netfive

RSIN

2024 - RS

3° EDIÇÃO

RELATÓRIO DE SEGURANÇA DA INFORMAÇÃO DA NETFIVE.

contato@netfive.com.br
www.netfive.com.br

Av. Palmeira, 330 - 7º e 11º andar
Petrópolis - Porto Alegre - RS
CEP: 90470-300

Av. Dr. Chucri Zaidan, 1240 - 21º andar
Morumbi - São Paulo - SP
CEP: 04711-130

SUMÁRIO

netfive

Vagner Christ

Service Director

Prezado Leitor,

A segurança cibernética tornou-se uma prioridade inegociável no cenário global, com ameaças cada vez mais sofisticadas e impactantes. **Este relatório abrangente oferece uma análise aprofundada das tendências e desafios que moldam a segurança da informação em 2024.** Ao longo destas páginas, você encontrará insights valiosos sobre as principais ameaças, desde ataques de ransomware e extorsões até a crescente sofisticação da engenharia social e o uso malicioso da inteligência artificial. Nosso objetivo é fornecer uma visão clara e estratégica para que você, como líder ou profissional de segurança, possa fortalecer suas defesas, antecipar riscos e garantir a resiliência de sua organização em um ambiente digital em constante evolução.

Acreditamos que a informação é a base para a tomada de decisões eficazes. Por isso, este relatório não se limita a listar ameaças, mas também **oferece recomendações práticas e estratégias comprovadas para mitigar riscos e proteger seus ativos mais valiosos.** Incentivamos você a explorar cada seção, refletir sobre as implicações para sua organização e implementar as medidas necessárias para construir uma postura de segurança robusta e adaptável.

Lembre-se de que a segurança cibernética é uma jornada contínua, não um destino. Convidamos você a se juntar a nós nesta missão crítica de proteger o mundo digital e construir organizações mais resilientes.

netfive

INTRODUÇÃO
RSIN 3°EDIÇÃO:

A segurança cibernética nunca esteve tão crítica para organizações em todos os setores. O aumento exponencial de ataques direcionados, a sofisticação de ameaças impulsionadas por **inteligência artificial**, e a exploração de **credenciais roubadas e vulnerabilidades em ambientes de nuvem** colocam empresas e governos em um cenário de alto risco.

O **RSIN 2024** é um relatório consolidado que reúne as principais descobertas dos relatórios mais relevantes do setor, incluindo:

- **The 2024 Crypto Crime Report (Chainalysis)**
- **27ª CEO Survey (PwC)**
- **Allianz Risk Barometer 2025**
- **Data Breach Investigations Report 2024 (Verizon - DBIR)**
- **Avaliação de Segurança e Risco para Fornecedores (WEF)**
- **State of the Phish 2024 (Proofpoint)**
- **Global Threat Report 2024 (CrowdStrike)**

A crescente sofisticação dos ataques exige que as empresas adotem uma **postura de segurança adaptativa e resiliente.** Neste relatório, que conta com a participação de mais de **160 empresas do Rio Grande do Sul**, são apresentadas recomendações planejadas para **fortalecer defesas, reduzir riscos e garantir a continuidade dos negócios.**

A segurança cibernética não deve ser tratada como um custo, mas como **um investimento estratégico essencial** para proteger ativos digitais, manter a confiança dos clientes e garantir a competitividade no mercado

Ao unir esses insights, este relatório oferece **uma visão estratégica e operacional** para executivos, líderes de segurança da informação e equipes técnicas, permitindo que as organizações antecipem ameaças e reforcem suas defesas contra ataques cibernéticos.

Resumo Executivo:

PRINCIPAIS AMEAÇAS E PREOCUPAÇÕES

A análise consolidada dos relatórios confirma **cinco tendências principais que moldam o cenário global de ameaças cibernéticas em 2024:**

netfive

1 Aumento de Ataques Baseados em Identidade e Engenharia Social

- **Fraudes de phishing continuam sendo o principal vetor de ataques cibernéticos.**
- **Comprometimento de e-mails corporativos (BEC) cresce exponencialmente,** com atacantes explorando **táticas avançadas de engenharia social.**
- **Roubo de credenciais impulsiona invasões:** hackers utilizam **credenciais roubadas e exploração de MFA** para acessar sistemas corporativos.
- **Autenticação multifator (MFA) está sendo contornada por ataques de proxy reverso (EvilProxy) e phishing baseado em telefone (TOAD).**

Impacto setorial: setores financeiro, tecnologia e governo são os mais afetados.

2 Ransomware e Extorsão de Dados se Tornam Mais Sofisticados

76% **De aumento** no número de vítimas listadas em sites de vazamento de ransomware.

- **Extorsão de dados supera a simples criptografia de arquivos:** grupos criminosos estão priorizando **vazamento e monetização de informações roubadas.**

- **Técnicas de tripla extorsão combinam ransomware, vazamento de dados e ataques DDoS.**

- **Infraestruturas críticas continuam sendo alvos estratégicos, com ataques mirando sistemas industriais e hospitais.**

Impacto setorial: saúde, manufatura e serviços financeiros estão entre os mais impactados.

3 Expansão dos Ataques à Nuvem e à Cadeia de Suprimentos

110%

de crescimento em ataques direcionados a ambientes de nuvem, aproveitando credenciais expostas e erros de configuração.

34

novos grupos de ameaças foram identificados explorando ambientes em nuvem, segundo a CrowdStrike.

- **Softwares confiáveis e fornecedores terceirizados são alvos estratégicos,** resultando em **maior número de ataques via supply chain.**

Impacto setorial: empresas de SaaS, tecnologia e grandes infraestruturas corporativas enfrentam desafios crescentes.

4 Inteligência Artificial (IA) Potencializa Ataques Cibernéticos

-2 MINUTOS

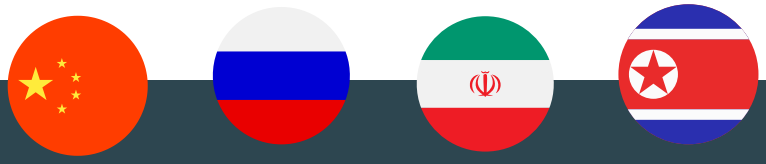
Hackers estão utilizando IA para automatizar ataques, reduzindo tempo de invasão para menos de 2 minutos em alguns casos.

- **IA generativa permite criação de fraudes altamente convincentes,** como deepfakes e mensagens de phishing hiperpersonalizadas.

- **Malwares polimórficos impulsionados por IA dificultam a detecção, exigindo novas estratégias de defesa.**

Impacto setorial: todos os setores estão vulneráveis, mas finanças, mídia e telecomunicações são os mais expostos.

5 Ameaças Geopolíticas e Espionagem Cibernética Crescem



China, Rússia, Irã e Coreia do Norte lideram operações de espionagem cibernética e sabotagem.

Ataques contra infraestruturas críticas estão aumentando, visando desestabilizar setores estratégicos.

2024 foi um ano crítico para eleições globais, com adversários explorando desinformação e manipulação digital.

2024

Impacto setorial: setores governamentais, telecomunicações e indústrias estratégicas são os principais alvos.

netfive

The 2024 Crypto Crime Report (Chainalysis)

A Chainalysis é uma referência global na análise de transações ilícitas envolvendo criptomoedas. Seu relatório de 2024 destaca uma queda significativa nos crimes financeiros digitais, **com exceção do ransomware, que voltou a crescer.**

Redução no volume de crimes financeiros

US$ 24,2 BILHÕES

movimentados em atividades ilícitas, representando

0,34%

de **volume**

Queda de

29,2%

nos golpes **financeiros** e

54,3%

na quantia **roubada por hackers.**

netfive

Adoção crescente de stablecoins por criminosos devido à menor volatilidade.

Ransomware em ascensão

Ransomware voltou a crescer, **impulsionado por grupos especializados em ataques sofisticados.**

Hackers exigem pagamentos em stablecoins, dificultando a rastreabilidade.

netfive

Sanções e Lavagem de Dinheiro

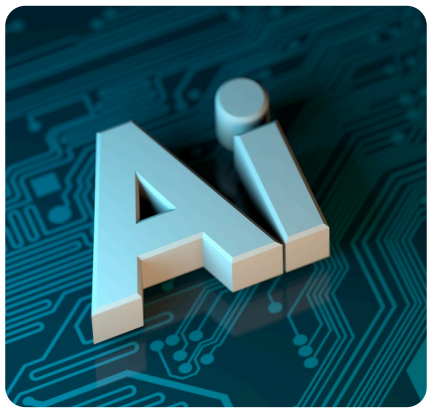
61,5%

das transações ilícitas envolveram entidades sancionadas por governos.

Os criminosos utilizam exchanges descentralizadas (DEXs) e serviços de ofuscação para ocultar movimentações ilícitas.

Impactos na Segurança da Informação

Maior uso de **IA por criminosos** para **automatizar fraudes e ataques cibernéticos.**



netfive

Aumento na sofisticação dos esquemas de lavagem de dinheiro **via blockchain.**

Setores Mais Afetados

Setor Financeiro: Exchanges de criptomoedas e bancos sofrem forte impacto regulatório.

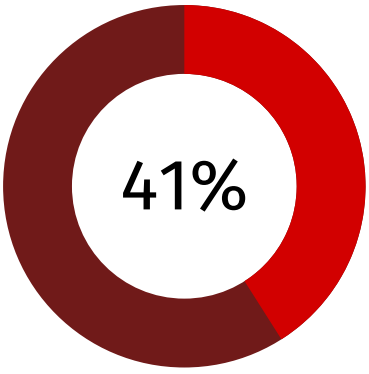
Setor de Tecnologia: Roubo de credenciais e exploração de carteiras digitais.

Órgãos Governamentais: Riscos aumentados de evasão fiscal e financiamento ilícito.

27ª CEO Survey (PwC)

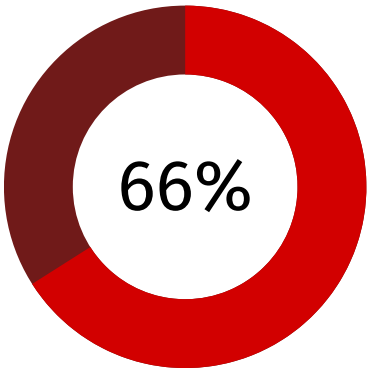
A pesquisa global da PwC abrange mais de **4.700 CEOs**, avaliando percepções sobre o futuro dos negócios. A edição de 2024 destaca **cibersegurança como prioridade estratégica** e a necessidade de **investimentos em IA e automação.**

Transformação Digital e Riscos Tecnológicos



dos **CEOs brasileiros** não acreditam que suas **empresas sobreviverão 10 anos** sem mudanças estratégicas.

dos **CEOs brasileiros** veem IA como essencial para **eficiência operacional.**



netfive

Cibersegurança no centro das decisões

Empresas aumentam **investimentos em proteção contra ransomware** e vazamento de dados.

Falta de talentos em cibersegurança ainda é um problema global.

?

Impactos na Segurança da Informação

Empresas estão investindo mais em **IA e automação para segurança cibernética.**

Fraudes financeiras e ataques a cadeias de suprimentos são as maiores preocupações.

Impactos na Segurança da Informação

Financeiro: Maior alocação de orçamento em cibersegurança.

Industrial e Manufatura: Riscos de espionagem industrial e ataques a OT (Operational Technology).

Tecnologia:

Crescimento de ataques a provedores de nuvem e infraestrutura digital.

Allianz Risk Barometer 2025

O Allianz Risk Barometer identifica **os principais riscos globais para empresas**, fornecendo insights sobre **ameaças cibernéticas, mudanças regulatórias e crises operacionais.**

Ranking Global de Riscos

38 % Incidentes cibernéticos

31 % Interrupção de negócios

25 % Catástrofes naturais

29 % Mudanças regulatórias e ESG

netfive

Ameaças cibernéticas continuam crescendo

Ataques a infraestruturas críticas **aumentaram globalmente.**

Empresas priorizam adoção de **Zero Trust Security.**

Setores Mais Afetados

Setor Financeiro: Bancos são os principais alvos de ataques cibernéticos.

Setor de Saúde: Vazamento de dados médicos continua sendo um crime lucrativo.

Setor de Energia e Indústria: Infraestruturas críticas estão na mira de hackers.

Data Breach Investigations Report 2024 (Verizon - DBIR)

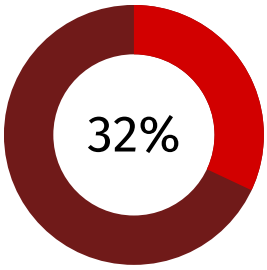
O **DBIR da Verizon** é uma das análises mais completas sobre violações de dados. A edição de 2024 apresenta um panorama detalhado das ameaças enfrentadas globalmente.

Principais Conclusões

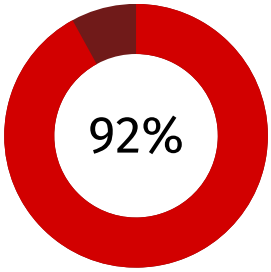
+ 10 MIL VISUALIZAÇÕES

violações confirmadas (recorde histórico).

Ransomware e **extorsão** cresceram



Afetando



das **indústrias analisadas.**

netfive

180%

Exploração de vulnerabilidades aumentou 180%, tornando-se a principal técnica usada por hackers.

Segurança da Informação e Cibersegurança

Empresas adotam Zero Trust Security, mas implementação ainda é lenta.

Erros humanos continuam sendo responsáveis por **68%** das **violações.**

68%

netfive

Setores Mais Afetados

Financeiro:

Alvo principal de phishing e ransomware.

Saúde:

Aumento no roubo de dados médicos.

Tecnologia:

Ataques direcionados a serviços em nuvem e IA.

State of the Phish 2024 (Proofpoint)

O relatório **State of the Phish 2024**, da Proofpoint, analisa tendências e riscos relacionados a **phishing, engenharia social e comportamento dos usuários.** O estudo se baseia em dados de **183 milhões de mensagens de phishing simuladas** e mais de **24 milhões de e-mails denunciados** por usuários.

Tendências Globais

71% **dos usuários realizaram ações arriscadas,** como reutilização de senhas e clique em links maliciosos.

96% **desses usuários sabiam que estavam assumindo um risco,** mas optaram por conveniência.

Ataques de **Business Email Compromise (BEC)** aumentaram significativamente, com mais de **1 milhão de ataques bloqueados mensalmente.**

1 MILHÃO

netfive

Phishing baseado em telefone (TOAD) e desvio de MFA (EvilProxy) continuam sendo ameaças críticas.

Ransomware segue afetando empresas globalmente, com um crescimento na sofisticação dos ataques.

Destaques sobre o Brasil

72% dos brasileiros admitem realizar ações arriscadas, ligeiramente acima da média global (71%).

72%

O "jeitinho brasileiro" influência a cultura de segurança, resultando em compartilhamento de senhas e negligência com boas práticas.

A maioria dos usuários acredita que a segurança deve ser "mais fácil" para ser priorizada.

netfive

Ransomware afetou 58% das empresas brasileiras, mas menos organizações pagaram resgates em 2024 em comparação a 2023.

58%

AUMENTO DE 8%

nos ataques BEC no Brasil, aproximando-se da média global.

Setores Mais Afetados

Setor financeiro: Alvo frequente de BEC e phishing.

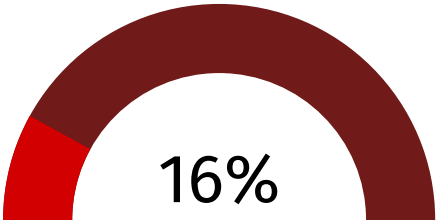
Setor de tecnologia: Crescente interesse dos atacantes devido à adoção de soluções em nuvem.

Indústria e manufatura: Impacto direto de ransomware e comprometimento da cadeia de suprimentos.

netfive

Principais Recomendações

Melhoria nos treinamentos de segurança: Apenas **16% das empresas brasileiras cobrem técnicas de engenharia social** nos treinamentos.



Adoção de tecnologias de proteção contra phishing, como autenticação avançada e proteção contra desvio de MFA.

Reforço na conscientização dos usuários, especialmente sobre os riscos de engenharia social e compartilhamento de senhas.

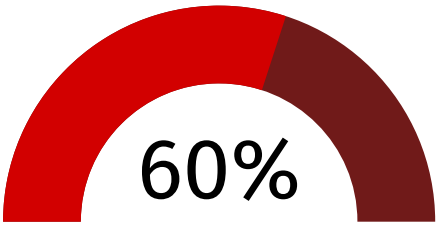
Global Threat Report 2024 (CrowdStrike)

O **Global Threat Report 2024** da CrowdStrike traz uma análise aprofundada sobre as **táticas e técnicas dos adversários, evolução do cenário de ameaças e tendências emergentes.** A pesquisa destaca um crescimento acelerado das ameaças baseadas em identidade e **a ascensão de ataques sofisticados impulsionados por inteligência artificial.**

O relatório foca em **ransomware, espionagem cibernética, ameaças à cadeia de suprimentos e exploração de vulnerabilidades em ambientes em nuvem.**

Tendências Globais

Aumento de 60% nas intrusões interativas (ataques manuais, sem malware).

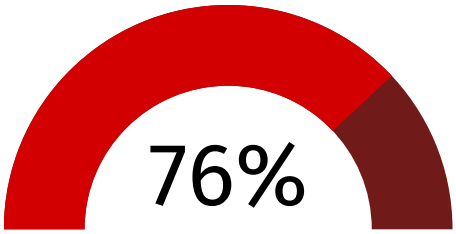


-22 MINUTOS

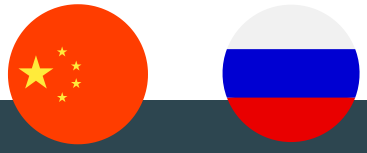
Redução do tempo de invasão: O tempo médio para um invasor se movimentar lateralmente na rede caiu de **84 minutos (2022) para 62 minutos (2023).**

Crescimento de 110% em ataques direcionados à nuvem, explorando configurações inadequadas e credenciais vazadas.

110%



de aumento no número de vítimas listadas em sites de vazamento de ransomware.

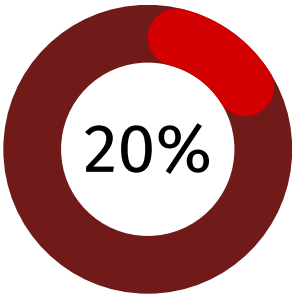


Adversários estatais continuam ativos: China e Rússia seguem liderando ataques de espionagem cibernética e operações de influência.

Cibersegurança e Segurança da Informação

Ataques baseados em identidade foram a principal ameaça cibernética de 2024.

Exploração de credenciais roubadas aumentou 20%, refletindo a sofisticação dos atacantes na obtenção de acessos legítimos.



Ransomware evoluiu para extorsão de dados, com grupos preferindo roubo de informações a bloqueio de sistemas.

O uso de IA por atacantes reduz barreiras para novos criminosos cibernéticos.

Setores Mais Afetados

Setor financeiro:

Crescimento das fraudes bancárias e ataques a APIs de pagamento.

Setor de tecnologia:

Empresas de SaaS e nuvem enfrentam ataques persistentes.

Setor industrial:

Infraestruturas críticas estão cada vez mais na mira de grupos estatais.

Principais Recomendações

Adoção de modelos de segurança Zero Trust: Com adversários explorando credenciais roubadas, **a autenticação baseada em comportamento é essencial.**

Monitoramento contínuo da cadeia de suprimentos:

Exploração de softwares confiáveis foi um dos vetores mais utilizados para acesso inicial.

Automação da detecção de ameaças: Respostas rápidas são essenciais, pois os ataques estão ocorrendo **em menos de 2 minutos em alguns casos.**

-2 MINUTOS

Resultado da pesquisa com as empresas:

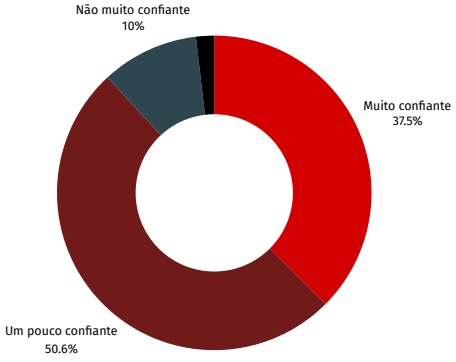
A crescente sofisticação dos ataques cibernéticos e a complexidade do ambiente digital exigem que as empresas adotem uma abordagem estruturada e proativa para a segurança da informação. Neste contexto, a **Pesquisa de Segurança da Informação (RSIN) 2024 3° EDIÇÃO** foi conduzida com gestores de diversas organizações para compreender os desafios, prioridades e níveis de maturidade em relação à cibersegurança. Neste relatório, que contou com a participação de mais de 160 empresas do Rio Grande do Sul, são apresentadas análises detalhadas sobre o cenário atual e recomendações estratégicas.

O objetivo principal da pesquisa foi identificar os pontos fortes e fracos das empresas em relação à proteção de dados, gestão de riscos e resposta a incidentes. Além disso, foram analisados fatores como treinamento de colaboradores, automação de processos, monitoramento contínuo e adoção de soluções avançadas para mitigação de ameaças.

Com um cenário de ameaças cada vez mais dinâmico, a pesquisa fornece uma visão detalhada do grau de preparo das empresas para lidar com os riscos cibernéticos, destacando áreas críticas que necessitam de maior atenção e investimento.

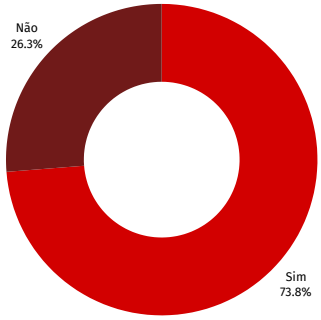
1 - O quão confiante você está nas decisões de gerenciamento de risco tomadas pela sua empresa?

- Muito confiante - 60 empresas
- Um pouco confiante - 81 empresas
- Não muito confiante - 16 empresas
- Não faz gerenciamento de risco - 3 empresas



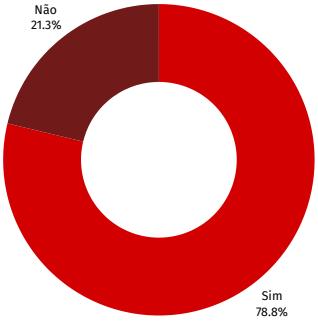
2 - A sua empresa conduz programas de treinamento e conscientização sobre as ameaças cibernéticas aos seus colaboradores?

- Sim - 118 empresas
- Não - 42 empresas



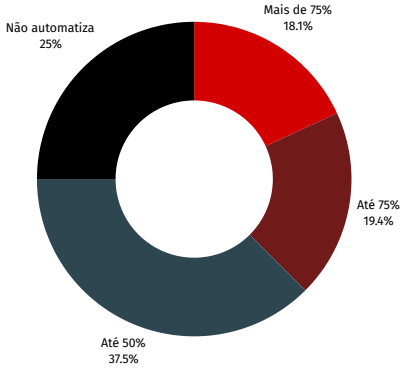
3 - A sua empresa possui um gerenciamento contínuo de vulnerabilidades (identificação, priorização e correção)?

- Sim - 126 empresas
- Não - 34 empresas



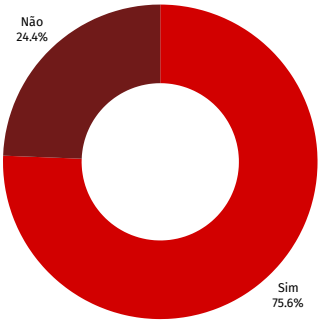
4 - Em relação às correções de vulnerabilidades, quantos % são automatizadas?

- Mais de 75% - 29 empresas
- Até 75% - 31 empresas
- Até 50% - 60 empresas
- Não automatiza - 40 empresas



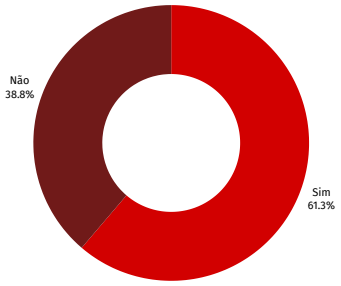
5 - A sua empresa possui planos de respostas a incidentes de segurança cibernética?

- Sim - 121 empresas
- Não - 39 empresas



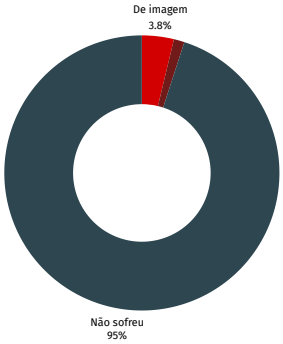
6 - A sua empresa adota alguma norma ou framework de segurança? Exemplo: instituto Norte-americano de Normas e Tecnologia (NIST), Organização Internacional de Normalização (ISO), Center for Internet Security (CIS), outros.

- Sim - 98 empresas
- Não - 62 empresas



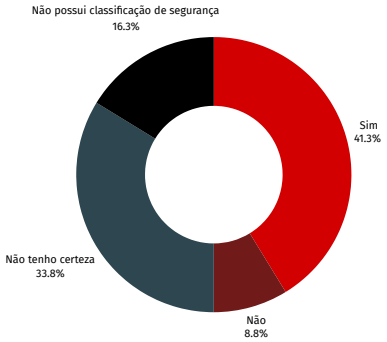
7 - A sua empresa sofreu impactos de um ataque bem-sucedido no último ano? Se sim, em qual aspecto você considera o maior dano?

- De imagem - 6 empresas
- Financeiro - 2 empresas
- Não sofreu - 152 empresas



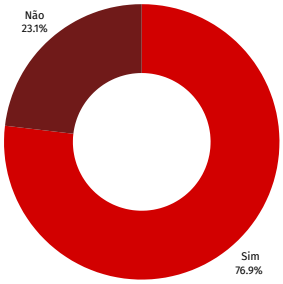
8 - Você acredita que a classificação de segurança atribuida à sua empresa é um reflexo preciso da realidade?

- Sim - 66 empresas
- Não - 14 empresas
- Não tenho certeza - 54 empresas
- Não possui classificação de segurança - 26 empresas



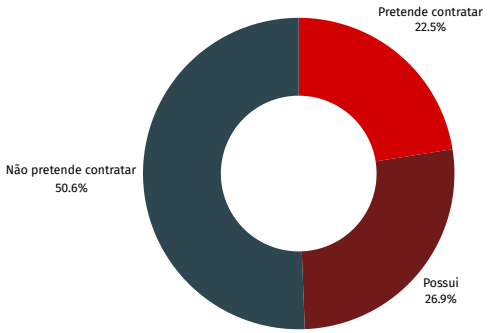
9 - Sua empresa tem implementado medidas para promover o alinhamento com os princípios de ESG (Ambiental, Social e Governança) ?

- Sim - 123 empresas
- Não - 37 empresas



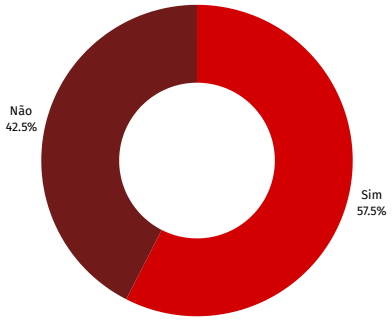
10 - A sua empresa possui ou pretende contratar seguro para riscos digitais nos próximos 3 anos?

- Pretende contratar - 36 empresas
- Possui - 43 empresas
- Não pretende contratar - 81 empresas



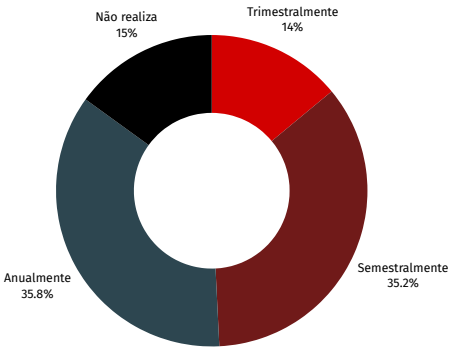
11- A sua empresa enfrenta dificuldades na contratação e retenção de profissionais de segurança cibernética?

- Sim - 92 empresas
- Não - 68 empresas



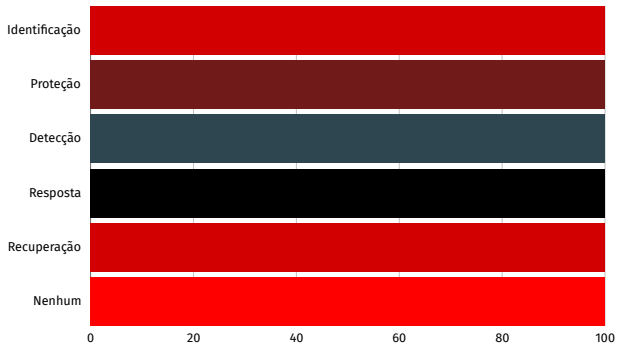
12 - A sua empresa realiza pentest com qual frequência?

- Trimestralmente - 27 empresas
- Semestralmente - 35 empresas
- Anualmente - 69 empresas
- Não realiza - 29 empresas



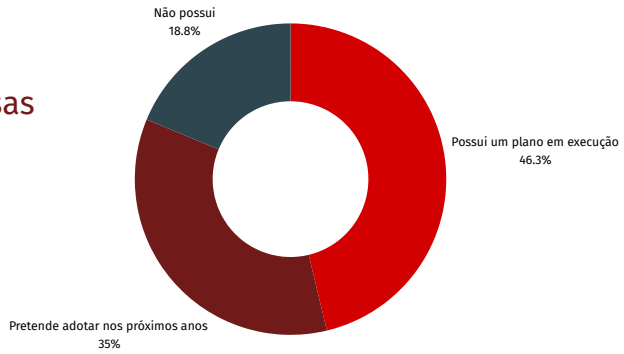
13 - Os investimentos de cibersegurança da sua empresa no próximo ano serão destinados a:

- Identificação - 75 empresas
- Proteção - 126 empresas
- Detecção - 99 empresas
- Resposta - 67 empresas
- Recuperação - 60 empresas
- Nenhum - 4 empresas



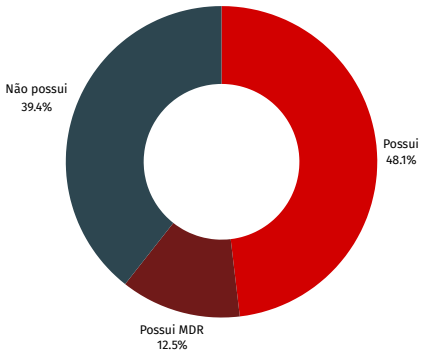
14 - Sua empresa adota um Plano Diretor de Segurança da informação?

- Possui um plano em execução - 74 empresas
- Pretende adotar nos próximos anos - 56 empresas
- Não possui - 30 empresas



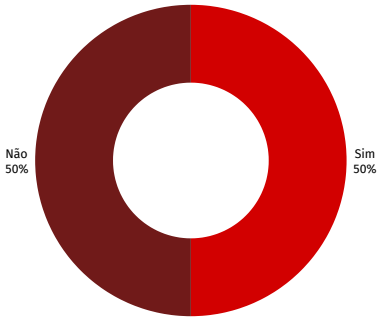
15 - Sua empresa conta com serviços de SOC/MDR?

- Possui SOC - 77 empresas
- Possui MDR - 20 empresas
- Não possui - 63 empresas



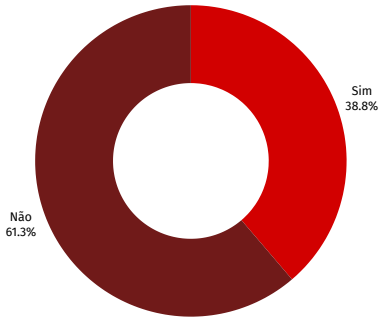
16 - Sua empresa conta com serviços/ferramentas para Detecção e Resposta para incidentes (ITDR) *Id entity Threat Detection and Response

- Sim - 80 empresas
- Não - 80 empresas



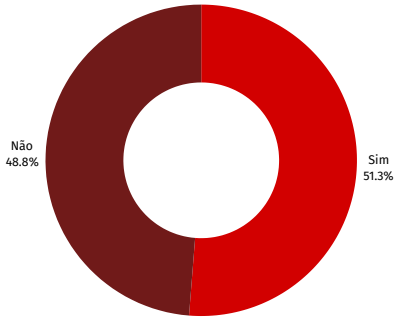
17 - Sua empresa conta com serviços de gestão de superfície externa de ataque (EASM)?

- Sim - 62 empresas
- Não - 98 empresas



18 - Sua empresa realiza avaliação de riscos de terceiros?

- Sim - 82 empresas
- Não - 78 empresas



Resultado da pesquisa

A análise dos dados revelou que muitas organizações ainda enfrentam desafios significativos na gestão de riscos e na implementação de boas práticas de segurança da informação. Entre os principais pontos identificados, destacam-se:

1 Baixa confiança na gestão de riscos

- Um número significativo de respondentes declarou estar apenas "um pouco confiante" nas decisões de gerenciamento de riscos da empresa, indicando falta de maturidade e governança no processo.

2 Falta de treinamento e conscientização em segurança cibernética

- Muitas empresas não realizam programas de conscientização para seus colaboradores, o que aumenta o risco de ataques baseados em engenharia social, phishing e credenciais comprometidas.

3 Gestão deficiente de vulnerabilidades

- Algumas empresas ainda não possuem um processo contínuo de identificação, priorização e correção de vulnerabilidades, tornando-se alvos fáceis para atacantes explorarem falhas conhecidas.

4 Baixo nível de automação na correção de vulnerabilidades

- Uma parte considerável das organizações ainda realiza correções de forma manual ou com baixa automação, o que pode gerar atraso na mitigação de riscos críticos.

5 Pouca adoção de SOC/MDR para monitoramento contínuo

- A falta de serviços de Security Operations Center (SOC) ou Managed Detection and Response (MDR) evidencia que muitas empresas não têm monitoramento contínuo, o que reduz a capacidade de resposta rápida a incidentes.

6 Falta de ferramentas de Detecção e Resposta para Identidades (ITDR)

- Poucas empresas contam com soluções para proteger identidades contra ataques como roubo de credenciais, movimentos laterais e comprometimento de contas privilegiadas.

7 Ausência de gestão de superfície externa de ataque (EASM)

- A maioria das empresas não possui um programa de gerenciamento de exposição externa, o que dificulta a identificação e remediação de ativos expostos a ataques.

8 Baixa maturidade na avaliação de riscos de terceiros

- Muitas organizações não realizam avaliações regulares de riscos em fornecedores e terceiros, criando lacunas de segurança na cadeia de suprimentos.

Principais Recomendações Estratégicas

O cenário de ameaças cibernéticas exige uma abordagem **proativa e integrada**, combinando **tecnologia, processos e governança** para garantir **resiliência organizacional.** A seguir, detalhamos as principais recomendações estratégicas com foco na **redução de riscos, detecção precoce e resposta eficiente a incidentes.**

Adoção de Modelos Zero Trust

A abordagem **Zero Trust (Confiança Zero)** redefine a segurança cibernética, eliminando o conceito de perímetro confiável e exigindo **verificação contínua de identidade e comportamento dos usuários e dispositivos.**

Recomendações Práticas:

Acesso mínimo necessário:

Implementar Princípio do Menor Privilégio (PoLP), garantindo que usuários e sistemas tenham **apenas os acessos estritamente necessários** para suas funções.

Autenticação contínua baseada em risco: Utilizar **autenticação multifator (MFA) adaptativa e verificação baseada em contexto** para evitar acessos indevidos.

Microsegmentação de rede: Dividir a infraestrutura em **pequenos segmentos de segurança**, limitando movimentações laterais em caso de comprometimento.

Monitoramento contínuo e resposta a anomalias:

Utilizar UEBA (User and Entity Behavior Analytics) para detectar **comportamentos suspeitos** e impedir acessos não autorizados.

Benefícios:

Redução do risco de **movimentação lateral de invasores.**
Minimização dos impactos de **vazamento de credenciais.**
Aumento da visibilidade e controle sobre usuários e dispositivos.

Fortalecimento das Defesas Contra Engenharia Social

Engenharia social continua sendo o **principal vetor de ataque,** explorando o fator humano para comprometer credenciais e acessar sistemas críticos.

Recomendações Práticas:

Treinamento contínuo e simulações de phishing: Realizar campanhas **frequentes e personalizadas,** garantindo que funcionários saibam reconhecer **e-mails fraudulentos e tentativas de BEC (Business Email Compromise).**

Política de verificação dupla para transações financeiras: Implementar **dupla checagem por telefone ou canais independentes** para aprovar transferências ou mudanças de credenciais sensíveis.

netfive

Tecnologias anti-phishing e análise de comportamento: Utilizar ferramentas que detectam **links maliciosos, tentativas de TOAD (Telephone-Oriented Attack Delivery)** e **mensagens fraudulentas em tempo real.**

Benefícios:

Redução do impacto de **fraudes via BEC e ataques direcionados. Aumento da conscientização dos colaboradores,** reduzindo **erros humanos críticos.**

Segurança na Nuvem e na Cadeia de Suprimentos

Com **110% de crescimento em ataques direcionados à nuvem e fornecedores,** é essencial implementar uma **estratégia de proteção integrada.**

Recomendações Práticas:

Auditoria rigorosa em terceiros:

Avaliar fornecedores **antes e durante a relação comercial**, exigindo **conformidade com normas de segurança (ISO 27001, SOC 2, CIS Controls).**

Gestão Contínua da Superfície de Ataque Externa (EASM - External Attack Surface Management): Monitorar **exposições inadvertidas de ativos na internet,** como **credenciais expostas, portas abertas e sistemas desatualizados.**

Proteção de workloads na nuvem:

Implementar **controle de identidade rigoroso (IAM), criptografia de dados e detecção de comportamento anômalo.**

Segurança de APIs: Monitorar **credenciais de acesso, consumo anômalo e endpoints vulneráveis.**

Benefícios:

- **Redução do risco de ataques à cadeia de suprimentos e vazamentos de dados.**
- **Maior controle e visibilidade sobre exposições de infraestrutura em nuvem.**

netfive

Proteção Contra Ransomware e Extorsão de Dados

Com o crescimento de ataques baseados em **sequestro e vazamento de dados,** organizações devem priorizar **resiliência contra ransomware e técnicas avançadas de extorsão.**

Recomendações Práticas:

Backup seguro e isolado:

Implementar **cópias offline e imutáveis** para evitar que ransomwares apaguem ou corrompam os dados.

Segmentação e restrição de acessos administrativos: Garantir que **contas privilegiadas tenham restrições rigorosas**, limitando movimentação lateral.

Monitoramento de credenciais vazadas: Usar serviços que rastreiam **credenciais e acessos expostos na dark web,** notificando e exigindo alterações de senha em caso de comprometimento.

Testes contínuos de resposta a incidentes:

Simular **cenários reais de ataques de ransomware,** garantindo que a equipe saiba **como agir rapidamente para mitigar impactos.**

Benefícios:

- **Redução do impacto financeiro e reputacional** em caso de ataques.
- **Maior capacidade de recuperação rápida,** evitando paralisação de operações.

Uso de Inteligência Artificial para Defesa Cibernética

Com atacantes usando IA para **automatizar ataques,** organizações devem adotar IA para **fortalecer segurança e detecção de ameaças.**

Recomendações Práticas:

Automação da detecção e resposta a incidentes (SOAR):

Implementar soluções de **detecção de ameaças em tempo real,** bloqueando atividades suspeitas automaticamente.

Análises preditivas e resposta antecipada: Utilizar **machine learning para detectar padrões de ataques** antes que comprometam o ambiente.

IA para combate a fraudes e deepfakes:

Aplicar IA para **analisar autenticidade de identidades e transações financeiras.**

Benefícios:

- Redução do tempo de resposta a ataques **de horas para minutos.**
- Capacidade de **prever ameaças emergentes antes que ocorram.**

Governança e Gestão de Riscos: Segurança Contínua e Resiliência Operacional

A segurança da informação **não é apenas uma questão tecnológica, mas de governança e gestão de riscos.** As organizações devem adotar uma **abordagem integrada**, garantindo **conformidade regulatória, resiliência operacional e resposta eficiente a incidentes.**

Recomendações Práticas:

Implementação de um Programa CTEM (Continuous Threat Exposure Management):

- Gestão **contínua de vulnerabilidades**, priorizando **correção de falhas críticas** antes que sejam exploradas.
- **Mapeamento de superfícies de ataque** para reduzir pontos expostos.
- **Testes contínuos de segurança ofensiva (pentest, Red Team).**

Gestão de riscos e conformidade:

Alinhar políticas **a normas como NIST, CIS Controls e ISO 27001,** garantindo **governança e transparência.**

Planos de Resposta a Incidentes e Recuperação de Desastres:

- Definir e testar **planos claros para conter ataques e restaurar sistemas.**
- **Treinar equipes periodicamente** para simular incidentes reais.

Benefícios:

- **Aumento da maturidade em segurança cibernética.**
- **Redução de impacto financeiro, Operacional e reputacional em ataques.**
- **Conformidade com regulações globais de proteção de dados (GDPR, LGPD).**

netfive

RSIN

2024 - RS

3° EDIÇÃO

RELATÓRIO DE SEGURANÇA DA
INFORMAÇÃO DA NETFIVE.

contato@netfive.com.br
www.netfive.com.br

Av. Palmeira, 330 - 7º e 11º andar
Petrópolis - Porto Alegre - RS
CEP: 90470-300

Av. Dr. Chucri Zaidan, 1240 - 21º andar
Morumbi - São Paulo - SP
CEP: 04711-130