

RELATÓRIO DE RESILIÊNCIA CIBERNÉTICA

Preparadas ou expostas ao risco:

A lacuna da resiliência cibernética nos serviços financeiros

Todos falam sobre detectar e impedir ataques cibernéticos, mas as manchetes contam uma história diferente. A prevenção e a detecção não são mais suficientes. Até as organizações mais avançadas estão sofrendo interrupções graves, que afetam desde a TI até a diretoria e além.

Para entender o motivo e o que separa as empresas resilientes daquelas que ainda enfrentam dificuldades, a Cohesity entrevistou 3.200 tomadores de decisões das áreas de TI e Operações de Segurança em 11 países. Entre eles, havia 390 participantes de organizações da área de serviços financeiros. As respostas deles revelam uma lacuna de resiliência crescente entre as empresas de serviços financeiros preparadas para o risco, que são capazes de se recuperar com rapidez e confiança, e aquelas expostas ao risco, que continuam vulneráveis a interrupções prolongadas e prejuízos financeiros.

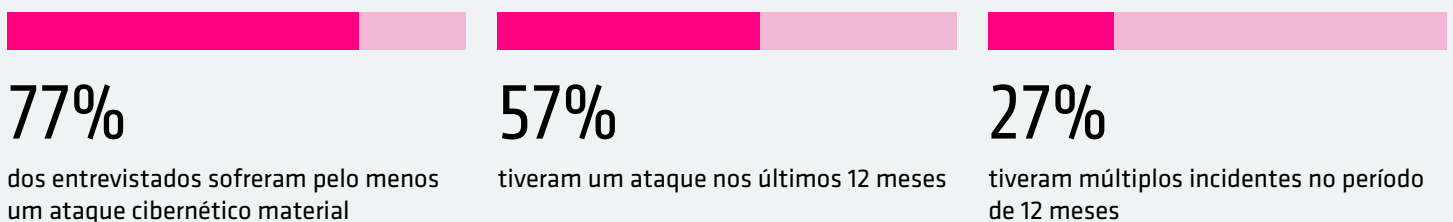
A nossa pesquisa examina os impactos de ataques cibernéticos no mundo real, como as organizações do setor de serviços financeiros avaliaram sua própria resiliência cibernética em relação às práticas recomendadas, e as etapas que elas adotaram para detectar, responder e se recuperar desses incidentes. Ela também destaca o que elas descobriram, e como estão buscando a IA e a automação para acelerar a resiliência e fechar a lacuna.



ATAQUES CIBERNÉTICOS MATERIAIS: A NOVA REALIDADE DAS EMPRESAS MODERNAS

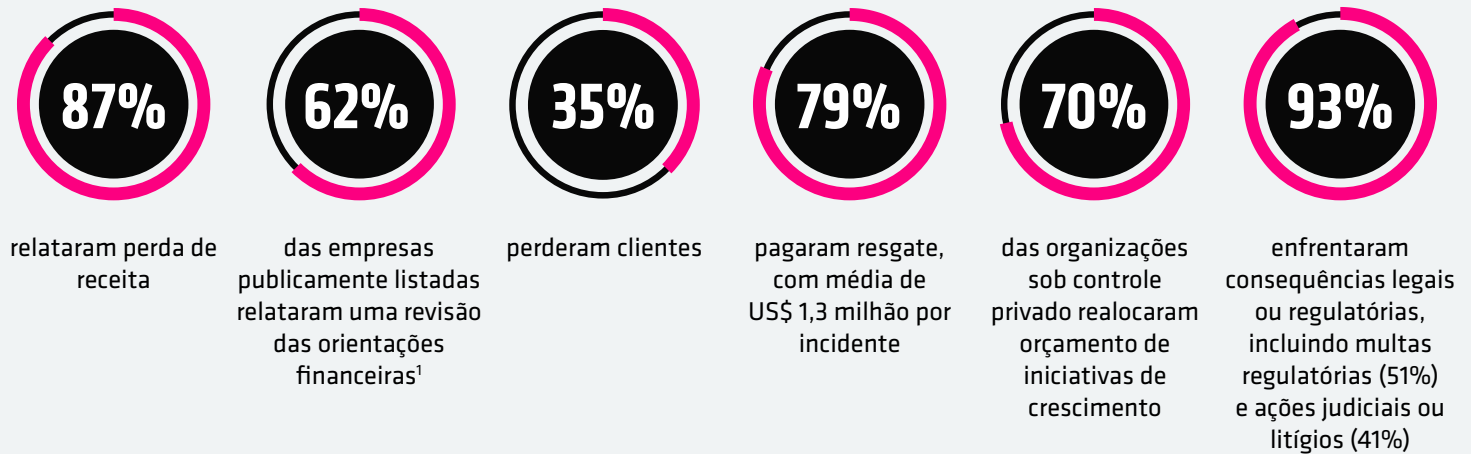
Os incidentes cibernéticos não são todos iguais. Muitas empresas de serviços financeiros gerenciam tentativas rotineiras de phishing, sondagens de malware ou interrupções de sistemas quase diariamente. Mas os ataques cibernéticos materiais são diferentes. A nossa pesquisa definiu um ataque cibernético material como um incidente que causou um impacto mensurável em termos financeiros, operacionais, reputacionais ou de rotatividade de clientes.

ESSES ATAQUES DE ALTO RISCO NÃO SÃO MAIS EVENTOS ISOLADOS PARA AS ORGANIZAÇÕES DO SETOR DE SERVIÇOS FINANCEIROS.



O CUSTO REAL DOS ATAQUES CIBERNÉTICOS MATERIAIS

HAVIA PRESSÕES FINANCEIRAS E REGULATÓRIAS SOBRE TODAS AS ORGANIZAÇÕES DO SETOR DE SERVIÇOS FINANCEIROS QUE NÓS ENTREVISTAMOS:



¹Embora relativamente poucas empresas tenham divulgado formalmente revisões de receita após um incidente cibernético, essas descobertas sugerem que os efeitos financeiros e operacionais vão muito além do que os registros públicos revelam.

CONFIANÇA DIANTE DAS CONSEQUÊNCIAS

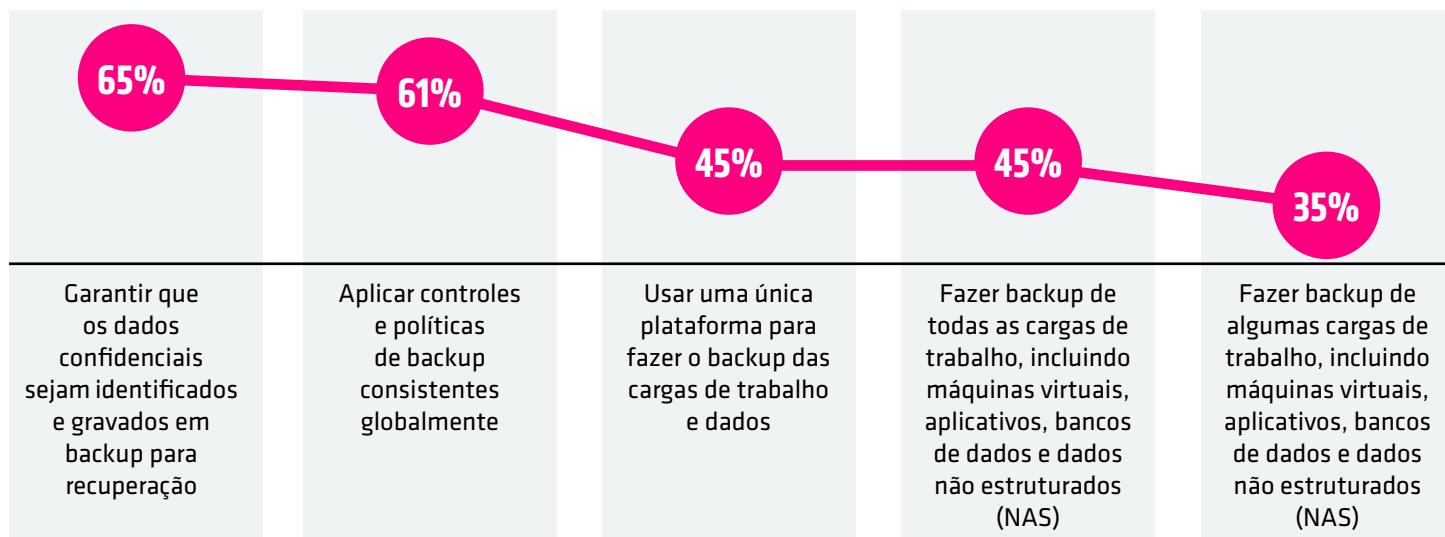
Considerando-se a escala dos prejuízos financeiros e operacionais revelados na nossa pesquisa, seria natural se houvesse uma preocupação generalizada com a resiliência organizacional. Porém, quase metade dos participantes (46%) confia totalmente na capacidade de sua estratégia de resiliência cibernética de suportar as ameaças de hoje. Esse nível de confiança tem um contraste marcante com os impactos materiais significativos que muitas dessas mesmas empresas sofreram.

O QUE AS ORGANIZAÇÕES ESTÃO (E NÃO ESTÃO) FAZENDO

Nós queríamos ver sob a superfície e descobrir onde existem lacunas de resiliência. Para isso, pedimos aos participantes para descreverem sua abordagem sobre práticas e capacidades associadas a cinco dimensões cruciais da resiliência cibernética: **proteção de dados, recuperação de dados, detecção e investigação de ameaças, resiliência de aplicativos e otimização da postura de risco de dados.**

A PROTEÇÃO DE DADOS CONTINUA FRAGMENTADA EM AMBIENTES HÍBRIDOS E MULTINUDEM

Quais das seguintes ações a sua organização faz para proteger todos os dados em ambientes híbridos e/ou multinuvm?



Quase dois terços das organizações do setor de serviços financeiros garante que os dados confidenciais sejam identificados e gravados em backup para recuperação, enquanto uma porcentagem um pouco menor aplica controles e políticas de backup consistentes globalmente. Menos da metade faz backup de todas as carga de trabalho ou usa uma única plataforma. Cerca de um terço faz backup apenas de cargas de trabalho selecionadas. Essa fragmentação limita a visibilidade e a consistência nos ambientes. Uma resiliência cibernética madura depende da unificação de backup e recuperação em uma única plataforma inteligente, protegida por princípios de Confiança Zero.

AS MEDIDAS DE RECUPERABILIDADE DOS DADOS SÃO COMUNS, MAS A MATURIDADE VARIA

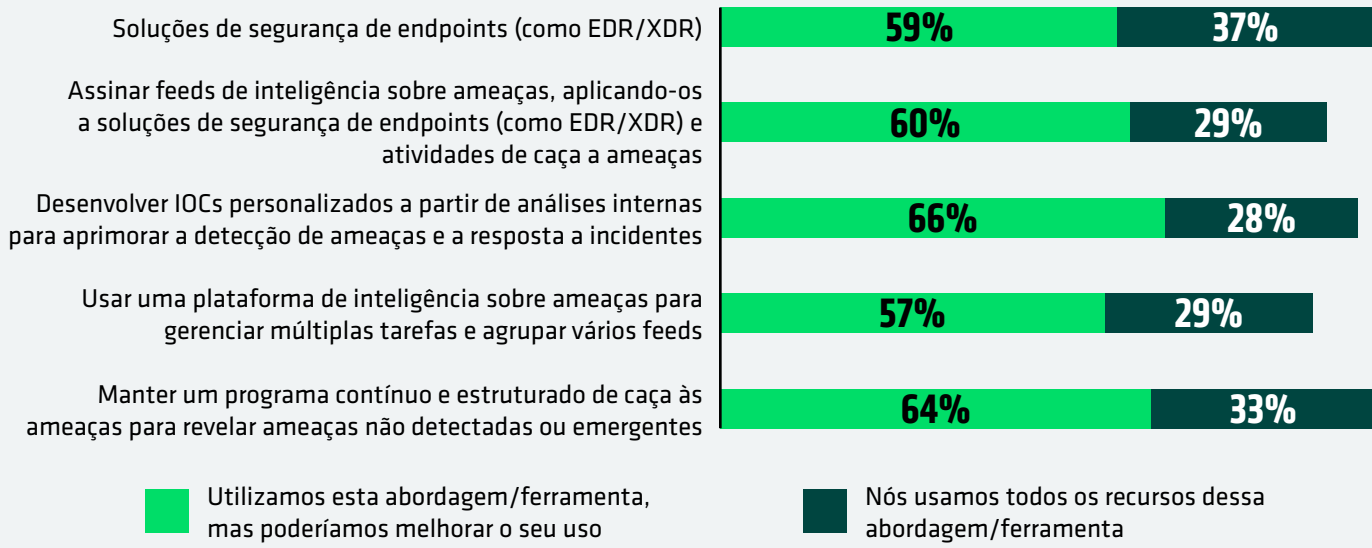
O que a sua empresa faz para garantir que seus dados sejam sempre recuperáveis?

64%	Exigir autorização adicional para tarefas de administração de alto risco associadas às soluções de backup e recuperação
61%	Autenticação multifator na nossa solução de backup
48%	Seguir a “regra de backup 3-2-1” (três cópias dos seus dados em duas mídias diferentes e uma cópia externa)
45%	Proteger dados cruciais com imutabilidade
41%	Direitos de acesso com privilégios mínimos para as cargas de trabalho gravadas em backup

Muitas organizações do setor de serviços financeiros fortaleceram os controles de acesso para os ambientes de backup, com quase dois terços delas exigindo autorização adicional do administrador para tarefas de alto risco, e um pouco mais da metade impondo autenticação multifator. Quase a metade segue a regra de backup 3-2-1, e um pouco menos da metade protege os dados cruciais com imutabilidade. Menos delas aplicam direitos de acesso com privilégios mínimos. Essas lacunas tornam uma recuperação completa mais incerta. Uma resiliência cibernética madura depende de cópias de recuperação verificadas, isoladas e à prova de adulteração.

AS FERRAMENTAS DE DETECÇÃO E INVESTIGAÇÃO DE AMEAÇAS SÃO POUCO UTILIZADAS

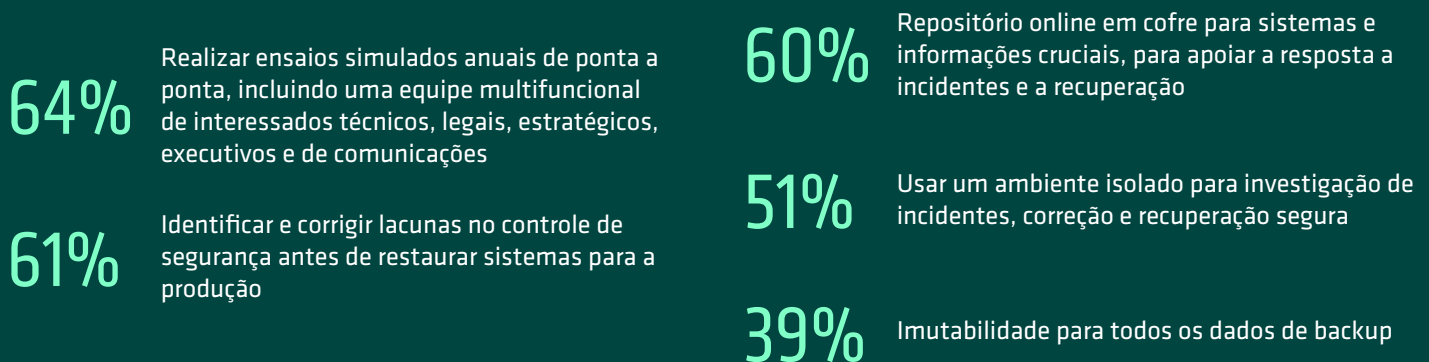
Em que medida a sua organização usa cada um dos seguintes métodos ou ferramentas para detectar e investigar ameaças?



As ferramentas de detecção e investigação de ameaças são amplamente implementadas, mas pouco usadas. A maioria das empresas de serviços financeiros usam segurança de endpoint, feeds de inteligência sobre ameaças e programas estruturados de caça a ameaças. Apesar disso, apenas uma minoria utiliza todo o potencial dessas ferramentas. A adoção de recursos avançados, como indicadores de comprometimento (IOCs) e plataformas de inteligência sobre ameaças, continua especialmente limitada. Uma resiliência cibernética madura depende da integração dessas ferramentas em um loop contínuo de inteligência que melhore a visibilidade, a detecção e a resposta.

AS ORGANIZAÇÕES ESTÃO VULNERÁVEIS À REINFECÇÃO

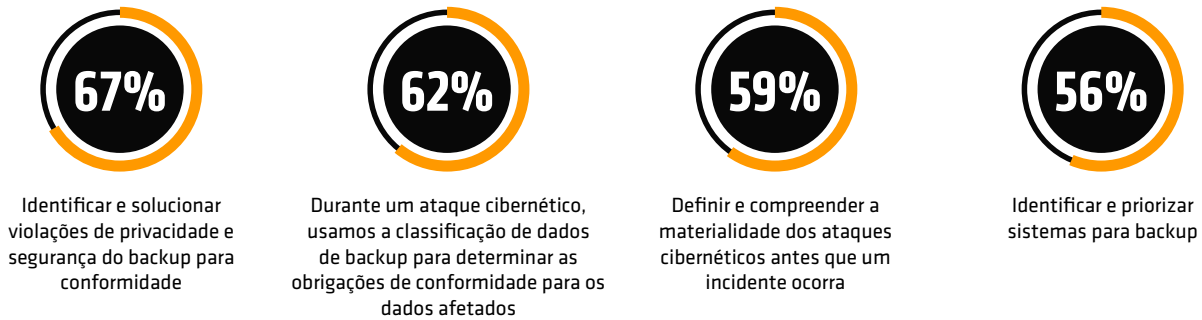
O que a sua organização faz ou faria para garantir a resiliência de aplicativos contra ataques cibernéticos?



As empresas de serviços financeiros estão avançando sua abordagem de resiliência de aplicativos, mas ainda há lacunas. Pouco mais da metade identificou lacunas no controle de segurança antes de restaurar sistemas, e quase dois terços realiza ensaios anuais de recuperação. Seis em cada dez mantêm repositórios em cofres online. Um pouco mais da metade usa ambientes isolados para investigação e recuperação seguras. Menos da metade aplica imutabilidade a todos os dados de backup. Essas lacunas deixam os processos de recuperação vulneráveis a reinfecções ou perda de dados. Uma resiliência cibernética madura combina a preparação com zonas de recuperação seguras e verificáveis.

A CLASSIFICAÇÃO DE DADOS GANHA IMPULSO, MAS O USO ORIENTADO A RISCOS AINDA EVOLUI

Como a sua organização usa abordagens/ferramentas de descoberta e classificação de dados para minimizar o risco de exposição em todo o acervo de dados?



As empresas de serviços financeiros estão usando a descoberta e a classificação dos dados de forma mais estratégica para conformidade, resposta e recuperação. Cerca de dois terços lidam com violações de segurança e privacidade, e usam a classificação para orientar a conformidade durante um ataque. Menos delas definem a materialidade antes de um incidente ou priorizam os backups com base no risco. Essas lacunas sugerem que o uso da classificação orientada a riscos ainda está evoluindo. Uma resiliência cibernética madura transforma a classificação em uma abordagem sistemática que otimiza a postura de risco de dados e informa a proteção, a resposta e a recuperação.

UMA IMAGEM MAIS CLARA DA MATURIDADE DA RESILIÊNCIA

Quando pontuadas coletivamente, as respostas dos participantes serviram como um barômetro de alto nível da maturidade da resiliência cibernética, revelando padrões claros no modo como as organizações do setor de serviços financeiros estão implementando (ou tendo dificuldades para implementar) a resiliência na prática. Embora a maioria esteja na fase de desenvolvimento, apenas 5% demonstram os recursos mais maduros e integrados que definem as organizações preparadas para o risco.

A CURVA DE MATURIDADE DA RESILIÊNCIA CIBERNÉTICA



Menos maduras (4%): Os backups, políticas e medidas de segurança estão praticamente ausentes ou são inconsistentes. MFA e controles de administrador são raramente protegidos, a recuperação muitas vezes não tem isolamento e as avaliações de conformidade ou materialidade são normalmente negligenciadas.

Emergentes (13%): Algumas práticas de resiliência estão implantadas, mas de forma inconsistente. As organizações podem fazer backup de dados confidenciais, aplicar políticas globais ou usar MFA, mas raramente combinados. As iniciativas de inteligência sobre ameaças e conformidade existem, mas ainda são incipientes e fragmentadas.

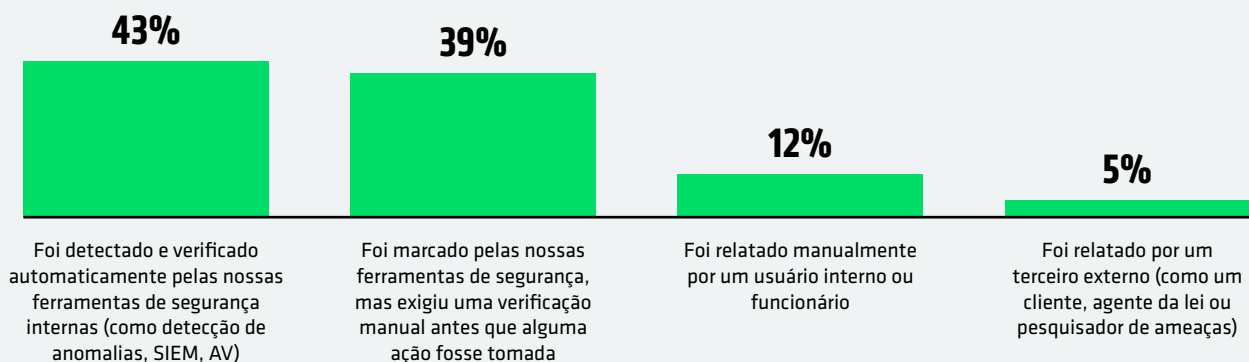
Em desenvolvimento (65%): As práticas básicas, como backup, controles de administrador e inteligência sobre ameaças são mais comuns, mas ainda desiguais. Ambientes de recuperação, verificações de conformidade e correção de lacunas de segurança são aplicadas esporadicamente, tornando os esforços de resiliência parcialmente eficazes.

Em avanço (13%): A maioria das práticas essenciais são impostas de modo consistente, incluindo políticas globais de backup, aprovações de administradores e correção antes da recuperação. A inteligência sobre ameaças é usada, mas não totalmente otimizada, e ainda restam lacunas na recuperação isolada e na cobertura da conformidade.

Mais maduras (5%): A resiliência é sistemática e abrangente. Os dados confidenciais são gravados em backup globalmente, a MFA e os controles de administrador são padronizados, a inteligência sobre ameaças é maximizada, a recuperação é protegida com correção e as medidas de conformidade são cumpridas de forma consistente.

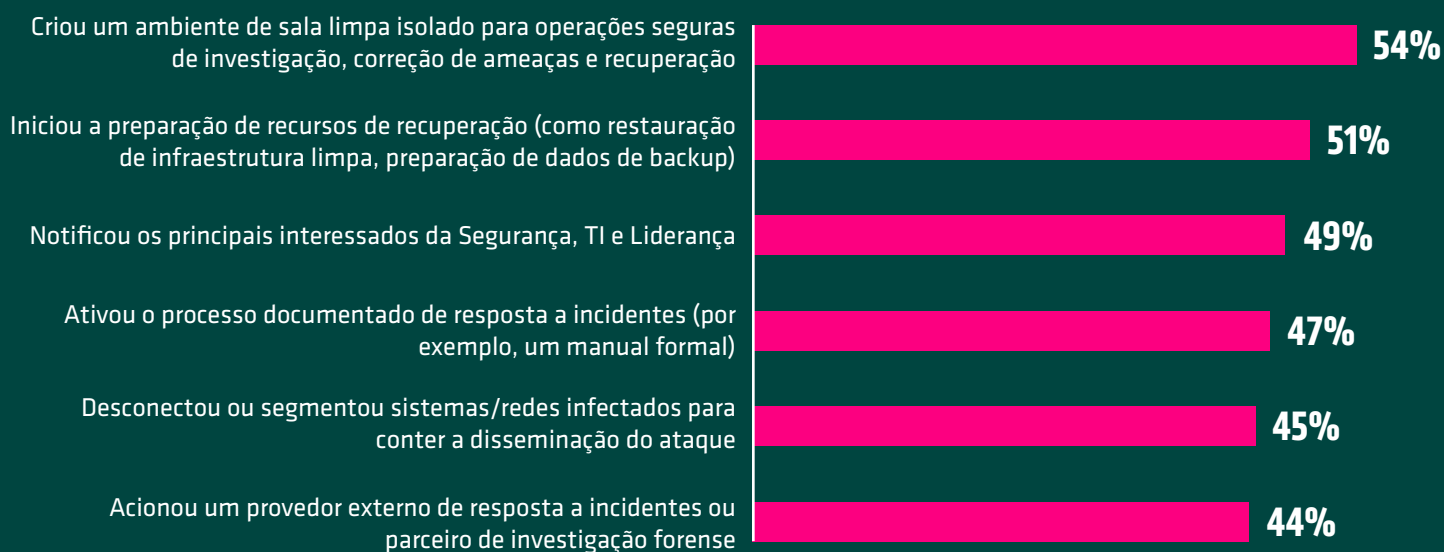
A RESILIÊNCIA SOB ATAQUE

COMO AS EQUIPES IDENTIFICARAM O ATAQUE



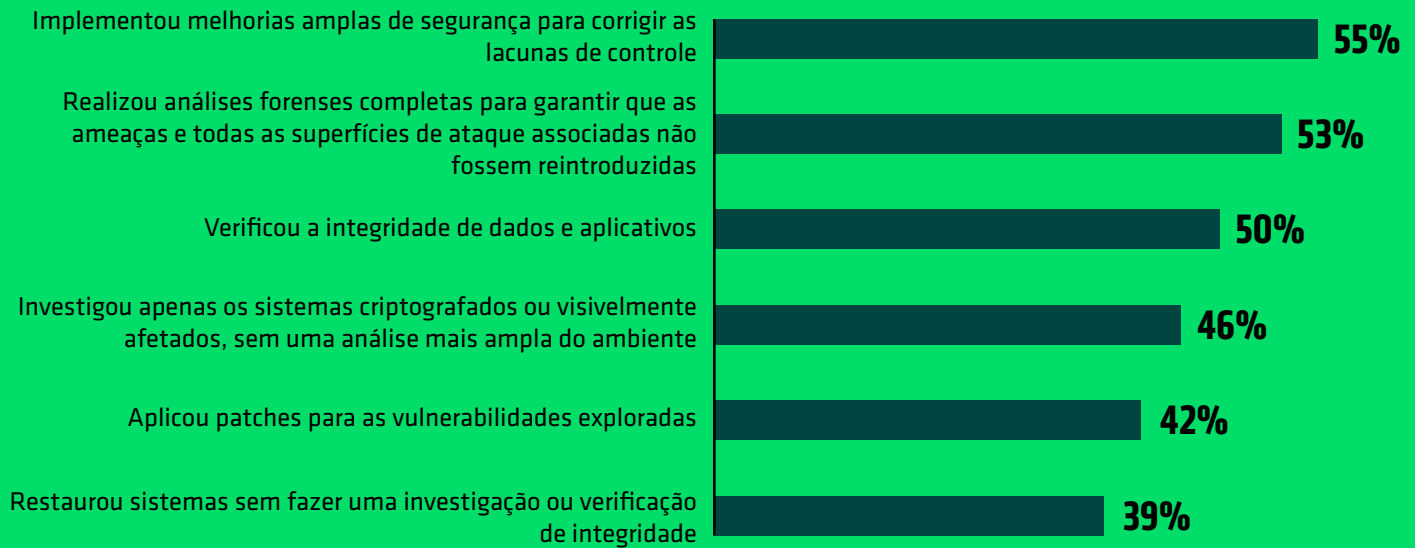
Em caso de um ataque cibernético, a maioria das empresas do setor de serviços financeiros detecta os incidentes internamente. Quase metade das empresas relataram que o ataque foi identificado e verificado automaticamente por suas próprias ferramentas de segurança, enquanto uma quantidade um pouco menor informou que os ataques foram marcados por ferramentas, mas exigiram verificação manual antes que alguma medida fosse tomada. Apenas uma pequena parte foi identificada por terceiros, indicando que a detecção aparece principalmente de modo interno, mas ainda dependente de confirmação humana.

AÇÕES REALIZADAS PELAS EQUIPES APÓS A CONFIRMAÇÃO DO ATAQUE



Depois da confirmação do ataque, as empresas de serviços financeiros adotaram uma série de medidas para dar suporte à recuperação. Um pouco mais da metade iniciou a restauração da infraestrutura limpa ou a preparação dos dados de backup, enquanto uma quantidade um pouco maior estabeleceu ambientes de sala limpa isolados para investigação e recuperação seguras. Uma parte menor das empresas notificou os principais interessados, conteve sistemas infectados, ativou manuais formais de resposta ou acionou especialistas externos de resposta a incidentes ou análise forense. Essas variações indicam que as ações de resposta ainda não estão totalmente padronizadas nas etapas cruciais.

MEDIDAS ADOTADAS ANTES DE COLOCAR SISTEMAS E DADOS ONLINE NOVAMENTE



Antes de colocar sistemas online novamente, as empresas de serviços financeiros adotaram uma combinação de medidas de análise forense e correção. Mais da metade implementou melhorias de segurança mais amplas ou implementou análises forenses completas. Metade delas também verificou a integridade dos dados e aplicativos. Uma quantidade menor investigou além dos sistemas visivelmente afetados ou corrigiu as vulnerabilidades exploradas. Mais de um terço restaurou sistemas sem uma investigação completa ou verificação de integridade, deixando lacunas para reinfecção e risco residual.

DESAFIOS ENFRENTADOS PELAS EQUIPES DURANTE O ATAQUE



As equipes relataram desafios significativos durante todo o processo. Muitas tiveram dificuldades de comunicação quando os sistemas críticos estavam offline. Quase metade delas se sentiu pressionada para restaurar as operações antes que a correção fosse concluída. A evasão de ferramentas de segurança, reinfecção e falta de pontos de recuperação limpos aumentaram as dificuldades, destacando a necessidade de medidas mais robustas de resiliência.

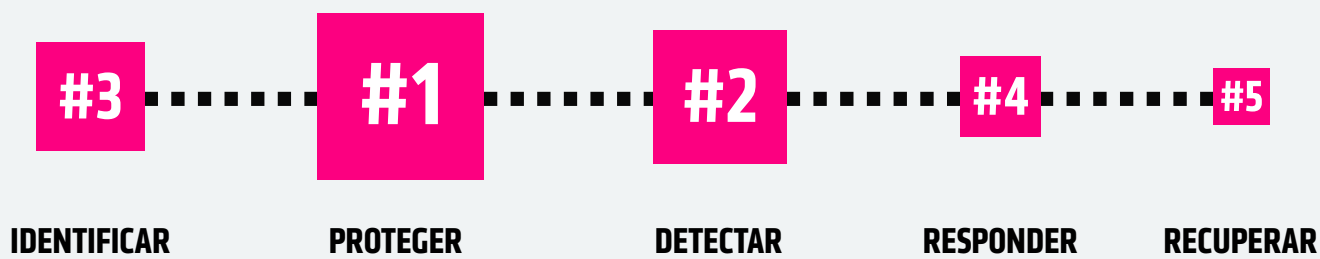
ONDE AINDA FALTAM INVESTIMENTOS EM RESILIÊNCIA

Até as empresas de serviços financeiros bem preparadas têm dificuldade para sustentar a resiliência quando um ataque acontece. Conforme a pressão operacional aumenta, as lacunas de coordenação, correções incompletas e riscos de reinfecção expõem o quanto a recuperação pode ser frágil sem processos unificados e garantia contínua.

Esses padrões refletem como as organizações do setor de serviços financeiros estão alocando seus orçamentos de resiliência cibernética hoje. Perguntamos aos participantes como eles dividem os gastos entre as cinco funções essenciais da estrutura de segurança cibernética NIST – Identificar, Proteger, Detectar, Responder e Recuperar. A maioria continua fazendo investimentos pesados em prevenção, proteção e detecção, enquanto orçamentos comparativamente menores são dedicados à resposta e à recuperação verificada. O resultado é uma curva de maturidade que ainda tende para a defesa em vez da restauração, destacando uma oportunidade inexplorada para fortalecer a resiliência quando ela mais importa: depois do ataque.

ESTRUTURA DE SEGURANÇA CIBERNÉTICA NIST

O tamanho da caixa mostra a proporção mais alta para a mais baixa dos investimentos em ciber-resiliência



IA E AUTOMAÇÃO SURGEM COMO MULTIPLICADORES DE RESILIÊNCIA

Os resultados também mostram que as organizações do setor de serviços financeiros encaram a IA como uma ferramenta poderosa para a resiliência cibernética, especialmente na melhoria da velocidade de detecção e na precisão da resposta. Quase todos os participantes classificaram ferramentas como detecção de anomalias, análise do comportamento do usuário e investigação/resposta a ameaças orientadas por IA como eficazes no fortalecimento de sua postura de segurança.

Até os assistentes mais novos baseados em IA generativa, capazes de utilizar consultas sobre ameaças em linguagem natural e análises contextuais, estão ganhando impulso como uma forma de simplificar e acelerar a tomada de decisões. 56% das organizações de serviços financeiros disseram que uma das maiores lições aprendidas após um ataque cibernético foi a necessidade de mais automação para detecção, resposta e recuperação. Isso reflete a demanda crescente por plataformas integradas de automação e orquestração, em que a IA age como um multiplicador de força, gerando mais eficiência, consistência e eficácia para esses processos.

Olhando para o futuro, a maioria deles espera que a IA tenha um papel cada vez mais estratégico na defesa cibernética até o final de 2026. 49% acreditam que a IA vai apoiar a tomada de decisões por humanos, aprimorando análises e recomendações, com os humanos continuando no controle das ações finais. 39% esperam que a IA se torne central para a detecção e a resposta, tomando até algumas decisões autônomas. Isso sinaliza uma trajetória clara: A IA está evoluindo da posição de assistente para a de uma base operacional crucial para a resiliência cibernética, capaz de aprimorar a velocidade, a precisão e a confiança da detecção, da resposta e da recuperação.

O FUTURO DA RESILIÊNCIA COMEÇA AGORA

Embora as organizações de serviços financeiros estejam fazendo progressos mensuráveis na resiliência cibernética, muitas ainda têm espaço para melhorar sua resposta, recuperação e validação de prontidão após um ataque. A resiliência cibernética é uma enorme vantagem competitiva. O futuro pertence às organizações que investem nas pessoas, produtos e processos para se recuperar mais rapidamente, preservar a confiança dos clientes e manter os negócios funcionando quando as outras não conseguem. Quando a interrupção é virtualmente inevitável, a resiliência não é apenas proteção: é desempenho.

Crie resiliência antes que a crise aconteça:

- [Agende um workshop de resiliência contra ransomware.](#)
- [Suba de nível com um plano de resiliência cibernética de 5 passos.](#)
- [Conheça as soluções de resiliência cibernética da Cohesity para serviços financeiros.](#)

METODOLOGIA

COHESITY

A Cohesity contratou a Vanson Bourne para entrevistar 3.200 tomadores de decisões nas áreas de TI e Segurança em setembro de 2025, formando a base destas descobertas. Os participantes representam organizações nos EUA (500), Brasil (200), Reino Unido (400), Alemanha (400), França (400), EAU/Arábia Saudita (100), Austrália (200), Coreia do Sul (200), Japão (400), Índia (200) e Singapura (200). As empresas tinham 1.000 funcionários ou mais e pertenciam a uma gama de setores públicos e privados, com foco nos setores de serviços, público e de saúde.



© 2026 Cohesity, Inc. Todos os direitos reservados.

Cohesity, o logotipo da Cohesity e outras marcas da Cohesity são marcas registradas da Cohesity, Inc. ou dos seus afiliados nos EUA e/ou internacionalmente. Outros nomes podem ser marcas registradas dos seus respectivos proprietários. Este material (a) tem como objetivo fornecer informações sobre a Cohesity e o nosso negócio e produtos; (b) acreditava-se ser verdadeiro e exato no momento em que foi escrito, mas está sujeito a alterações sem aviso prévio; e (c) é fornecido "TAL COMO ESTÁ". A Cohesity rejeita todas as condições, representações e garantias expressas ou implícitas de qualquer tipo.

COHESITY

[cohesity.com](https://www.cohesity.com)

1-855-926-4374

2625 Augustine Drive, Santa Clara, CA 95054

2000081-001-PT-BR 5-2026