2025

Pesquisa CISO Brasil

kaspersky

kaspersky.com.br

Introdução

Os profissionais de cibersegurança do mundo inteiro enfrentam desafios cada vez maiores para manter os dados e sistemas de suas organizações em segurança. Os ativos digitais têm um papel mais importante do que nunca em todos os setores, o volume e a sofisticação dos ciberataques cresce e muda rapidamente, e há novas tecnologias disponíveis para os cibercriminosos e também para quem se defende deles.

Os tomadores de decisões de cibersegurança do Brasil consideram difícil estabelecer prioridades para suas organizações e conseguir orçamento para soluções que se integrem com os sistemas existentes e atualizem as medidas de proteção de modo efetivo para suprir as demandas, que mudam continuamente. Segundo um novo estudo comissionado pela Kaspersky, muitos reconhecem que a abordagem proativa é a única base segura para o avanço da proteção cibernética; contudo, a maioria das organizações não implementou soluções correspondentes. Na prática, nem a implementação de medidas de proteção padrão foi concluída.

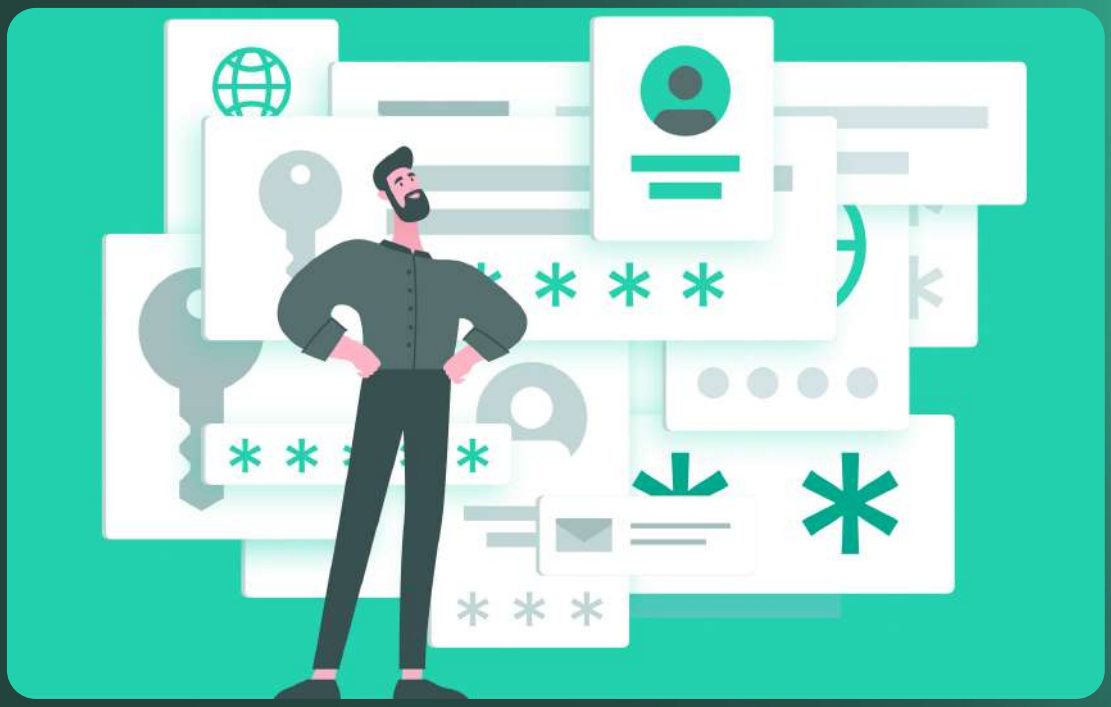
Evidentemente, falta entender o status dos esquemas de proteção atuais e também oportunidades para criar sistemas mais resilientes no geral. Assim, além das soluções mais recentes, é fundamental oferecer acesso a informações e consultoria para empresas de todos os tamanhos no Brasil.

"Tomadores de decisões de cibersegurança consideram difícil estabelecer prioridades para suas organizações"

A Kaspersky comissionou um estudo do mercado na América Latina com o objetivo de compreender o estado atual do gerenciamento da cibersegurança e obter percepções sobre novas soluções e tecnologias para garantir a segurança futura de sistemas, redes e informações.

A amostra englobou 300 entrevistas realizadas com profissionais de cibersegurança e importantes tomadores de decisões da área de segurança de rede e de informações (CIOs, CISOs, CTOs, profissionais de InfoSec que lidam com segurança de rede e de informações e/ou avaliações de segurança, analistas de SOC, especialistas em TI que lidam pelo menos parcialmente com tarefas de InfoSec). Todos trabalham em organizações de diversos setores com equipes de TI dedicadas. Os mercados incluídos foram Argentina (n=50), Brasil (n=50), Chile (n=50), Colômbia (n=50), México (n=50) e Peru (n=50). O trabalho de campo foi realizado entre 25 e 31 de março de 2025.

Principais resultados



Todos os profissionais de cibersegurança do Brasil confiam muito em sua capacidade atual de identificar ameaças cibernéticas de maneira efetiva e acreditam que seu histórico de responder rapidamente a ciberincidentes é excelente. Ainda assim, conforme mostra o estudo, a implementação de tecnologias de cibersegurança em muitas organizações é incompleta e desatualizada, e a eficácia da resposta e da resolução está longe do ideal. Refletindo essa realidade, 30% afirmam que um tempo de resposta rápido é essencial para fechar as lacunas em seus esquemas de cibersegurança, assim como planos específicos para adquirir mais softwares com essa finalidade (66%) e mais investimentos na detecção de ameaças (50%).

Em relação ao futuro, as pessoas responsáveis pela cibersegurança não expressam a mesma certeza: 86% afirmam que há trabalho a ser feito para que os sistemas e dados de suas empresas continuem seguros daqui a dois anos, e 44% dizem que isso exigirá muito trabalho. Talvez isso não seja surpresa, já que a maioria observou um aumento significativo nos ataques cibernéticos a suas organizações nos últimos dois anos (88%), e eles não crescem apenas em número, mas também em nível de sofisticação (84%).

Quando se trata de tecnologias mais avançadas, menos da metade (42%) das organizações brasileiras usa o SIEM (gerenciamento de informações e eventos de segurança), 34% das empresas usam o XDR e apenas 32% usam o EDR (detecção e resposta nos endpoints). Tratando de futuro, 26% das organizações têm planos definidos para implementar essas tecnologias mais avançadas de XDR, outras 30% SIEM e 32% em EDR. Além das tecnologias mais voltadas para o futuro, são necessários mais investimentos em detecção de ameaças (50%) e em ferramentas para incrementar a efetividade da cibersegurança (46%).

Apesar de reconhecer a necessidade clara de diversas melhorias, continua sendo difícil priorizá-las, e 48% das empresas não têm um cronograma regular de avaliações de risco. Em vez disso, reagem aos ataques ou eventos externos, que servem como gatilhos para avaliações da cibersegurança vigente. A análise de causas básicas (54%) e a identificação de ameaças em tempo real (36%) são relatadas como sendo as partes mais demoradas do processo de resposta a incidentes, o que reflete uma possível falta de entendimento dos benefícios da maior automação.

As percepções das tecnologias como proativas ou reativas mostram uma ampla controvérsia sobre o que torna uma tecnologia proativa – de firewalls ao XDR, alguns os definirão como proativos, outros como reativos. Ainda assim, muitos concordam sobre os benefícios de usar tecnologias proativas, especialmente o gerenciamento aprimorado de riscos (54%), a detecção precoce de ameaças (50%) juntamente com os tempos menores de resposta a incidentes (50%), seguido da detecção de ameaças mais avançadas (44%).

As informações sobre os avanços tecnológicos mais recentes para reforçar a segurança de informações e sistemas vêm principalmente dos fornecedores (58% obtêm informações deles), mas grande parte da inteligência de ameaças é compilada manualmente (54%).

A promoção da cibersegurança atual até o nível de desempenho necessário para enfrentar diretamente as ameaças futuras é amplamente reconhecida como um desafio importante, mas muitos não têm uma ideia clara dos passos necessários ou do que as tecnologias avançadas podem oferecer para ajudá-los a avançar na direção de uma abordagem de cibersegurança realmente mais proativa.

Gerenciando a cibersegurança hoje

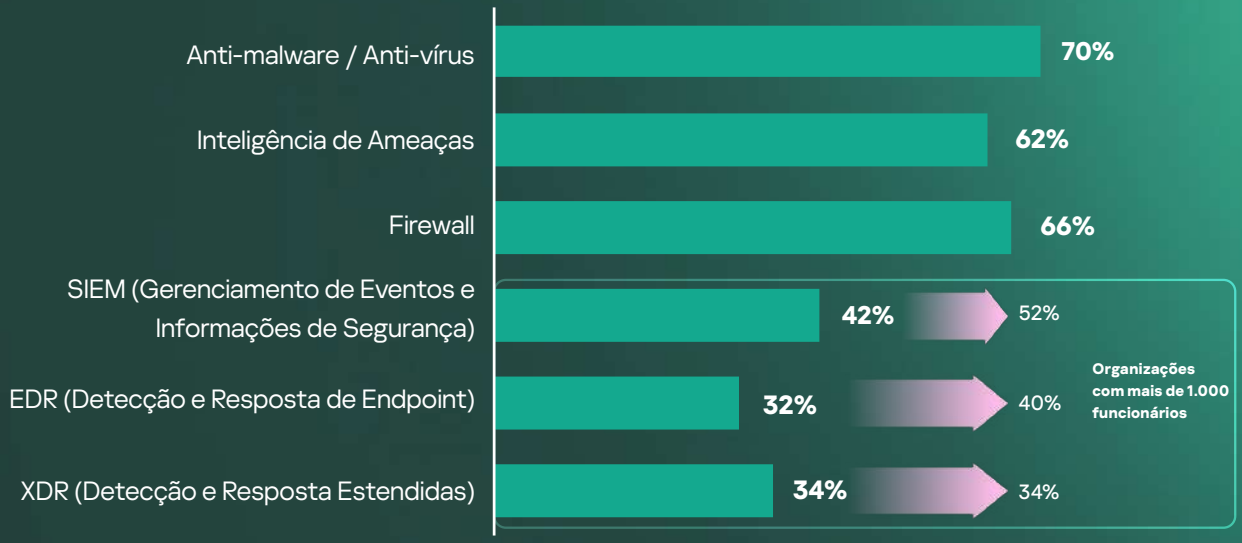
Todas as organizações que participaram do estudo têm equipes de TI dedicadas, utilizando recursos internos e terceirizados para acessar a competência e a mão-de-obra de que precisam. Mais da metade (62%) tem uma equipe interna, 32% associam profissionais de TI internos e externos em suas equipes, e apenas 6% têm equipes totalmente externas. Como seria de se esperar, as organizações menores são mais propensas a terceirizar as rotinas de TI, pois normalmente têm menos recursos humanos disponíveis internamente – 32% das PMEs (até 499 funcionários) têm equipes totalmente externas, 6% das que têm mais de 1.000 funcionários adotam essa abordagem.

"Organizações menores são mais propensas a terceirizar a capacidade de TI,"

Geralmente, a confiança da proteção das empresas brasileiras é alta: todas, em geral, afirmam ter total confiança em sua capacidade de identificar ciberameaças de modo efetivo e acreditam que seu histórico de responder rapidamente a elas é excelente.

80% das empresas acreditam que os dados e sistemas de suas organizações estão atualmente muito bem ou extremamente bem protegidos, e quase todas elas (98%) enfatizam que a prevenção de ciberincidentes é uma prioridade básica em suas organizações. No todo, todas alegam terem feito investimentos consideráveis para evitar vulnerabilidades em suas redes e sistemas.

As tecnologias de cibersegurança utilizadas no momento refletem predominantemente abordagens tradicionais, e mesmo a implementação de medidas de proteção padrão ainda não foi concluída. Quase um terço (30%) não usa software antivírus/antimalware, mais de um terço (37%) não usa inteligência de ameaças e 44% não têm um firewall. SIEM, EDR e XDR são usados por ainda menos organizações, mas a probabilidade de serem usados pelas grandes empresas é significativamente maior.



Quais das tecnologias de segurança a seguir já fazem parte da sua estratégia atual de segurança de informações?

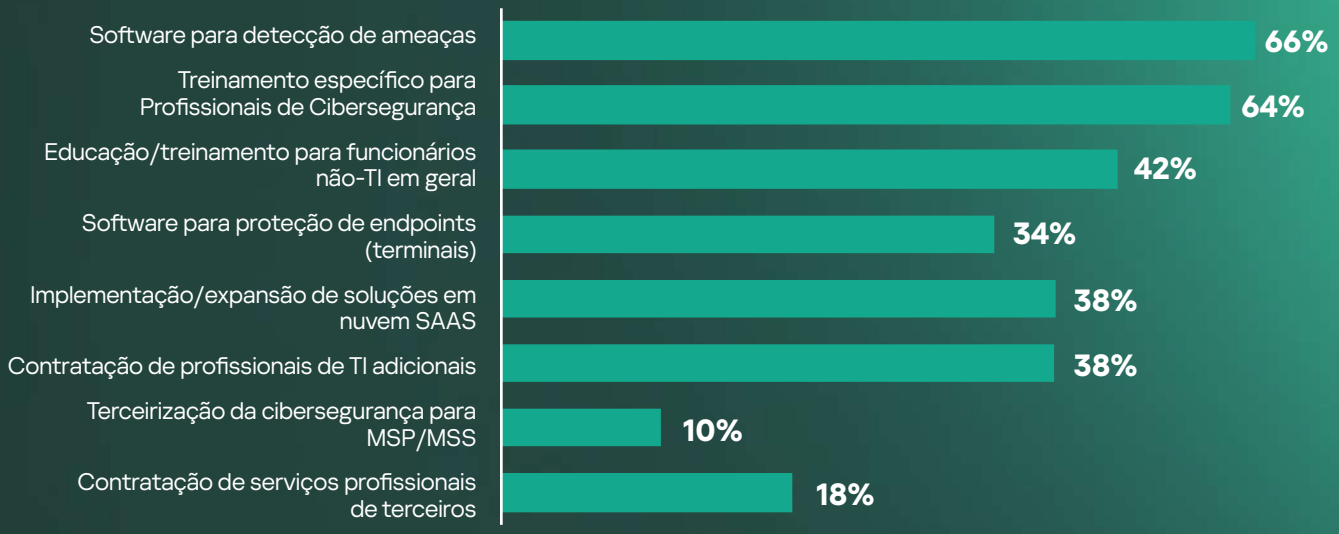
Apesar da confiança, os profissionais de cibersegurança preocupam-se com um cenário de ameaças que muda rapidamente: 88% observaram um volume muito maior de ciberataques nos dois últimos anos, e 84% relatam que esses ataques são substancialmente mais sofisticados. Como reflexo dessa preocupação, apenas 14% acreditam que seu esquema atual de proteção digital está preparado para o futuro, enquanto até 44% afirmam que será necessário muito trabalho para garantir a segurança dos dados e sistemas de suas organizações no futuro.

Seguindo essa lógica, uma proporção importante das empresas que ainda não usam tecnologias avançadas pretende fazê-lo em breve: 26% desejam incluir o XDR em seu arsenal de defesa, 30% o SIEM e 32% o EDR. Outros (30%) também planejam começar a usar a inteligência de ameaças para melhorar suas funcionalidades de cibersegurança.

No todo, “mais ferramentas para aumentar a eficácia de seu esquema de proteção” é mencionado por 46% como prioridade para reduzir a defasagem de cibersegurança, 44% consideram mais investimentos em geral como necessários e, no topo da lista, está mais investimento em detecção de ameaças (50%).

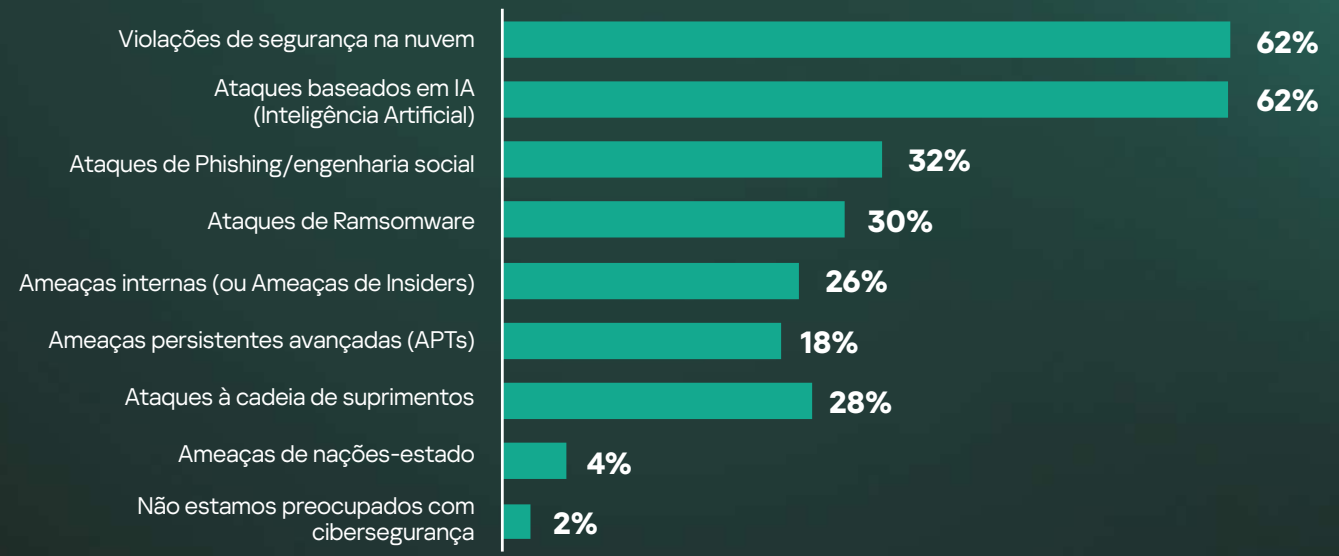
Para a maioria, é difícil estabelecer prioridades para aprimorar sua proteção, mas os planos concretos de investimento para os próximos 12 a 18 meses estão alinhados

com as necessidades atuais: 66% pretende investir em ferramentas para melhorar a detecção de ameaças, e quase a mesma proporção (64%) em treinamento específico para profissionais de cibersegurança. Outros 42% vão investir na educação de funcionários de outras áreas que não a TI, o que indica a importância de defender-se da crescente onda de ataques de engenharia social (uma forte preocupação para 32%).



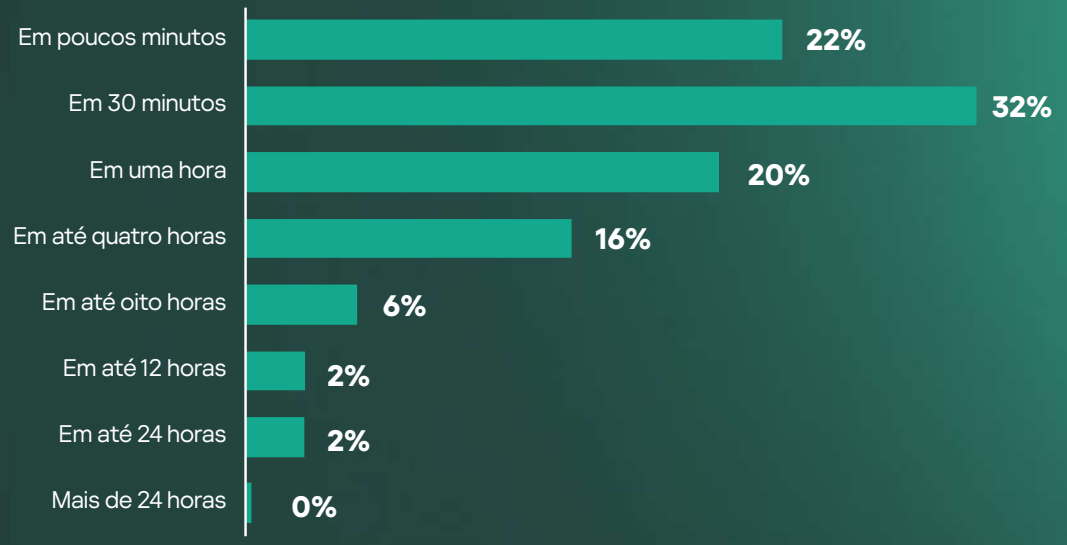
Em que área da cibersegurança é mais provável que sua empresa faça investimentos nos próximos 12 a 18 meses?

As duas maiores preocupações das empresas são as violações de segurança na nuvem (62%), empatada com as ameaças baseadas em IA (62%). O phishing e outros ataques de engenharia social ocupam o terceiro lugar, com 32%. Apenas um número muito pequeno de organizações não tem preocupações de segurança (2%).



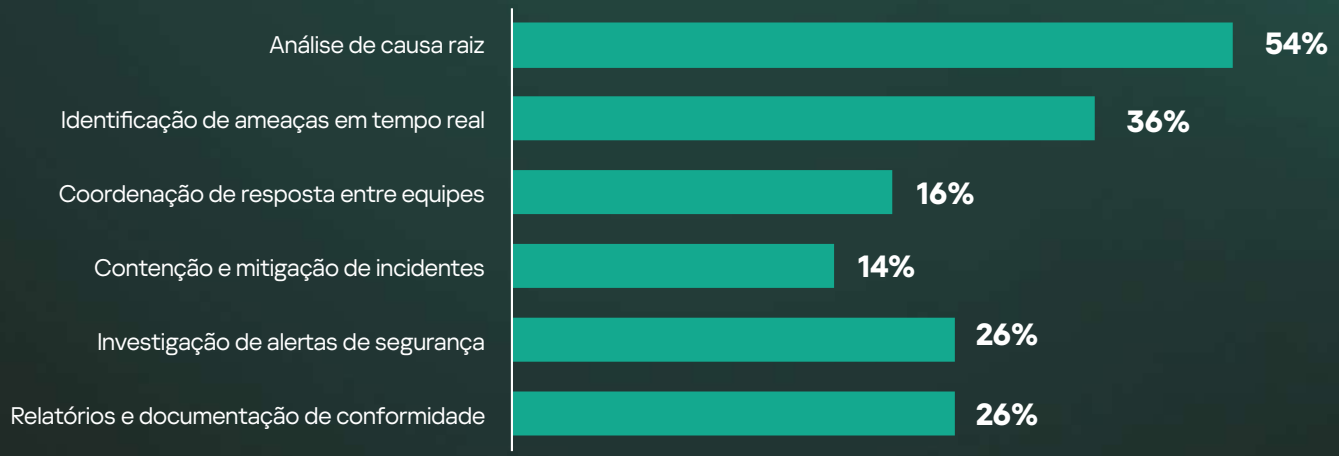
Quais ameaças de cibersegurança mais preocupam a sua organização? (escolha até três opções)

Embora a detecção de ciberameaças precise claramente de melhorias (66% pretendem investir em software para melhorá-la), quando perguntamos sobre seu tempo de resposta médio, 22% afirmam que normalmente consegue uma resposta poucos minutos depois de perceber um ataque e 32% menciona um tempo de resposta inferior a 30 minutos.



Quanto tempo normalmente leva para sua empresa responder a um incidente, depois que percebe que está ocorrendo um ataque?

Ainda assim, ao examinar todos os fatores que retardam o processo de resposta, eles indicam algumas lacunas fundamentais nas funcionalidades: a identificação de ameaças em tempo real é um problema comum (42%), superado apenas pelo tempo que leva para conduzir uma análise de causas básicas (44%). A coordenação da resposta entre as equipes é relatada por 26% das organizações e a contenção e a mitigação de eventos é um problema para 22%. Um em cada cinco (20%) tem dificuldades para investigar alertas de segurança rapidamente. Tudo isso mostra a necessidade de entender mais claramente o potencial de automatizar as principais partes do processo de resposta a incidentes.

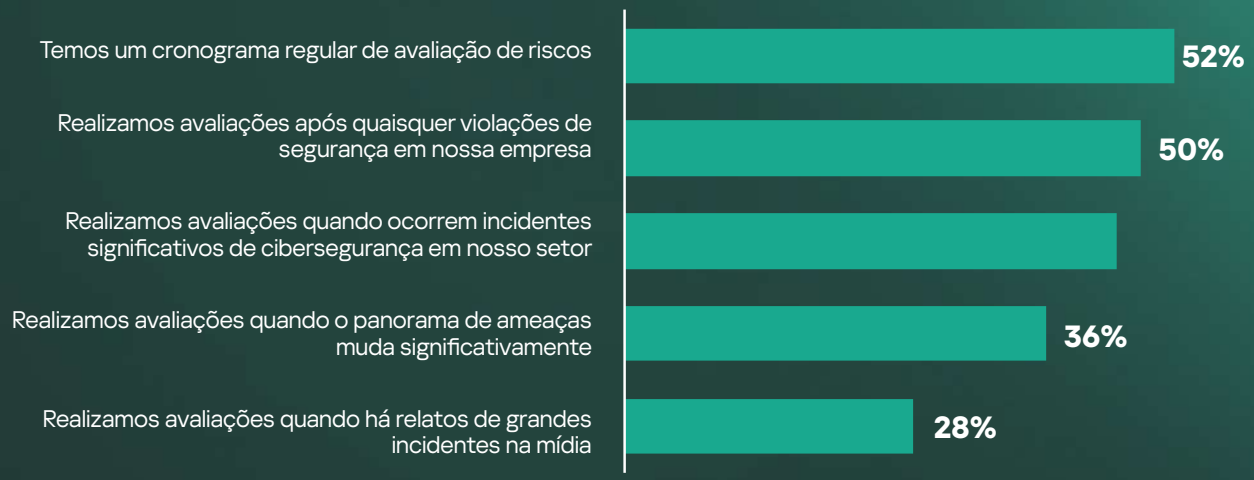


Qual é a parte mais demorada do processo de resposta a incidentes da sua organização? (escolha até quatro opções)

Avaliando e mitigando riscos

A eficácia da avaliação de riscos, priorização de ameaças e preparação para possíveis incidentes é fundamental para uma proteção digital bem-sucedida, especialmente quando a tecnologia transforma o nível e a complexidade dessas ameaças em velocidades sem precedentes. Surpreendentemente, 48% das organizações não têm um cronograma regular de avaliação de ameaças em vigor; em vez disso, reagem a eventos internos ou externos à empresa.

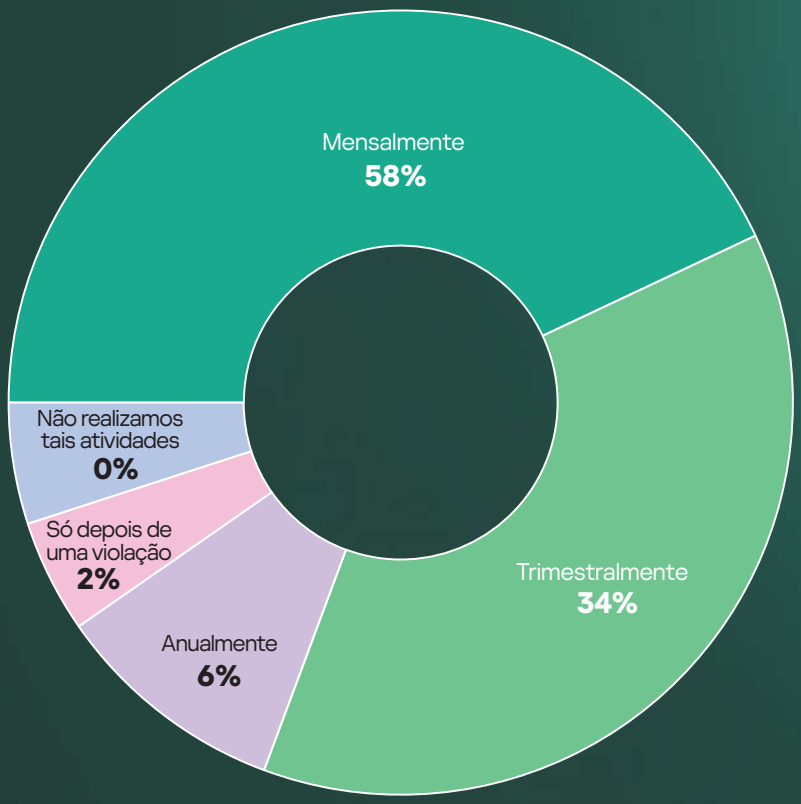
Isso se aplica especialmente a empresas menores (com menos de 500 funcionários); 62% delas não têm um cronograma regular de avaliação de riscos, em comparação com 45% das empresas com mais de 500 funcionários. A maioria reage com uma avaliação de violações de segurança na própria organização (50%) e/ou a ciberincidentes importantes no setor (48%). O nível de gatilho mais baixo para uma análise são as notícias na mídia sobre incidentes importantes.



O que desencadeia uma avaliação de riscos em sua empresa?

Normalmente, avaliações de riscos programadas e regulares são realizadas mensalmente (por 65% das organizações que têm um cronograma definido, aumentando para 83% no caso de organizações com 1.000 funcionários ou mais), e trimestralmente por 35%). Como esperado, aquelas que realizam avaliações de riscos em reação a eventos externos fazem isso com menos frequência: apenas 79% conduzem avaliações mensalmente, 21% as realizam trimestralmente.

A falta de uma prevenção proativa fica ainda mais evidente quando se avalia as defesas digitais feitas a partir de simulações e exercícios de resposta a ameaças: em todas as organizações, apenas 58% os realizam mensalmente, 34% o fazem a cada trimestre, 6% fazem simulações e exercícios de resposta a ameaças uma vez por ano, 2% apenas depois que ocorre uma violação na organização. Todas fazem ao menos de algum modo.



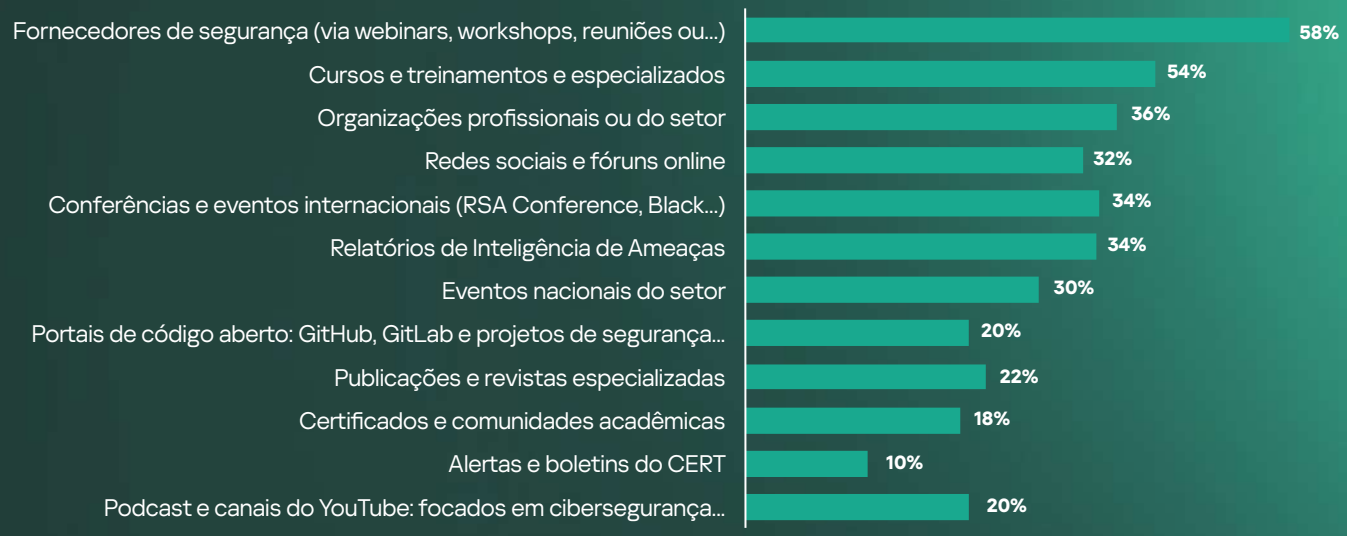
Com que frequência sua empresa realiza exercícios de resposta a ameaças e simulações para se preparar para possíveis violações de cibersegurança?

As políticas de cibersegurança são revisadas com frequência semelhante: 48% reavaliam suas políticas de segurança mensalmente (51% quando analisamos apenas as empresas maiores com mais de 1.000 funcionários), 48% fazem revisões trimestrais, 4% as examinam uma vez por ano e nenhuma (0%) não têm nenhum processo de revisão de políticas de proteção digital.

Adquirindo inteligência

Mais de metade (58%) obtém informações sobre tendências tecnológicas para respaldar a segurança das informações e sistemas de proteção por meio de webinars, workshops, encontros ou materiais como relatórios e whitepapers. Isso aplica-se especialmente às organizações maiores: 65% utilizam os fornecedores de cibersegurança para ter acesso à informação.

Cursos e treinamentos especializados (54%), organizações profissionais ou setoriais (36%) e redes sociais e fóruns on-line (32%) são outras fontes importantes.



Onde vocês obtêm informações sobre as últimas evoluções da tecnologia para respaldar a segurança de informações e sistemas?

Cerca da metade das organizações adquire inteligência de ameaças das equipes internas de segurança, que a organiza manualmente (54%); esse número aumenta para 60% em grandes organizações com mais de 1.000 funcionários. Provedores comerciais de inteligência de ameaças são utilizados por 58% (46% no caso de organizações com mais de 1.000 funcionários), e 32% a obtêm por meio de provedores terceirizados de MDR ou SOC, que também são responsáveis por fornecer serviços de inteligência de ameaças. Apenas 6% não usam nenhum serviço do tipo.

Quase metade (48%) ainda trabalha com um ou dois provedores comerciais de inteligência de ameaças, 14% trabalham com três provedores e 34% trabalham com quatro ou mais (esse percentual aumenta para 37% no caso das organizações maiores, com mais de 1.000 funcionários).

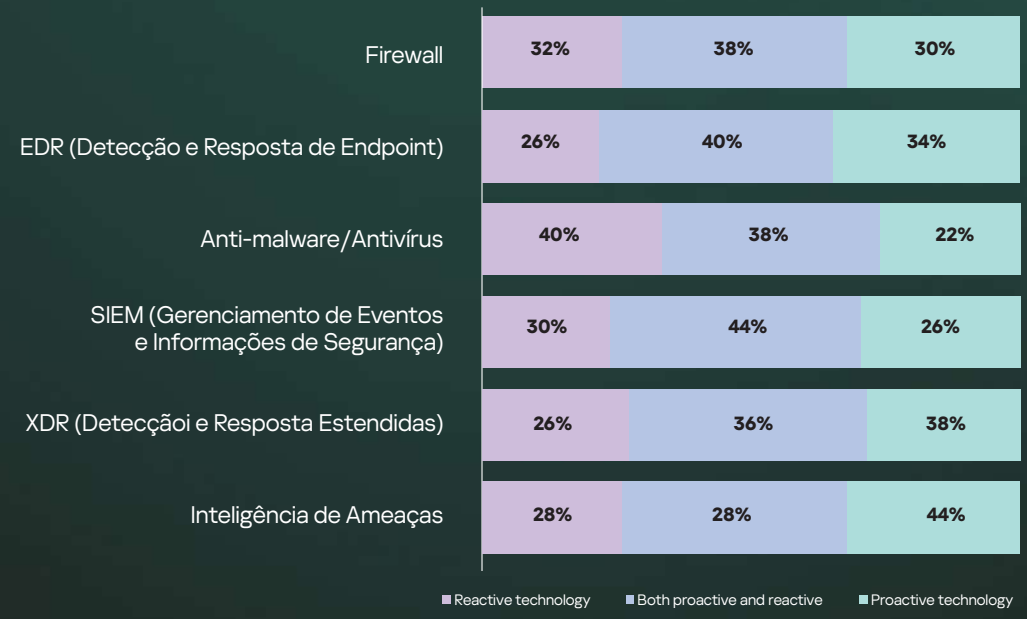
Da reação à proatividade

A perspectiva dos profissionais de cibersegurança em relação a sua estratégia de defesa influencia de maneira decisiva o design e o esquema das ferramentas e tecnologias utilizadas para proteger os dados e sistemas de suas organizações. Quando perguntado se é utilizada uma abordagem de segurança de informações e sistemas reativa (reagindo a ameaças e ataques quando eles acontecem) ou proativa (focando a prevenção de ataques antes que ocorram), 82% classificaram sua abordagem como proativa (com pontuação de 7 a 10 em uma escala de 1 a 10), e apenas 8% como reativa (com pontuação de 1 a 4). Em relação ao futuro, 66% dos participantes disseram que mudariam para uma estratégia mais proativa nos próximos 12 meses, mas 22% afirmaram que se tornariam mais reativos em sua abordagem.

Os níveis atuais de investimento não refletem os níveis informados de proatividade, pois apenas 22% afirmam que metade ou mais de seus investimentos em cibersegurança são destinados ao XDR e à inteligência de ameaças para respaldar a defesa proativa, 48% investem entre 25% e 50% e 30% investem menos de um quarto de seu orçamento em XDR e inteligência de ameaças.

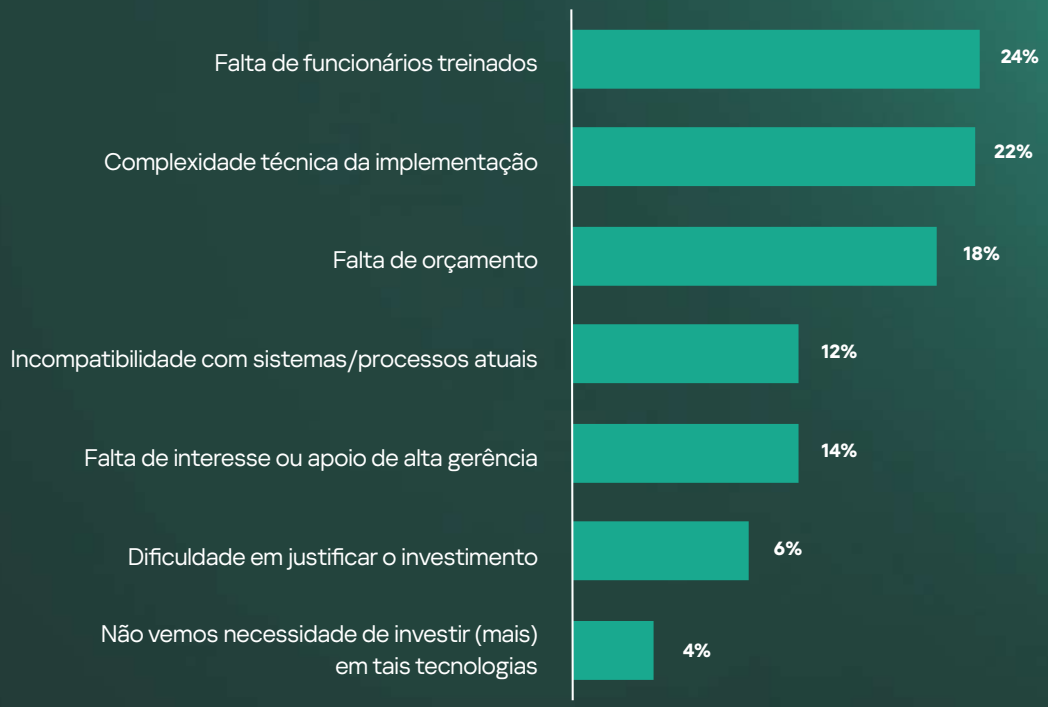
Em linhas gerais, podemos definir defesa proativa como a capacidade de evitar ataques antes que eles ocorram, produzindo resiliência no próprio sistema, em vez de reagir a incidentes conforme eles surgem. É importante reagir a violações de segurança de maneira rápida e eficaz, mas não há um entendimento suficiente do papel e da funcionalidade das tecnologias proativas e de como elas podem ser usadas para ter o impacto ideal.

Ao pedir que profissionais de cibersegurança identifiquem as tecnologias conhecidas como proativas, reativas ou ambas, tivemos alguns resultados surpreendentes:



A confusão entre esses conceitos reflete-se no grande número de profissionais de cibersegurança que consideram XDR, inteligência de ameaças e EDR como tecnologias reativas e antivírus/antimalware como tecnologias proativas. Isso mostra que a mentalidade de prevenção está se expandindo na comunidade de profissionais de cibersegurança, mas também que ela ainda não foi evidenciada na estratégia implementada.

Os maiores desafios que impedem mais investimentos nessas áreas são a falta de pessoal de TI qualificado (24%), a complexidade técnica da implementação (22%) e a falta de orçamento (18%). Apenas 4% não vê motivo para investir em XDR ou inteligência de ameaças.



Qual é o maior desafio que sua organização enfrenta para investir (mais) em tecnologias como XDR e inteligência de ameaças? (selecione uma opção)

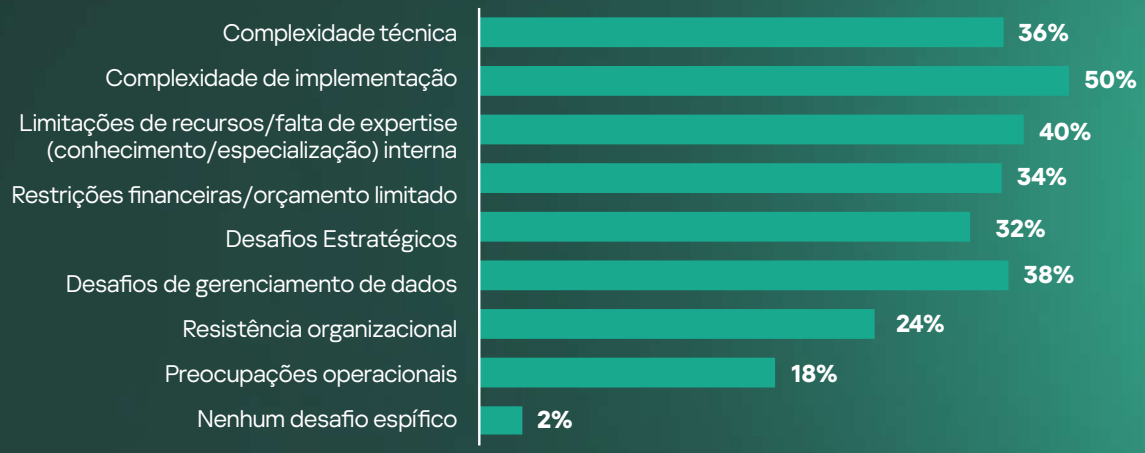
A postura em relação às tecnologias proativas é positiva e há um reconhecimento comum dos benefícios de sua adoção. O gerenciamento aprimorado de riscos (54%), seguido da detecção precoce de ameaças (50%), e menores tempos de resposta a incidentes (50%), e a detecção de ameaças mais avançadas (44%) são os principais pontos positivos da tecnologia.

Quais benefícios, se houver, a (potencial) adoção de tecnologias proativas tem ou poderia ter para organizações como a sua?

Aqueles que identificam a detecção precoce como um benefício essencial destacam a identificação de possíveis ameaças antes que possam causar danos como o benefício mais importante (84%), seguida da transição mais rápida entre o comprometimento e a detecção de uma ameaça (60%) e o monitoramento do comportamento da rede para detectar anomalias (32%).

Para 52%, o gerenciamento aprimorado de riscos se converte na avaliação e priorização contínua de riscos de segurança como principal benefício. A implementação automática de controles de segurança (44%) e o fornecimento de visibilidade em tempo real na conduta de segurança (41%) são outros aspectos positivos do gerenciamento aprimorado de riscos.

Como mencionado acima, ao lado dos benefícios claramente reconhecidos, os profissionais de cibersegurança enfrentam uma série de desafios para transferir investimentos para as tecnologias proativas; os mais comumente identificados são a complexidade da implementação (50%), a falta de expertise de especialistas internos (40%) e os desafios de gerenciamento de dados por 38%. Em seguida, são apontadas a complexidade técnica (36%), restrições financeiras (34%) e os desafios estratégicos (32%).



Se houver, quais são os desafios que a adoção de tecnologias proativas representa?

Os desafios de complexidade técnica variam da necessidade de expertise especializada para implementar e gerenciar essas soluções (61%), dos problemas de compatibilidade com a infraestrutura herdada (44%) e aos desafios de integração com a infraestrutura existente (22%).

"Considerando o esforço geral para melhorar a eficácia da cibersegurança para proteger efetivamente dados e sistemas no futuro, a inteligência de ameaças terá um papel fundamental para todas as organizações comerciais."

A necessidade de planejamento e testes criteriosos (44%) é um obstáculo importante dentro da complexidade da implementação, juntamente com os processos de implementação demorados (44%). Em seguida, temos a coordenação de vários departamentos (20%).

As limitações de recursos também se dividem em vários aspectos: falta de profissionais de cibersegurança qualificados (55%), equipes de segurança com carência de pessoal (45%) e a expertise interna limitada à implementação (40%).

A restrição financeira mais desafiadora é o alto custo inicial das soluções de segurança avançadas (82%). As despesas permanentes de licenciamento e manutenção também são uma questão para mais da metade (65%).

Considerando o esforço geral para melhorar a eficácia da cibersegurança para proteger efetivamente dados e sistemas no futuro, a inteligência de ameaças terá um papel fundamental para todas as organizações comerciais, ajudando-as a entender os grupos especializados, suas táticas e possíveis vulnerabilidades dos sistemas, respaldando estratégias de defesa mais eficazes e a melhor resolução de incidentes.

A tradução dessas informações em soluções práticas exigirá habilidades adicionais e o suporte de fornecedores profissionais para o desenvolvimento e a seleção das soluções proativas mais adequadas para cada organização, a fim de vencer os desafios e maximizar os benefícios associados ao avanço na direção da resiliência digital.

Recomendações da Kaspersky

As medidas de cibersegurança dos especialistas da Kaspersky que colaboraram nesse estudo visam fortalecer a ciber-resiliência das organizações, reduzindo o tempo de resposta a incidentes, ampliando a capacidade de detecção e prevenção de ameaças e promovendo uma cultura de segurança integrada à estratégia de negócio.

As sugestões foram reunidas em três grandes pilares: Governança e Estratégia, Tecnologia e Infraestrutura e Capacitação e Recursos Humanos.

1. Governança e Estratégia

- Definir papéis e responsabilidades formais para a governança de segurança.
- Realizar avaliações de risco constantemente, com periodicidade definida (pelo menos trimestral).
- Ter planos de resposta a incidentes testados regularmente por meio de simulações.
- Revisar periodicamente políticas de segurança e controles críticos.
- Implantar indicadores de desempenho e risco (KPIs e KRIs) que conectem cibersegurança e resultado de negócio.
- Priorizar medidas fundamentais de proteção: gestão de vulnerabilidades, backups automatizados e autenticação multifator.
- Adotar frameworks reconhecidos de maturidade e governança, como o NIST Cybersecurity Framework, ISO/IEC 27001 e CIS Controls, para orientar políticas e práticas corporativas.
- Implementar processos de gestão de riscos de terceiros e da cadeia de fornecimento (supply chain), avaliando controles de segurança de parceiros e prestadores de serviços críticos.
- Criar comitês de segurança interdepartamentais, unindo TI, segurança e áreas de negócio para decisões conjuntas.
- Incorporar métricas de segurança e resiliência nos painéis de performance executiva.
- Assegurar conformidade com legislações de proteção de dados e privacidade, incluindo a LGPD (Brasil), Ley 25.326 (Argentina), Ley de Protección de Datos Personales (México) e Habeas Data (Colômbia, Peru) – ou alinhar o programa de segurança à Estratégia Nacional de Cibersegurança na região.

2. Tecnologia e Infraestrutura

- Garantir o uso completo e atualizado das ferramentas básicas: proteção de endpoint, firewall, backup e controle de acesso.
- Integrar novas soluções com sistemas legados para eliminar lacunas de cobertura.
- Adotar automação nos fluxos de detecção e resposta, reduzindo o tempo de reação a incidentes.
- Avaliar e priorizar a adoção de soluções avançadas (EDR, XDR, SIEM) para ampliar visibilidade e capacidade de correlação de eventos — permitindo detectar incidentes nos estágios iniciais.
- Incorporar inteligência de ameaças integrada às plataformas de segurança, permitindo detecção de comportamentos anômalos.
- Fortalecer parcerias com provedores de inteligência e laboratórios de pesquisa para atualização contínua sobre TTPs recentes.
- Promover integração entre SOC, TI e áreas de negócio para resposta coordenada.
- Estabelecer políticas de atualização, testes e manutenção preventiva para toda a infraestrutura crítica.
- Implementar um programa estruturado de gestão de vulnerabilidades, com varreduras periódicas, priorização por criticidade e correção ágil.
- Reforçar o gerenciamento de identidades e acessos (IAM) com políticas de menor privilégio e autenticação multifator em todos os sistemas.
- Conduzir simulações regulares de incidentes para validar a eficiência técnica e os fluxos de comunicação.
- Adotar arquiteturas escaláveis e resilientes, com segmentação de rede e modelo Zero Trust.
- Utilizar orquestração e automação de incidentes (SOAR) para reduzir dependência de intervenção manual.
- Desenvolver e manter planos de continuidade de negócios (BCP) e recuperação de desastres (DRP), testando-os regularmente.
- Realizar Business Impact Analysis (BIA) para identificar processos e ativos críticos à operação.

3. Capacitação e Recursos Humanos

- Realizar campanhas de conscientização contínuas e não pontuais sobre phishing, engenharia social e boas práticas digitais.
- Oferecer capacitação técnica permanente para equipes de TI e segurança em:
- Resposta a incidentes.
- Análise de malware.
- Uso de ferramentas de Threat Intelligence.
- Incentivar certificações profissionais e participação em fóruns e comunidades especializadas.
- Criar centros de competência internos dedicados a threat intelligence, gestão de vulnerabilidades e resposta a incidentes.
- Desenvolver programas avançados de formação em threat hunting, análise forense e risco digital.
- Estabelecer parcerias estratégicas com provedores de inteligência, universidades e centros de pesquisa.
- Integrar práticas de segurança no ciclo de desenvolvimento (DevSecOps), aproximando segurança, TI e inovação.
- Promover treinamentos de crise e comunicação em incidentes, preparando executivos e líderes para decisões sob pressão e mensagens consistentes ao público interno e externo.
- Utilizar metodologias práticas como KIPS (Kaspersky Interactive Protection Simulation) e exercícios tabletop, para testar respostas em tempo real.
- Estimular a criação de uma cultura de segurança contínua, onde boas práticas e vigilância digital sejam parte do dia a dia da organização.

kaspersky