netfive

2023 RSIN

RELATÓRIO DE SEGURANÇA DA INFORMAÇÃO DA NETFIVE.

+51 3061-4446
contato@netfive.com.br
www.netfive.com.br

Avenida Ipiranga, 6681, Tecnopuc,
Prédio 96E, sala 126, Porto Alegre - RS

Sobre este Documento

Este documento, que traz um compilado de informações geradas a partir de pesquisa exclusiva conduzida pela Netfive, busca extrair dados de relatórios de riscos, bem como de indicadores de ataque, e compará-los com a maturidade de segurança da informação de empresas de pequeno, médio e grande porte.

O objetivo é contribuir para uma maturidade das empresas em relação à cultura da Segurança da Informação - uma preocupação que precisa estar no topo das preocupações dos gestores.

Sobre a Netfive

A TI do futuro é invisível e está em todo lugar. Segurança é palavra de ordem em um mundo onde a informação é um ativo cada vez mais valioso e estratégico. Para nós, evolução é no presente. Queremos nos conectar com clientes que buscam se reinventar hoje porque sabem que a mudança é imperativa e pede agilidade. E é aí que a gente entra: propondo soluções para que a sua infraestrutura de TI acompanhe e promova crescimento sustentável.

Não sabemos ao certo como o futuro será, mas enxergamos a TI como um meio de pensar negócios e queremos estar presentes impulsionando a performance das empresas através de soluções inteligentes e que melhoram o hoje pensando no amanhã.

12+ **Segmentos atendidos**

100+ **Clientes**

15+ **Anos de experiência**

1 RELATÓRIOS DE RISCOS

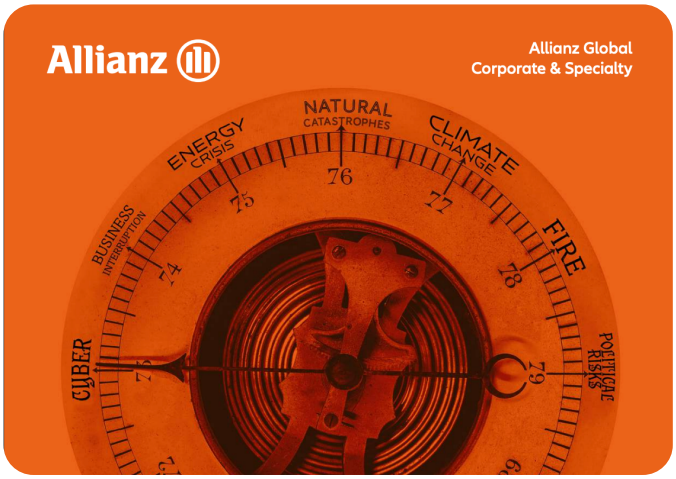
2 RELATÓRIOS DE CRIMES CIBERNÉTICOS

3 RELATÓRIOS DE SI DA NETFIVE (RSIN)

Os relatórios de riscos que serão apresentados a seguir são produzidos por grandes organizações e entidades que monitoram riscos em escala global. As pesquisas foram conduzidas junto a empresas de pequeno, médio e grande porte, e envolveram consultas a analistas de riscos, diretores e gestores, com o respaldo acadêmico na geração dos dados.

ALLIANZ RISK BAROMETER 2023

A décima segunda edição do relatório de riscos comerciais global, produzido pela Allianz, mostra que o risco de um incidente diminuiu de 44% para 34% mantendo-se em primeiro lugar, junto de interrupções do negócio.



Fonte:
https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2023.pdf

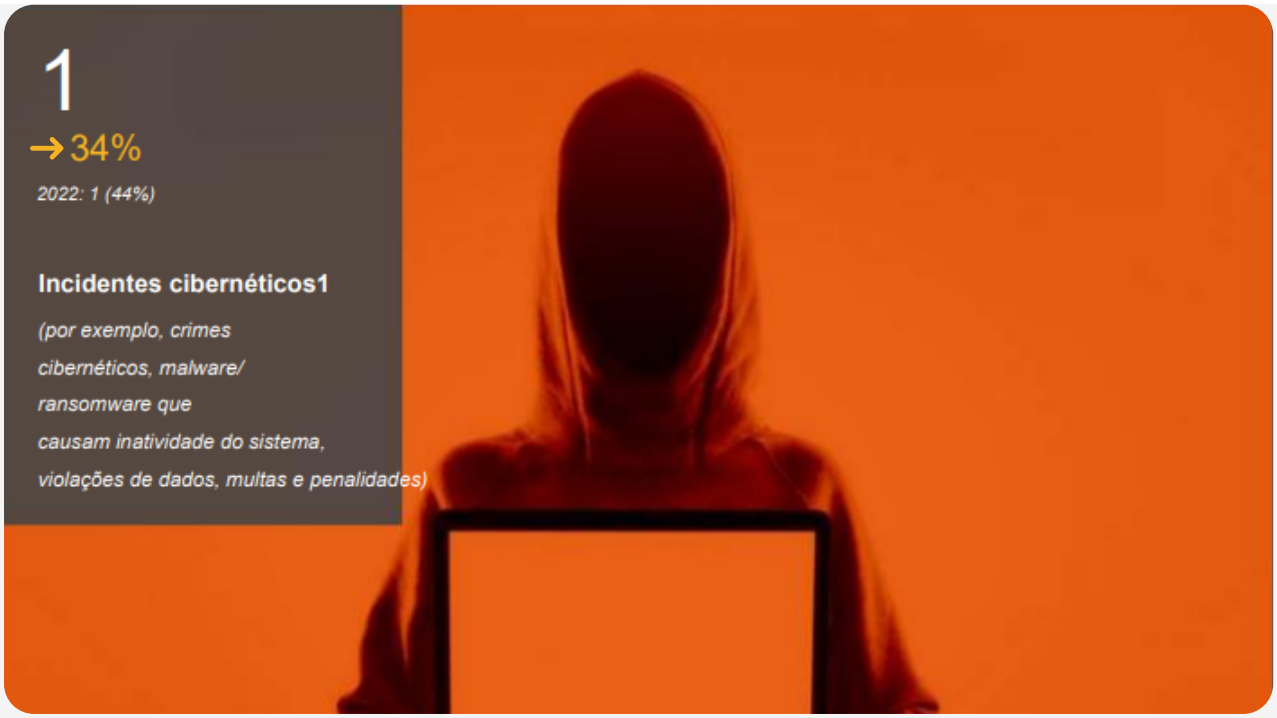
2,712
respondents

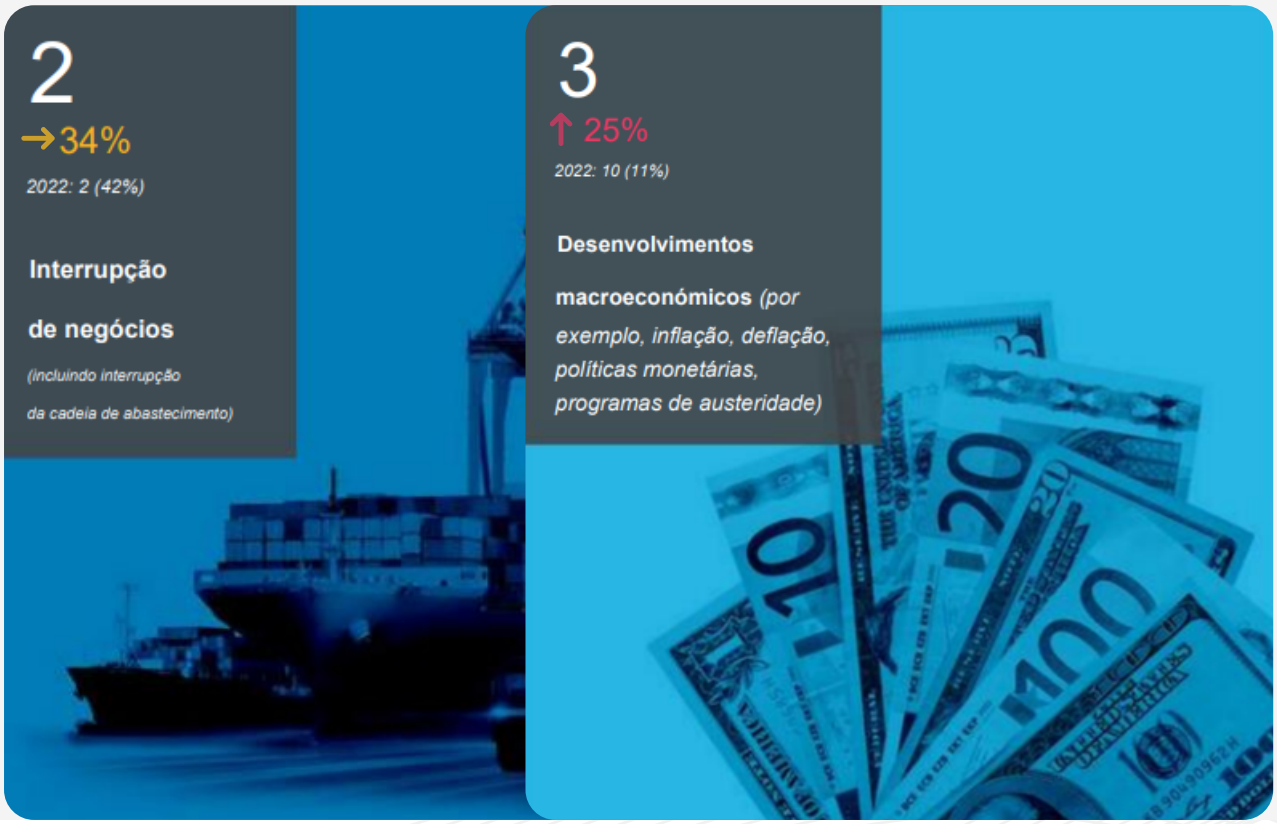
94
countries and territories

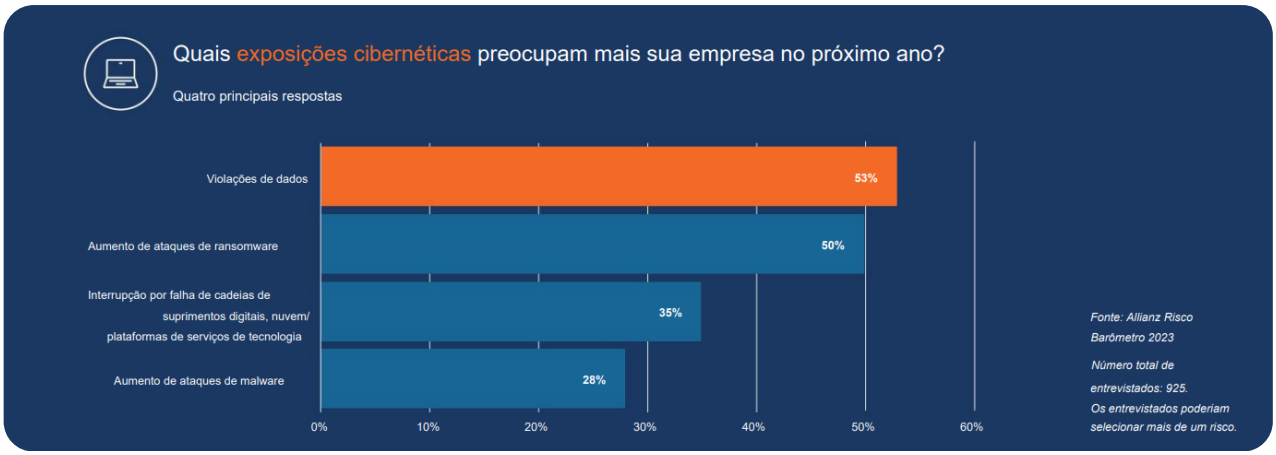
23
industry sectors

47% das respostas foram de grandes empresas, com mais de US$ 500 milhões de dólares de faturamento anual.

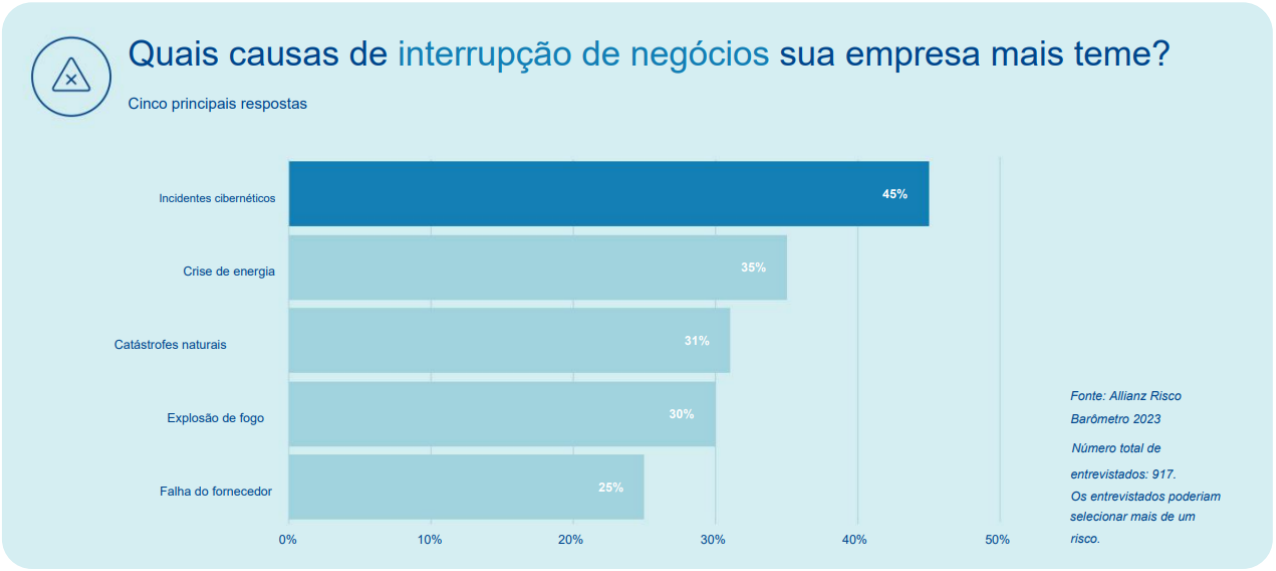
19% das respostas foram de médias empresas, com faturamento entre US$250 e US$500 milhões de dólares.


1
→34%
2022: 1 (44%)
Incidentes cibernéticos1
(por exemplo, crimes cibernéticos, malware/ ransomware que causam inatividade do sistema, violações de dados, multas e penalidades)


2
→34%
2022: 2 (42%)
Interrupção de negócios
(incluindo interrupção da cadeia de abastecimento)
3
↑ 25%
2022: 10 (11%)
Desenvolvimentos macroeconómicos (por exemplo, inflação, deflação, políticas monetárias, programas de austeridade)



O vazamento de informações e os ataques de ransomware inverteram suas posições em comparação com o ano de 2022. As preocupações com o trabalho remoto saíram do ranking em 2023.

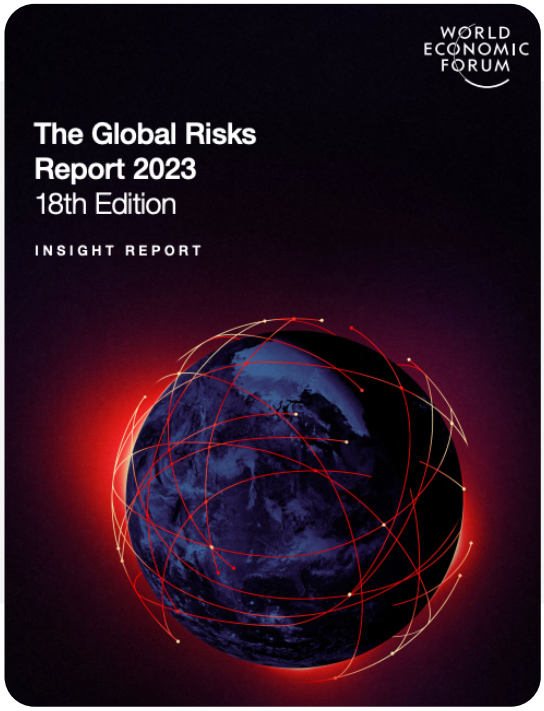


As preocupações com interrupções de negócios relacionadas a incidentes cibernéticos continuam sendo as maiores, com 45% (em comparação com 52% em 2022).

WEF - THE GLOBAL RISKS REPORT 2022 17TH EDITION

A 18ª edição do Relatório de Riscos Globais do Fórum Econômico Mundial analisa riscos diversos para os países, entre eles, os sociais, ambientais e tecnológicos. É produzido em parceria com Marsh McLennan, SK Group and Zurich Insurance Group, além da National University of Singapore, University of Oxford e University of Pennsylvania.

Aplicada em aproximadamente mil e duzentos líderes e/ou especialistas, a pesquisa de percepção de risco está dividida em diversos segmentos, incluindo: Pandemia; Relação de pontos de vista individualizados com riscos mundiais; Senso de urgência; Efeito cascata de riscos; Cooperação em políticas internacionais e Avaliação de tendências.



O viés político presente no relatório pode influenciar a maneira como se percebe a gravidade dos ataques cibernéticos em comparação com outros estudos. No entanto, é importante notar que, mesmo com essa possível influência, o relatório mostra que tanto em 2 quanto em 10 anos, o número de respostas que classificam os crimes cibernéticos ou falhas na cibersegurança na oitava posição permanece consistente.

Fonte: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2023.pdf

PWC 26TH ANNUAL GLOBAL CEO SURVEY

Todos os anos, a PwC conduz uma pesquisa mundial com CEOs de grandes empresas com o objetivo de mapear a visão desses líderes para identificar padrões e tendências na economia mundial que podem ajudar na tomada de decisões das organizações.

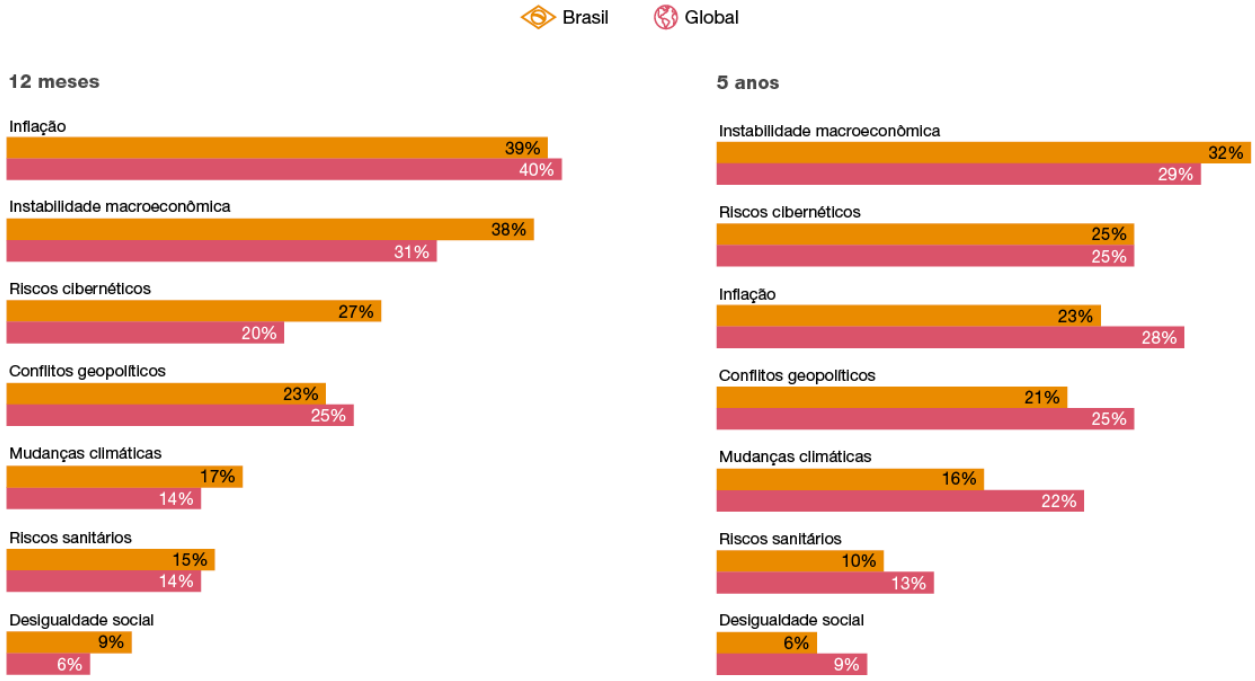
PwC's 26th Annual Global CEO Survey

Winning today's race while running tomorrow's

4.410 CEO's de 105 países.

Pergunta: Quão exposta sua empresa estará às seguintes ameaças nos próximos...?

Nota: percentuais consideram respostas "muito" e "extremamente exposta"

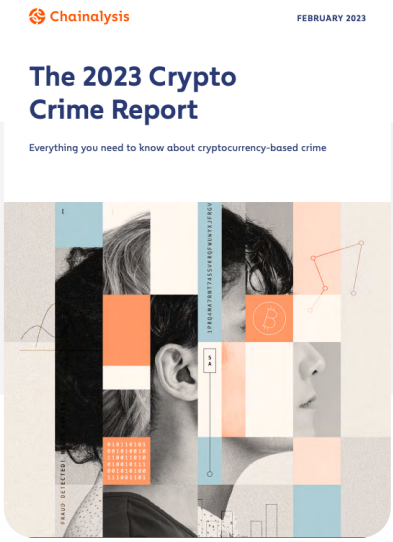


Quando analisamos os relatórios da consultoria PriceWaterhouseCoopers, observamos que, nos próximos 12 meses, os riscos cibernéticos estão entre as 3 maiores preocupações dos CEOs brasileiros, 7% a mais se comparado com o cenário global. Para os próximos 5 anos, os riscos cibernéticos avançam para a segunda posição e os CEOs brasileiros se preocupam na mesma proporção que no resto do mundo.

Fonte: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

Sabemos que a popularização das criptomoedas é um dos fatores que contribuiu para transformar o crime de sequestro de dados em um negócio. Elas tornaram impossível rastrear o destino do valor do resgate, dando maior liberdade para a ação desses criminosos. Por isso, este ano incluímos no relatório dados de crimes cibernéticos relacionados às criptomoedas.

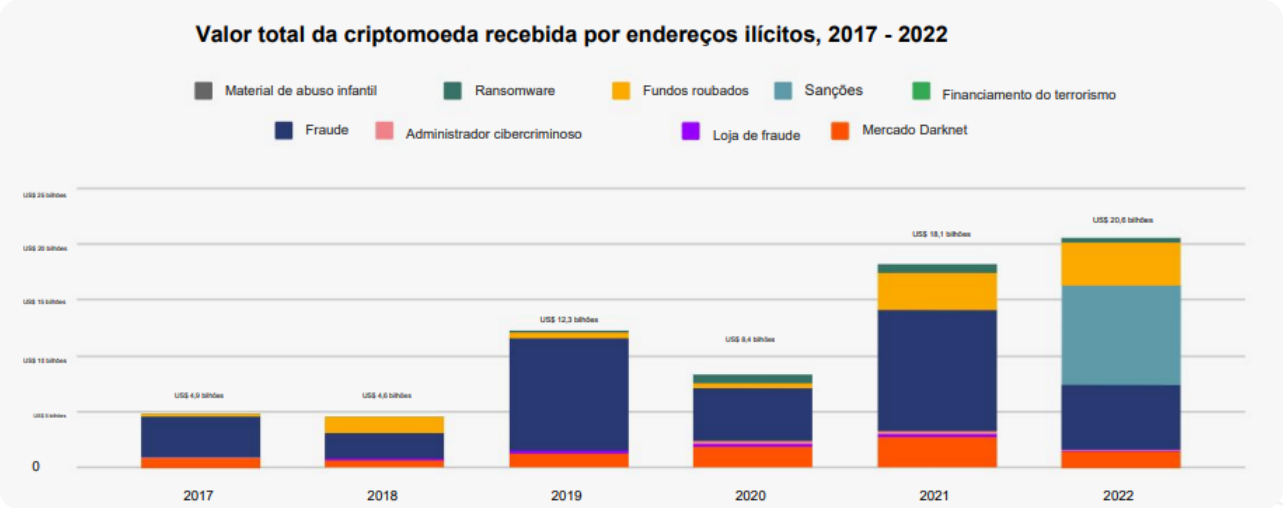
THE 2023 CRYPTO CRIME REPORT (FEVEREIRO 2023)



Chainalysis é uma plataforma de dados de blockchain. Eles fornecem dados, software, serviços e pesquisas para entidades governamentais, instituições financeiras, seguradores e empresas de cyber segurança em mais de 60 países.

O gráfico abaixo retrata uma estimativa dos valores recebidos por endereços de grupos criminosos. Os números surpreendem. É preciso ter em mente que 43% do volume de transações ilícitas em 2022 veio de atividades associadas a entidades sancionadas, em um ano no qual a OFAC lançou algumas das suas sanções criptográficas mais difíceis de serem aplicadas.

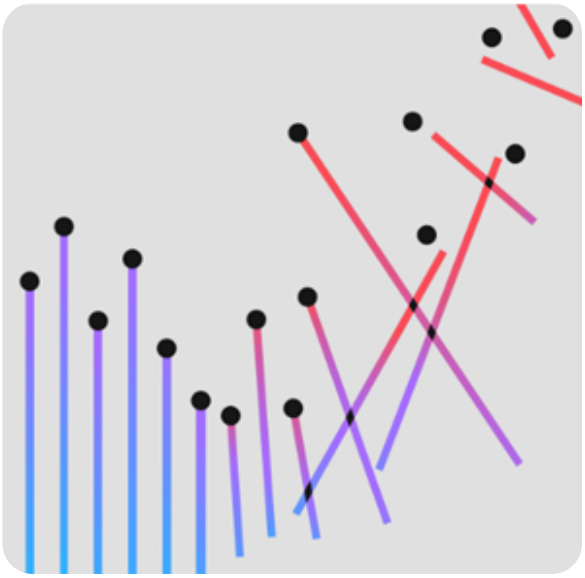
$20.6 bilhões foi a maior quantia recebida em 2022.



Fonte: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf

Os próximos destaques são relativos a relatórios de incidentes e vazamento de dados. Eles foram elaborados por grandes players de mercado para obter informações sobre os impactos de um ataque nas organizações. O objetivo é entender o que as organizações do mundo todo estão passando e como os ataques podem ser evitados.

IBM: COST OF A DATA BREACH REPORT 2023



Quanto custa uma violação de dados? O relatório anual da IBM analisou 553 empresas de pequeno, médio e grande porte, de 16 países, para responder esta questão.
A pesquisa foi conduzida de março de 2022 até março de 2023.

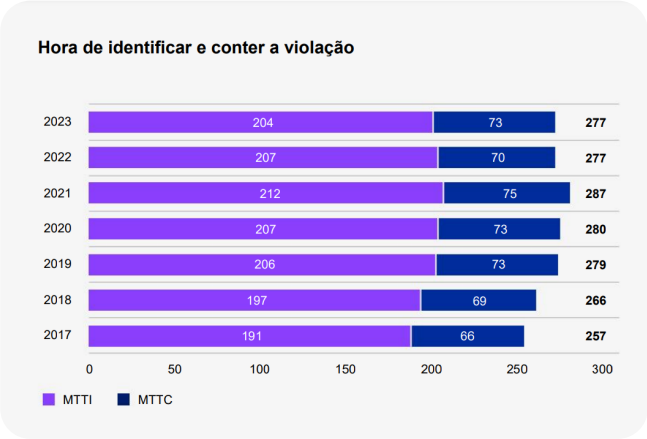
Em 2023, o custo médio de um ataque de ransomware foi de US$ 4,45 milhões, um aumento de 2.3% em relação a 2022 e 15.3% em relação a 2020.

- 51% das empresas planejam investir mais em segurança após sofrerem um vazamento.
- Apenas 1/3 das empresas identificaram brechas com seus times próprios.
- 67% das violações foram reportadas por parceiros ou pelos próprios atacantes.
- 82% dos vazamentos envolveram dados armazenados em núvens públicas.

Fonte: https://www.ibm.com/downloads/cas/E3G5JMBP

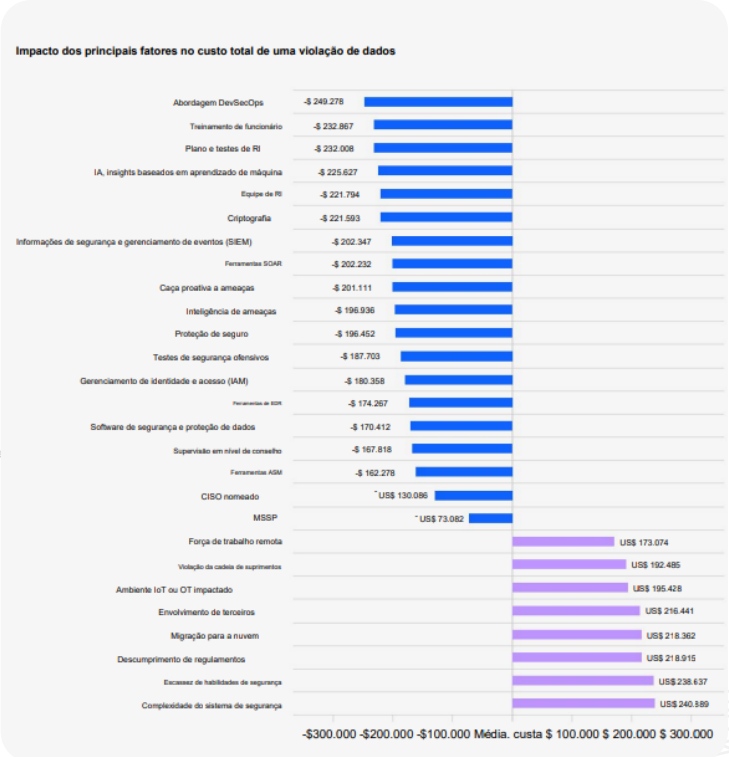
O vetor de ataque inicial mais comum - **phishing**, foi responsável por 16% das violações. O custo médio de vazamento de dados causado por phishing foi de USD 4,90 milhões - o que evidencia ainda mais a importância do treinamento e conscientização das equipes em relação à Segurança da Informação. Em segundo lugar ficou credenciais comprometidas, com 15% das violações. Em terceiro lugar está configurações incorretas em nuvens públicas.

Em 2022, as organizações levaram, em média, 207 dias para identificar uma violação de segurança. Em contraste, em 2023, esse período diminuiu em 3 dias. Por outro lado, em 2023, as organizações levaram, em média, 73 dias para conter violações, enquanto em 2022, esse período era, em média, de 70 dias. Os maiores tempos médios para conter e identificar violações ocorreram em 2021, com 212 e 75 dias, respectivamente.



Brasil possui o menor custo por vazamento em 2023. Houve uma redução de $1.38M (2022) para $1.22M (2023).

Os três fatores classificados como mais eficazes na mitigação de custos - aqueles associados à maior redução de custos - são a adoção de uma abordagem DevSecOps, o treinamento de colaboradores e o planejamento de resposta a incidentes e testes.



Os maiores amplificadores de custos foram a segurança complexidade do sistema, escassez de talentos na area de segurança, e descumprimento de regulamentos.

Fonte: https://www.ibm.com/downloads/cas/E3G5JMBP

DBIR 2023: DATA BREACH INVESTIGATIONS REPORT

O relatório de investigações de violação de dados da Verizon Threat Research Advisory Center (VTRAC) analisa casos trazidos pelos pesquisadores da empresa, relatórios dos colaboradores externos, além de incidentes divulgados publicamente.

953,894 incidentes analisados, com 254,968 confirmações de vazamento de dados.

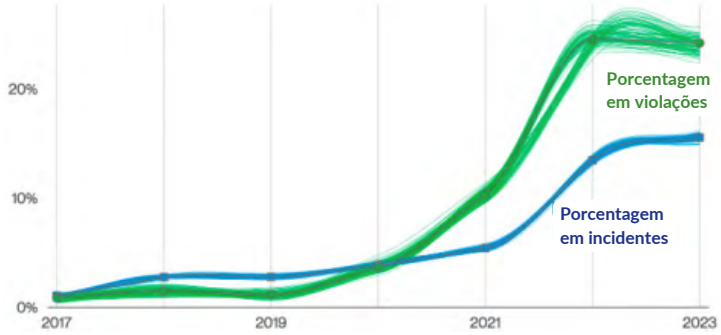
Mais de 32% de todas as verificações do Log4j atividade ao longo do ano aconteceu dentro de 30 dias após seu lançamento, (com o maior pico de atividade ocorrendo dentro de 17 dias).

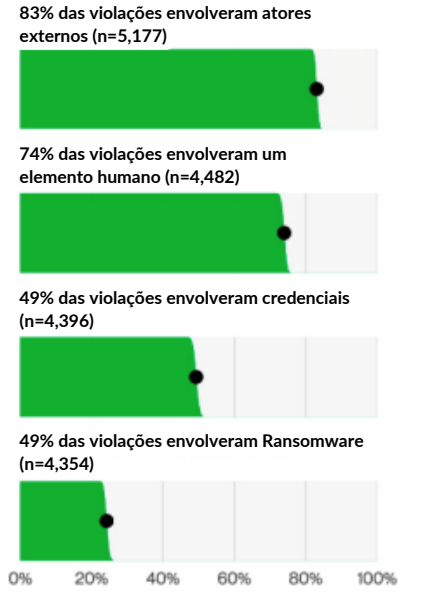
Esta velocidade é uma comparação interessante versus o tempo médio das organizações para corrigir, que atualmente é de 49 dias para casos de vulnerabilidades críticas, um número que permaneceu relativamente consistente ao longo dos anos.

Apoiadores na construção do DBIR:

Fonte: https://www.verizon.com/business/resources/Ta89/reports/2023-data-breach-investigations-report-dbir.pdf

O ransomware continua seu reinado como um dos principais tipos de ação presentes em violações, manteve-se estatisticamente estável em 24%. Ransomware é onipresente entre organizações de todos os tamanhos e em todas as indústrias.



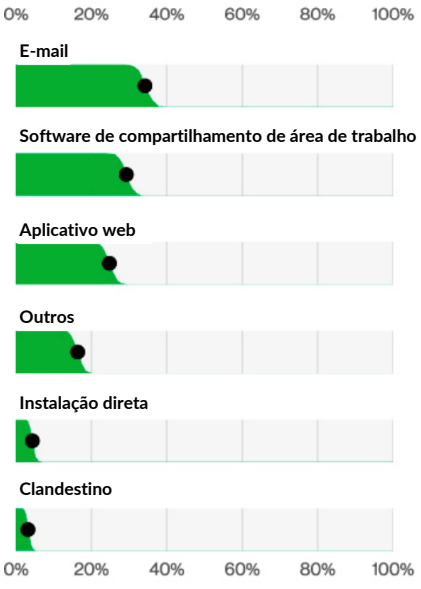


O gráfico ao lado mostra claramente que o treinamento dos colaboradores é indispensável na defesa contra ransomware.

74% de todas as violações incluem elemento humano, com pessoas estando envolvidas por erro, uso indevido de privilégio, uso de credenciais roubadas ou Engenharia Social.

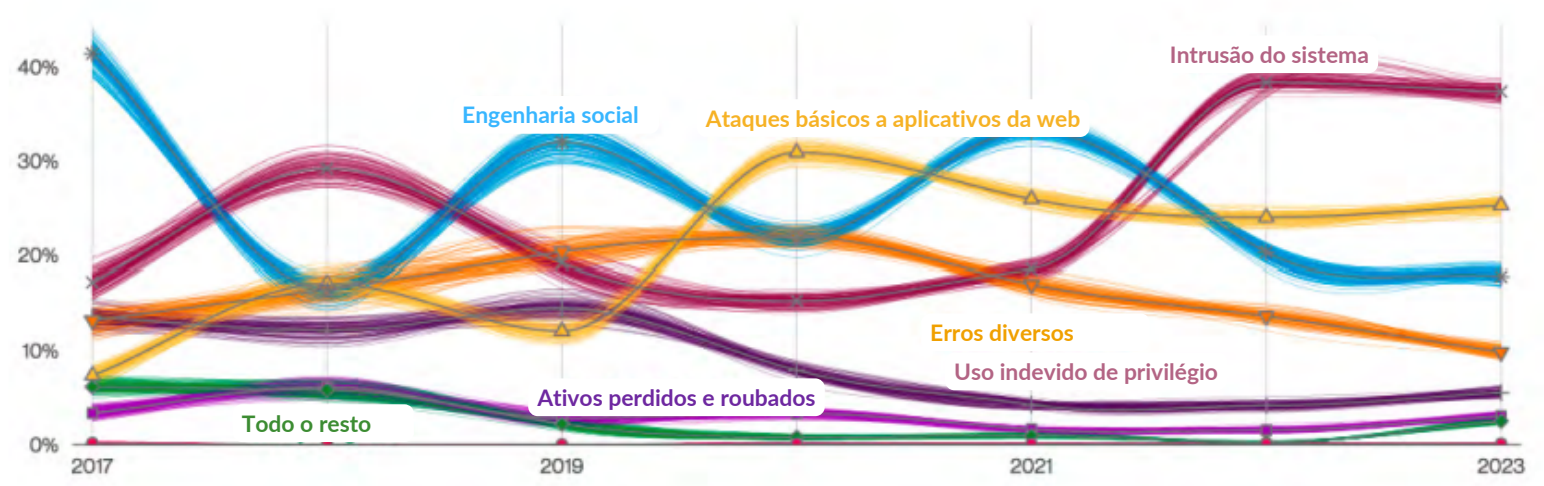
83% das violações envolveram atores externos e a principal motivação para os ataques continuam a ser financeira , em 95% das violações.

As três principais maneiras pelas quais invasores acessam uma organização são credenciais roubadas, phishing e exploração de vulnerabilidades



Os maiores vetores de ataque são acesso por phishing e softwares de compartilhamento de desktop.

Fonte: https://www.verizon.com/business/resources/Ta89/reports/2023-data-breach-investigations-report-dbir.pdf



Intrusão de sistemas através de vulnerabilidades **(~40%)**, ataque a aplicações web **(~25%)**, e engenharia social **(~18%)** são os padrões de ataques.

Na america latina os maiores motivadores dos ataques são:

Financeiro (93%)

Fonte: https://www.verizon.com/business/resources/Ta89/reports/2023-data-breach-investigations-report-dbir.pdf

DADOS SEPARADOS POR REGIÕES:

Região	Frequência	Principais padrões	Atores de ameaças	Motivos do ator	Dados comprometidos
APAC	699 incidentes, 164 com divulgação de dados confirmada	Engenharia social, Intrusão do sistema e Aplicativo Web Básico Os ataques representam 93% das violações	Externo (92%), Interno (9%), Parceiro (2%), Múltiplo (2%) (violações)	Financeiro (61%), Espionagem (39%), Conveniência (2%), Rancor (2%), Secundário (1%) (violações)	Interno (56%), Segredos (42%), Outros (33%), Credenciais (29%) (violações)
EMEA	2.557 incidentes, 637 com divulgação de dados confirmada	Intrusão do Sistema, Social Engenharia e Básico Ataques a aplicações web representam 97% das violações	Externo (98%), Interno (2%), Múltiplo (1%) (violações)	Financeiro (91%), Espionagem (8%), Ideologia (1%), Diversão (1%) (violações)	Credenciais (53%), Interno (37%), Sistema (35%), Outros (15%) (violações)
LACA	535 incidentes, 65 com divulgação de dados confirmada	Intrusão do Sistema, Social Engenharia e Básico Ataques a aplicações web representam 94% das violações	Externo (95%), Interno (5%), Parceiro (2%), Múltiplo (2%) (violações)	Financeiro (93%), Espionagem (11%), Ideologia (2%) (violações)	Sistema (55%), Interno (32%), Classificado (23%), Credenciais (23%), Outros (19%) (violações)
N/D	9.036 incidentes, 1.924 com divulgação de dados confirmada	Intrusão de Sistema, Básica Ataques a aplicações web e engenharia social representam 85% das violações	Externo (94%), Interno (12%), Múltiplo (9%), Parceiro (2%) (violações)	Financeiro (99%), Espionagem (1%), Rancor (1%) (violações)	Credenciais (67%), Interno (50%), Pessoal (38%), Outros (24%) (violações)

America Latina e Caribe.

535
INCIDENTES

EM

65
CASOS

Com vazamentos de dados confirmados!

O número é significativamente menor em comparação com a América do Norte, onde foram registrados 9.036 incidentes, incluindo 1.924 casos confirmados de vazamento de dados. No Brasil, não existe uma legislação que obrigue as empresas a divulgar incidentes, a menos que ocorra um vazamento de dados pessoais.

Fonte: https://www.verizon.com/business/resources/Ta89/reports/2023-data-breach-investigations-report-dbir.pdf

ANÁLISE DE DADOS POR SEGMENTO:

Número de incidentes e violações de segurança por setor, vítima e tamanho da organização.

	Incidentes				Violações			
Indústria	Total	Pequeno (1–1.000)	Grande (mais de 1.000)	Desconhecido	Total	Pequeno (1–1.000)	Grande (mais de 1.000)	Desconhecido
Total	16.312	694	489	15.129	5.199	376	223	4.600
Alojamento (72)	254	4	2	248	68	4	1	63
Administrativo (56)	38	8	14	16	32	8	11	13
Agricultura (11)	66	1	5	60	33	0	3	30
Construção (23)	87	7	1	79	66	4	1	61
Educação (61)	496	63	15	418	238	28	8	202
Entretenimento (71)	432	13	3	416	93	10	1	82
Finanças (52)	1.829	70	30	1.729	477	38	18	421
Saúde (62)	522	28	15	479	433	23	15	395
Informação (51)	2.105	45	110	1.950	380	23	19	338
Gestão (55)	9	1	0	8	9	1	0	8
Fabricação (31–33)	1.814	37	24	1.753	259	18	15	226
Mineração (21)	25	2	0	23	13	2	0	11
Outros serviços (81)	143	7	2	134	100	6	1	93
Profissional (54)	1.396	176	54	1.166	421	85	32	304
Administração Pública (92)	3.270	87	110	3.073	582	48	39	495
Imobiliário (53)	83	15	5	63	59	10	2	47
Varejo (44–45)	404	62	44	298	191	33	28	130
Transporte (48–49)	349	13	25	311	106	8	13	85
Utilitários (22)	117	12	6	99	33	3	3	27
Comércio Atacadista (42)	96	42	22	32	53	23	11	19
Desconhecido	2.777	1	2	2.774	1.553	1	2	1.550
Total	16.312	694	489	15.129	5.199	376	223	4.600

Fonte: https://www.verizon.com/business/resources/Ta92/reports/2023-data-breach-investigations-report-dbir.pdf

COMO ESTÁ A REALIDADE DAS EMPRESAS ?

A evolução das ameaças cibernéticas indica que a Segurança da Informação precisa ganhar cada vez mais importância nas decisões estratégicas das empresas. Dessa forma, a chamada cultura da segurança da informação deixou de ser um assunto a ser tratado somente na iminência de um ataque - é preciso um trabalho contínuo para reduzir os riscos de um incidente desse tipo, que impacta nos resultados dos negócios. É necessário que a cultura da segurança faça parte das organizações pois, para ser efetiva, ela deve envolver todos os setores.

Após uma análise do cenário mundial, fica o questionamento: como está a realidade das empresas? O Relatório de Segurança da Informação da Netfive tem como objetivo responder esta pergunta e, além disso, mapear a maturidade de SI das organizações.

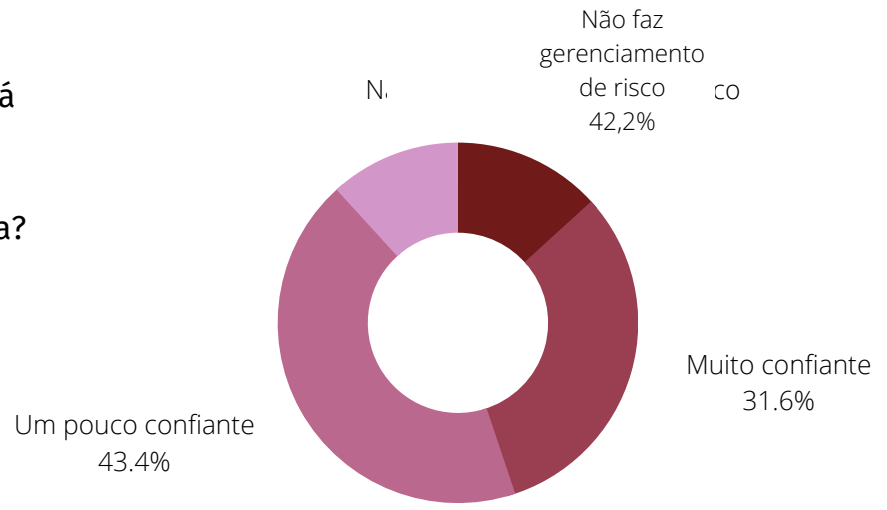
Para isso, foi aplicado um questionário anônimo em uma amostra da região Sul e São Paulo de médio e grande porte. Um SCAN de vulnerabilidades também foi rodado com outra amostra, de 136 organizações de médio e grande porte.

A análise dos resultados nos permitiu ter uma visão do cenário atual da Segurança da Informação no nosso Estado, como mostraremos a seguir de forma detalhada e analítica.

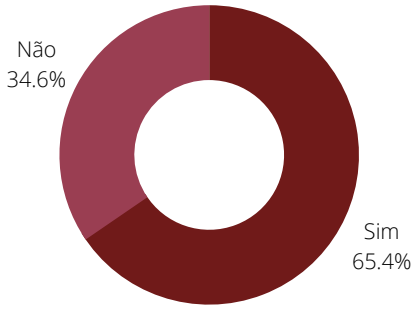
Este é o terceiro ano da realização desta pesquisa RSIN, e o trabalho foi realizado com o apoio da **Fritsch Consulting**. Agradecemos ao parceiro Inácio Fritsch pelo apoio na elaboração do relatório.

RESULTADOS: TOTAL DE 136 RESPOSTAS

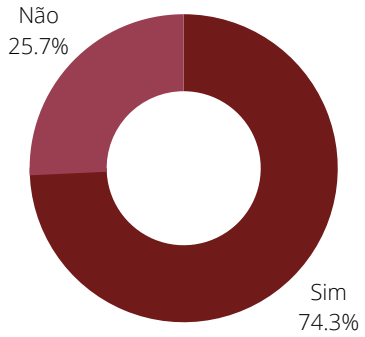
O quão confiante você está nas decisões de gerenciamento de risco tomadas pela sua empresa?



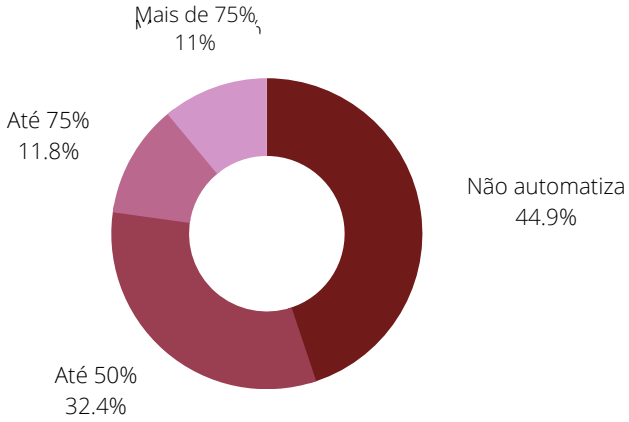
A sua empresa conduz programas de treinamento e conscientização sobre as ameaças cibernéticas aos seus colaboradores?



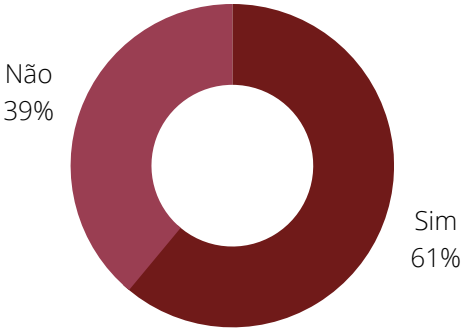
A sua empresa possui um gerenciamento contínuo de vulnerabilidades (identificação, priorização e correção)?



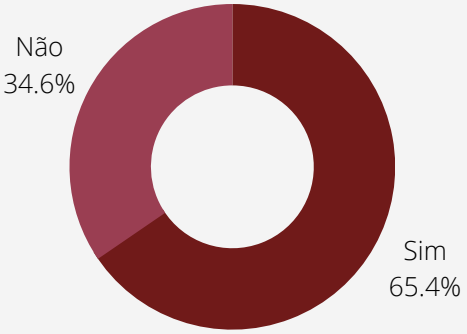
Em relação às correções, quantos % são automatizadas?



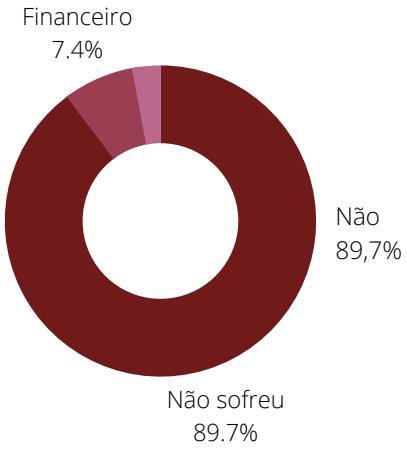
A sua empresa possui planos de respostas a incidentes de segurança cibernética?



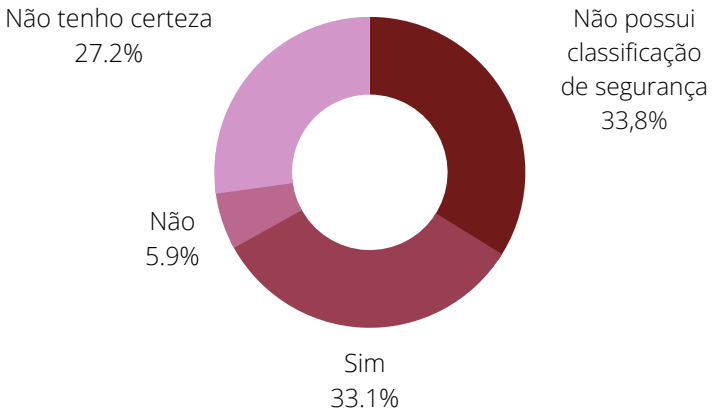
A sua empresa adota alguma norma ou framework de segurança? Exemplo: Instituto Norte-americano de Normas e Tecnologia (NIST), Organização Internacional de Normalização (ISO), Center for Internet Security (CIS), outros.



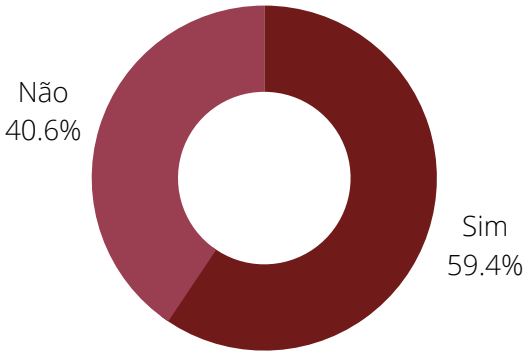
A sua empresa sofreu impactos de um ataque bem-sucedido no último ano? Se sim, em qual aspecto você considera o maior dano?



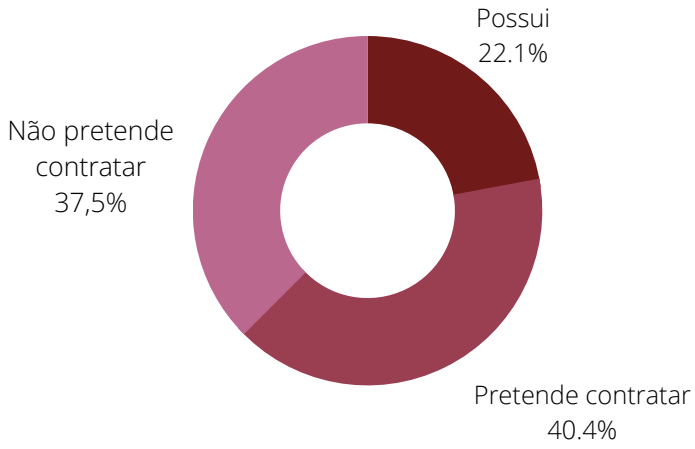
Você acredita que a classificação de segurança atribuída à sua empresa é um reflexo preciso da realidade?



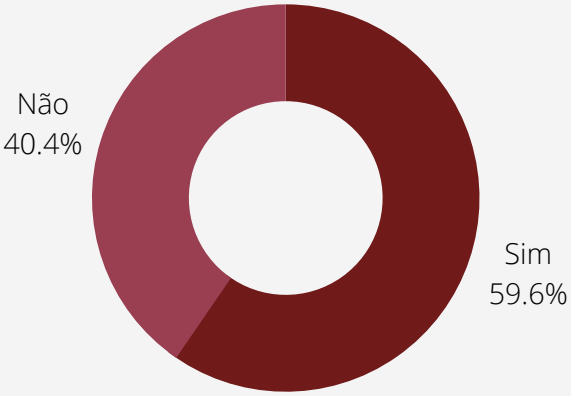
Sua empresa tem implementado medidas para promover o alinhamento com os princípios de ESG (Ambiental, Social e Governança)?



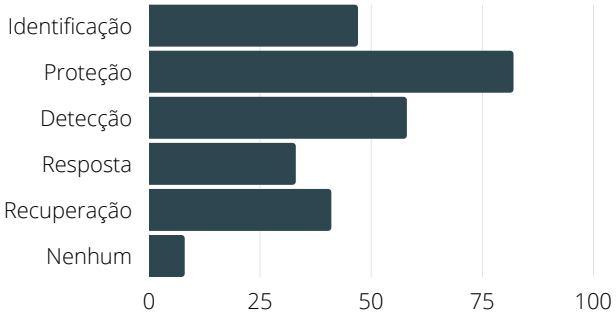
A sua empresa possui ou pretende contratar seguro para riscos digitais nos próximos 3 anos?



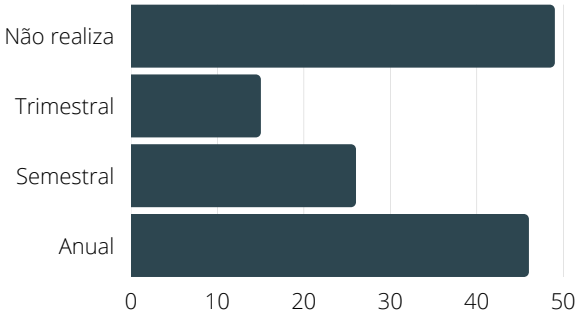
A sua empresa enfrenta dificuldades na contratação e retenção de profissionais de segurança cibernética?



Foco em investimento:

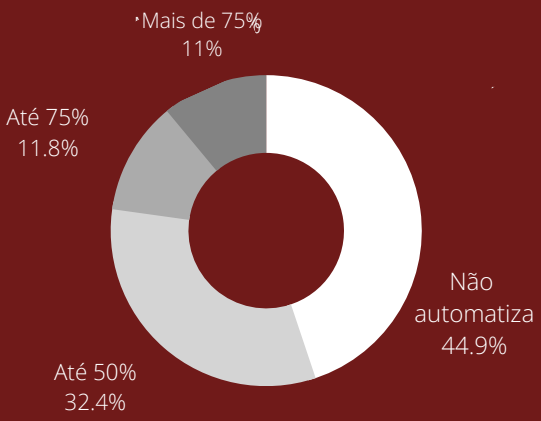


Periodicidade de pentest:

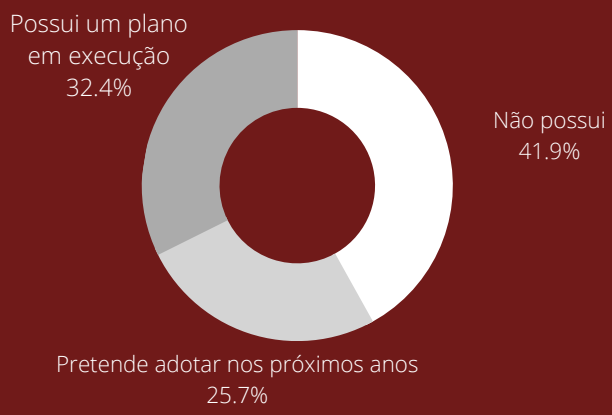


PERGUNTAS INSERIDAS NESSE ANO:

Em relação às correções de vulnerabilidades, quantos % são automatizadas?



Sua empresa adota um plano diretor de segurança da informação?



RESULTADO DO SCAN

272
Empresas escaneadas

16% das empresas têm, ao menos, **1 vulnerabilidade crítica.**

A proporção de empresas com vulnerabilidades críticas aumentou 10%, porém a quantidade de vulnerabilidades por empresa reduziu para 1.

Essas vulnerabilidades têm um alto potencial de causar danos e são facilmente exploradas. Portanto, é possível afirmar que o risco geral aumentou, considerando que a presença de apenas uma delas permitiria o acesso ao ambiente da organização.

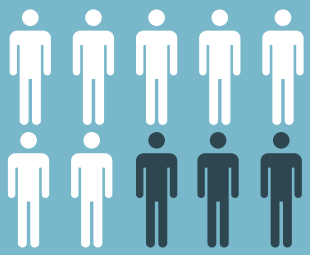
83% das empresas possuem **erros de configuração** que expõem dados sensíveis (CWE-200).

A proporção de empresas com vulnerabilidades com risco alto foi **10% maior do que em 2022,** e o número de **vulnerabilidades por empresa aumentou 30%.**

CONCLUSÕES

O número de ataques por região chama a atenção pelo baixo número na América Latina. Isso pode ocorrer porque os ataques não são reportados, pela inexistência de logs completos ou porque o foco principal do ataque não é a nossa região.

O SCAN mostrou que a maioria dos assets de empresas está localizado em datacenters nos EUA, o que pode aumentar a chance de ataques. Também foi identificado que DevSecOps*, treinamento de funcionários e planejamento de Resposta a Incidentes são os maiores mitigadores de custos durante uma violação. Veja a seguir outras conclusões:



74% dos casos de vazamento de dados têm relação com erros humanos.

93%

dos ataques são motivados pelo retorno financeiro.

Cada ataque de ransomware causa, em média, prejuízos de **R$6,8 milhões.**

A maior quantia recebida por grupos criminosos foi de **$20.6 bilhões em 2022.**

O custo médio de uma violação diminuiu em 2022 no Brasil. **O total baixou de $1,38 milhões para $1,22 milhões de dólares.**

*DevSecOps é uma abordagem de desenvolvimento de software que integra a segurança (Sec) desde o início (Dev) do ciclo de vida do desenvolvimento e operações (Ops). Ela visa automatizar e incorporar práticas de segurança de forma contínua em todas as etapas do processo de desenvolvimento de software.

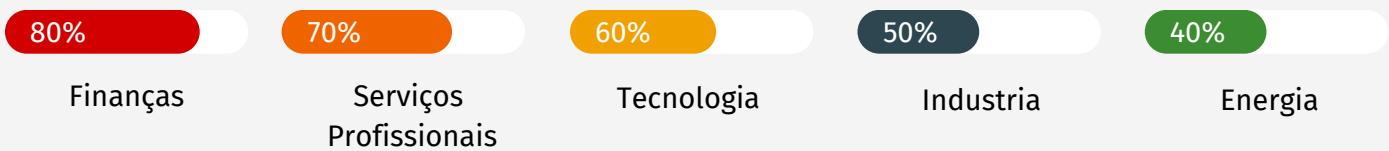
Ataques cibernéticos continuam nas **top 3 preocupações dos CEOs,** perdendo apenas para instabilidades macroeconômicas e inflação.

O mercado mostra necessidade de profissionais de SI. **Cerca de 530 mil vagas abertas na América Latina.**

O tempo médio para recuperação de um ataque manteve-se igual (277 dias). Fato curioso está na redução de 3 dias para detectar, porém, houve um aumento de 3 dias para responder.

E o tempo médio para as empresas corrigirem vulnerabilidades está muito acima (49 dias) se comparado ao tempo que os atacantes exploram o ambiente a ser atacado.

PRINCIPAIS ALVOS POR SEGMENTO:



PONTOS POSITIVOS E NEGATIVOS

74% fazem gestão de vulnerabilidades (72% em 2022). Neste ano também questionamos as empresas se havia automação no seu processo de gestão de vulnerabilidades, e somente 22.8% delas automatizam um volume significativo.

72% fazem gestão de risco. É um ótimo resultado, ainda mais sabendo que é 6% maior do que no ano passado. Esse dado mostra que as empresas estão preocupadas com os riscos.

65.4% fazem treinamento e capacitação. Houve um aumento de apenas 4% treinamento e capacitação com relação ao ano passado. É um bom sinal! Porém, a meta é chegar a 100%, e para isso temos um longo caminho pela frente.

40% querem fazer seguro, representando uma diminuição de 5% em relação ao estudo anterior.

Somente 21% dos investimentos são direcionados à detecção. Os investimentos em detecção e recuperação precisam aumentar. Pois o tempo médio de detecção e recuperação dos ambientes são de 277 dias.

61% têm plano de respostas à incidentes de SI. O plano é fundamental para orquestrar as atividades numa situação crítica. Ainda é um ponto negativo, apesar de ter aumentado 8%.

59% têm dificuldade de contratação, uma pequena redução em relação ao ano anterior (63%). Acreditamos que a falta de profissionais vai continuar sendo um problema pelos próximos anos.

36% não fazem pentest. Um pentest de redes vem sendo substituído por uma gestão de superfície de ataque contínua, o que pode ser uma alternativa para estas empresas. Lembrando que se um pentest for contratado, deve incluir teste de aplicações e API.

53% utilizam algum framework. A falta de uso de framework pode gerar entregas com qualidade inferior ao esperado.

QUESTIONÁRIO APLICADO

- O quão confiante você está nas decisões de gerenciamento de risco tomadas pela sua empresa?
- A sua empresa conduz programas de treinamento e conscientização sobre as ameaças cibernéticas aos seus colaboradores?
- A sua empresa possui um gerenciamento contínuo de vulnerabilidades (identificação, priorização e correção)?
- Em relação às correções, quantos % são automatizadas?
- A sua empresa possui planos de respostas a incidentes de segurança cibernética?
- Você acredita que a classificação de segurança atribuída à sua empresa é um reflexo preciso da realidade?
- Sua empresa adota um plano diretor de segurança da informação?
- A sua empresa sofreu impactos de um ataque bem-sucedido no último ano? Se sim, em qual aspecto você considera o maior dano?
- A sua empresa possui ou pretende contratar seguro para riscos digitais nos próximos 3 anos?
- A sua empresa enfrenta dificuldades na contratação e retenção de profissionais de segurança cibernética?
- A sua empresa realiza pentest com qual frequência?
- Os investimentos de cibersegurança da sua empresa no próximo ano serão destinados a:
- A sua empresa adota alguma norma ou framework de segurança? Exemplo: Instituto Norte-americano de Normas e Tecnologia (NIST), Organização Internacional de Normalização (ISO), Center for Internet Security (CIS), outros.

SOBRE O SCAN

Para o SCAN de vulnerabilidades foram utilizadas as mesmas técnicas que um atacante usaria. Iniciamos somente com o domínio da organização e a partir dele foram enumerados subdomínios e tecnologias utilizadas nos sistemas. Após a enumeração, foram executados programas opensource que identificam vulnerabilidades conhecidas (CVEs) e classificam o risco como baixo, médio ou alto, baseado no impacto que a vulnerabilidade explorada pode causar na organização.

RECOMENDAÇÕES

1. As empresas precisam **adotar mecanismos de correção automática de vulnerabilidades** para tornar eficaz o programa de gestão de vulnerabilidades e liberar o tempo das equipes de TI/SI para outras demandas.

2. **Identificar ameaças e atores antes que causem impactos à organização precisa estar no topo dos investimentos para o próximo ano,** sendo o MDR o melhor custo/benefício.

3. **Garantir a recuperação do ambiente continua sendo fundamental,** as empresas que não atingiram essa maturidade precisam endereçar esse assunto em caráter de urgência

2023 RSIN

RELATÓRIO DE SEGURANÇA DA INFORMAÇÃO DA NETFIVE.

netfive

FALE COM UM ESPECIALISTA

Entre em contato diretamente conosco

51. 3061-4446

contato@netfive.com.br

Henrique Schneider

CEO

Vagner Christ

Security Specialist