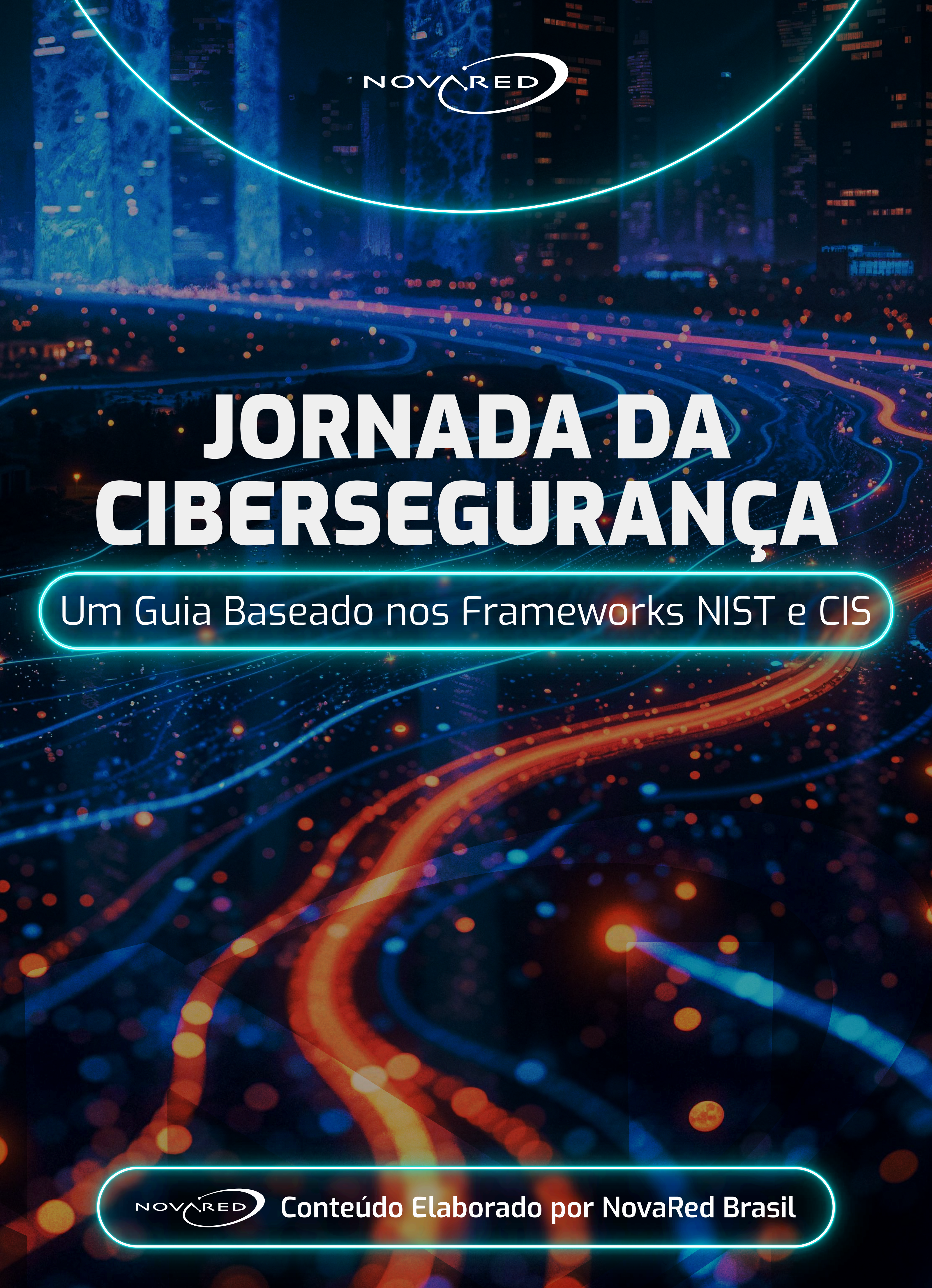




NOVARÉD

JORNADA DA CIBERSEGURANÇA

Um Guia Baseado nos Frameworks NIST e CIS

NOVARÉD

Conteúdo Elaborado por NovaRed Brasil



0. INTRODUÇÃO

A segurança cibernética deixou de ser um tema restrito aos bastidores da TI e passou a permear todas as áreas da organização.

À medida que os riscos digitais se intensificam e as regulamentações se tornam mais exigentes, **a área de Segurança da Informação assume um papel cada vez mais estratégico**, guiando decisões, protegendo ativos e garantindo a continuidade dos negócios. ◆



◆ Mas por onde começar?

Como estruturar essa jornada de forma clara e eficiente?

Neste eBook, reunimos a experiência de três décadas da NovaRed com dois dos frameworks mais reconhecidos do mercado — o **NIST Cybersecurity Framework** e os **Controles CIS v8** — para ajudar você a entender, planejar e fortalecer a maturidade da sua empresa em segurança da informação.

Você vai descobrir como organizar essa jornada em cinco etapas essenciais: **Identificação, Proteção, Detecção, Resposta e Recuperação**, com dicas práticas e comparativos que facilitam a aplicação no dia a dia.

Seja você um gestor de TI, CISO ou profissional interessado no tema, este material é para apoiar sua tomada de decisão e trazer mais segurança, agilidade e confiança ao ambiente digital da sua empresa.

APROVEITE A LEITURA.

E vamos juntos construir um futuro mais seguro.



A importância da segurança cibernética no cenário atual

Vivemos uma era em que os riscos digitais ultrapassam os limites da área de TI. Ameaças como ransomware, ataques via e-mail, vazamentos de dados e golpes baseados em engenharia social se tornaram parte do cotidiano de empresas de todos os portes e setores.

O cibercrime evoluiu — e agora opera como um verdadeiro modelo de negócio global, impulsionado por tecnologias como a IA generativa e estruturas como o Cybercrime-as-a-Service.

Não se trata mais de “se” uma organização será alvo, mas de “quando” e “como” ela será testada em sua capacidade de defesa. Nesse novo contexto, investir em segurança da informação deixou de ser uma questão técnica para se tornar uma prioridade estratégica, ligada à reputação, continuidade e valor de mercado das empresas.





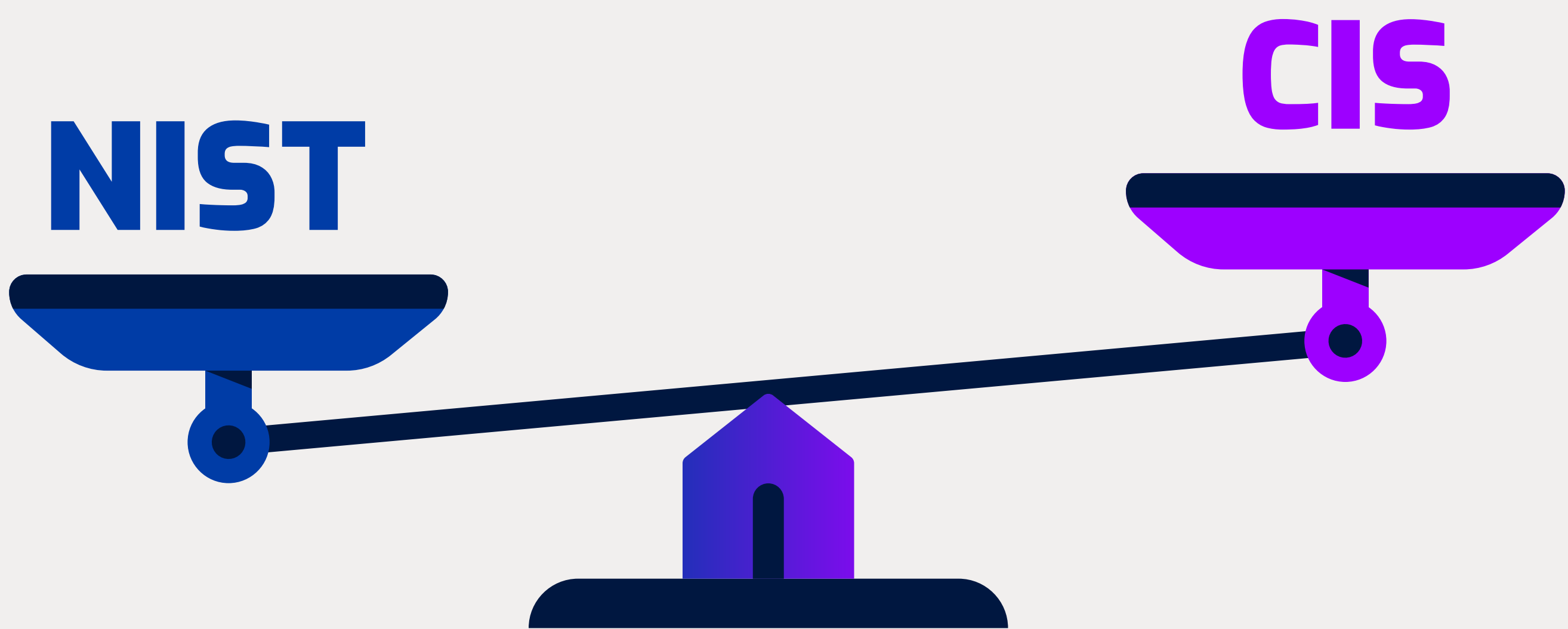
O que é uma jornada de segurança cibernética e por que ela deve ser estruturada

Segurança cibernética não é um projeto pontual, e sim uma jornada contínua de amadurecimento. Cada empresa está em um estágio diferente — algumas ainda precisam mapear seus ativos críticos, enquanto outras já operam SOC's avançados. O importante é entender que não basta reagir a incidentes: **é preciso estruturar uma estratégia de prevenção, resposta e resiliência.**

Pensar a segurança como uma jornada **permite priorizar investimentos, identificar lacunas e envolver toda a organização** — da operação à alta liderança. Estruturar essa caminhada é o que dá consistência às ações de proteção, aumenta a eficiência dos controles e fortalece a cultura interna de segurança.

Frameworks NIST e CIS: os guias da sua jornada

Para ajudar as organizações a seguirem essa trilha de forma segura e comprovada, existem frameworks reconhecidos internacionalmente — como o NIST Cybersecurity Framework e o CIS Controls. **Cada um deles traz um conjunto de boas práticas, fases e controles que servem como bússola para estruturar a jornada de segurança.**



O **NIST** estrutura a jornada em cinco grandes funções: **Identificar, Proteger, Detectar, Responder e Recuperar**. Já os controles do CIS (atualmente na versão 8) trazem uma abordagem **mais operacional**, com **recomendações concretas** e **priorizadas** que facilitam a adoção de práticas eficazes de proteção.

Neste eBook, vamos explorar como esses dois frameworks se complementam e como usá-los de forma prática para guiar sua empresa rumo a um estágio mais maduro de cibersegurança.



Tabela Comparativa:

NIST vs. CIS Controls v8

Critério	NIST Cybersecurity Framework (CSF)	CIS Controls v8
Objetivo	Gerenciar e reduzir riscos cibernéticos	Estabelecer controles técnicos e práticos
Abordagem	Baseada em funções e resultados	Baseada em ações e controles
Estrutura	5 funções: Identificar, Proteger, Detectar, Responder e Recuperar	18 controles divididos por prioridade (IG1, IG2, IG3). <i>Confira a tabela abaixo.</i>
Flexibilidade	Alta – adaptável a vários setores	Alta – controles escalonáveis
Indicação de Maturidade	Enfatiza evolução contínua	Foca em prioridades conforme perfil da empresa
Público-alvo	Organizações de todos os portes	Especialmente PMEs e empresas em crescimento
Conformidade Regulamentar	Forte alinhamento com legislações e normas como ISO e LGPD	Útil para implementação prática da conformidade
Ferramentas recomendadas	Framework, Profiles, Tiers, Roadmaps	Planilhas, ferramentas de priorização, guias técnicos

CIS Controls v8:

Como Priorizar os Controles IG1, IG2 e IG3

Grupo de Implementação	O que é?	Para quem é?
IG1 	Conjunto básico de controles de segurança considerados mínimos e essenciais para qualquer organização.	Organizações de todos os portes e setores. É obrigatório como ponto de partida — ideal para pequenas e médias empresas.
IG2 (inclui IG1) 	Controles adicionais que requerem mais recursos e maturidade, com foco em segurança operacional e gestão de dados sensíveis	Empresas que processam informações confidenciais , operam com equipes de TI internas e precisam de maior visibilidade sobre riscos.
IG3 (inclui IG1 e IG2) 	Conjunto avançado voltado à proteção contra ameaças sofisticadas e persistentes , com foco em resiliência e resposta a incidentes.	Organizações de alta criticidade , como bancos, governo, infraestrutura crítica e grandes corporações com alto perfil de risco.



Mesmo empresas pequenas devem implementar integralmente o IG1 — ele é a base da proteção digital moderna



Jornada

Identificar, Proteger, Detectar, Responder e Recuperar

Para que a jornada de segurança cibernética seja clara, prática e aderente aos diferentes níveis de maturidade das organizações, estruturamos este guia com base nas cinco funções definidas pelo NIST Cybersecurity Framework (*Identificar, Proteger, Detectar, Responder e Recuperar*) e nos controles técnicos e operacionais priorizados pela versão 8 do CIS Controls.

A sinergia entre esses dois frameworks permite uma visão integrada, ao mesmo tempo estratégica e executável, para proteger ativos, antecipar ameaças e garantir a resiliência digital.

nist

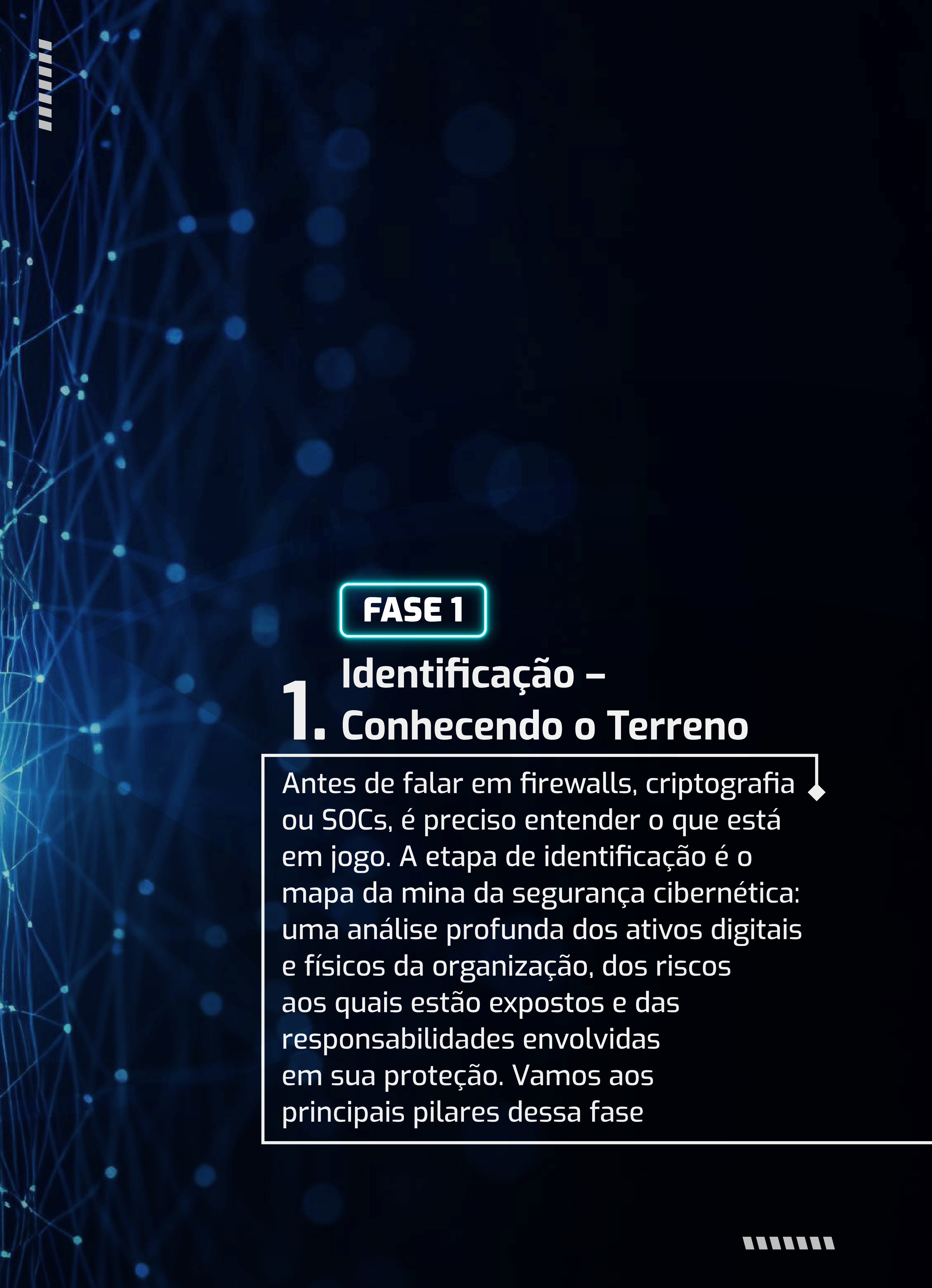




Fase da Jornada	Função do NIST	Controles CIS v8 Relacionados
1. Identificação	Identify	CIS 1 (Inventário), CIS 2 (Gerenciamento de Ativos), CIS 3 (Proteção de Dados), CIS 15 (Serviços de Terceiros), CIS 17 (Governança), CIS 5 (Gestão de Contas), CIS 18 (Testes de Segurança)
2. Proteção	Protect	CIS 4 (Controle de Acesso), CIS 5 (Gestão de Contas), CIS 6 (Configuração Segura), CIS 7 (Defesa contra Malware), CIS 8 (Gerenciamento de Dados), CIS 12 (Segurança de Dispositivos Móveis), CIS 13 (Segurança na Nuvem), CIS 14 (Gestão de Aplicações), CIS 15 (Serviços de Terceiros), CIS 16 (Treinamento de Segurança), CIS 18 (Testes de Segurança)
3. Detecção	Detect	CIS 9 (Monitoramento de Segurança), CIS 10 (Detecção de Anomalias), CIS 13 (Segurança na Nuvem), CIS 14 (Gestão de Aplicações), CIS 18 (Testes de Segurança)
4. Resposta	Respond	CIS 17 (Planejamento de Incidentes e Continuidade de Negócios), CIS 15 (Serviços de Terceiros), CIS 16 (Treinamento de Segurança), CIS 18 (Testes de Segurança)
5. Recuperação	Recover	CIS 11 (Recuperação de Sistemas e Continuidade de Negócios), CIS 13 (Segurança na Nuvem), CIS 17 (Planejamento de Incidentes), CIS 18 (Testes de Segurança)

A partir dessa estrutura integrada, vamos explorar nos próximos capítulos cada fase da jornada em detalhes.

O objetivo é orientar sua empresa na implementação de boas práticas de cibersegurança, de forma progressiva, priorizada e adaptável à realidade do seu negócio.



FASE 1

1. Identificação – Conhecendo o Terreno

Antes de falar em firewalls, criptografia ou SOC's, é preciso entender o que está em jogo. A etapa de identificação é o mapa da mina da segurança cibernética: uma análise profunda dos ativos digitais e físicos da organização, dos riscos aos quais estão expostos e das responsabilidades envolvidas em sua proteção. Vamos aos principais pilares dessa fase



◆ Mapeamento de ativos e dados críticos

Essa é a base de toda estratégia de proteção. Imagine tentar proteger um castelo sem saber quantas entradas ele tem. É exatamente isso que acontece quando a empresa não tem clareza sobre o que precisa proteger.

Nesta etapa, é necessário:

- ◆ **Inventariar todos os ativos:** servidores, estações de trabalho, dispositivos móveis, sistemas em nuvem, aplicativos, sensores IoT e outros.
- ◆ **Classificar os dados conforme sua criticidade:** dados sensíveis, operacionais, pessoais, financeiros, regulatórios etc.
- ◆ Mapear onde estão armazenados, como trafegam na rede e quem tem acesso.

O objetivo é formar uma visão clara, atualizada e integrada do ambiente digital da organização — inclusive dos ativos de terceiros e ambientes híbridos.

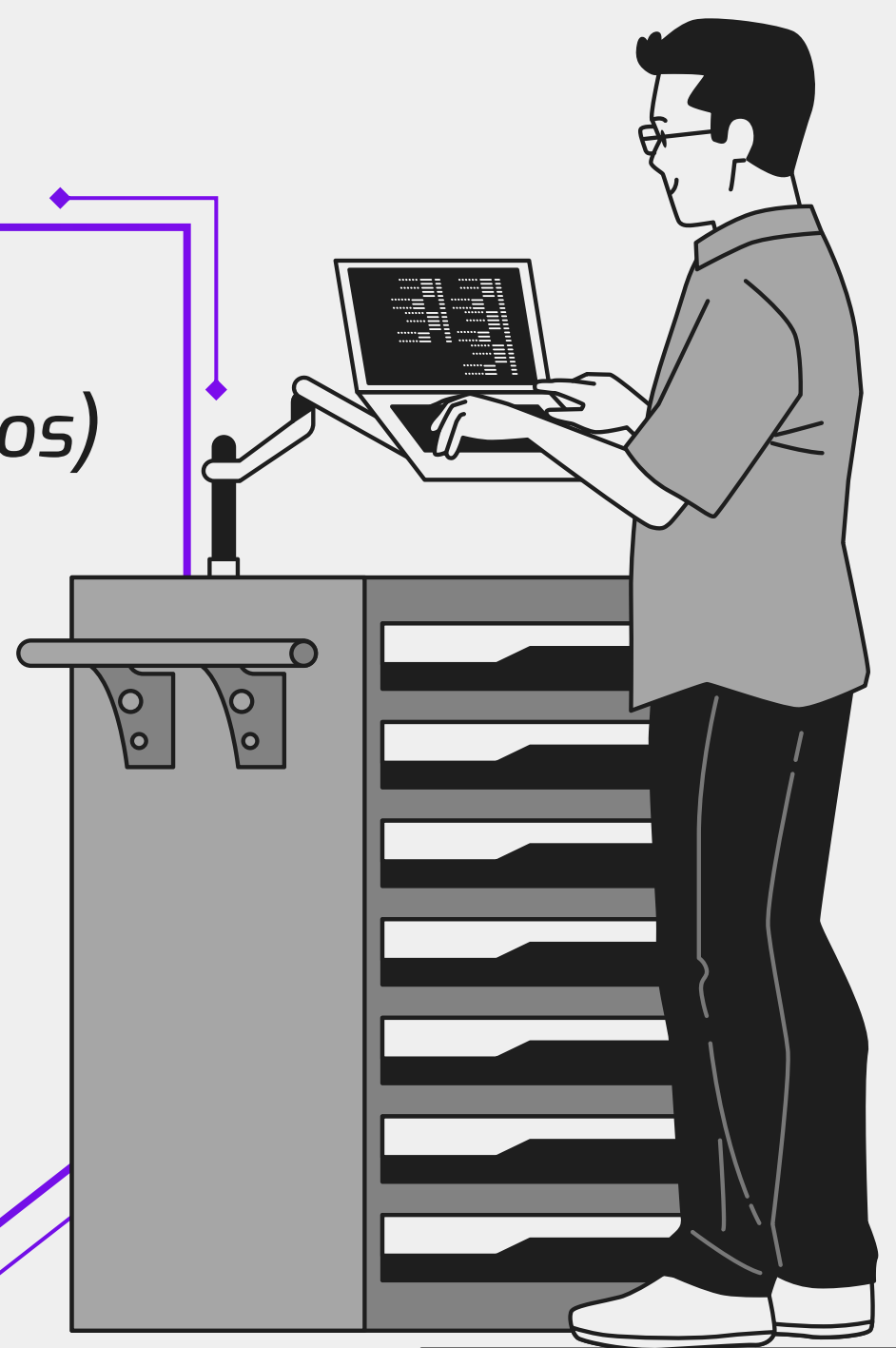
Para entender se um ativo é crítico ou não, é importante entender o risco associado caso ele pare de funcionar ou seja extraído. Quanto mais ele afeta na continuidade do negócio mais crítico ele é.

Avaliação de riscos e vulnerabilidades

Com os ativos identificados, é hora de entender os perigos ao redor. A avaliação de riscos consiste em **analisar a probabilidade e o impacto** de diferentes tipos de ameaças: ciberataques, falhas humanas, desastres naturais, interrupções operacionais, entre outras.

Essa avaliação deve considerar

- ◆ Vulnerabilidades técnicas (*por exemplo, sistemas desatualizados ou mal configurados*)
- ◆ Vulnerabilidades humanas (*como falta de treinamento ou privilégios excessivos*)
- ◆ Dependências críticas (*terceiros, serviços em nuvem, conexões remotas*)
- ◆ Ameaças externas e internas (*incluindo insiders mal-intencionados*)



A identificação de riscos permite priorizar ações com base em dados reais e construir defesas proporcionais à exposição de cada área.

Governança e definição de responsabilidades

Segurança da informação não é apenas um tema de TI. Ela precisa estar inserida na **governança corporativa**, com papéis bem definidos e o engajamento de todas as áreas da empresa, especialmente da alta liderança.



Nesta etapa, recomenda-se

- ◆ Criar ou atualizar políticas de segurança e privacidade
- ◆ Definir quem são os responsáveis por decisões estratégicas e operacionais
- ◆ Estabelecer o papel do CISO (ou responsável pela segurança) e sua integração com áreas como jurídico, compliance, tecnologia, operações e RH
- ◆ Garantir que a cultura de segurança seja disseminada por toda a organização

A clareza na governança reduz falhas de comunicação, evita sobreposições e acelera a resposta a incidentes.

Alinhamento com regulamentações e compliance

Em um cenário de crescente regulação, conformidade não é opcional, mas sim parte da estratégia de continuidade do negócio. E estar em dia com as normas exige conhecimento, processos e documentação.



Nesta frente, é preciso

- ◆ Mapear quais normas e leis impactam a organização (LGPD, DORA, HIPAA, ISO 27001, NIS 2, entre outras)
- ◆ Garantir que os controles internos estejam alinhados a essas exigências
- ◆ Registrar e auditar os processos de tratamento de dados e resposta a incidentes
- ◆ Promover capacitações sobre compliance cibernético

O alinhamento com regulamentações fortalece a reputação da empresa, evita sanções e prepara o ambiente para auditorias e certificações.



FASE 2

2. Proteção – Construindo Defesas Sólidas

Depois de mapear os ativos e identificar os riscos, é hora de agir para proteger sua organização. A fase de Proteção concentra-se na implementação de barreiras técnicas, humanas e operacionais que dificultem — ou idealmente impeçam — a ação de agentes mal-intencionados. Aqui, a prevenção é o foco. ↗

◆ Implementação de controles de acesso e identidade

Antes de definir políticas e controles, é importante iniciar com um **assessment** para entender como funcionam as identidades, acessos e diferentes funções dentro do ambiente. Identificados todos os casos de uso, é possível avançar para automatizar a gestão de identidades e permissões.

Proteger quem acessa o quê é um dos pilares da cibersegurança moderna. A aplicação do modelo de **acesso baseado no princípio do menor privilégio**, aliada à **autenticação multifator (MFA)**, reduz significativamente os riscos de violação.

É essencial adotar práticas robustas de **gestão de identidades e acessos (IAM)**, com políticas claras para criação, modificação e desativação de contas, incluindo terceirizados. Frameworks como o CIS v8 reforçam a necessidade de controles contínuos (Controle 4 e 5), garantindo que apenas as pessoas certas tenham acesso ao que precisam — nem mais, nem menos.

Proteção de endpoints, redes e aplicações

A superfície de ataque cresceu. Com usuários remotos, dispositivos móveis e ambientes em nuvem, proteger endpoints (notebooks, smartphones, servidores) se tornou ainda mais crítico.

Boas práticas incluem

- ◆ Antivírus/EDR com resposta automatizada a ameaças
- ◆ XDR (Extended Detection and Response), que amplia a proteção integrando dados e respostas entre endpoints, redes, e-mail e nuvem, permitindo detecção mais rápida e respostas coordenadas
- ◆ Segmentação de rede para limitar o movimento lateral de invasores
- ◆ Firewalls e políticas de segurança para aplicações web (WAF)
- ◆ Hardening de sistemas operacionais conforme benchmarks reconhecidos (ex: CIS Benchmarks)

Os controles **CIS 7, 8, 12, 13 e 14** oferecem diretrizes práticas para essas proteções técnicas, adaptáveis ao tamanho e maturidade da empresa.

Gestão de vulnerabilidades e atualizações

Mesmo com defesas instaladas, um sistema desatualizado ou mal configurado é uma porta aberta. Por isso, é fundamental estabelecer rotinas de varredura de vulnerabilidades, com análise contínua e correção via patching estruturado e automatizado sempre que possível.



O patching é uma das práticas mais importantes na redução de riscos, mas exige atenção às diferenças entre os tipos de correção.



Ferramentas de Gestão Contínua de Vulnerabilidades (GCV) já oferecem visibilidade sobre sistemas desatualizados e lacunas de patch, facilitando a priorização e correção de riscos. Quando combinada com práticas estruturadas de gestão de patches, essa abordagem reduz significativamente as superfícies de ataque e reforça a postura de segurança, especialmente quando integrada a soluções de ASM, EASM, ESM e ERM, que ampliam a detecção e o controle sobre os ativos expostos.

P P P P P P P
A A A A A A A
T T T T T T T
C C C C C C C
H H H H H H H
I I I I I I I
N N N N N N N
G G G G G G G

Além disso, é necessário manter um inventário atualizado de softwares e plugins utilizados, o que se conecta diretamente aos controles CIS 2 (gestão de ativos) e 7 (proteção contra malware).

TPRM: Gestão de Riscos de Terceiros Além dos Muros da Empresa



À medida que as organizações se tornam mais conectadas e dependentes de parceiros externos (como fornecedores, prestadores de serviços e desenvolvedores terceirizados), os riscos que vêm “de fora” se tornam tão críticos quanto os internos.

◆ Nos primeiros meses de 2025, diversos ataques de grande impacto chamaram a atenção para os riscos associados à cadeia de fornecedores. No Brasil, a C&M Software, parceira do Banco Central, foi alvo de criminosos que exploraram credenciais comprometidas, resultando no roubo de **R\$ 140 milhões de contas em seis bancos.**

Já a Uber enfrentou, em 2022, uma das violações mais comentadas do setor. O ataque ocorreu após o comprometimento das credenciais de um colaborador, permitindo que o invasor acessasse sistemas internos, painéis administrativos e ferramentas de segurança.

O incidente expôs falhas no controle de acessos e na gestão de privilégios, reforçando como a segurança de identidade e o monitoramento contínuo são pilares essenciais na prevenção de incidentes desse tipo.



Embora as motivações e técnicas variem de falhas internas a ataques diretos em parceiros, esses casos evidenciam como a cadeia de fornecimento se tornou um dos pontos mais explorados pelos cibercriminosos. Setores como saúde, varejo e locadoras de veículos nos Estados Unidos também registraram incidentes semelhantes.

Esses episódios não são exceções

Segundo o relatório Imprivata/Ponemon 2025,

47% das organizações sofreram uma violação ou ataque envolvendo acesso de terceiros à rede nos últimos 12 meses.

Isso reforça a necessidade de um programa sólido de Third-Party Risk Management (TPRM), capaz de identificar, monitorar e mitigar vulnerabilidades que estão além dos muros da empresa



Boas Práticas de TPRM alinhadas aos frameworks CIS v8 e NIST Cybersecurity Framework (CSF)

Diante deste cenário, a gestão de riscos de terceiros (Third Party Risk Management – TPRM) deve ser uma prioridade na jornada de resiliência cibernética. Afinal, proteger seus ativos também significa garantir que seus parceiros sigam os mesmos padrões de segurança.



Confira as boas práticas de VRM alinhadas aos frameworks CIS v8 e NIST CSF

Boa prática de VRM	CIS v8	NIST CSF
Mapeamento de fornecedores com acesso a sistemas e dados críticos	CIS Control 1 e 2 (Inventário de ativos)	ID.AM-3 (Mapeamento de recursos externos)
Classificação de terceiros por criticidade e tipo de acesso	CIS Control 12 (Defesa de fronteira)	ID.RA-3 (Avaliação de riscos de terceiros)
Controles de acesso segmentados e baseados no menor privilégio para terceiros	CIS Control 6 (Controle de acesso)	PR.AC-4 (Gerenciamento de acesso)
Due diligence de segurança na contratação e renovação de contratos	CIS Control 15 (Gerenciamento de provedores)	ID.SC-3 (Critérios de seleção de terceiros)
Auditoria e monitoramento de acessos realizados por terceiros	CIS Control 8 (Auditoria e registro)	DE.CM-7 (Monitoramento de acessos externos)
Inclusão de cláusulas contratuais de notificação e resposta a incidentes	CIS Control 17 (Resposta a incidentes)	RS.CO-5 (Comunicação com stakeholders externos)
Testes regulares de resposta a incidentes envolvendo fornecedores	CIS Control 17 (Resposta a incidentes)	RS.IM-1 (Resposta a incidentes simulados)

Conscientização e treinamento contínuo

A maioria dos ataques começa com erro humano e isso torna os colaboradores um elo decisivo. A **educação contínua em cibersegurança**, por meio de campanhas internas, simulações de phishing e treinamentos regulares, transforma o time em uma linha de defesa.

Os controles CIS 14 e 16 reforçam essa frente, especialmente em empresas com grande rotatividade ou forte atuação em home office. Treinar os usuários não apenas reduz riscos, como também cria uma cultura de segurança em toda a organização.



FASE 3

3. Detecção – Monitorando e Antecipando Ameaças

Uma organização só pode responder ao que consegue detectar. Por isso, a fase de Detecção (Detect, segundo o NIST Cybersecurity Framework) é essencial para transformar a visibilidade em ação. Os controles CIS relacionados a essa fase – CIS Control 9 (Monitoramento de Segurança), CIS Control 10 (Detecção de Anomalias e Eventos), CIS 13 (Segurança em Nuvem), CIS 14 (Gestão de Aplicações) e CIS 18 (Testes de Segurança) – reforçam a necessidade de monitoramento contínuo, análise comportamental e testes regulares.

◆ Visibilidade total é meta, mas ainda um desafio:

Segundo a pesquisa da **KPMG Cybersecurity Survey 2024**, embora **91% dos líderes de segurança** afirmem ter visibilidade completa sobre seus riscos, **40% sofreram uma violação significativa no último ano**. Além disso, menos de um terço (**32%**) acompanha regularmente o tempo médio de resposta (**MTTR**), o que pode indicar uma falsa sensação de controle.

As principais práticas desta fase incluem

- ◆ Implantação de um Security Operations Center (SOC), próprio ou terceirizado, com processos definidos para triagem e resposta a alertas.
- ◆ Uso de tecnologias como SIEM (Security Information and Event Management), EDR/XDR e ferramentas de detecção de anomalias comportamentais.
- ◆ Monitoramento em tempo real dos eventos de segurança, incluindo logs, tráfego de rede e endpoints.
- ◆ Integração com feeds de inteligência de ameaças e indicadores de comprometimento (IoCs).
- ◆ Testes regulares de segurança e simulações de ataque (como Red Team ou exercícios purple team) para validar a eficácia dos sistemas de detecção.

Implementação de um Security Operations Center (SOC)

Ter um Centro de Operações de Segurança (SOC) estruturado é essencial para monitorar, detectar e responder a ameaças. O SOC funciona como uma central de comando, reunindo profissionais especializados, processos e ferramentas para supervisionar continuamente os eventos de segurança.

No entanto, muitos líderes ainda enfrentam desafios nesse quesito

De acordo com o estudo da KPMG, 50% das lideranças têm dificuldade em avaliar a performance de seu SOC, principalmente pela falta de dados confiáveis e métricas consistentes. Além disso, 45% relatam escassez de talentos especializados em ameaças emergentes, o que compromete a qualidade e agilidade da resposta.

As funções do SOC incluem:

- ◆ Coleta e análise de logs;
- ◆ Correlação de eventos;
- ◆ Detecção de ameaças emergentes;
- ◆ Emissão de alertas e respostas imediatas.

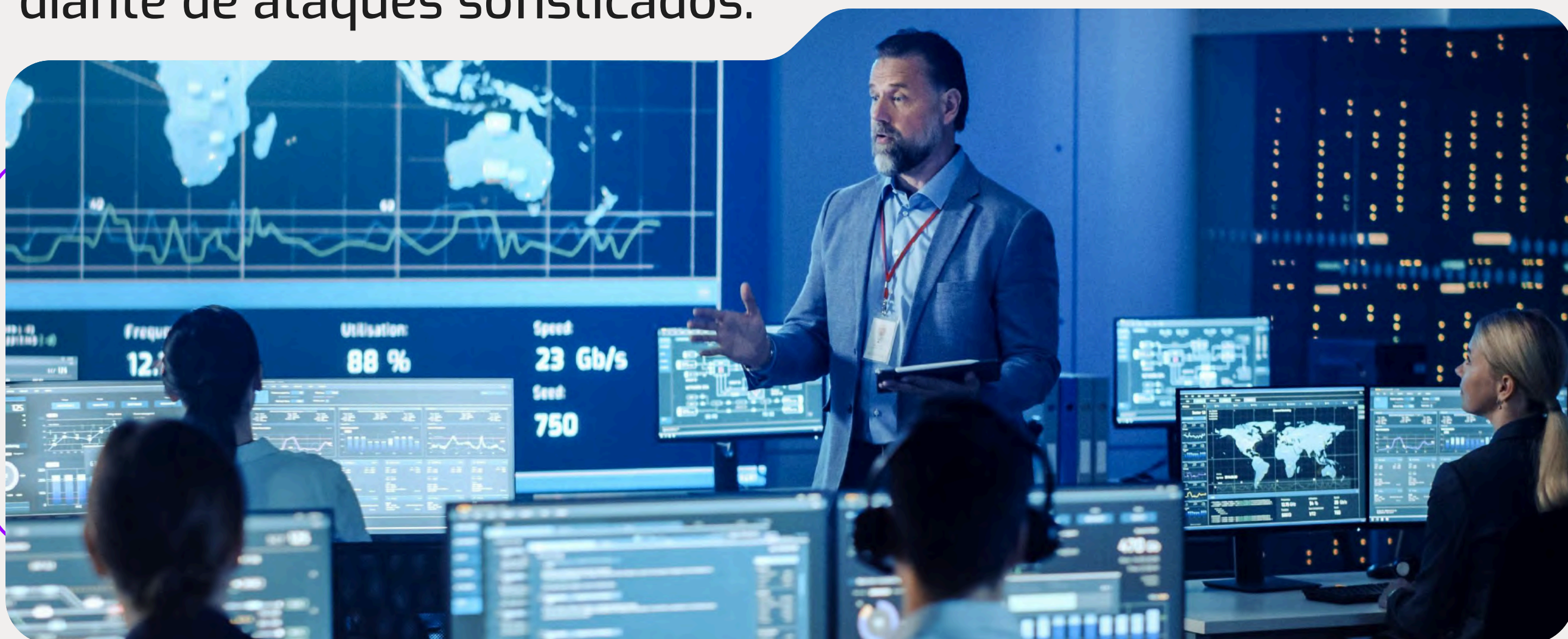
Esse componente está diretamente alinhado ao framework NIST (função Detect) e aos controles CIS 9, 10 e 18.

Monitoramento avançado com SIEM, XDR e MDR

O monitoramento é o centro da operação de segurança. Soluções como SIEM, XDR e MDR oferecem diferentes caminhos para alcançar o mesmo objetivo: detectar e responder rapidamente às ameaças.

O SIEM (Security Information and Event Management) centraliza e correlaciona logs de múltiplas fontes, ajudando a identificar comportamentos suspeitos em tempo real, especialmente em ambientes com SOC's estruturados. Já o XDR (Extended Detection and Response) leva essa capacidade além do endpoint, integrando camadas como rede, e-mail e nuvem, para oferecer uma visão mais contextual e automatizada da segurança.

O **MDR (Managed Detection and Response)**, por sua vez, entrega o mesmo propósito com uma operação totalmente gerenciada por especialistas, dispensando a necessidade de manter um SIEM interno ou equipes dedicadas de análise. Geralmente, as empresas optam por uma dessas abordagens, de acordo com seu nível de maturidade e modelo operacional. Todas, porém, têm o mesmo papel: aumentar a visibilidade, reduzir o tempo de detecção e resposta e automatizar ações diante de ataques sofisticados.



Essas soluções permitem

- ◆ Consolidar eventos de diferentes origens;
- ◆ Reduzir o tempo de detecção e resposta;
- ◆ Ampliar a visibilidade contra ataques sofisticados;
- ◆ Automatizar e orquestrar respostas.

Inteligência de ameaças e análise comportamental

A detecção moderna vai além de regras estáticas. Ferramentas que aplicam análise comportamental detectam desvios em relação ao padrão usual de uso dos sistemas. A integração com bases de inteligência de ameaças (Threat Intelligence) também enriquece a capacidade de antecipação.

Benefícios dessa abordagem:

- ◆ Detecção de ataques ainda não conhecidos (zero-day);
- ◆ Contextualização de riscos com base em tendências globais;
- ◆ Reforço das estratégias preditivas.

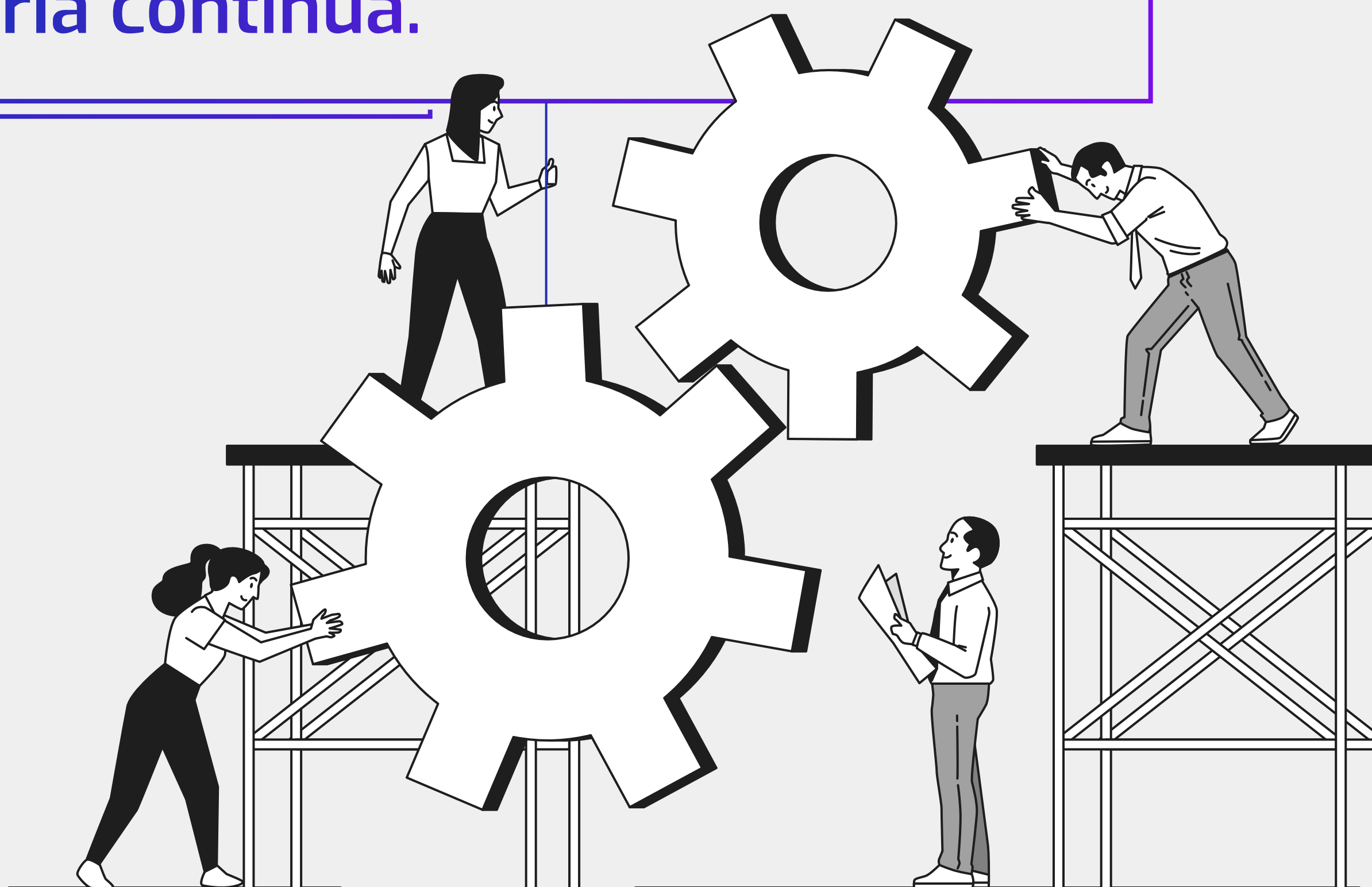
Segundo o relatório Ponemon 2025,

A detecção precisa ser acompanhada de uma capacidade de resposta ágil. A automação de respostas (como o isolamento de endpoints ou bloqueio de acessos) permite mitigar danos rapidamente.

A fase de Detecção não se resume a encontrar problemas, mas a antecipar movimentos e transformar dados em ações. Um ecossistema de monitoramento eficiente é o que diferencia empresas resilientes das que apenas reagem.

IMPORTANTE!

A resposta eficaz não depende apenas da TI, ela envolve toda a organização. É preciso transformar incidentes em oportunidades de aprendizado e melhoria contínua.



FASE 4

Resposta – Agindo com Eficiência em 4. Caso de Incidentes

Quando uma ameaça é confirmada, é a capacidade de resposta que define a extensão dos impactos. Essa fase é dedicada a garantir que a organização saiba exatamente como agir em diferentes cenários, reduzindo danos, retomando operações e aprendendo com o ocorrido. ↑

◆ Planejamento e testes de resposta a incidentes

Ter um plano de resposta (IRP – Incident Response Plan) é essencial, mas testá-lo regularmente é o que garante sua efetividade. O NIST recomenda a execução de simulações periódicas para verificar se os processos, pessoas e ferramentas estão prontos para atuar em um incidente real.

A resposta eficaz envolve

- ◆ Sistemas de decisão com autorizações pré-estabelecidas;
- ◆ Documentação e registros das ações tomadas.
- ◆ Equipes treinadas e com papéis definidos;
- ◆ Fluxos de comunicação claros;

Contenção, erradicação e recuperação

Essas são as três frentes operacionais da resposta:

1 Contenção: impedir a propagação da ameaça (por exemplo, isolando máquinas afetadas);

2 Erradicação: eliminar a causa raiz (como remoção de malware ou reconfiguração de acessos);

3 Recuperação: restaurar sistemas e serviços afetados com segurança.

Esse processo deve ser documentado e revisado para alimentar a melhoria contínua da jornada de segurança.

Comunicação interna e externa em crises

A transparência na comunicação é essencial para preservar a reputação e manter a confiança de clientes, parceiros e stakeholders. A empresa deve definir:

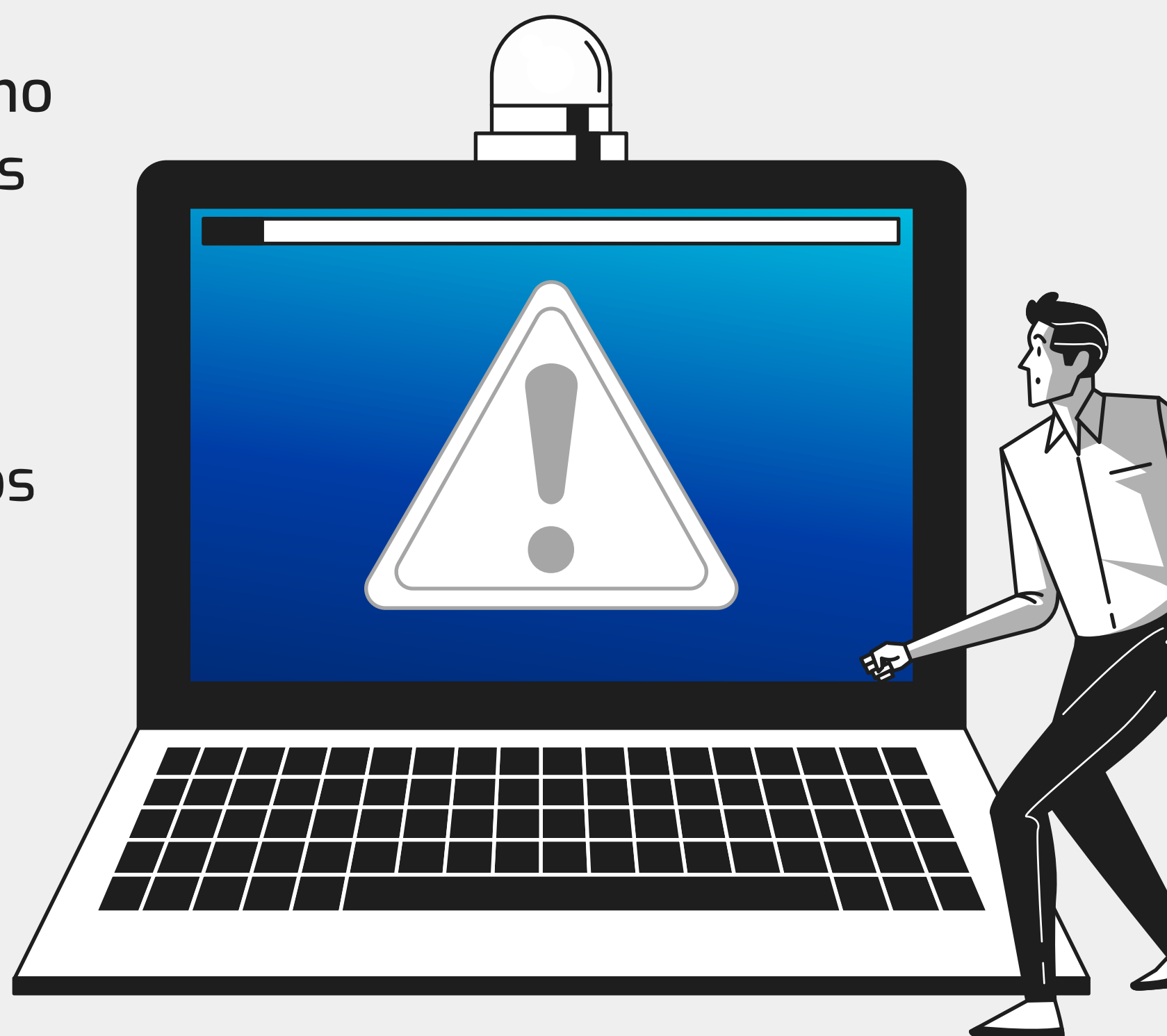
- ◆ Porta-vozes e linhas de comunicação oficiais;
- ◆ Prazos e escopo para divulgação de informações;
- ◆ Processos de notificação a órgãos reguladores (como a ANPD no caso de LGPD);
- ◆ Alinhamento com o departamento jurídico para mitigar riscos legais.

Aprendizados pós-incidente e melhoria contínua

Cada incidente deve ser visto como uma oportunidade de evolução.

Recuperar-se de um incidente não é apenas restaurar sistemas: é garantir que a organização volte a operar com confiança e segurança.

O NIST define essa função como a capacidade de manter planos de recuperação, restaurar serviços e comunicar com stakeholders. Já os controles CIS reforçam a importância dos testes de backup, redundância e plano de continuidade de negócios (BCP).



A etapa final da resposta inclui

- ◆ Revisão do ocorrido (post-mortem);
- ◆ Atualização de planos e controles com base nas falhas detectadas;
- ◆ Treinamento adicional com base nas vulnerabilidades exploradas;
- ◆ Compartilhamento de lições aprendidas com stakeholders internos.

Uma boa resposta é aquela que, mesmo diante de um impacto, consegue proteger os ativos críticos e fortalecer a organização para o futuro.



FASE 5

5. Recuperação – Voltando à Normalidade com Resiliência

A recuperação é a etapa em que a empresa demonstra sua capacidade de se reerguer após um incidente. Mais do que restaurar sistemas, trata-se de recuperar a confiança, retomar processos com segurança e avaliar como evitar novos impactos.

Segundo o relatório Ponemon 2025,

empresas que sofreram ataques por terceiros levaram, em média, **35 dias para restaurar plenamente suas operações**, gerando prejuízos financeiros e reputacionais. Além disso, falhas nos testes de recuperação foram um dos fatores mais citados como agravantes de crises.

Estratégias de continuidade de negócios e recuperação de desastres

Ter um plano de continuidade de negócios (BCP – Business Continuity Plan) e um plano de recuperação de desastres (DRP – Disaster Recovery Plan) é fundamental para minimizar o tempo de inatividade e evitar prejuízos.

As diretrizes incluem:

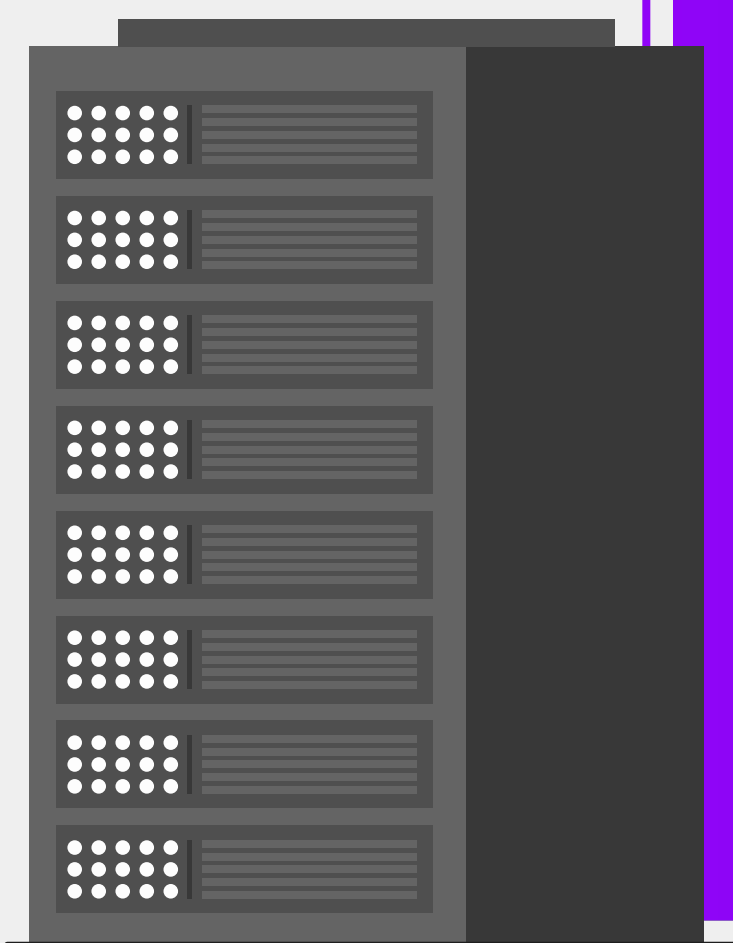
- ◆ RTO (Recovery Time Objective): tempo máximo aceitável de indisponibilidade;
- ◆ RPO (Recovery Point Objective): volume de dados que pode ser perdido sem impacto significativo;
- ◆ Classificação dos sistemas críticos para priorização de retomada.

Testes de backup e redundância de sistemas críticos

Backups não testados são apenas uma ilusão de segurança. A recuperação efetiva depende de:

- ◆ Monitoramento dos processos de backup automatizado;
- ◆ Testes regulares de restauração de dados e sistemas;
- ◆ Uso de ambientes redundantes e tolerantes a falhas.

Os controles CIS 11 e 13 e as funções Recover do NIST reforçam essa necessidade.



Avaliação pós-incidente e ajustes na estratégia de segurança

A recuperação não é o fim da jornada, mas um ponto de partida para melhorias. Avaliar o que funcionou (ou não) garante que os mesmos erros não se repitam. A etapa inclui:

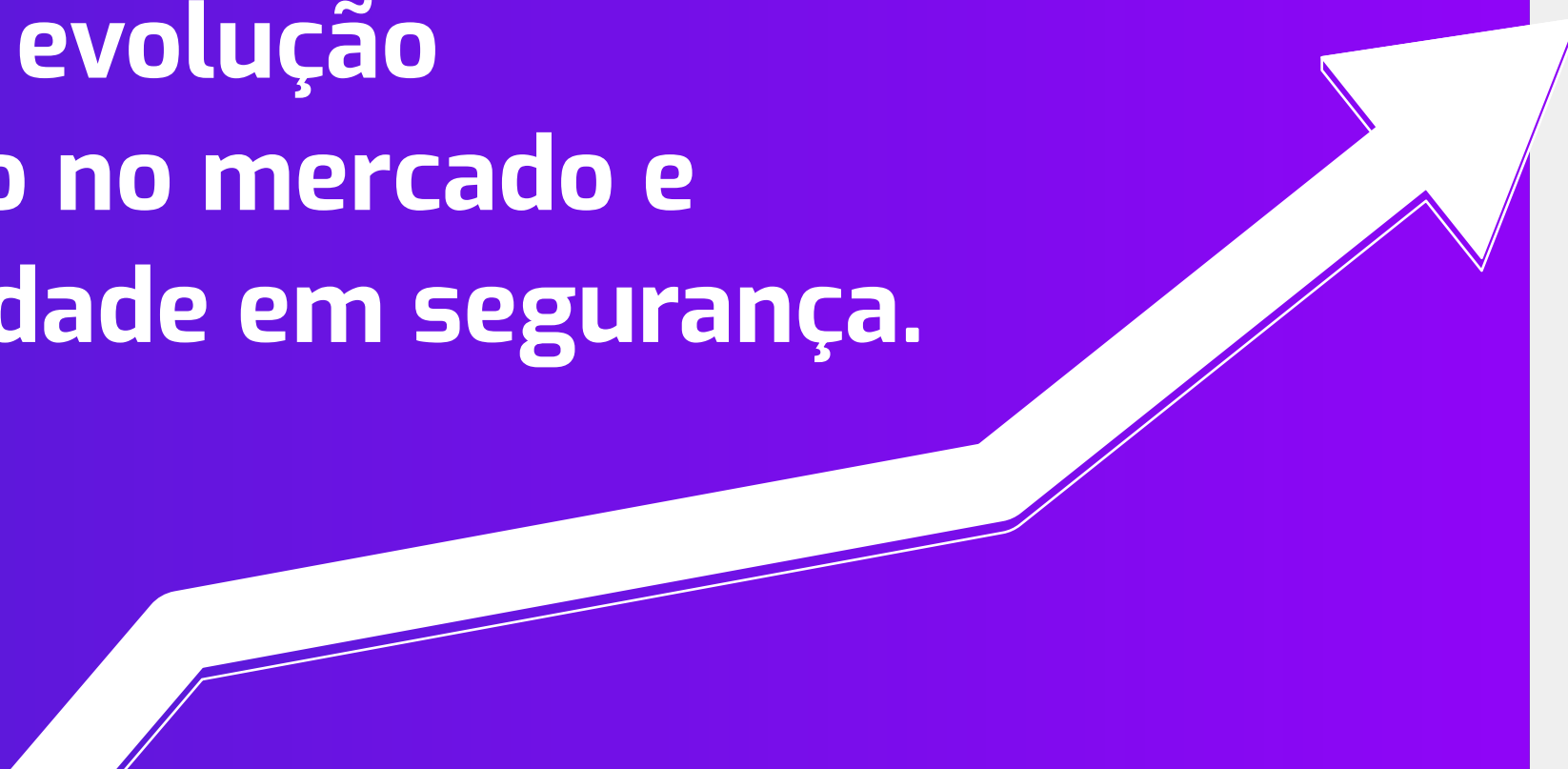
- ◆ Auditorias de conformidade;
- ◆ Reavaliação de fornecedores e terceiros afetados;
- ◆ Análise dos indicadores de tempo e eficácia de resposta;
- ◆ Atualização de planos de continuidade, resposta e comunicação.

Cultura de segurança cibernética como diferencial competitivo

Empresas que tratam a segurança como parte da cultura são mais resilientes e confiáveis. Integrar os aprendizados da recuperação à estratégia e à comunicação com stakeholders é o que transforma a segurança em diferencial.

Recuperar é, acima de tudo, fortalecer. Cada incidente superado é uma oportunidade de crescimento e inovação.

Vale reforçar que o foco não é apenas “voltar ao normal”, mas “voltar melhor”. Organizações que tratam a recuperação como oportunidade de evolução fortalecem sua posição no mercado e aumentam sua maturidade em segurança.



6. Conclusão e Próximos Passos

A jornada da cibersegurança é mais do que um conjunto de boas práticas: é uma mudança cultural e estratégica. Ao seguir os frameworks do NIST e do CIS, sua empresa constrói uma base sólida para se defender, responder e evoluir em um cenário de ameaças em constante transformação. ↑

◆ O primeiro passo é reconhecer onde sua organização está hoje.

O segundo, é construir um roadmap realista, priorizando controles críticos e promovendo uma abordagem integrada entre pessoas, processos e tecnologias.

A NovaRed está pronta para ser sua parceira nessa jornada, oferecendo consultoria especializada, ferramentas de diagnóstico, treinamentos e soluções personalizadas que ajudam sua empresa a amadurecer em cibersegurança.



**Se você chegou até aqui,
já deu um passo importante.**

Agora, conte conosco para seguir com confiança.



7. Recursos adicionais e recomendações de aprofundamento

◆ Checklist da Jornada de Segurança Cibernética

Antes de avançar em sua estratégia de cibersegurança, é essencial entender onde sua organização está e quais são os próximos passos. Abaixo, apresentamos um checklist prático dividido por fases da jornada, com base nos frameworks NIST e CIS, para ajudar sua empresa a avaliar o nível atual de maturidade e identificar pontos de atenção.

Este checklist serve como uma ferramenta de autodiagnóstico: use-o para revisar práticas já adotadas, detectar lacunas e priorizar iniciativas que fortalecem a postura de segurança cibernética da sua organização. Afinal, segurança é um processo contínuo — e mapear o caminho é o primeiro passo para trilhá-lo com confiança.

Fase da Jornada	Checklist de Ações	X ou V
Identificação	Inventariar ativos de TI e dados sensíveis	
Identificação	Realizar avaliação de riscos	
Identificação	Definir políticas e responsabilidades de segurança	
Identificação	Garantir alinhamento com regulamentações (LGPD, ISO, etc.)	

Fase da Jornada	Checklist de Ações	X ou V
Proteção	Implementar controles de identidade e acesso (IAM)	
Proteção	Proteger endpoints e redes com antivírus e firewall	
Proteção	Gerenciar vulnerabilidades e aplicar patches regularmente	
Proteção	Realizar treinamentos e campanhas de conscientização	
Deteccção	Implantar ferramentas de monitoramento (SIEM, XDR)	
Deteccção	Configurar alertas de comportamento anômalo	
Deteccção	Integrar inteligência de ameaças	
Deteccção	Manter equipe de SOC atuante	

Fase da Jornada	Checklist de Ações	X ou V
Resposta	Documentar plano de resposta a incidentes (IRP)	
Resposta	Simular incidentes periodicamente	
Resposta	Estabelecer canais de comunicação de crise	
Resposta	Registrar lições aprendidas e ajustar planos	
Recuperação	Implementar plano de continuidade de negócios (BCP)	
Recuperação	Testar backups e sistemas de redundância	
Recuperação	Avaliar impacto e revisar riscos após incidentes	
Recuperação	Promover cultura organizacional voltada à segurança	

Sobre a NovaRed

Com mais de 30 anos de atuação, a NovaRed é o maior conglomerado ibero-americano especializado em cibersegurança, com presença consolidada no Brasil, Chile, Argentina e Espanha. A empresa combina experiência técnica, inovação contínua e profundo conhecimento regulatório para proteger o que é mais essencial: a continuidade dos negócios e a confiança digital. Seu time conta com mais de 400 especialistas, + de 1.000 certificações em tecnologias líderes de mercado e três Centros de Operações de Segurança (SOC) que funcionam 24x7, garantindo respostas rápidas e eficazes a incidentes.

Mais do que uma fornecedora de soluções, a NovaRed atua como parceira estratégica das organizações em suas jornadas de maturidade em segurança da informação. Seja por meio de consultoria especializada, serviços gerenciados, capacitação técnica ou apoio em compliance, a NovaRed ajuda empresas a se adaptarem a um cenário cada vez mais complexo e regulado, promovendo uma cultura de segurança resiliente e sustentável.

Para saber mais

-  NovaRed Brasil
-  @novaredbrasil
-  NovaRed Brasil
-  @NovaRedBrasil
-  @NovaRedBrasil
-  www.novared.com.br



Fontes para Estudo – Frameworks NIST & CIS

Framework NIST (National Institute of Standards and Technology)

NIST Cybersecurity Framework (CSF)

Documento base com as funções Identify, Protect, Detect, Respond, Recover.

 [link aqui](#)

NIST Special Publication 800-53 (Controles de Segurança e Privacidade)

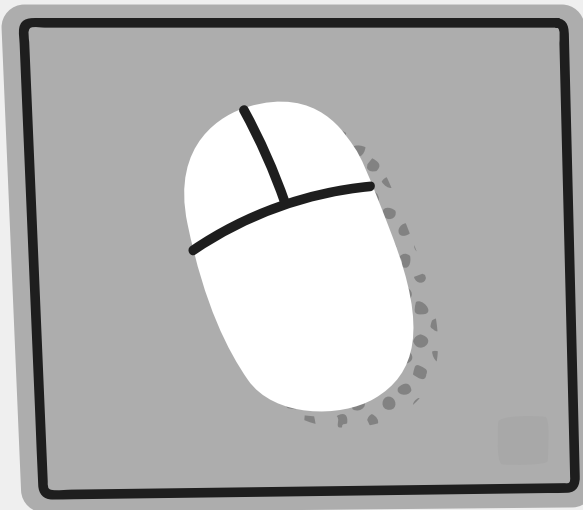
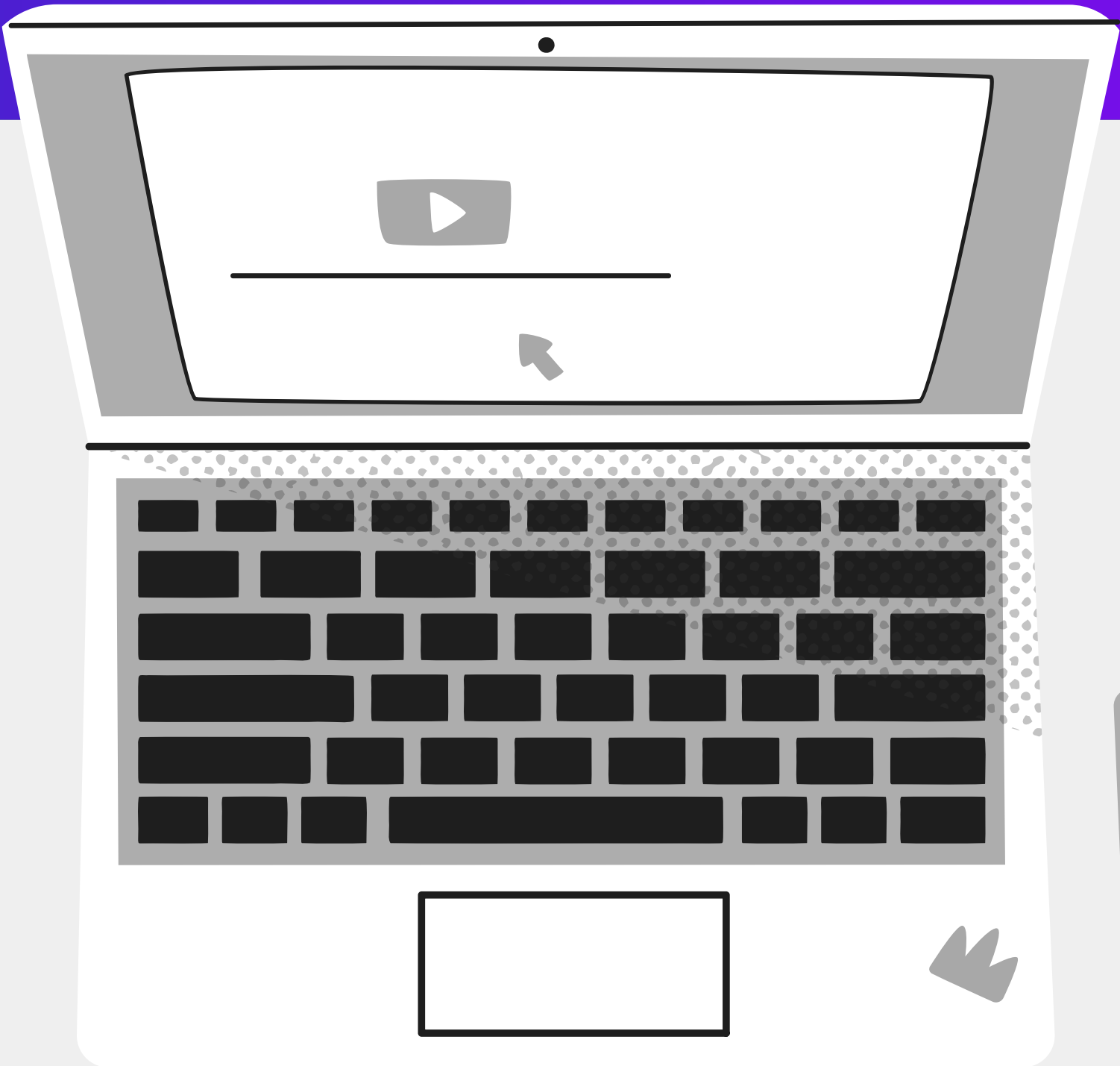
Catálogo extenso de controles aplicáveis a diferentes tipos de sistemas.

 [link aqui](#)

CSF 2.0 (versão mais recente – 2024)

Estrutura atualizada com foco em governança e melhoria contínua.

 [link aqui](#)



Fontes para Estudo – Frameworks NIST & CIS

Framework NIST (National Institute of Standards and Technology)

Controles CIS (Center for Internet Security)

CIS Controls v8

Lista com 18 controles prioritários divididos por níveis de implementação.



[link aqui](#)

CIS Benchmarks

Guias técnicos para configuração segura de sistemas (Windows, Linux, Cloud, etc.).



[link aqui](#)

CIS Community Defense Model (CDM)

Modelo que mostra como os controles CIS ajudam a mitigar ameaças reais.



[link aqui](#)





RETHINKING CYBER SECURITY

