

RELATÓRIO DE RESILIÊNCIA CIBERNÉTICA

Preparadas ou expostas ao risco:

A lacuna da resiliência cibernética no setor público

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 399 participantes de organizações do setor público. As respostas deles revelam uma lacuna de resiliência crescente entre as empresas 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.

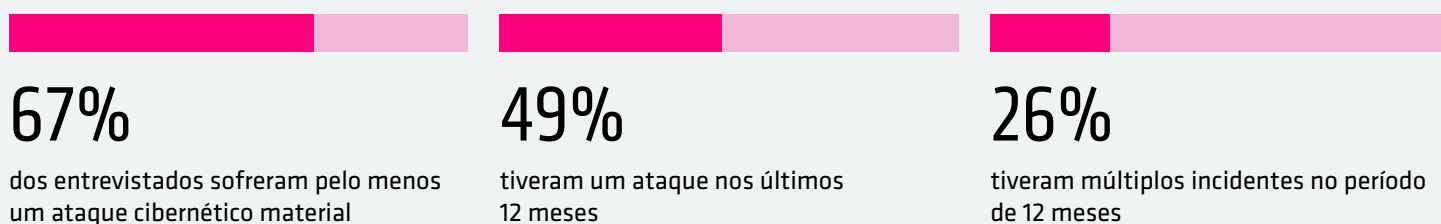
A nossa pesquisa examina os impactos de ataques cibernéticos no mundo real, como as organizações do setor público avaliaram sua própria resiliência cibernética em relação às práticas recomendadas, e as etapas que elas adotaram para detectar, responder e se recuperar desses incidentes. Ela também destaca 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

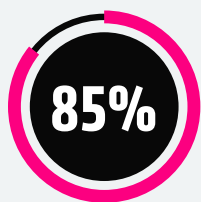
Os incidentes cibernéticos não são todos iguais. Muitas empresas gerenciam tentativas rotineiras de phishing, sondagens de malware ou interrupções de sistemas quase diariamente. Mas os ataques cibernéticos materiais são diferentes. A nossa pesquisa definiu um ataque cibernético material como um incidente 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 PÚBLICO.

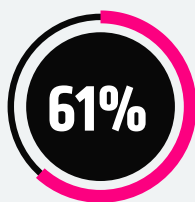


O CUSTO REAL DOS ATAQUES CIBERNÉTICOS MATERIAIS

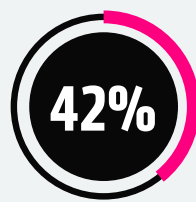
HAVIA PRESSÕES FINANCEIRAS E REGULATÓRIAS SOBRE TODAS AS ORGANIZAÇÕES DO SETOR PÚBLICO QUE NÓS ENTREVISTAMOS:



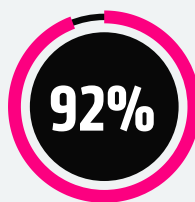
relataram perda de receita



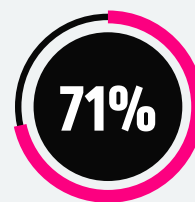
das organizações publicamente listadas relataram uma revisão das orientações financeiras¹



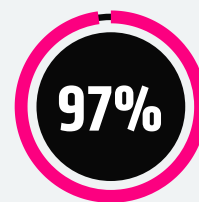
perderam clientes



pagaram resgate, com média de US\$ 1,3 milhão por incidente



das organizações sob controle privado realocaram orçamento de iniciativas de crescimento



enfrentaram consequências legais ou regulatórias, incluindo multas regulatórias (45%) e ações judiciais ou litígios (40%)

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

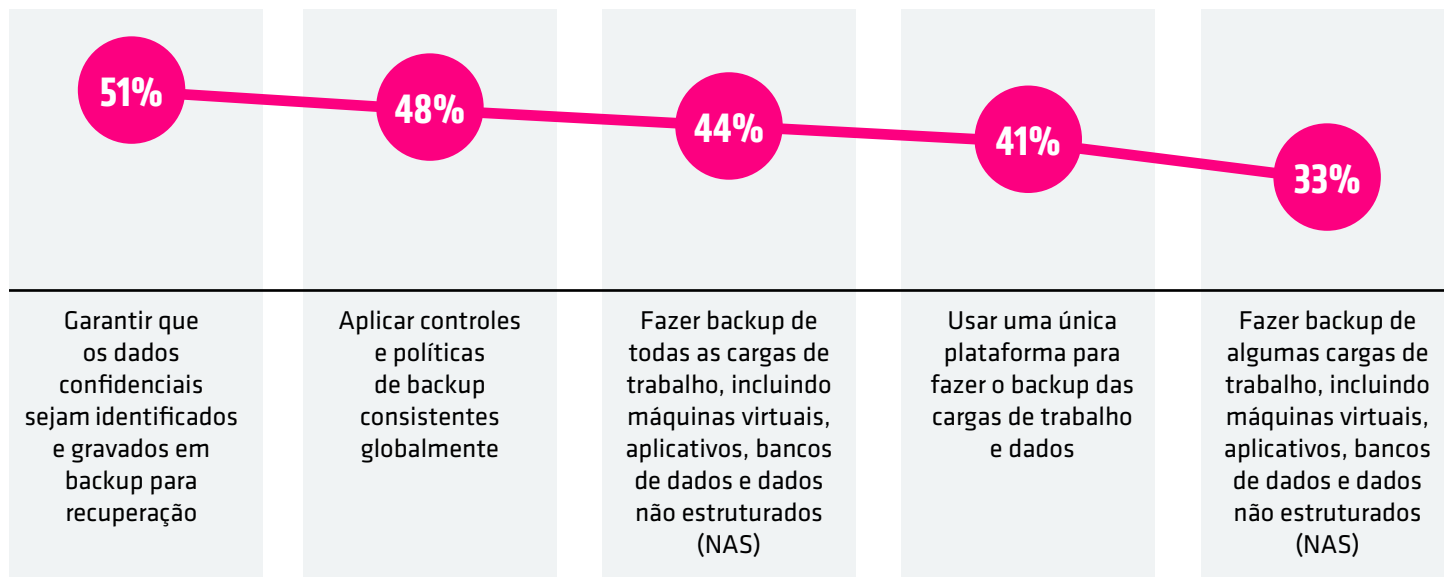
Considerando-se a escala dos prejuízos financeiros e operacionais revelados na nossa pesquisa, seria natural se houvesse uma preocupação generalizada com a resiliência organizacional. Porém, a maioria dos participantes (54%) confia totalmente na capacidade de sua estratégia de resiliência cibernética 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?



Pouco mais da metade das organizações do setor público garante que os dados confidenciais sejam identificados e gravados em backup para recuperação, enquanto quase metade delas aplica controles e políticas de backup consistentes globalmente. Menos da metade faz backup de todas as cargas de trabalho ou usa uma única plataforma para proteger as cargas de trabalho e dados. 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

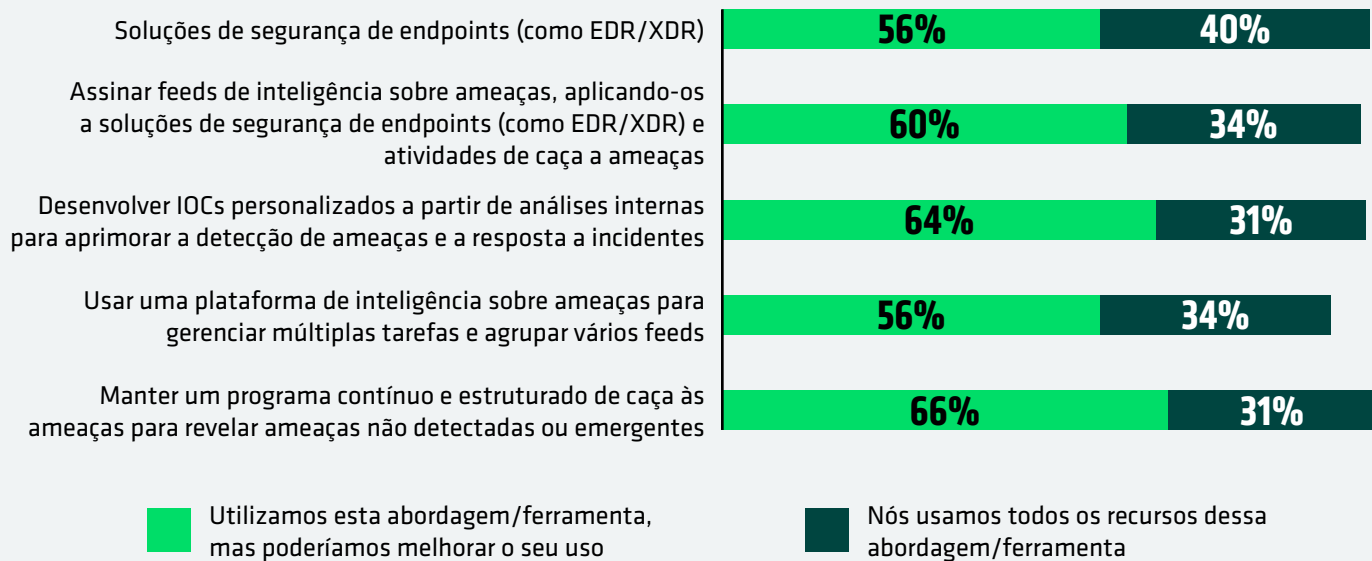
O que a sua empresa faz para garantir que seus dados sejam sempre recuperáveis?

50%	Exigir autorização adicional para tarefas de administração de alto risco associadas às soluções de backup e recuperação
47%	Seguir a “regra de backup 3-2-1” (três cópias dos seus dados em duas mídias diferentes e uma cópia externa)
46%	Autenticação multifator na nossa solução de backup
46%	Direitos de acesso com privilégios mínimos para as cargas de trabalho gravadas em backup
38%	Proteger dados cruciais com imutabilidade

Muitas organizações do setor público fortaleceram os controles de acesso para os ambientes de backup, com metade delas exigindo autorização adicional do administrador para tarefas de alto risco. Cerca de metade delas impõe a autenticação multifator, segue a regra de backup 3-2-1 e aplica direitos de acesso com privilégios mínimos. Menos delas protegem dados cruciais com imutabilidade. 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

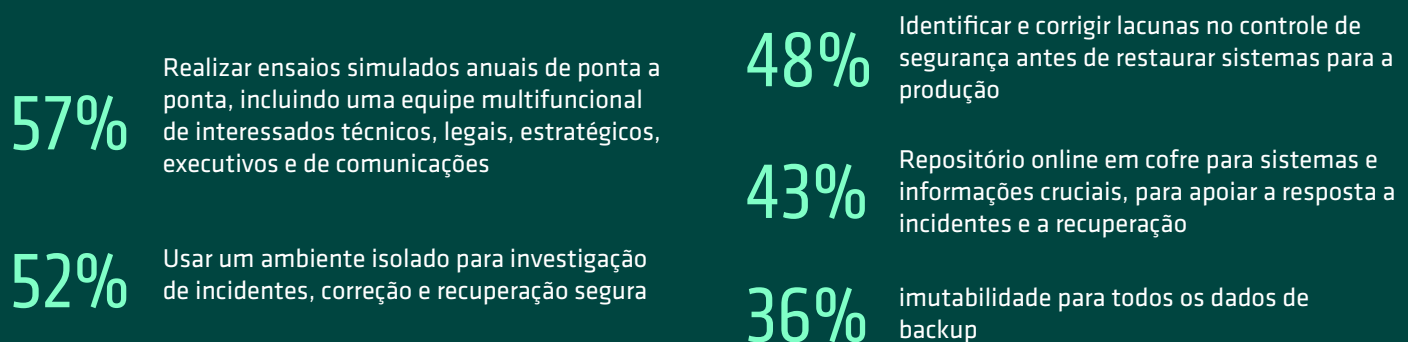
Em que medida a sua organização usa cada um dos seguintes métodos ou ferramentas para detectar e investigar ameaças?



As ferramentas de detecção e investigação de ameaças são amplamente implementadas, mas pouco usadas. A maioria das organizações do setor público usam segurança de endpoint, feeds de inteligência sobre ameaças, IOCs personalizados, plataformas de inteligência sobre ameaças e programas estruturados de caça a ameaças. Apesar disso, apenas uma minoria utiliza todo o potencial dessas ferramentas. 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

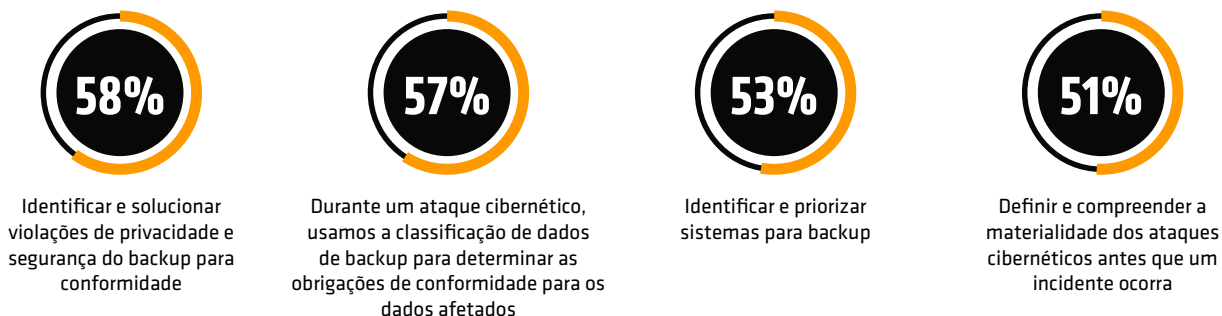
O que a sua organização faz ou faria para garantir a resiliência de aplicativos contra ataques cibernéticos?



As empresas do setor público estão avançando sua abordagem de resiliência de aplicativos, mas ainda há lacunas. Quase metade delas identificou lacunas no controle de segurança antes de restaurar sistemas, e mais da metade realizou ensaios anuais de recuperação. Pouco mais de metade delas manteve repositórios em cofres online. Um número menor usou ambientes isolados para investigação e recuperação seguras. Uma porcentagem ainda menor aplica imutabilidade em 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 do setor público estão usando a descoberta e a classificação dos dados de forma mais estratégica para conformidade, resposta e recuperação. Mais da metade lida com violações de segurança e privacidade, enquanto cerca de metade usa a classificação para orientar a conformidade durante um ataque e definir a materialidade antes de um incidente. Uma proporção similar prioriza os backups com base em risco. Esses padrões 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 público estão implementando (ou tendo dificuldades para implementar) a resiliência na prática. Embora a maioria esteja na fase de desenvolvimento, apenas 4% demonstram os recursos mais maduros e integrados que definem as organizações preparadas para o risco.

A CURVA DE MATURIDADE DA RESILIÊNCIA CIBERNÉTICA



Menos maduras (11%): 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 (22%): 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.

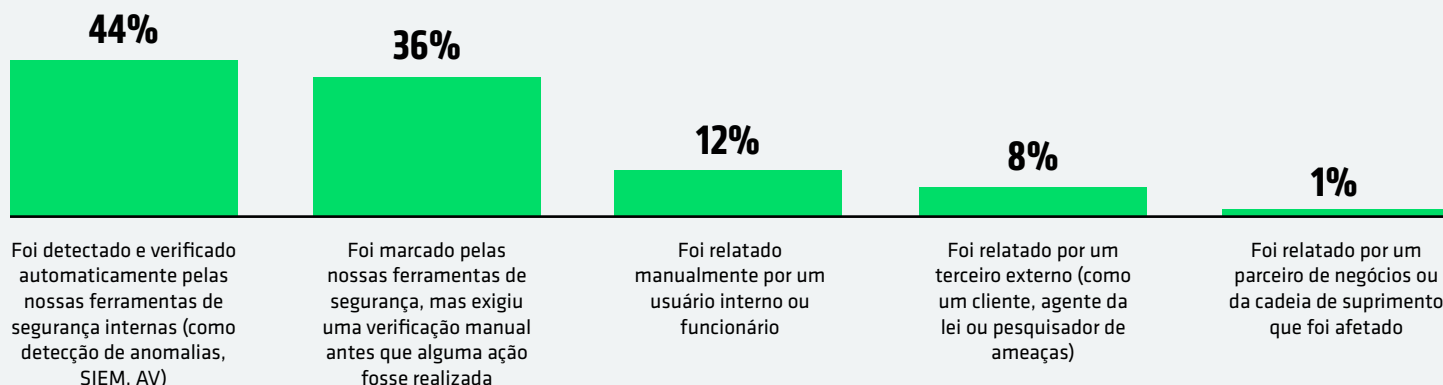
Em desenvolvimento (57%): As práticas básicas, como backup, controles de administrador e inteligência sobre ameaças são mais comuns, mas ainda desiguais. Ambientes de recuperação, verificações de conformidade e correção de lacunas de segurança são aplicadas esporadicamente, tornando os esforços de resiliência parcialmente eficazes.

Em avanço (8%): 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 (4%): 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.

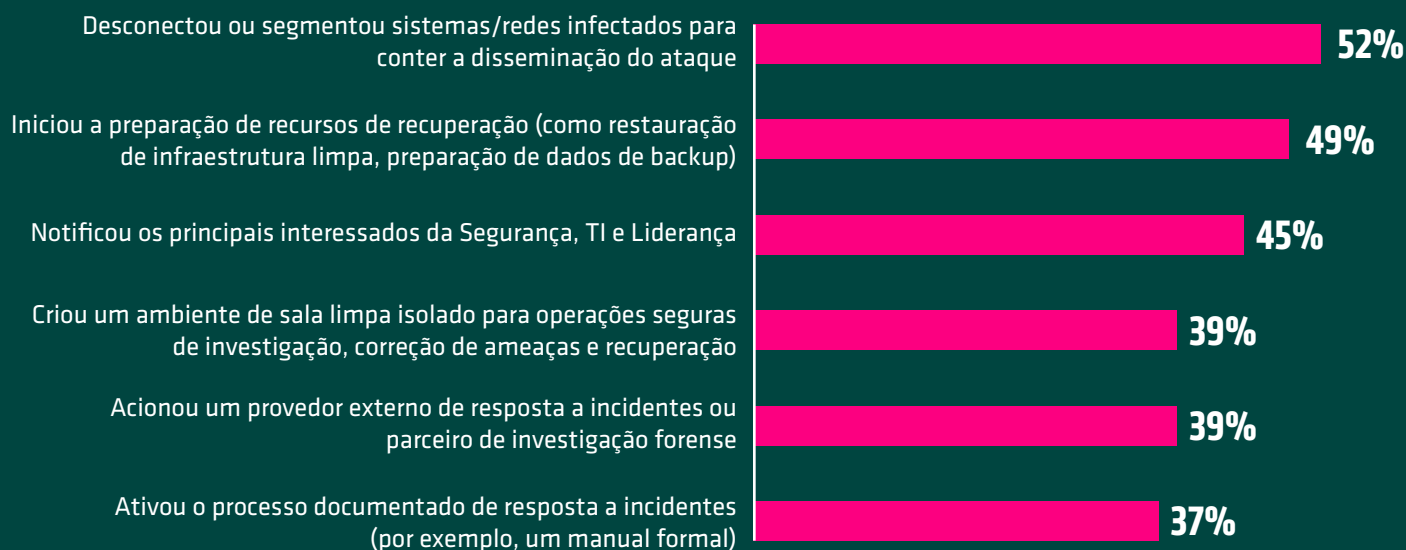
A RESILIÊNCIA SOB ATAQUE

COMO AS EQUIPES IDENTIFICARAM O ATAQUE



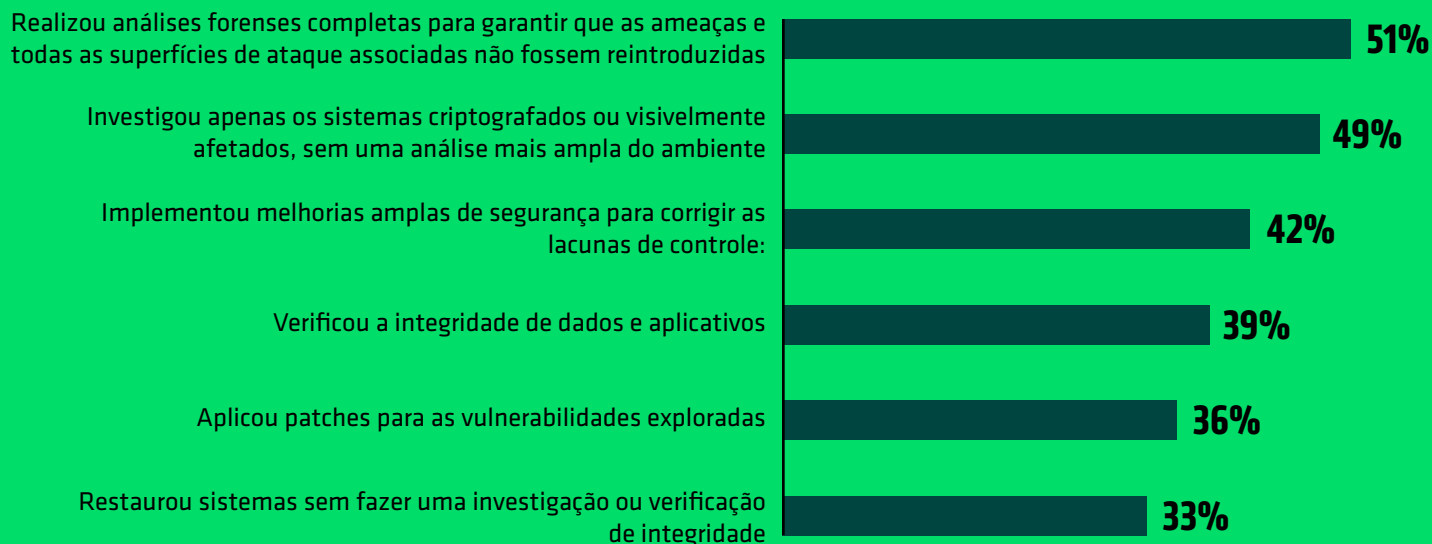
Em caso de um ataque cibernético, a maioria das empresas do setor público detecta os incidentes internamente. A maior parte é identificada automaticamente e verificada por ferramentas de segurança, enquanto muitas outras são marcadas por ferramentas, mas exigem verificação manual. Uma quantidade bem menor de incidentes são relatados por funcionários ou terceiros. A detecção é orientada principalmente por ferramentas, embora a validação humana ainda tenha um papel importante.

AÇÕES REALIZADAS PELAS EQUIPES APÓS A CONFIRMAÇÃO DO ATAQUE



Depois de confirmarem um ataque, as organizações do setor público tomaram medidas variadas para conter a ameaça e iniciar a recuperação. Cerca de metade das empresas desconectou sistemas infectados ou começou a preparar recursos para recuperação limpa, enquanto muitas notificaram os principais interessados. Menos delas criaram ambientes de sala limpa isolados, ativaram manuais formais de resposta ou acionaram parceiros externos de resposta a incidentes. Essas diferenças sugerem que as iniciativas de resposta não são padronizadas de forma consistente em ações cruciais.

MEDIDAS ADOTADAS ANTES DE COLOCAR SISTEMAS E DADOS ONLINE NOVAMENTE



Antes de colocar sistemas e dados online novamente, as empresas do setor público adotaram várias medidas de análise forense e correção. Cerca de metade delas fez uma análise forense completa ou focou apenas nos sistemas visivelmente afetados, enquanto uma quantidade menor implementou melhorias de segurança mais amplas, verificaram a integridade ou corrigiram as vulnerabilidades exploradas. Um dado notável é que cerca de um terço restaurou sistemas sem investigação ou verificação, deixando possíveis lacunas que podem aumentar o risco de reinfecção ou de exposição residual.

DESAFIOS ENFRENTADOS PELAS EQUIPES DURANTE O ATAQUE



As equipes enfrentaram desafios técnicos e operacionais significativos durante o ataque. Muitas tiveram dificuldades de comunicação quando os sistemas críticos estavam offline e se sentiram pressionadas para restaurar os sistemas antes que a correção fosse concluída. Outras relataram evasão de ferramentas de segurança, backups atacados, falta de pontos de recuperação limpos e até reinfecção após a recuperação. Essas dificuldades destacam as lacunas na prontidão, que podem complicar a resposta e prolongar a interrupção.

ONDE AINDA FALTAM INVESTIMENTOS EM RESILIÊNCIA

Até as empresas 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 público 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 SURTEM COMO MULTIPLICADORES DE RESILIÊNCIA

Os resultados também mostram que as organizações do setor público 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 do setor público 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. 43% acreditam que a IA vai apoiar a tomada de decisões por humanos, aprimorando análise e recomendações, com os humanos continuando no controle das ações finais. 42% 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 do setor público 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 o setor público.
 - [Governo federal](#)
 - [Governo estadual e municipal, e educação](#)

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.

