark do setor um ano depois.”

melhores práticas, políticas de segurança e Lei Geral de Proteção de Dados, mantiveram o ritmo de seu benchmark do setor um ano depois. Por outro lado, aquelas com baixo nível de conformidade, tiveram um desempenho significativamente inferior. Em média, o grupo de empresas com altos índices de

> “Em média, o grupo de empresas com altos índices de conformidade experimentou um declínio máximo médio de 62% menor do que as empresas com baixo nível de conformidade.”

conformidade experimentou um declínio máximo médio de 62% menor do que as empresas com baixo nível de conformidade. É importante notar que estar em conformidade com a LGPD não endereça todos os riscos digitais enfrentados por uma organização, especialmente aquelas que possuem dependência operacional em ambientes interconectados de automação – como indústrias, setor elétrico, saneamento. No ano de 2022, houve um aumento de 86% dos ataques voltados a sistemas operacionais, o que trouxe um grande acúmulo de perdas a diversos setores.

As ameaças cibernéticas em sistemas de controle industrial tem se tornado frequentes, e empresas que negligenciam ações proativas de segurança tem sido eleitas como alvo dos criminosos, afetando toda a cadeia de suprimentos. Assim como na adequação à LGPD, há um custo financeiro associado a essa priorização e implementação proativa. A avaliação de riscos, a identificação do cenário de ameaças em constante mudança e crescimento, bem como a colocação de medidas para prevenir e mitigar são cada vez mais caras para as empresas. Especialmente considerando uma abordagem proativa, onde as ameaças podem não se traduzir exatamente em realidade.

Alternativamente, uma abordagem reativa pode ser mais custosa, pois informações e sistemas críticos podem ser comprometidos, corrompidos ou, por fim, destruídos. Por exemplo, considere um ataque de ransomware, em que empresas e usuários ficam à mercê dos invasores. Ataques a sistemas *on premise* podem causar danos físicos a equipamentos críticos. O ambiente físico em torno desses sistemas pode ser afetado, por exemplo, no caso de um incêndio. Reputações manchadas podem levar à redução de lucros, e ações judiciais podem resultar desse tipo de ataque com base

na falha na proteção de dados ou na recuperação de violações que terminam em ações regulatórias. Além disso, a resposta a incidentes pode ser cara, dependendo da urgência e gravidade do ataque.

Hoje, todas as empresas, independentemente do ramo que atuam, possuem a dependência de algum tipo tecnologia. No entanto, os investimentos voltados ao gerenciamento deste crescente risco ainda são vistos como um custo e não como necessidade e até mesmo investimento. Empresas não hesitam em investir em ações de mitigação em relação a impactos que se originam no ambiente físico, então porque não investir em ações preventivas? Quando falamos em riscos tradicionais como chance de incêndio, roubo ou uma quebra de equipamento, há investimentos sendo feitos na prevenção e até mesmo na adoção de seguros para minimizar os impactos financeiros.

Por isso, ambientes onde há controle sob o risco cibernético, por meio da implementação das melhores práticas de segurança geram maior conformidade e, consequentemente, melhor preparação para limitar dados de possíveis ataques, mantendo a confiança dos investidores.

Segundo dados da corretora Howden, em uma análise de comparativo de severidade de incidentes, empresas que investem em ferramentas de proteção como MFA (Multi Factor Authentication) podem ter 8% de redução do impacto financeiro de um incidente, assim como aquelas que possuem uma ferramenta de EDR em 10%.

Por fim, o risco de ataque cibernético é um dos riscos ESG mais imediatos e financeiramente relevantes e que devem ser analisados a fundo pelas empresas, em especial, pelos Conselhos de Administração e Executivos. A crescente frequência e gravidade dos incidentes cibernéticos exigem ações rápidas, efetivas e constantes. O primeiro grande passo são os administradores entenderem qual o nível de conformidade das suas empresas em relação as melhores práticas, políticas de segurança e lei geral de proteção de dados e, com base nisso, iniciarem discussões para implementação de um plano de ação. O entendimento desta maturidade pelos administradores ajuda muito na tomada de decisão.

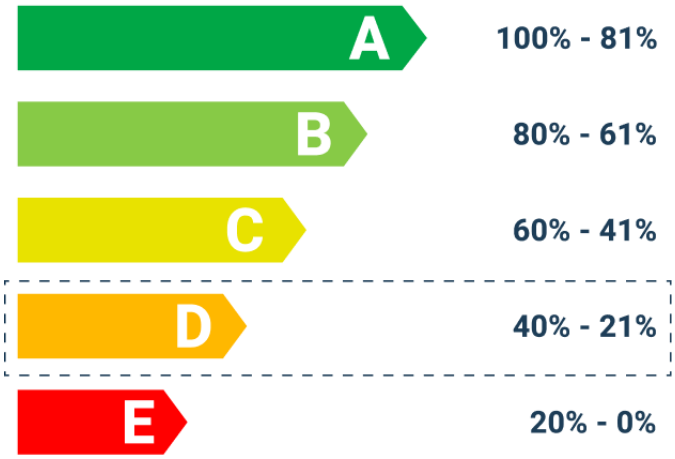
> “O risco cibernético não é mais um problema, exclusivo, das áreas técnicas, mas sim um problema Corporativo. A redução da área de exposição das Companhias requer ações coordenadas, que envolvam diversas áreas da empresa, incluindo TI, Segurança da informação, Comitê de Risco, C-Level e Conselho de Administração. A coordenação das ações deve ser realizada pelas áreas de Compliance, devido a multidisciplinaridade que o tema exige.”

Capítulo 5

A Pesquisa

Metodologia *Cyber Score*

Introdução



O **Cyber Score** é uma metodologia que foi criada numa linguagem adequada para que Investidores, Conselheiros e altos Executivos possam entender o nível de conformidade de suas Companhias, em relação as melhores práticas e políticas de segurança mundiais, bem como acompanhar a evolução delas a cada novos controles adotados pelas áreas técnicas para mitigar os riscos.

O **Cyber Score** utiliza, como base, as regulações e melhores práticas e políticas de segurança que são publicadas pelas mais respeitadas agências e organizações mundiais definidoras de regulações e padrões, tais como: NIST, ANSSI, ETSI, FIDO, SEC, ENISA, entre outras. Os assessments são gerados a partir das publicações destas agências e organizações.

A equipe do SDL e seus parceiros desenvolvem os assessments que visam compreender este nível de maturidade, que será traduzido no **Cyber Score**. As perguntas que compõem os assessments são extraídas de um ou mais documentos publicados pelos principais órgãos reguladores ou entidades definidoras de padrões, sendo esta definição realizada a partir de um escopo prévio definido, com base no objetivo do assessment.

O **Cyber Score** permite que as Companhias meçam o nível de maturidade e risco em cibersegurança. A avaliação pode ser no nível da Companhia ou de um determinado produto, sistema ou solução.

A Metodologia

A metodologia é composta por 7 fases, sendo elas:

Fase 1 – Definição do Escopo e Pesquisa das Fontes

As perguntas que compõem um *assessment* são extraídas de um ou mais documentos publicados pelos órgãos reguladores ou entidades definidoras de padrões, sendo esta definição realizada a partir de um escopo prévio definido por nossa equipe, com base no objetivo do *assessment*.

Fase 2 – Definição das Fontes que serão utilizadas no *Assessment*

Uma vez cobertos todos os itens do escopo, inicia-se a segunda fase do trabalho, que visa a definição de quais documentos serão utilizados como fonte de dados para a construção do *assessment*. Esta fase consiste em analisar cada documento e verificar qual a melhor ou as melhores fontes para compor cada item do escopo. Uma vez encontradas uma ou mais fontes que abranjam integralmente um determinado item do escopo, dá-se preferência a sua utilização em detrimento das demais. Quando não se encontra uma única fonte que abranja um determinado item do escopo, opta-se por utilizar mais de uma fonte, para garantir a cobertura completa do item.

Fase 3 – Extração do conteúdo de cada fonte

Tendo definido os documentos que serão utilizados, inicia-se a fase 3, que visa extrair as perguntas a serem utilizadas no *assessment*. Extrai-se todas as recomendações e melhores práticas e transforma-se os controles em um questionário, para facilitar o preenchimento do *assessment*. As questões são alocadas dentro de cada item do escopo, compondo a primeira base de dados do *assessment*.

Fase 4 – Inserções de perguntas adicionais

Finalizada a extração das perguntas de cada item do escopo, inicia-se a fase de análise do conteúdo. Nesta etapa verifica-se se a coleta de informações, que auxiliam na análise subjetiva. O objetivo é verificar a possível ausência de perguntas intermediárias e não pontuáveis para o *Cyber Score*, que auxiliam o entendimento na análise do *assessment*. Havendo a necessidade de incluir estas perguntas intermediárias, elas serão extraídas de outros documentos ou geradas pela equipe do SDL, facilitando o preenchimento e entendimento sobre o *assessment*, proporcionando maior fluidez nas avaliações.

Fase 5 – Definição das questões pontuáveis

Finalizada a construção do questionário, inicia-se a etapa para definir a quais perguntas serão atribuídas notas para compor o *Cyber Score,* bem como as perguntas que não serão atribuídas notas, sendo estas usadas apenas para facilitar o entendimento.

Fase 6 – Definição do nível de Criticidade de cada controle

Definidas as questões pontuáveis, inicia-se a etapa de separação das questões por nível de criticidade de cada controle. As questões são separadas em 3 grupos com base na importância de cada controle:

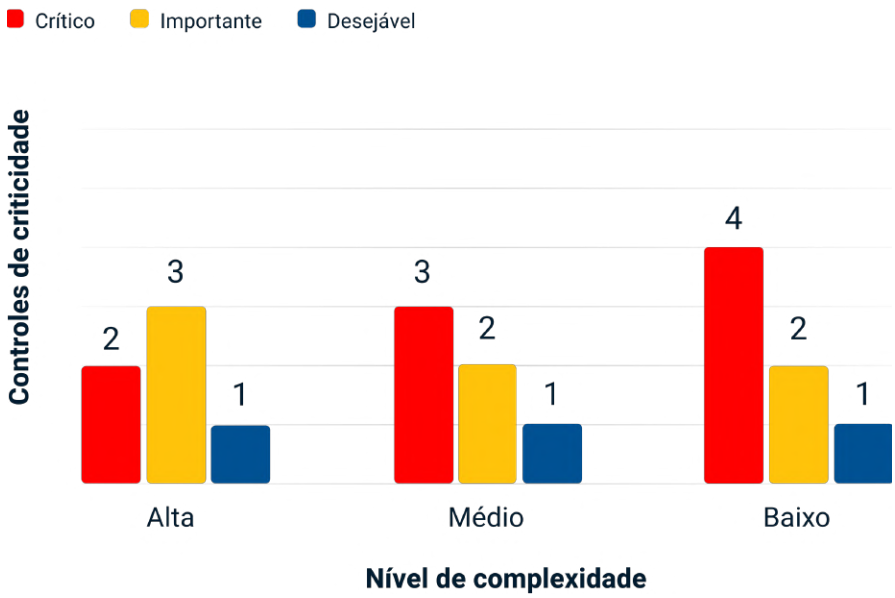
· **Controles Críticos**: são aqueles que, se não implementados, tem potencial de afetar a continuidade do negócio e/ou causar um grande dano/prejuízo à operação e/ou causar enormes danos financeiros a Companhia e acionistas;

· **Controles Importantes**: são aqueles que, se não implementados, podem causar danos financeiros médios e/ou causar danos de imagem e/ou afetar terceiros de maneira substancial e/ou gerar multas de reguladores;

· **Controles Desejáveis**: são aqueles que, se não implementados, podem causar prejuízos pontuais a operação e/ou causar danos financeiros pequenos.

Fase 7 – Definição do nível de Complexidade para Implementação de cada Controle

A próxima etapa é a definição do nível de complexidade para implementar cada um dos controles. Importante compreender que, uma vez classificado como crítico, não necessariamente um controle possui alto nível de complexidade para ser implementado; esta não é a base para a análise. Esta definição é feita, literalmente, de acordo com a dificuldade de implementá-lo, levando-se em conta os fatores como tempo, esforço, time e habilidades técnicas. Considerando esta definição, os controles recebem 3 níveis de complexidade de implementação:



· **Alta Complexidade**: são aqueles controles, cuja implementação não é simples, pois requerem mudanças na estrutura de tecnologia e/ou alteram a regra de negócios e/ou requerem uma política de uso complexa e/ou tem um prazo de implementação elevado e/ou requerem um time experiente e com habilidades específicas para realizar a entrega;

· **Média Complexidade**: são aqueles controles, cuja implementação requer menos esforço, pois não requerem mudanças significativas na estrutura de tecnologia e/ou não alteram regras de negócios e/ou não requerem uma política de uso de complexa e/ou prazo de implementação não é tão elevado e/ou requerem um time com experiência intermediária e habilidades específicas para realizar a entrega;

· **Baixa Complexidade**: são aqueles controles, cuja implementação é simples, pois requerem mínimas mudanças na estrutura de tecnologia e/ou não alteram regras de negócios e/ou requerem uma política de uso simples e/ou prazo de implementação é baixo, e/ou requerem um time com habilidades básicas para realizar a entrega.

A Pesquisa

A Pesquisa Setorial em Cibersegurança, realizada pela **Abrasca**, coletou dados entre 10 de maio e 11 de agosto de 2023. Mais de 150 empresas preencheram a pesquisa, sendo que os resultados aqui apresentados contam com apenas os dados de 109 empresas de capital aberto, conforme o foco da pesquisa.

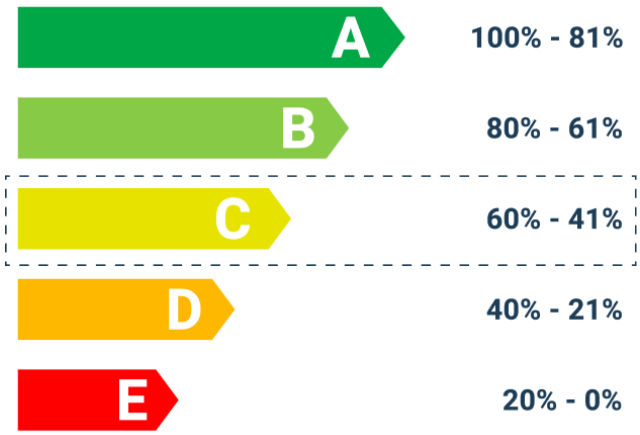
A metodologia utilizada é o **Cyber Score** desenvolvido pelo SDL, que baseia-se em múltiplos guias, regulações e documentos de melhores práticas e políticas, recomendadas pelas principais agências mundiais de cibersegurança. Ao todo foram coletadas informações de 89 controles, divididos em 12 seções. Os controles abrangem 3 grandes pilares, sendo eles: tecnologia, processo e pessoas (RH).

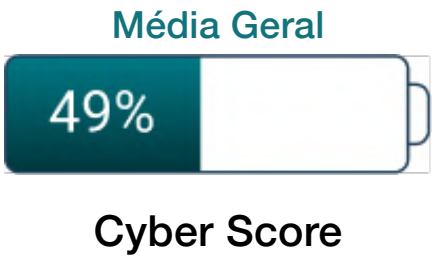
O processo e relatório privado do **Cyber Score** visa possibilitar às Companhias entenderem o seu nível de conformidade em relação as melhores práticas e políticas de segurança, permitindo, em especial, aos administradores (C-Level e Conselheiros de Administração) e pessoas não técnicas, entenderem, numa visão gerencial, o grau de maturidade e desafios de cibersegurança de suas companhias.

As companhias participantes receberam seu relatório privado e os dados anonimizados foram usados para o resultado deste relatório.

Resultados

A média geral do Cyber Score das 109 empresas de capital aberto participantes ficou em 49%, demonstrando muito espaço para melhoras mas um cenário não destoante das informações e pesquisas globais.

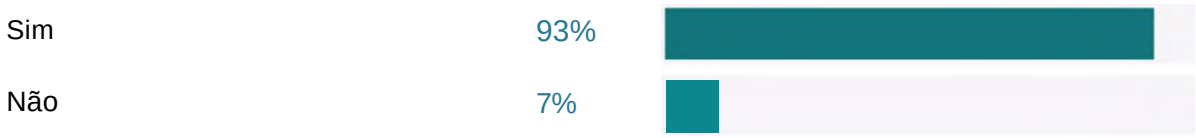




Respostas ao questionário

Seção Introdutória

1. Sua organização possui algum mecanismo para detectar ataques cibernéticos?



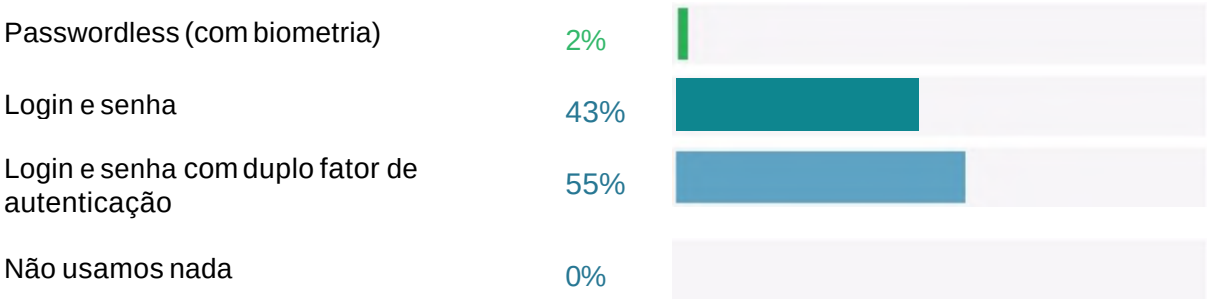
2. Se existirem mecanismos de detecção, você consegue estimar quantos ataques cibernéticos sua organização sofreu no último trimestre ou ano?

Seção 1 - Identificação, Autenticação, e Provedores de Identidade

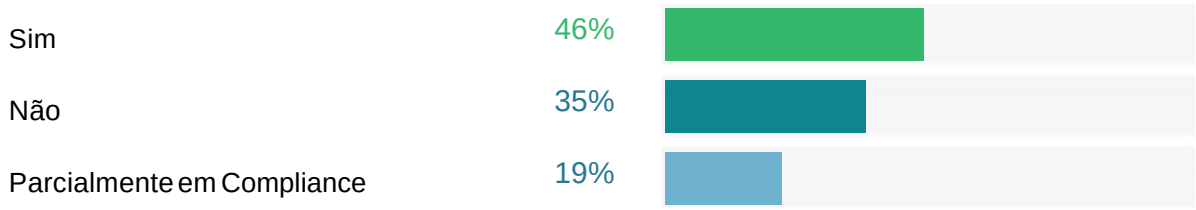
Autenticação é o processo de verificação da identidade de um usuário ou sistema. Os provedores de identidade (IdPs) são entidades confiáveis que gerenciam e autenticam identidades de usuários, desempenhando um papel fundamental nesse processo. Os IdPs oferecem uma forma segura e centralizada de confirmar as identidades dos usuários, garantindo que o acesso a vários serviços e aplicativos seja concedido apenas a indivíduos autorizados.

Os provedores de autenticação e identidade são essenciais para estratégias modernas de segurança cibernética. Eles simplificam o acesso, aumentam a segurança e proporcionam uma experiência de usuário perfeita no cenário digital interconectado de hoje.

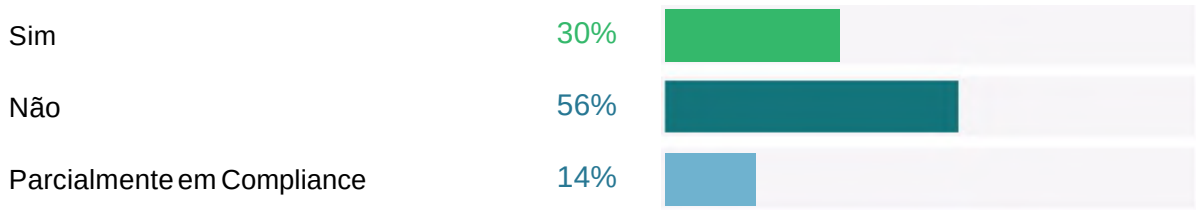
3. Como seus usuários se autenticam em sistemas e dispositivos críticos?



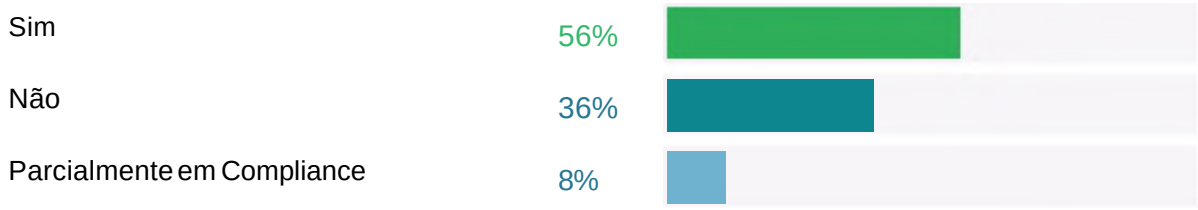
4. Sua organização usa MFA (Autenticação de Múltiplos Fatores) ou 2FA (Segundo Fator de Autenticação) para sistemas e dispositivos não críticos?



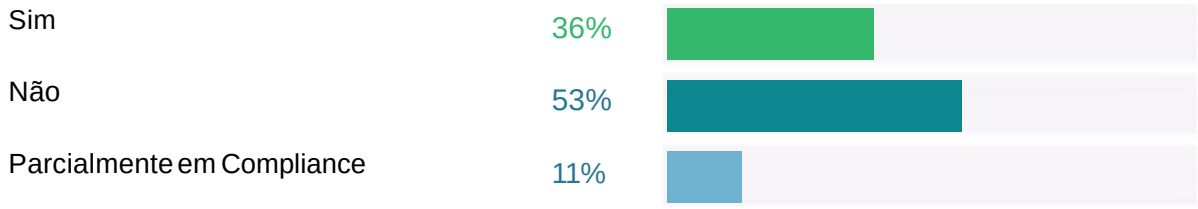
5. Sua organização usa autenticação baseada em risco? Por exemplo, uma combinação de fatores como endereço IP, informação do dispositivo, ou localização?



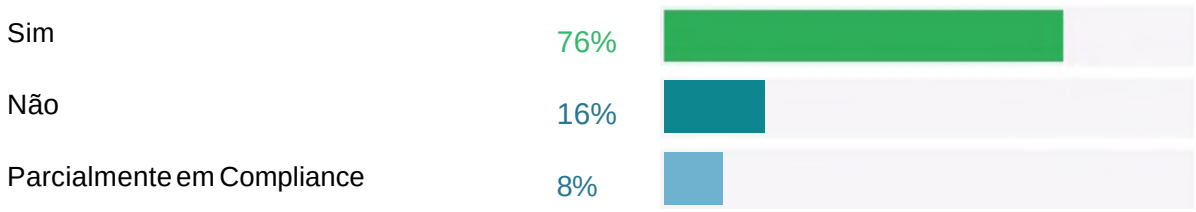
6. Sua organização implementa políticas de expiração de conta?



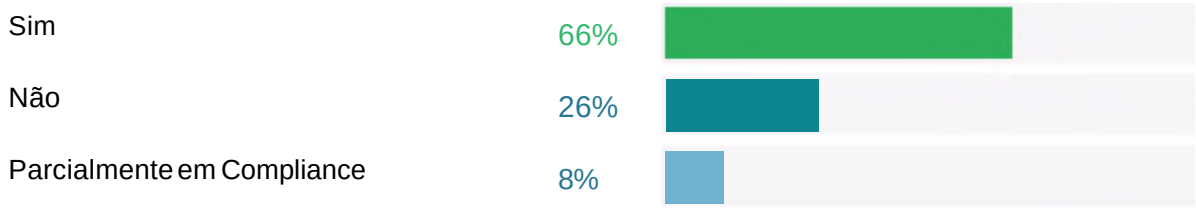
7. As contas de serviço podem ser uma fonte de problemas de segurança cibernética. Diante disso, sua organização possui alguma ferramenta para gerenciar contas de serviço?



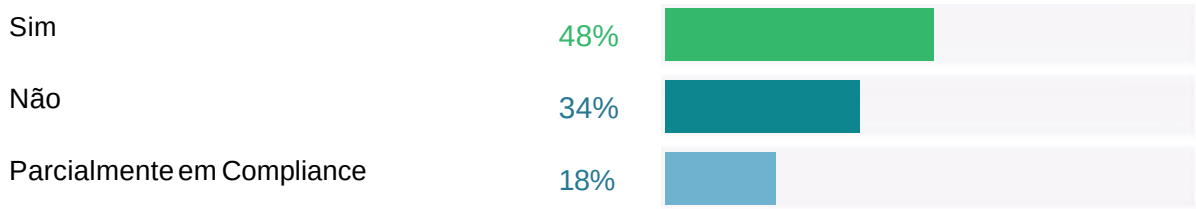
8. Sua organização possui processos e métodos para revogação de credenciais?



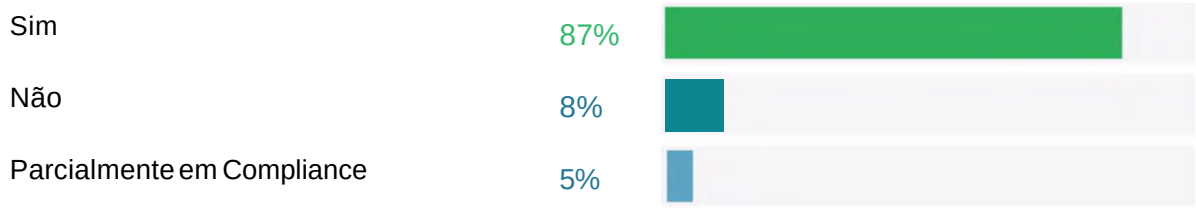
9. Sua organização tem controle sobre as credenciais revogadas, de forma que seja possível realizar auditorias?



10. Seus sistemas implementam reautenticação em alguns eventos, como mudança de credenciais ou papéis, quando ocorrem mudanças de categorias em sistemas, quando da execução de funções privilegiadas, após um espaço de tempo determinado ou periodicamente?



11. Sua organização identifica o status (papel) do usuário (força de trabalho, terceiro, temporário, etc.)?

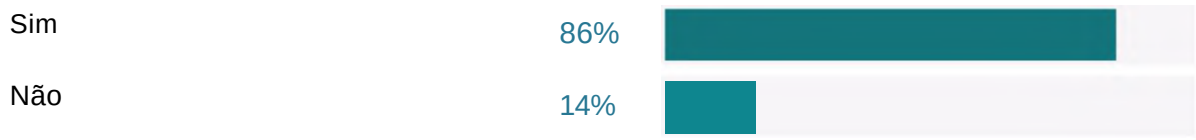


Seção 2 - Nuvem, On-premises e Controle de Acessos

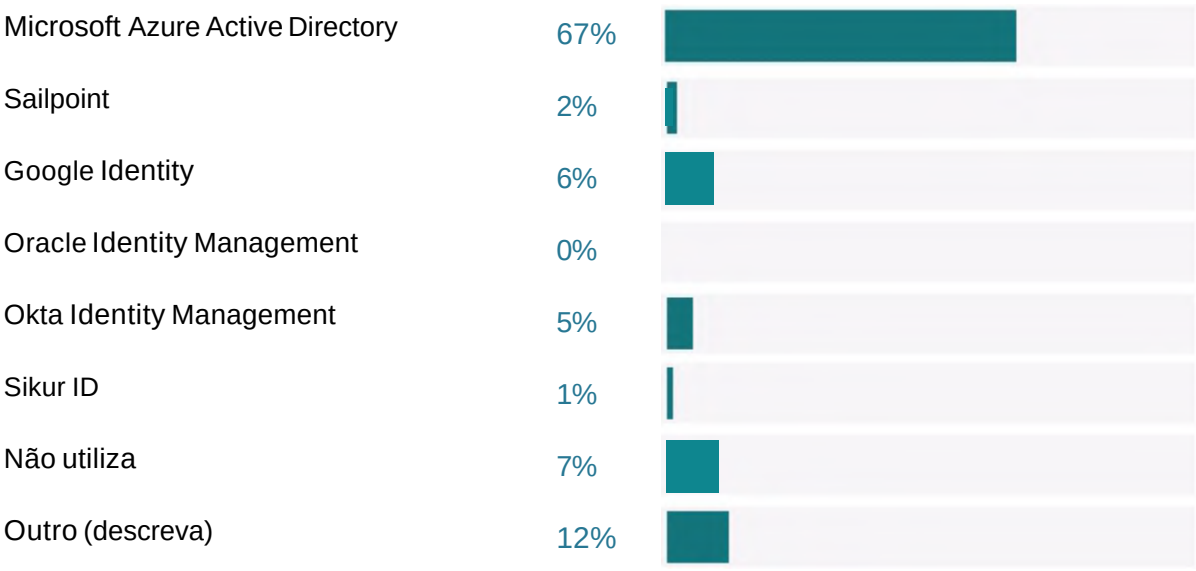
Em vez de possuir e manter infraestrutura e servidores físicos, as organizações agora podem acessar recursos de computação pela Internet por meio de provedores de serviços em nuvem. Este modelo permite flexibilidade, agilidade e eficiência na implantação de aplicativos e no gerenciamento de dados. Com a nuvem, as empresas podem aumentar ou diminuir suas operações conforme necessário, reduzindo despesas de capital e liberando recursos para outras aplicações.

O controle de acesso é um componente fundamental dos sistemas de segurança que regula quem pode acessar recursos, dados ou áreas específicas. Serve como uma barreira protetora contra acesso não autorizado, garantindo que apenas indivíduos ou sistemas autorizados possam entrar ou utilizar determinados ativos. Os mecanismos de controle de acesso incluem autenticação (verificação de identidade) e autorização (determinação de permissões). Esta prática crítica de segurança é vital para proteger informações, ativos e ambientes digitais confidenciais, servindo como pedra angular das estratégias modernas de segurança cibernética.

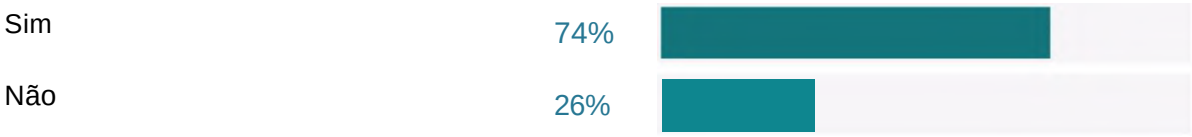
12. Sua organização possui infraestrutura local?



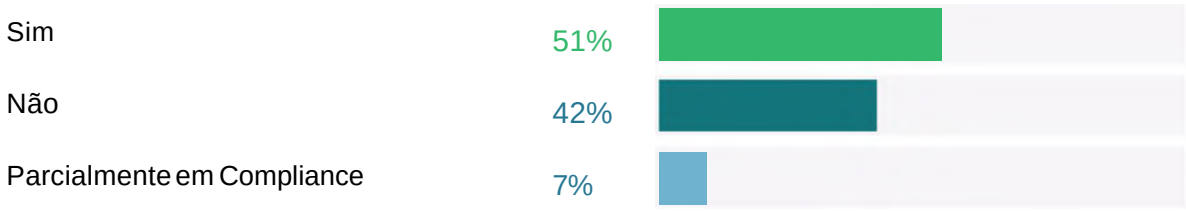
13. Sua organização usa algum desses provedores de identidade?



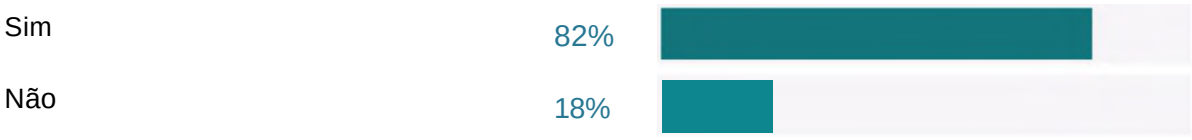
14. Existe algum sistema próprio baseado em nuvem acessível através da web?



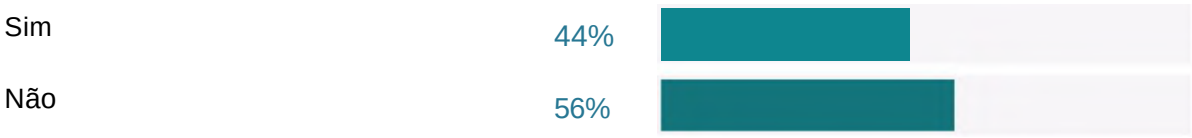
15. Sua organização tem um inventário de nuvem?



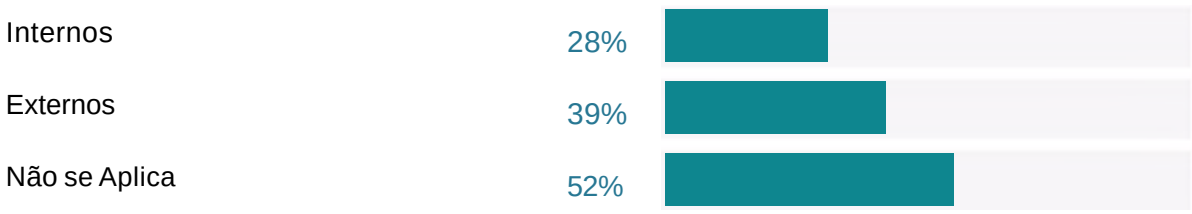
16. Sua organização controla, de alguma forma (com equipe própria ou terceiros),os sistemas internos e o desenvolvimento de aplicativos?



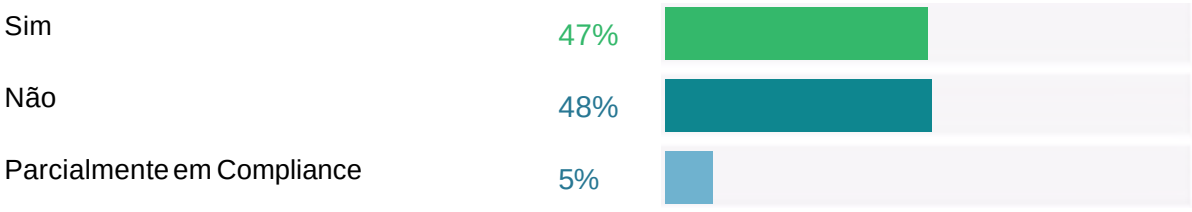
17. Sua organização possui aplicativos móveis publicados nas App Stores?



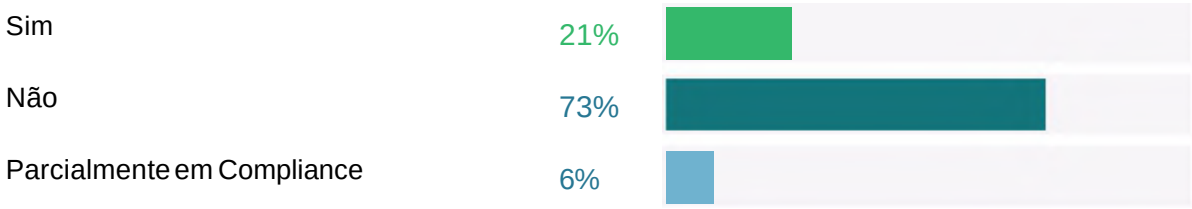
18. Tendo apps móveis, eles atendem os clientes externos da organização ou são de uso interno?



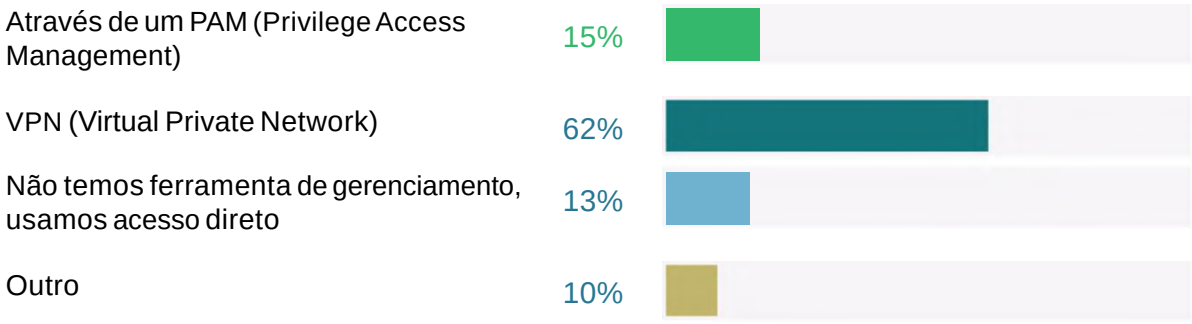
19. A organização possui um sistema centralizado de gerenciamento de acesso (acesso privilegiado) para sistemas críticos de TI?



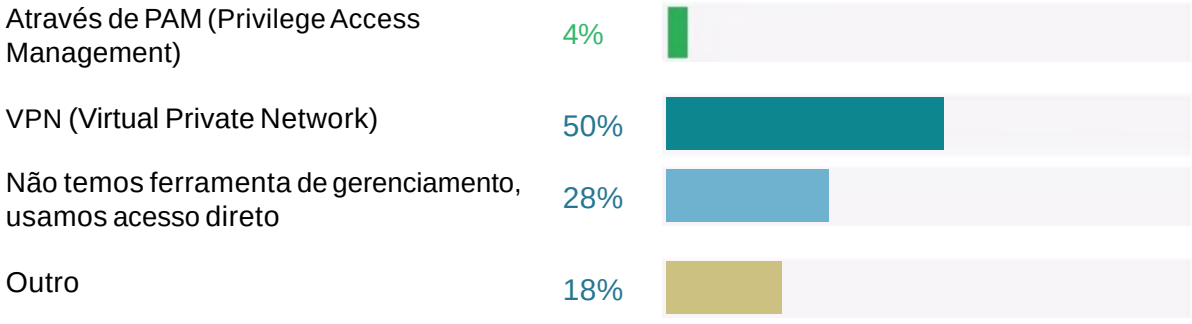
20. Sua organização possui um sistema centralizado de gestão de acesso privilegiado (PAM - Privileged Access Management) para sistemas de OT (Tecnologia Operacional) ou ICS (Sistemas de Controle Industrial)?



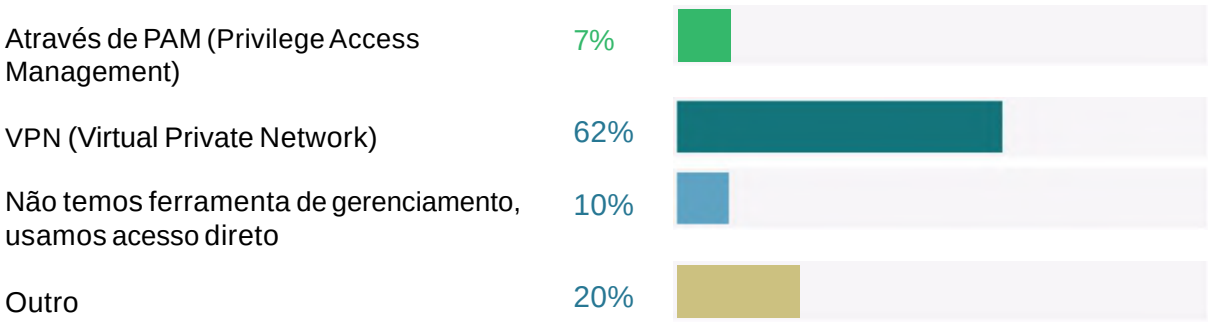
21. Como o time de TI da sua organização gerencia remotamente a infraestrutura local ou em nuvem?(Sistemas de Controle Industrial)?



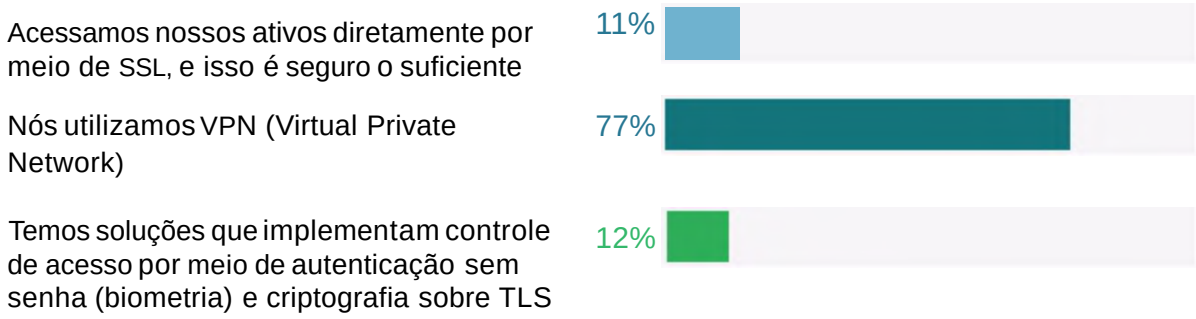
22. Os funcionários (força de trabalho) têm acesso a sistemas em nuvem? Se sim, descreva como.



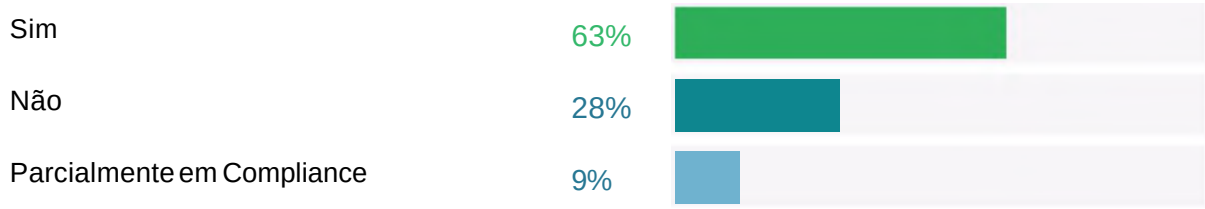
23. Como a organização gerencia o acesso de terceiros (cadeia de suprimentos) a sistemas e recursos privados?



24. Como o acesso remoto (para gerenciamento de TI ou força de trabalho) geralmente ocorre por meio de uma rede não segura, como sua organização evita ataques comuns como MiTM (Man-in-The-Middle) e Phishing, (ou outros tipos de ataques) ?



25. Ao planejar políticas de acesso remoto, sua organização presume que não se pode confiar em dispositivos de clientes, que a sua rede não é segura, ou ainda, pode estar infectada por malware?

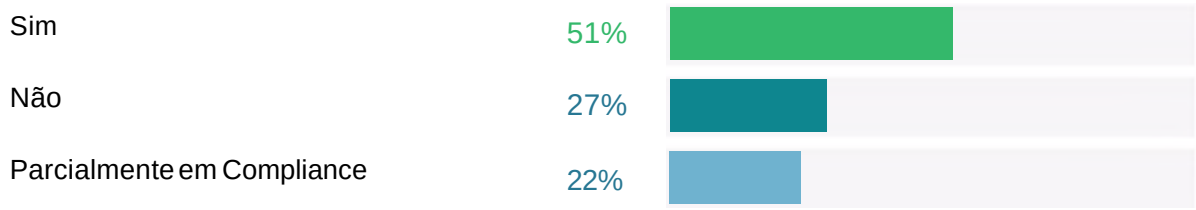


Seção 3 - Mecanismos de Auditoria

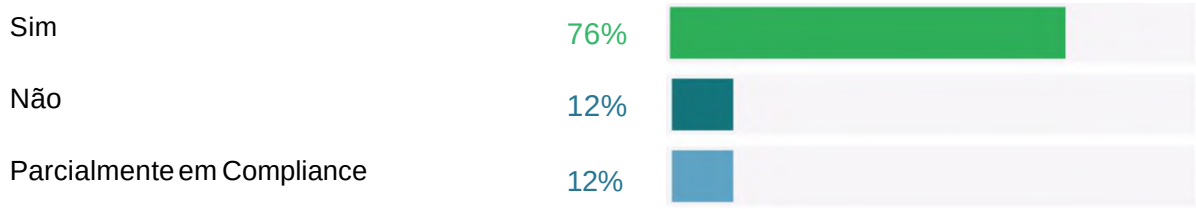
Os mecanismos de auditoria fornecem informações cruciais sobre quem fez o quê, quando e por que, tornando possível investigar incidentes, avaliar riscos e melhorar a eficiência operacional global. Desempenham um papel fundamental no reforço da segurança cibernética, da governança e da responsabilização, permitindo que as organizações protejam os seus ativos e mantenham a confiança das partes interessadas.

Além disso, são indispensáveis no atual ambiente orientado por dados e em conformidade com as regulamentações, servindo como uma ferramenta vital para manter a segurança e a responsabilização.

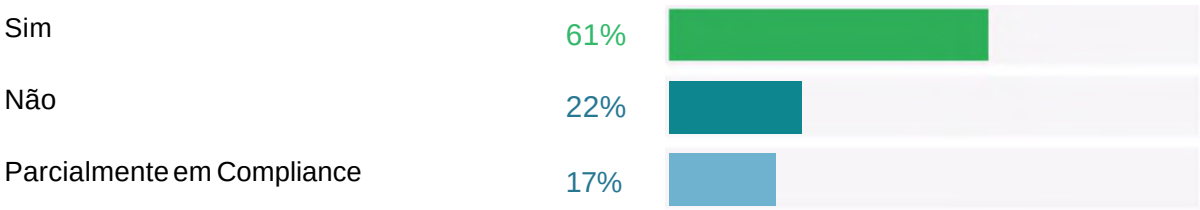
26. Sua organização possui documentação bem definida para processos, funções, escopos, responsabilidades, compromisso de gerenciamento, conformidade?



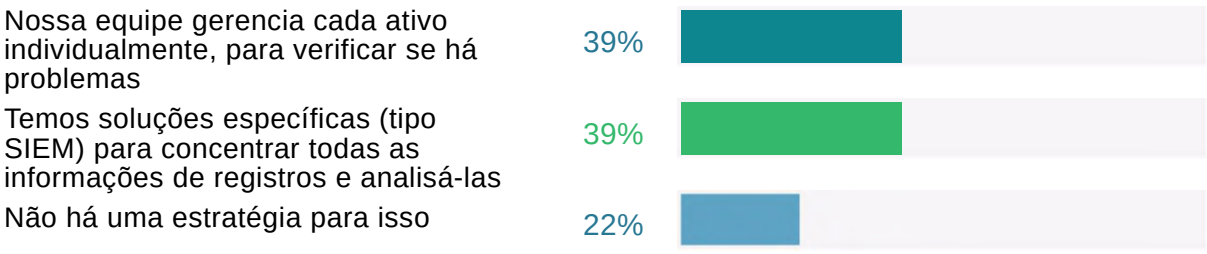
27. Sua organização tem conhecimento de quais sistemas podem gerar logs para uma auditoria posterior?



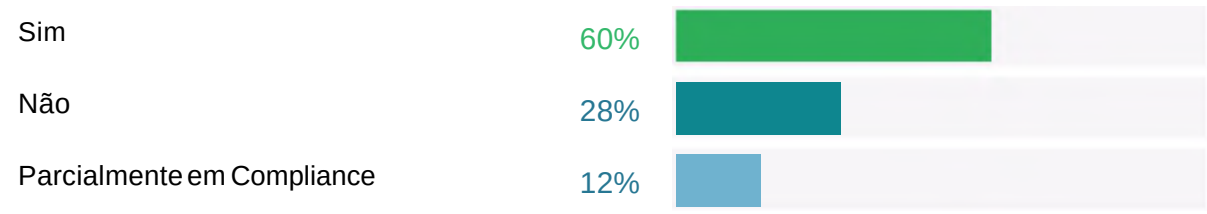
28. Ao definir quais sistemas podem gerar logs, você consegue dizer se as informações coletadas identificam investigações posteriores para problemas de segurança?



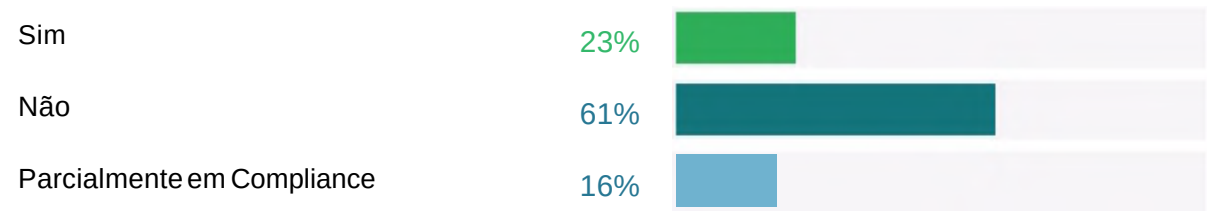
29. Como sua organização gerencia informações de log para auditoria posterior?



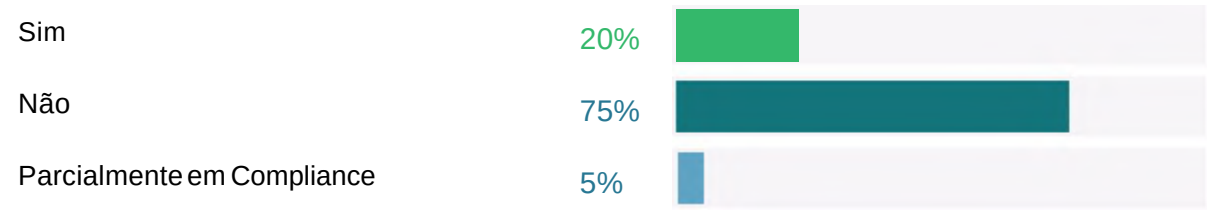
30. Sua organização possui mecanismos para controlar o acesso a logs e informações de auditoria?



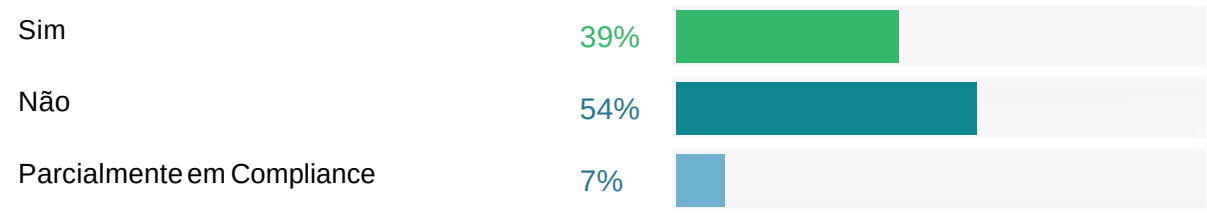
31. No processo de auditoria, sua organização implanta mecanismos de não-repúdio?



32. Sua organização implementa recursos de gravação de sessão (keylloger, gravação de sessão de vídeo, etc.) para ativos críticos de forma seletiva?



33. Sua organização possui dashboards para dar suporte ao processo de análise de dados de auditoria?

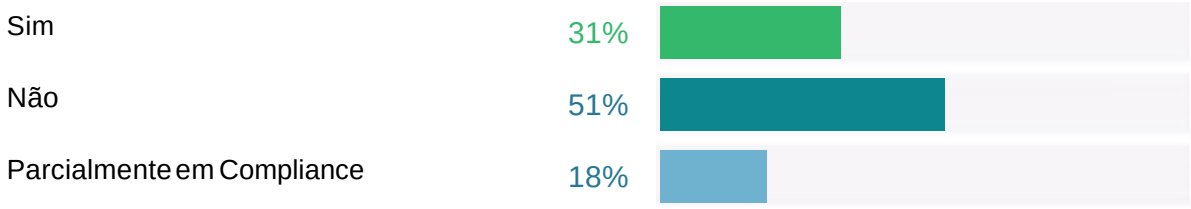


Seção 4 - Continuidade de Negócios, Backup e Disaster Recovery

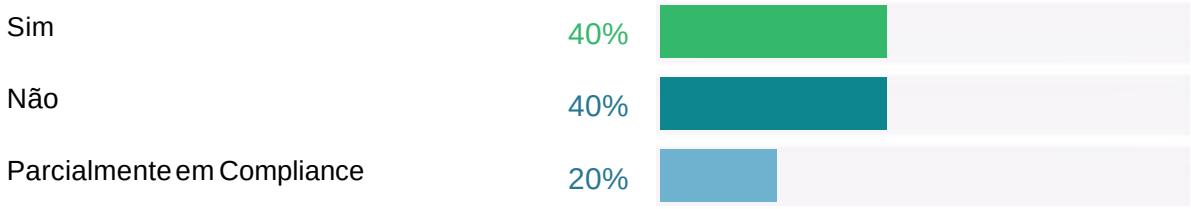
A continuidade dos negócios é uma abordagem estratégica que garante que as funções e operações críticas de uma organização possam continuar ininterruptas durante interrupções por ataques ou desastres inesperados. Envolve planejamento proativo, avaliação de riscos e desenvolvimento de estratégias robustas para mitigar ameaças potenciais, como ataques cibernéticos ou sequestro de dados.

O backup é uma prática simples, mas indispensável, que faz parte da estratégia de continuidade de negócios, garantindo a integridade dos dados. Ao manter cópias redundantes de informações importantes, as organizações e os indivíduos podem navegar com confiança no cenário digital, sabendo que os seus dados estão protegidos e recuperáveis quando necessário.

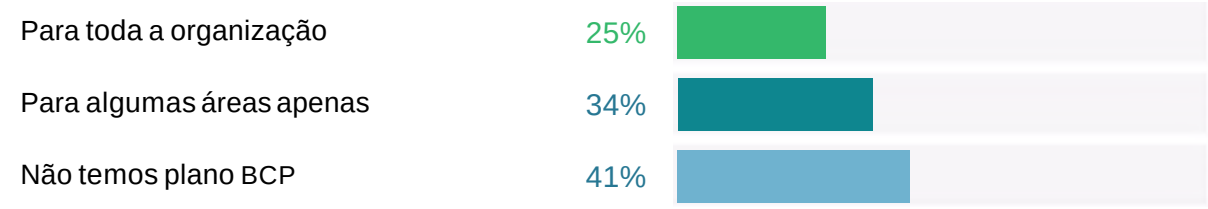
34. A BIA (Business Impact Analysis) é uma etapa fundamental do Plano de Continuidade. Sua organização possui componentes de sistema, processos de missão/negócios suportados e suas interdependências estabelecidas?



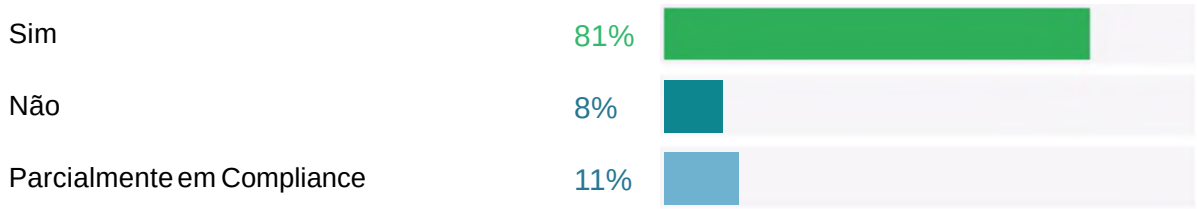
35. O BCP (Processo de Continuidade de Negócios) se concentra em sustentar a missão/processos de negócios de uma organização durante e após uma interrupção. Sua organização tem um plano para um evento de interrupção?



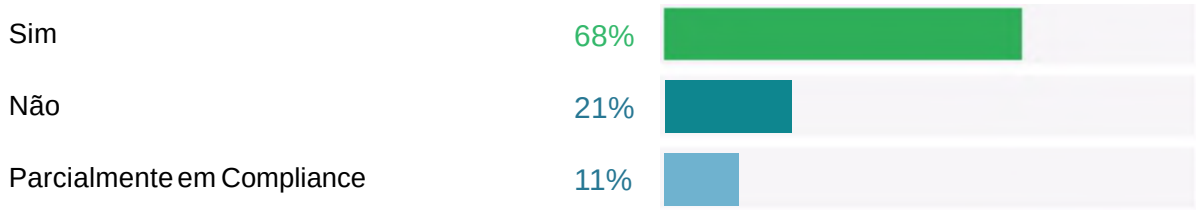
36. Seu plano BCP (Processo de Continuidade de Negócios) mapeia os processos críticos para áreas selecionadas ou para toda a organização?



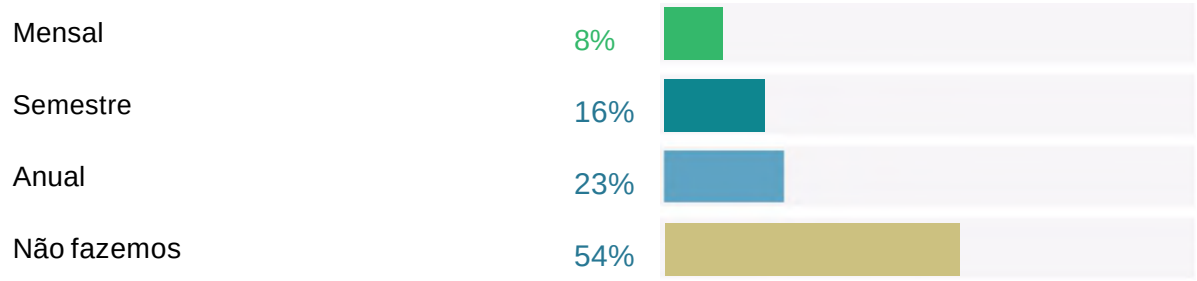
37. Métodos e estratégias de backup e restore devem restaurar rapidamente e de forma eficiente as operações da organização após uma parada de serviço. Sua organização possui um plano de backup implementado?



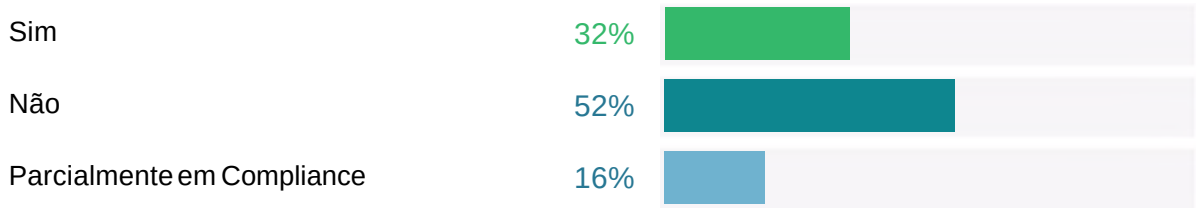
38. Sua organização possui um plano de restauração?



39. Com que frequência sua organização simula um disaster recovery?



40.Sua organização implementa mecanismos DLP (Data Loss Prevention)?

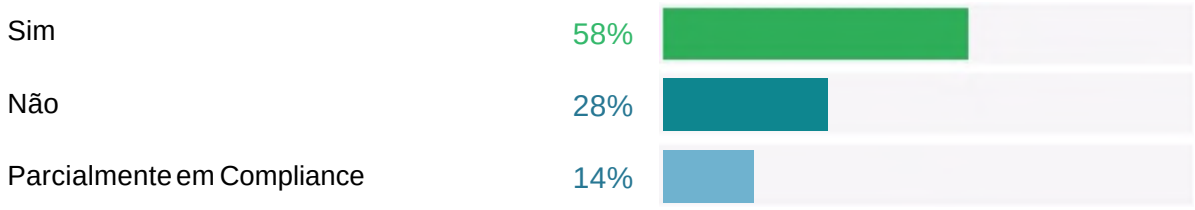


Seção 5 - Criptografia e Gerenciamento de Chaves

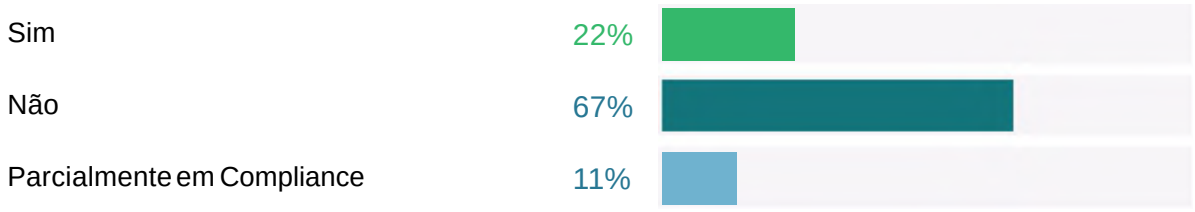
No mundo digital de hoje, a criptografia desempenha um papel crucial na segurança de dados confidenciais, incluindo informações pessoais, transações financeiras e comunicações privadas. Garante a confidencialidade e privacidade dos dados, evitando que partes não autorizadas interceptem e/ou leiam as informações.

A criptografia é uma pedra angular da segurança da informação moderna, fornecendo uma defesa robusta contra ameaças cibernéticas e ajudando organizações e indivíduos a manter a confidencialidade e a integridade dos seus ativos digitais.

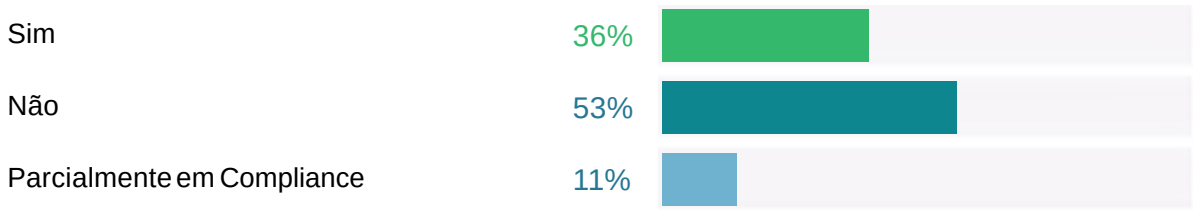
41. Quando em trânsito, os dados dos seus sistemas são criptografados?



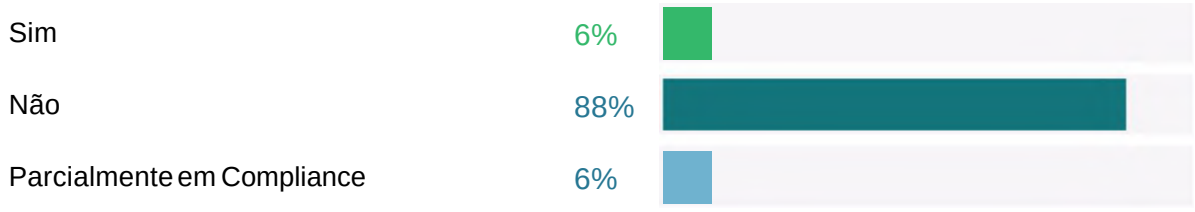
42. Existe algum mecanismo para criptografar dados em sua origem?



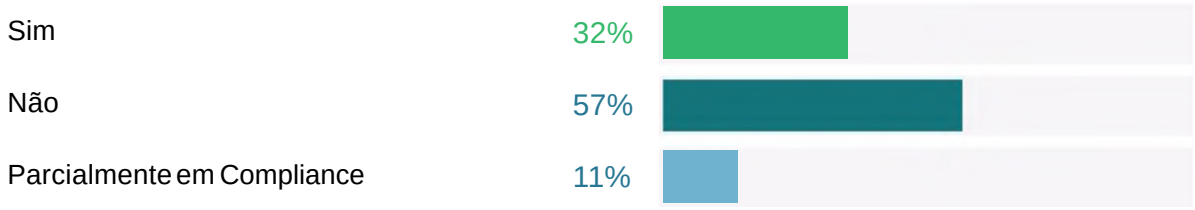
43. Os dados do seu sistema são criptografados quando em repouso?



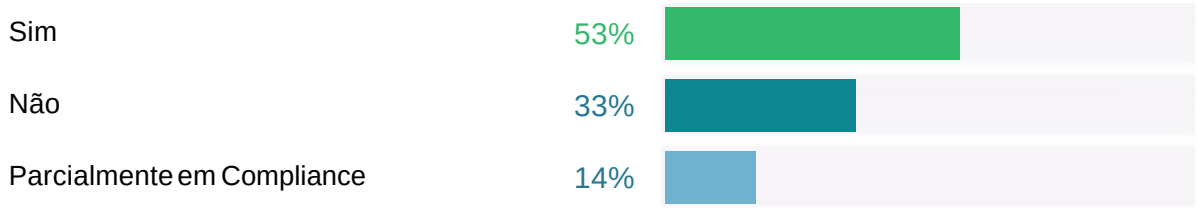
44. Sua organização possui (ou utiliza) um HSM (Hardware Security Module)?



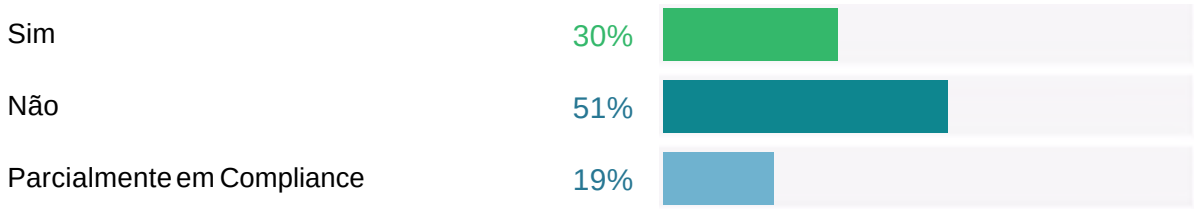
45. Existe algum mecanismo de controle sobre a criação de chave de criptografia?



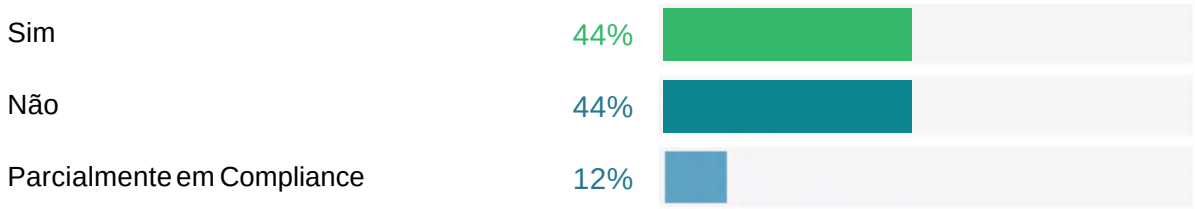
46. Sua organização implanta criptografia ou certificação digital para aplicações de uso diário, como e-mail, acesso remoto, etc.?



47. Sua organização implanta assinaturas de chave pública para transações de dados, mensagens e outros tipos de dados?



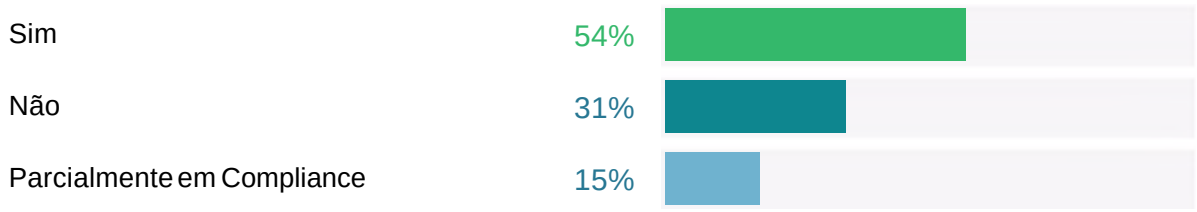
48. Ao enviar e receber mensagens, os sistemas que sua organização utiliza, comprovam a entrega das mesmas (proof of delivery)?



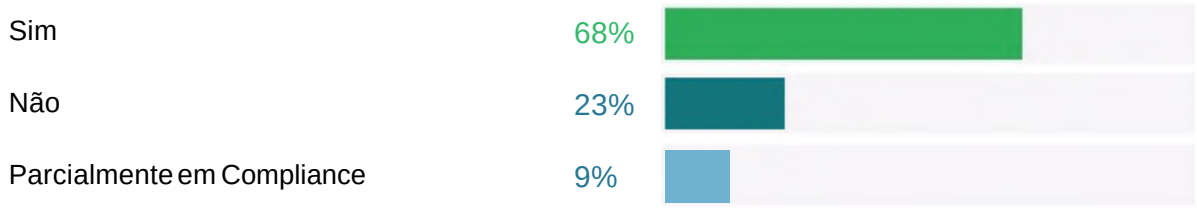
Seção 6 - Chat Corporativo e Mensagens

Essas plataformas fornecem comunicação baseada em texto em tempo real, permitindo trocas instantâneas e eficientes de informações, ideias e atualizações. Estas ferramentas facilitam a tomada rápida de decisões, o compartilhamento de documentos e as discussões em grupo, aumentando a produtividade e a conectividade entre os membros das equipes, independentemente de sua localização geográfica.

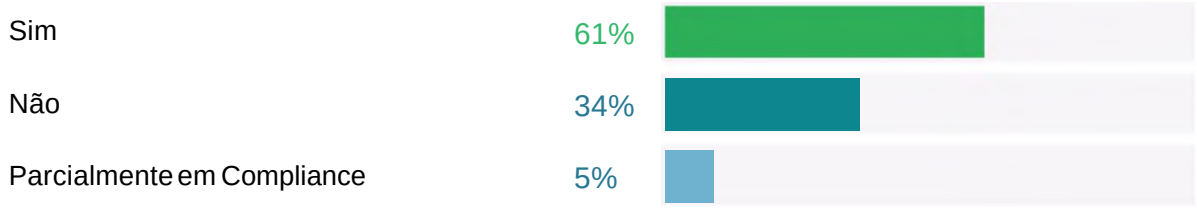
49. Pensando em suas ferramentas de comunicação atuais, sua organização está preparada para as próximas regras de regulamentação de segurança cibernética quando se trata de bate-papo e mensagens?



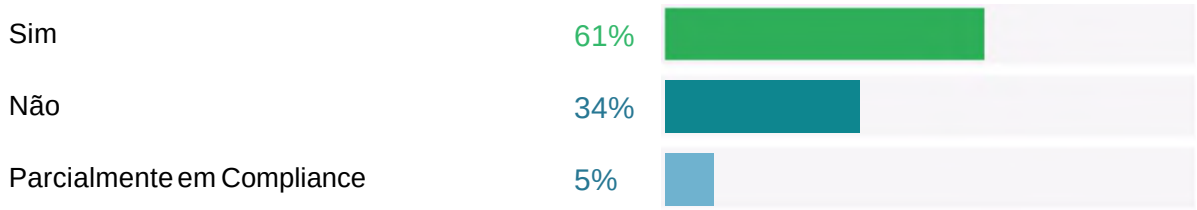
50. Ao enviar e receber mensagens instantâneas e bate-papo, as ferramentas da sua organização protegem os dados em trânsito e em repouso?



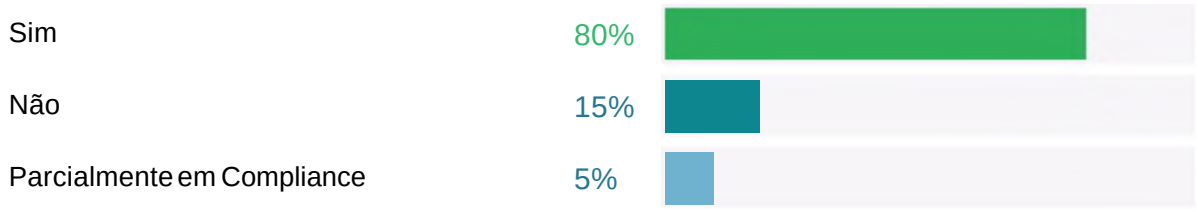
51. Os participantes podem confirmar com quem estão se comunicando?



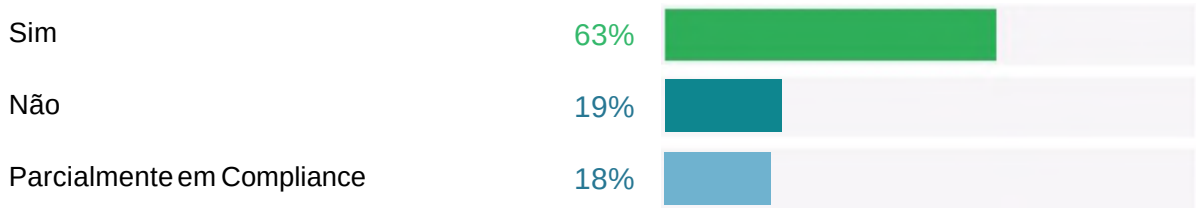
52. Os nós da rede que gerenciam o material da chave criptográfica estão protegidos adequadamente?



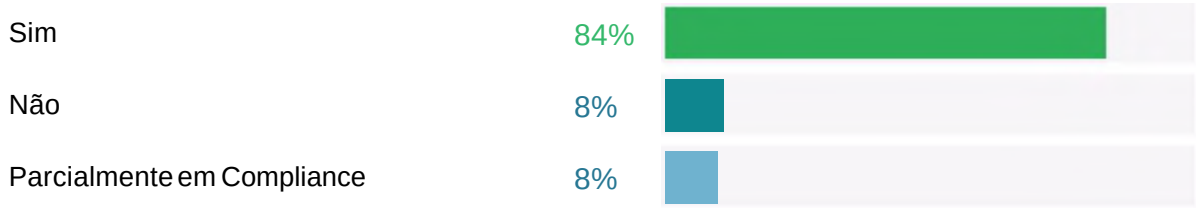
53. O acesso do usuário ao serviço é protegido?



54. O dispositivo do usuário está devidamente protegido?



55. A administração e o gerenciamento são protegidos e restritos?

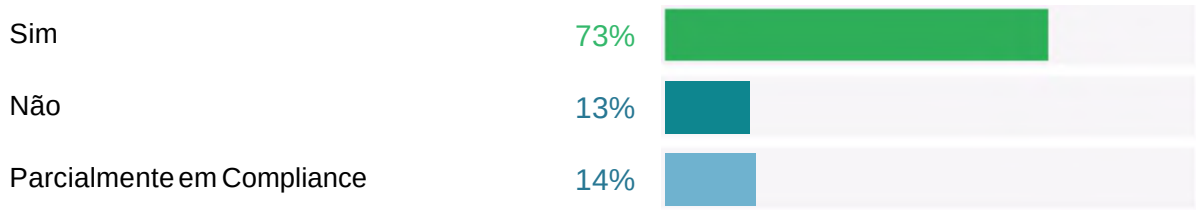


Seção 7 - Conformidade com os Regulamentos de Proteção de Dados

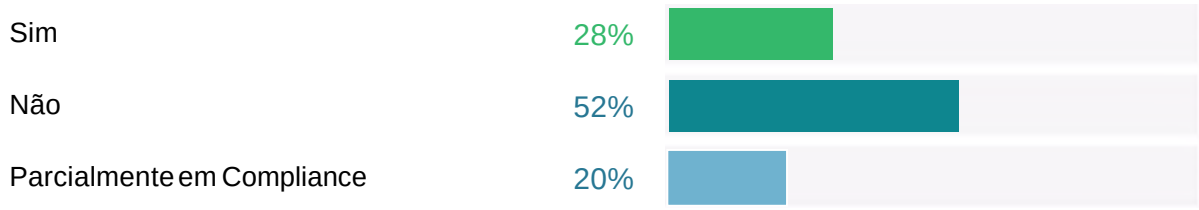
Os regulamentos de proteção de dados são leis e regras que regem a coleta, processamento, armazenamento e compartilhamento de dados pessoais. Estes regulamentos foram concebidos para salvaguardar os direitos de privacidade dos indivíduos e garantir que as organizações tratam os seus dados de forma responsável e segura.

A conformidade com estes regulamentos não é apenas um requisito legal, mas também essencial para construir a confiança dos clientes e manter uma reputação sólida. As organizações que não cumprirem os regulamentos de proteção de dados podem enfrentar multas pesadas e danos à sua marca.

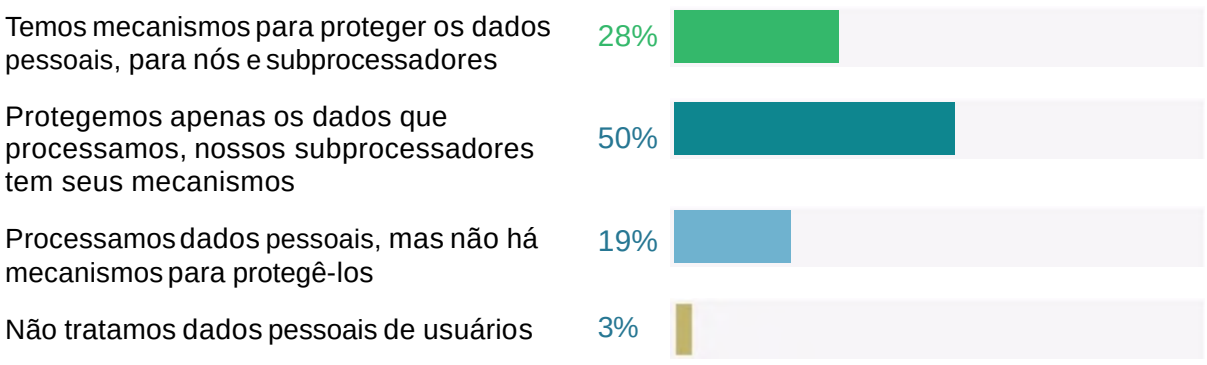
56. A sua organização promove a separação de funções e mínimos privilégios, garantindo que os funcionários tenham acesso apenas às informações ou sistemas aplicáveis à sua função de trabalho?



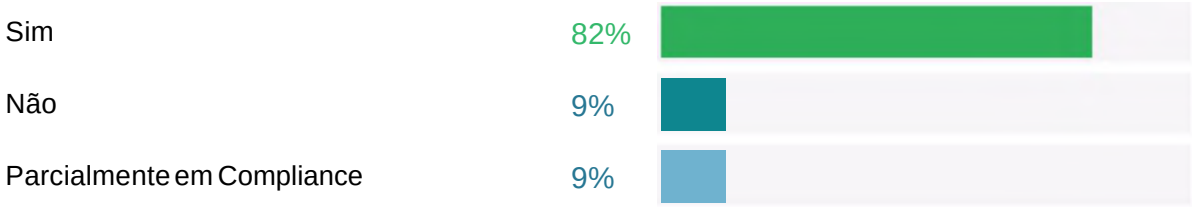
57. Sua organização implementa criptografia e pseudonimização, como criptografia em bancos de dados, informações em repouso e em trânsito?



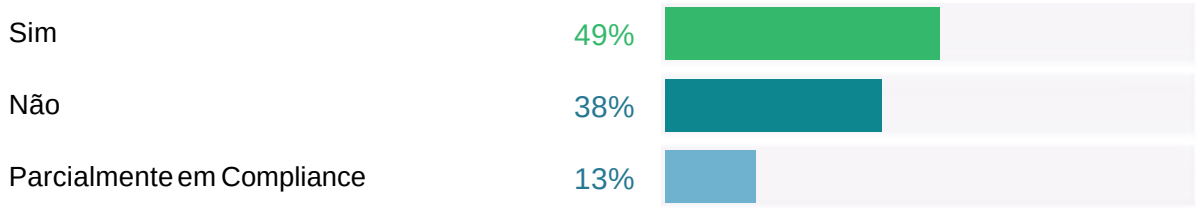
58. O processamento de dados é um tópico muito sensível para os regulamentos de dados. Como sua organização lida com o processamento de dados pessoais ou subprocessadores, quando ocorrem violações?



59. O gerenciamento de políticas é uma base para a conformidade com a regulamentação de dados. A sua organização tem uma política de segurança em vigor?



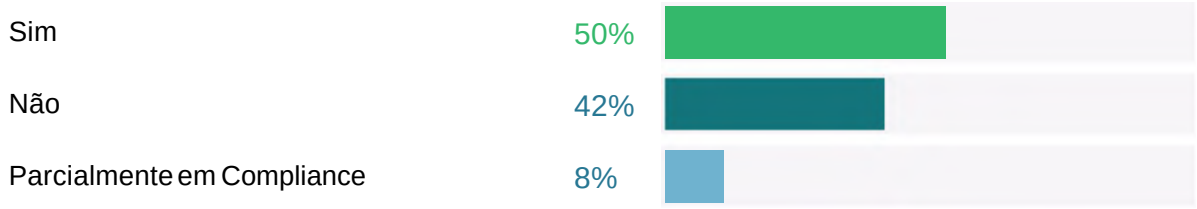
60. Sua organização tem um programa de treinamento para educar periodicamente os usuários sobre os controles e ferramentas da política de segurança?



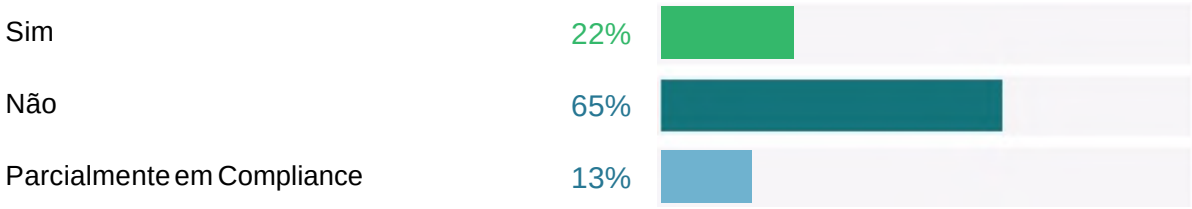
Seção 8 - Resposta a Incidentes

A resposta a incidentes é uma abordagem sistemática para abordar e gerenciar incidentes de segurança cibernética dentro de uma organização. Envolve um esforço coordenado para detectar, avaliar, conter e mitigar prontamente violações de segurança ou ataques cibernéticos. Um plano de resposta a incidentes bem preparado e executado pode ajudar as organizações a minimizar perdas financeiras, proteger a sua reputação e manter a continuidade dos negócios face a ataques cibernéticos e violações de dados.

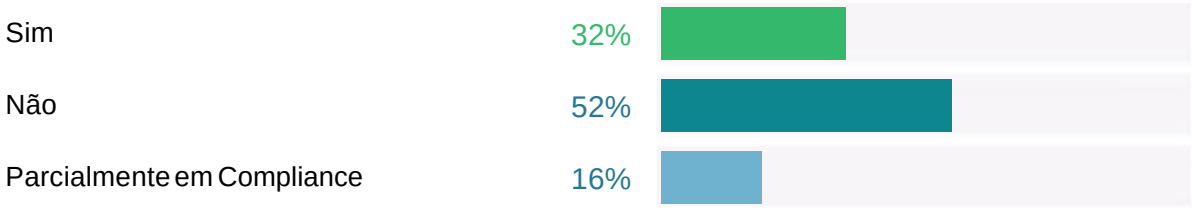
61. Sua organização possui um IRP (Plano de Resposta a Incidentes)?



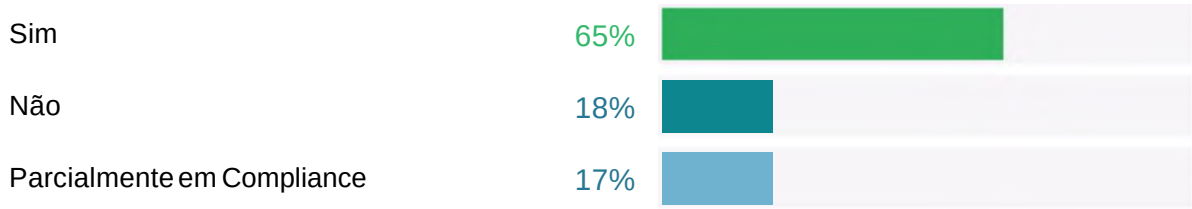
62. Sua organização possui, de forma recorrente, um treinamento de Plano de Resposta a Incidentes?



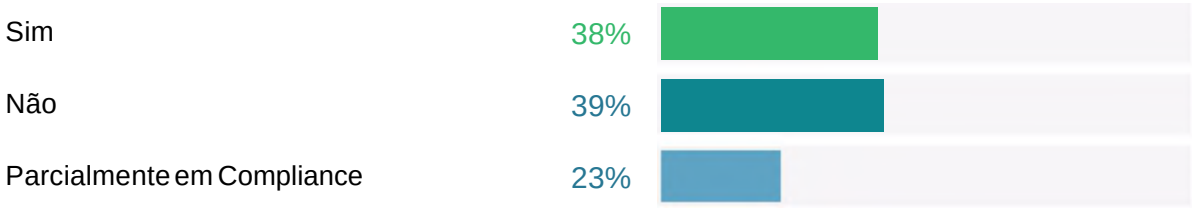
63. Sua organização oferece treinamento de resposta a incidentes, incluindo tópicos sobre como identificar e responder a vazamentos e brechas de segurança, e como reportar tais eventos?



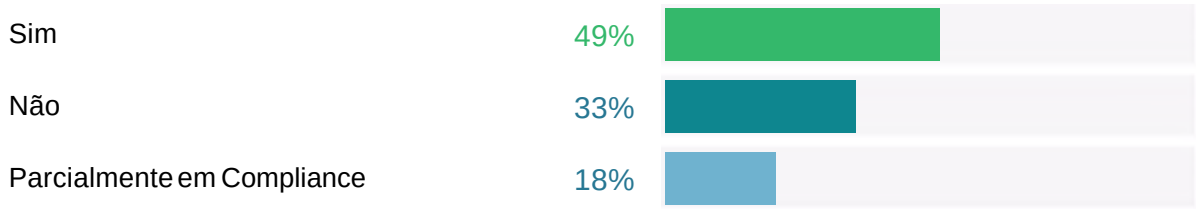
64. Sua organização é capaz de identificar e agir em reposta a incidentes, para assegurar a continuidade do negócio e suas funções?



65. A Cadeia de Suprimentos (Supply Chain) é uma parte crucial em um incidente de segurança. Sua organização possui mecanismos para identificar e controlar os papéis desta cadeia em um incidente?



66. Sua organização possui procedimentos para reportar incidentes, incluindo a coordenação com fornecedores externos e toda a Cadeia de Suprimentos?

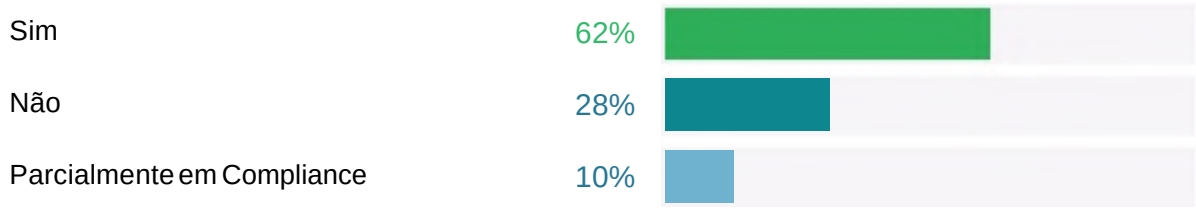


Seção 9 - Proteção de Mídias Digitais

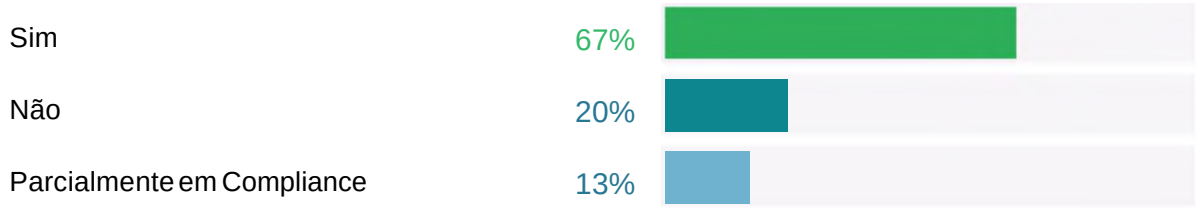
A proteção de mídia física envolve a proteção de dispositivos de armazenamento tangíveis, como CDs, DVDs, discos rígidos e unidades USB, para evitar perda, roubo, danos ou acesso não autorizado aos dados armazenados nesses formatos físicos.

A proteção dos meios físicos é um aspecto crítico da segurança dos dados e do planejamento da continuidade, garantindo que informações valiosas permaneçam acessíveis e seguras num formato que persiste juntamente com as alternativas digitais.

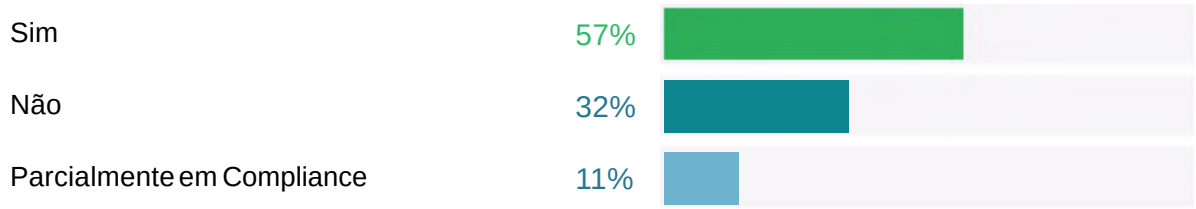
67. Existem mecanismos implementados para controlar e restringir o acesso a mídias digitais (drives, disquetes, fitas magnéticas, discos removíveis externos ou internos (ex. SSD, magnéticos), CDs e DVDs?



68. Sua organização possui procedimentos de limpeza de mídias digitais, antes do descarte, doação ou reuso fora da organização?



69. Existe algum mecanismo para restringir ou proibir o uso de mídias digitais ou dispositivos de armazenamento portáteis não aprovados em ambiente corporativo?

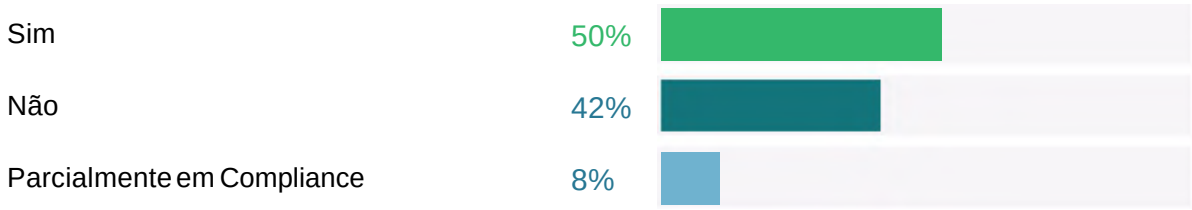


Seção 10 - Governança e Segurança da Informação

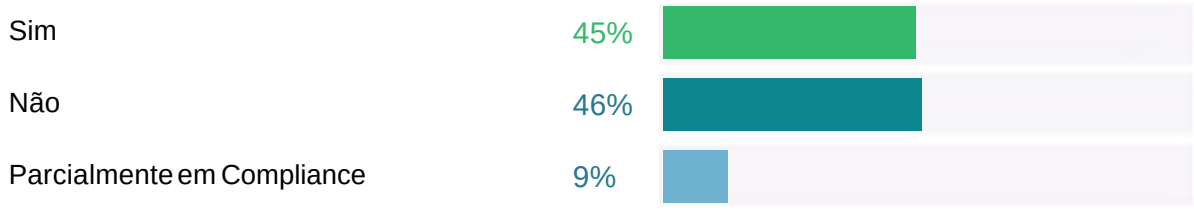
Trata-se de uma estrutura abrangente que as organizações implementam para gerenciar e proteger seus ativos de informação de forma eficaz. Abrange políticas, procedimentos e práticas que garantem a confidencialidade, integridade e disponibilidade de dados confidenciais, ao mesmo tempo que cumprem os regulamentos relevantes.

A Governança da Informação de Segurança é uma abordagem estratégica para o gerenciamento e a segurança da informação. Ajuda as organizações a gerir eficazmente os seus dados, a reduzir os riscos de segurança e a garantir a conformidade com as leis de proteção de dados e os padrões da indústria, protegendo, em última análise, os seus valiosos ativos de informação.

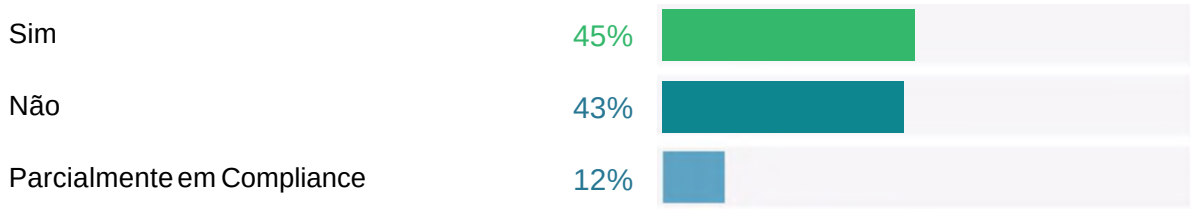
70. As organizações dependem fortemente de TI para seu sucesso e vantagem competitiva, mas para isto é necessário governança. Sua organização possui um CISO (Chief Information Security Officer), ou similar, responsável pela segurança da informação?



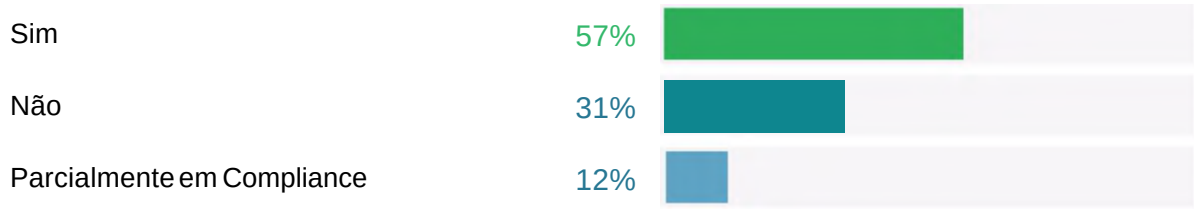
71. As organizações devem integrar suas atividades de governança de segurança com a estrutura e atividades gerais da companhia, garantindo a participação adequada dos funcionários da empresa na supervisão da implementação dos controles de segurança da informação em toda a companhia. Sua organização possui um comitê de segurança para promover essa integração?



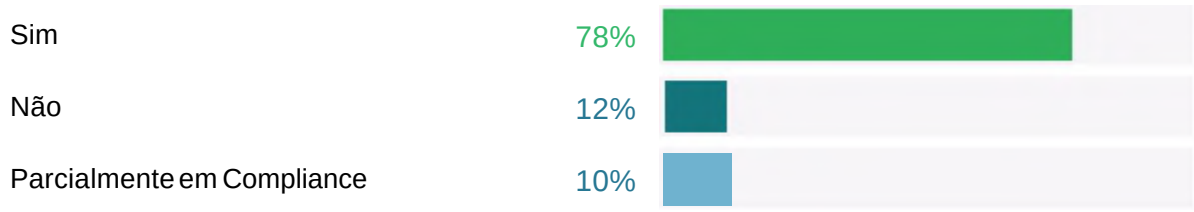
72. A estratégia de segurança da informação da sua organização estabelece uma estrutura abrangente para permitir o desenvolvimento, institucionalização, avaliação e melhoria do programa de segurança da informação da companhia?



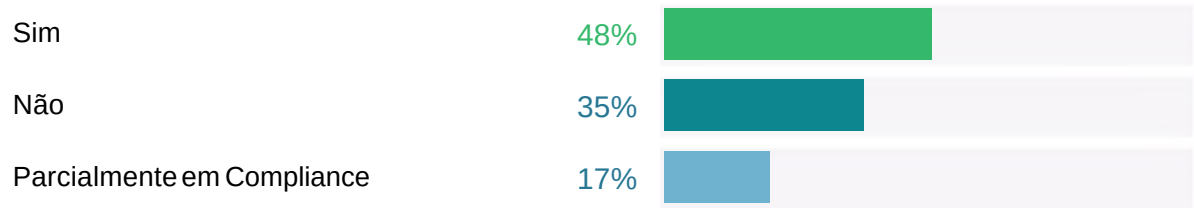
73. Papéis e responsabilidades são essenciais para as operações de segurança da informação. Sua organização garante que a política, os procedimentos e as práticas de segurança da informação sejam adequados e implementados?



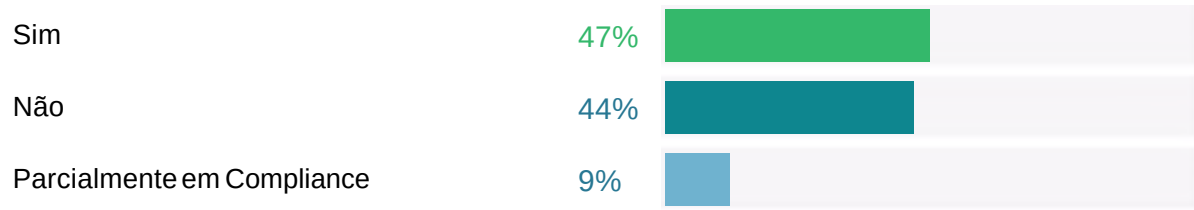
74. Sua organização implementa controles de segurança física como parte da estratégia de segurança da informação, como controle de acesso, autorização, controle de visitantes, entrada e saída de equipamentos?



75. Um programa de governança de segurança da informação eficaz requer revisão constante. Sua organização monitora o status de seus programas para garantir que as políticas e procedimentos em andamento estejam em vigor e alinhados com as tecnologias em evolução?



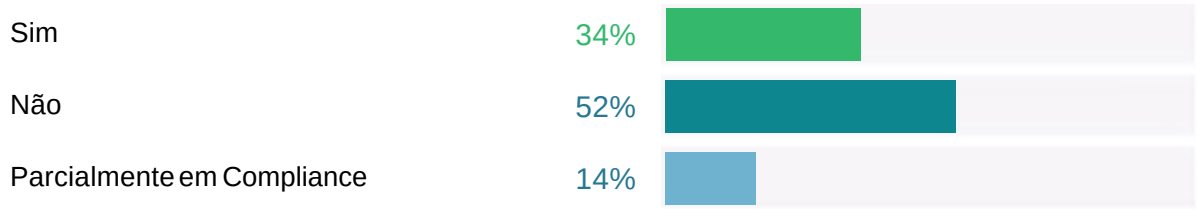
76. O programa de conscientização e treinamento em segurança é um componente crítico do programa de segurança da informação. É o veículo de divulgação de informações de segurança de que a força de trabalho, incluindo os gerentes, precisa para desempenhar sua função. Sua organização implementa um programa regular de treinamento em segurança da informação, mantendo-o atualizado e alinhado com a estratégia de negócios da companhia?



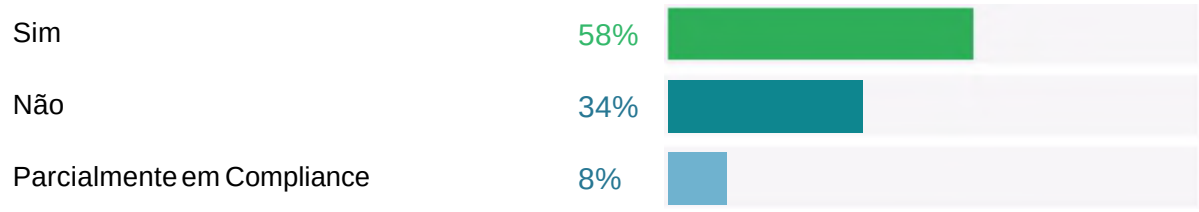
Seção 11 - Gerenciamento de Risco da Cadeia de Suprimentos (Supply Chain)

A gestão de riscos da cadeia de suprimentos é uma abordagem estratégica que as organizações empregam para identificar, avaliar e mitigar potenciais ameaças e vulnerabilidades nas suas cadeias de abastecimento que possam ser impactadas por ataques e falhas de segurança, muitas vezes ocorridas em outras organizações, interrompendo o fluxo de bens, serviços ou informações, impactando as operações.

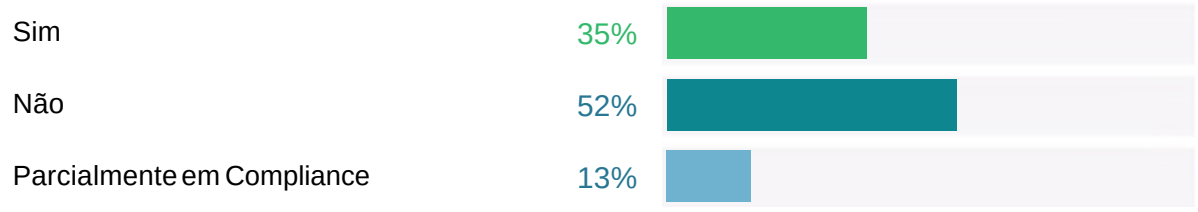
77. Sua organização possui procedimentos para desenvolver, documentar e disseminar uma estratégia de Gestão de Risco para Supply Chain?



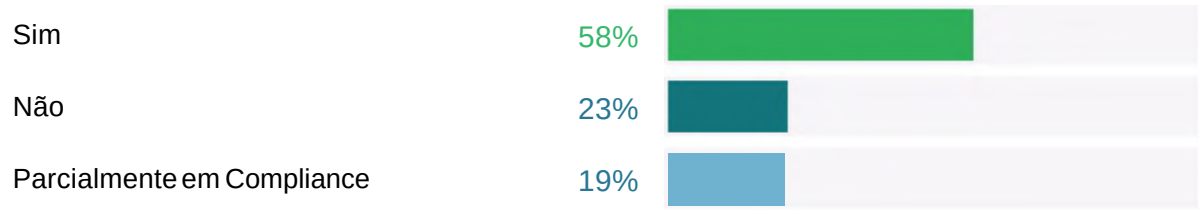
78. Sua organização procura diversificar as fontes e fornecedores da Cadeia de Suprimentos, incluindo seus componentes, sistemas e serviços?



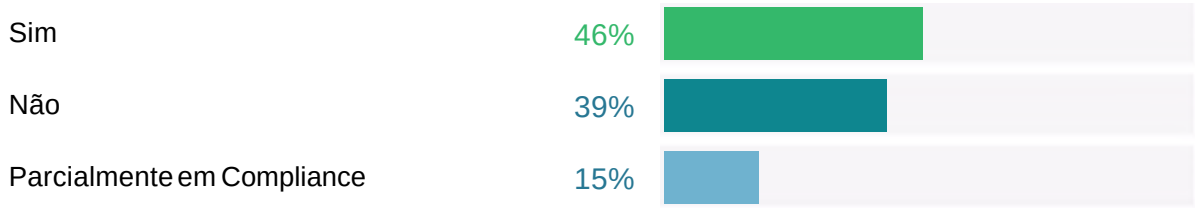
79. Sua organização implementa controles para limitar danos, partindo de adversários potenciais que identificam e elegem como alvo sua Cadeia de Suprimentos?



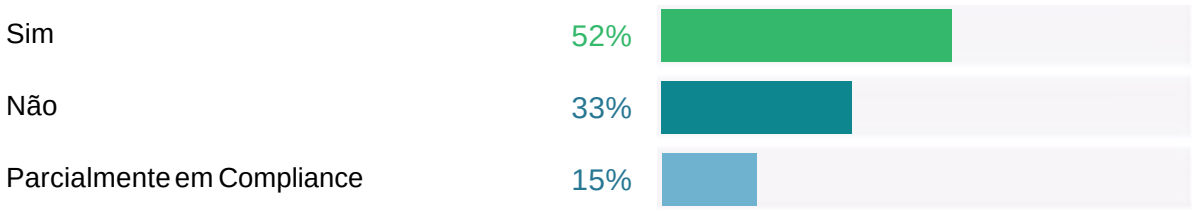
80. Sua organização documenta, monitora, e mantém válida a procedência dos sistemas, seus componentes, e dados associados?



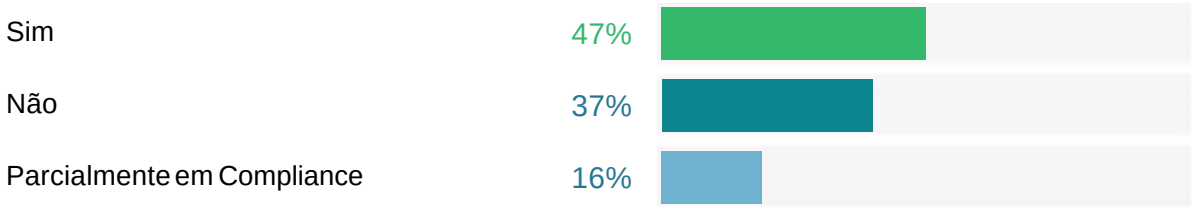
81. Sua organização conduz assessments nos serviços ou produtos da Cadeia de Suprimentos antes de utilizá-los como parte da estratégia de negócios da sua companhia?



82. Sua organização implementa controles de operação de cibersegurança para proteger informações de Cadeia de Suprimentos relacionadas a sistemas, componentes de sistemas ou serviços?



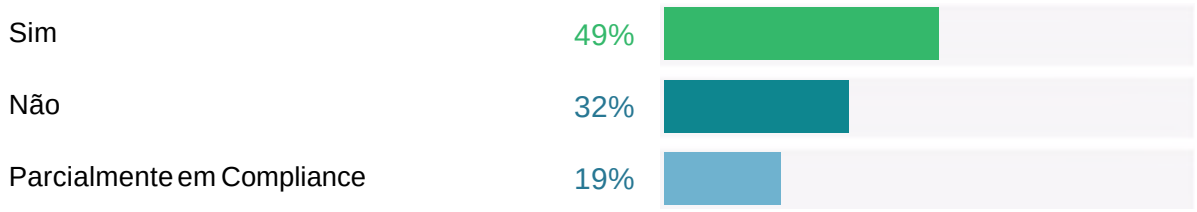
83. Sua organização estabelece procedimentos e acordos de notificação com as entidades envolvidas em incidentes de cibersegurança da Cadeia de Suprimentos para sistemas, componentes ou serviços?



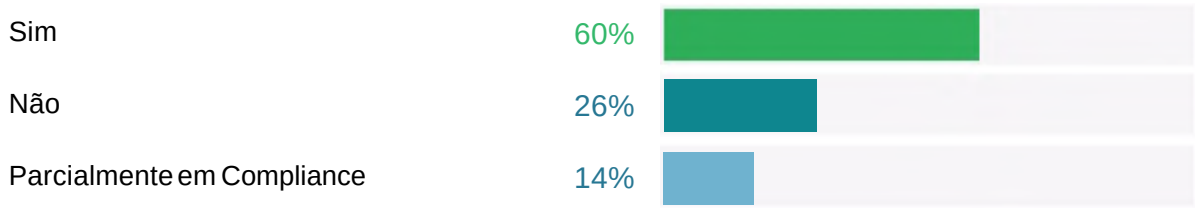
Seção 12 - Dispositivos Conectados

São dispositivos como câmeras de CFTV, catracas, sensores, software e conectividade para trocar dados e executar funções via rede privada ou Internet. Esses dispositivos podem variar de termostatos inteligentes e rastreadores de fitness vestíveis a sensores industriais e veículos autônomos.

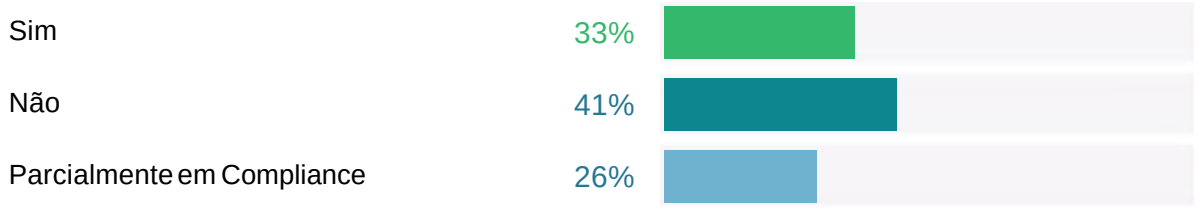
84. Sua organização possui um inventário para dispositivos conectados (OT e ICS)?



85. Seus dispositivos conectados possuem controle de autenticação?



86. Dados chegando e saindo do dispositivo conectado estão protegidos por criptografia?



Conclusão

Olhando para dentro das companhias, a cibersegurança deixou de ser um problema da área de tecnologia e se tornou um problema corporativo, potencialmente afetando todos os stakeholders, e entrando para ficar no dia a dia de administradores e conselheiros. Ao mesmo tempo, ao olharmos para fora, investidores, reguladores e governo também estão adicionando ao seu tema dia a dia às rotinas em escala global, ou seja, cibersegurança se tornou um capítulo extra no Mercado de Capitais.

Com este cenário, é essencial o crescente debate e conscientização sobre o tema, junto com dados e entendimento por parte das Companhias, para evitar a amplificação de custos de maneira desmedida e gerar um avanço saudável do Mercado de Capitais brasileiro. Afinal, estamos falando de diversos aspectos que podem afetar seriamente a competitividade das Companhias, encarecer seu processo de financiamento e acesso a mercado de capitais e colocar em xeque a continuidade de negócios.

Os resultados da pesquisa são instigadores de toda dessa discussão e, ao mesmo tempo, mostram que as Companhias abertas brasileiras estão caminhando no tema e não parecem estar menos maduras mas, como no mercado global, existe muito trabalho a ser feito.

Termos técnicos chave para o entendimento

Algoritmos: O algoritmo é o conjunto de instruções e regras que um programa de computador (mas não apenas ele) possui para executar suas funções.

Assessments: Avaliação ou análise dos sistemas de segurança de uma empresa.

Autenticação em dois fatores: O que eu possuo (digital, facial) e o que eu conheço (senha).

Backup: Em informática, cópia de segurança ou salvaguarda é a cópia de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.

Benchmark: Padrão de referência para comparações.

Criptografia: Criptografia em segurança virtual é a conversão de dados de um formato legível em um formato codificado. Os dados criptografados só podem ser lidos ou processados depois de serem descriptografados.

DPIA (Avaliação de Impacto à Proteção de Dados): A DPIA é um processo que envolve a avaliação dos riscos e impactos que atividades de tratamento de dados pessoais podem ter sobre a privacidade e os direitos dos titulares dos dados. Ela é uma ferramenta de gestão de riscos que ajuda as organizações a identificar potenciais problemas de privacidade antes de iniciar um projeto que envolva o processamento de dados pessoais.

Due-diligence: Investigação ou análise feita sobre uma empresa, antes de fechar uma negociação com ela.

EDR: Endpoint Detection and Response (EDR), também conhecido como detecção de endpoint e resposta a ameaças (EDTR), é uma solução de segurança de endpoint que monitora continuamente os dispositivos do usuário final para detectar e responder a ameaças cibernéticas, como ransomware e malware.

Engenharia social: Outra forma de ataque que explora aspectos psicológicos e sociais das pessoas. É uma técnica empregada pelos criminosos virtuais destinada a induzir usuários desavisados a enviar dados confidenciais, infectar seus computadores com malware ou abrir links para sites infectados.

Firewall: Sistema de segurança colocado entre uma rede privada e a pública.

ICS: Na manufatura, o sistema de controle industrial (ICS) é um termo geral usado para descrever a integração de hardware e software com conectividade de rede para oferecer suporte à infraestrutura crítica.

Logs: Log de dados é uma expressão utilizada para descrever o processo de registro de eventos relevantes. Um arquivo de log pode ser utilizado para auditoria e diagnóstico de problemas.

Malware: É um software instalado em um computador ou smartphone sem o consentimento do usuário e que executa ações maliciosas.

Não Repúdio: Conceito de segurança da informação que visa garantir que uma parte envolvida em uma transação ou comunicação não possa negar posteriormente sua participação ou ação no evento.

On-premises: Ambiente computacional dentro e sob responsabilidade da empresa.

OTP: Uma senha de uso único (OTP), também conhecida como PIN de uso único, código de autorização de uso único (OTAC) ou senha dinâmica, é uma senha válida para apenas uma sessão ou transação de login.

Passwordless: Autenticação sem senha, geralmente com biometria: digital ou facial.

Phishing: Forma de ataque cibernético para se obter dados confidenciais.

Recovery: Recuperação de dados é um processo de recuperação de dados excluídos, inacessíveis, perdidos, corrompidos, danificados ou formatados de armazenamento secundário, mídia removível ou arquivos.

ROPA (Relatório de Impacto à Proteção de Dados Pessoais): O ROPA é um documento que descreve as atividades de tratamento de dados pessoais realizadas por uma organização e avalia os impactos dessas atividades na privacidade e proteção de dados dos indivíduos.

Ransomware: Ransomware é um software de extorsão que pode bloquear o seu computador e depois exigir um resgate para desbloqueá-lo.

SCADA *(Supervisory Control and Data Acquisition*): é uma categoria de aplicativos de software para controle de processos industriais, que é a coleta de dados em tempo real de locais remotos para controlar equipamentos e suas condições.

Sistemas de detecção de intrusão: Dispositivo ou aplicativo de software que monitora uma rede ou sistemas em busca de atividades maliciosas ou violações de políticas.

Table Top: Uma atividade de preparação para incidentes de segurança, conduzindo os participantes pelo processo de lidar com um cenário de incidente simulado.

Vulnerabilidade: Condição que, quando explorada por um atacante, pode resultar em uma violação de segurança.

VPN: Uma VPN, ou rede virtual privada, é um túnel seguro entre seu dispositivo e a internet. As VPNs protegem você contraespionagem, interferência e interceptação.

Vetores de ataque: Caminhos ou métodos pelos quais uma plataforma pode ser atacada.

Realização:

abrasca

Idealizadores:

Capital Markets Lab

The Security Design Lab

Patrocinadores:

BIDWEB

howden

URBANO VITALINO ADVOGADOS

Alvarez & Marsal

Akamai

ELYTRON SECURITY

Apoio Institucional:

Women's Club

Movimento Inovação Digital

FGV

RYTO public affairs

Université Côte d'Azur IMREDD

fit

Inatel

Insper

Eldorado Inspiração pelo Novo

FIPECAFI Cultura Contábil, Atuarial e Financeira

ABES

cesar school

DATAPREV

ABCIS Associação Brasileira CIO Saúde