VLK ADV

Onde o Direito
Impulsiona o futuro

MAPA DE PREPARAÇÃO PARA INCIDENTES CIBERNÉTICOS

Da prevenção à recuperação: percorra os cinco territórios essenciais para avaliar e fortalecer a preparação da sua organização diante de incidentes cibernéticos.

WWW.VLKLAW.COM.BR

Sumário

01 Por que este mapa?

02 Frameworks e bases técnicas

03 Os 5 territórios

04 Território 1 - Contexto

05 Território 2 - Papéis & Responsabilidades

06 Território 3 - Políticas & Procedimentos

07 Território 4 - Detecção

08 Território 5 - Testes & Melhorias

09 Conclusão

10 Autores

11 Sobre nós

Instruções: Este é um documento interativo. **Clique** em cima do tópico para **acessar a página de seu interesse.**



Por que este mapa?

Segundo o NIST, no documento Incident Response Recommendations and Considerations for Cybersecurity Risk Management, a resposta a incidentes integra a gestão dos riscos de cibersegurança, organizada em seis funções:

GOVERNAR

Definir e comunicar a estratégia, as responsabilidades e as políticas de gestão dos riscos de cibersegurança.

IDENTIFICAR

Conhecer os ativos da organização e os riscos de cibersegurança a que estão expostos.

PROTEGER

Implementar medidas de proteção para gerenciar os riscos identificados.

DETECTAR

Identificar e analisar sinais de possíveis ataques e comprometimentos de segurança.

RESPONDER

Adotar medidas para gerenciar, conter e mitigar os incidentes detectados.

RECUPERAR

Restabelecer os ativos e as operações afetados pelo incidente.

As três primeiras funções **(governar, identificar e proteger)** sustentam a preparação da organização

As três últimas **(detectar, responder e recuperar)** compõem o ciclo de resposta ao incidente. Essas funções são interligadas e devem ser continuamente aprimoradas com base nas lições aprendidas.

A preparação permite agir com rapidez e coordenação quando um incidente ocorre. Definir previamente responsabilidades, procedimentos, recursos e canais de comunicação facilita a detecção e a contenção, reduz o tempo de interrupção das operações e ajuda a limitar perdas financeiras e outros impactos sobre a organização e as pessoas afetadas.

O objetivo deste mapa

é auxiliar você a melhor preparar a sua organização.

Como utilizar o mapa

Esse mapa vai lhe apoiar a preparar a sua organização etapa por etapa.

Em cada etapa do mapa iremos apresentar alguns quesitos, baseados em **frameworks**, como:

Incident Response Recommendations and Considerations for Cybersecurity Risk Management do NIST

NBR ABNT ISO/IEC 27001:2024

NBR ABNT ISO/IEC 27002:2022

Percorra os cinco territórios e reflita sobre cada pergunta, identificando uma das seguintes opções:

IMPLEMENTADO

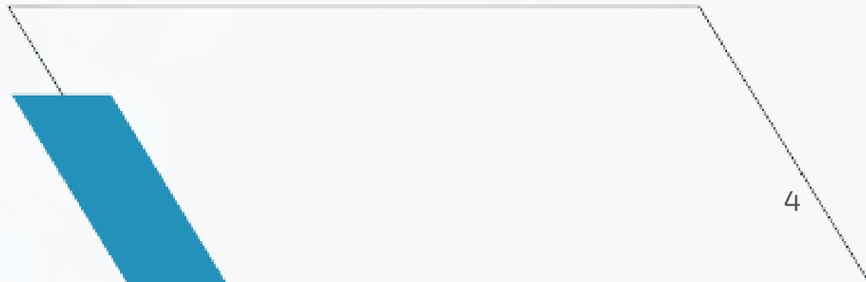
A prática está estruturada, é conhecida pelos responsáveis e está em funcionamento, com evidências de sua aplicação.

PARCIALMENTE IMPLEMENTADO

A prática existe, mas apresenta lacunas de definição, aplicação, cobertura ou comprovaçã

AINDA NÃO IMPLEMENTADO

A prática não foi estabelecida ou sua implementação ainda não foi iniciada.



Os 5 territórios

A preparação para incidentes cibernéticos envolve diferentes áreas, decisões e processos que precisam funcionar de forma coordenada. Para ajudar sua organização a identificar o que já está estruturado e o que precisa ser aprimorado, **dividimos o mapa em cinco territórios que se conectam:**

01

CONTEXTO

02

PAPÉIS E RESPONSABILIDADES

03

POLÍTICAS & PROCEDIMENTOS

04

DETECÇÃO

05

TESTES E MELHORIAS



TERRITÓRIO 1

CONTEXTO

O QUE ESTE TERRITÓRIO DEVE EXPLORAR

A governança da resposta a incidentes deve considerar a missão da organização, as necessidades e expectativas das partes interessadas (stakeholders), as dependências internas e externas e as obrigações legais, regulatórias e contratuais aplicáveis.

Este território do mapa ajudará você a compreender esse contexto e a definir prioridades para a resposta e a recuperação, considerando tanto os serviços essenciais para a organização quanto aqueles que ela presta a terceiros.

POR QUE ESTE TERRITÓRIO É RELEVANTE?

A compreensão do contexto organizacional é essencial para que a resposta a incidentes seja proporcional aos riscos e alinhada às prioridades do negócio. Sem essa visão, decisões tomadas durante um incidente podem desconsiderar serviços críticos, dependências relevantes, obrigações aplicáveis ou impactos sobre clientes, parceiros e outras partes interessadas.

Ao identificar previamente esses elementos, a organização consegue estabelecer critérios mais claros para priorização, escalonamento, comunicação, continuidade e recuperação, contribuindo para respostas mais rápidas, coordenadas e consistentes com seus objetivos institucionais.

PRINCIPAIS ASPECTOS QUE DEVEM SER CONSIDERADOS:

MISSÃO E OBJETIVOS DA ORGANIZAÇÃO

Compreender quais atividades são essenciais ao cumprimento da missão e como um incidente pode afetá-las.

PARTES INTERESSADAS INTERNAS E EXTERNAS

Identificar quem participa da resposta e quem pode ser afetado pelo incidente.

OBRIGAÇÕES LEGAIS, REGULATÓRIAS E CONTRATUAIS

Mapear os requisitos aplicáveis à resposta a incidentes, incluindo deveres de comunicação, prazos, destinatários, preservação de evidências e proteção de dados pessoais.

COMUNICAÇÃO DO CONTEXTO ÀS EQUIPES RESPONSÁVEIS

Assegurar que essas informações sejam fornecidas às partes responsáveis por responder ao incidente.

TERRITÓRIO 1

PONTOS PRELIMINARES PARA VALIDAÇÃO



01

As obrigações legais, regulatórias e contratuais aplicáveis à resposta a incidentes foram identificadas, incluindo os prazos e requisitos de comunicação de incidentes e de proteção de dados pessoais?

02

Requisitos contratuais relevantes para o acionamento de prestadores que apoiem a resolução dos incidentes, como seguradoras e empresas de investigação forense, foram identificados?

03

Os objetivos e as prioridades da resposta e da recuperação foram definidos considerando a missão da organização?

04

As partes interessadas internas e externas foram identificadas, e suas necessidades e expectativas em relação à resposta a incidentes foram compreendidas e consideradas?

05

Os serviços e as capacidades essenciais que clientes, parceiros e outras partes interessadas esperam da organização ou dos quais dependem foram identificados e comunicados às equipes responsáveis pela resposta e pela recuperação?

06

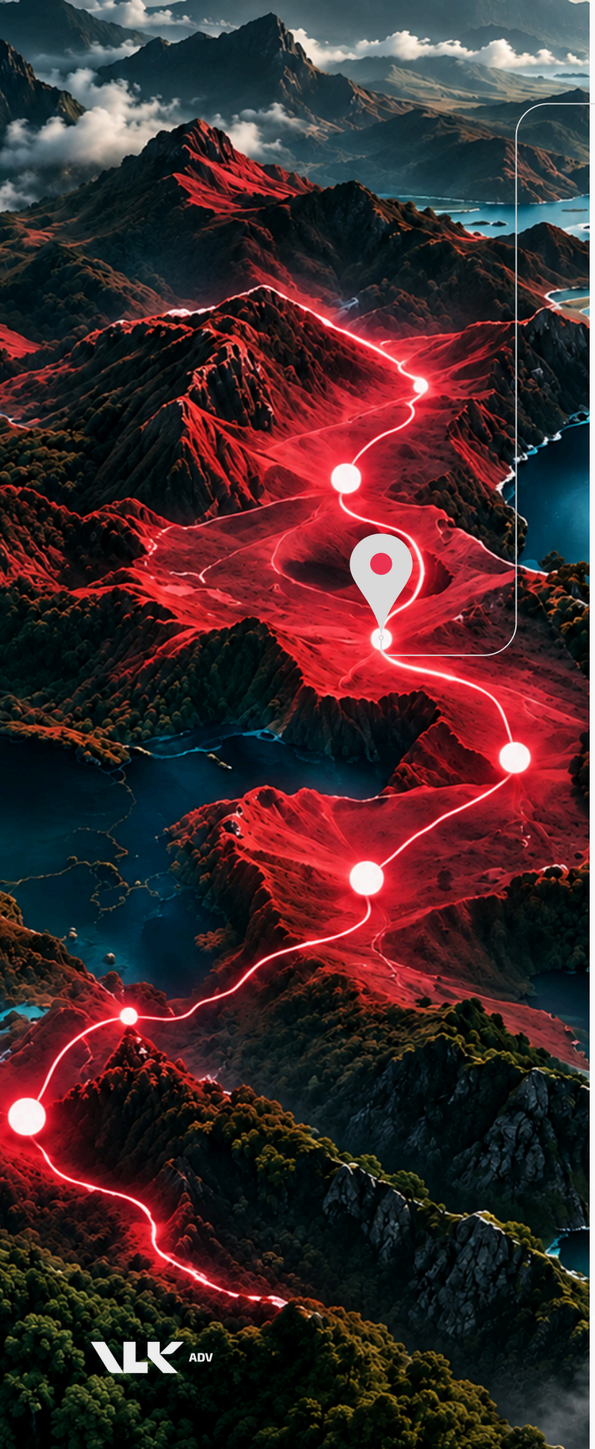
Os serviços, recursos e fornecedores dos quais a organização depende foram identificados, e essas dependências foram comunicadas às equipes responsáveis pela resposta e pela recuperação?

07

Os ativos de informação foram inventariados, incluindo sistemas, ambientes em nuvem, bases de dados e repositórios de arquivos, com identificação de sua criticidade, localização, responsáveis e categorias de informações tratadas?

08

As informações sobre ativos, serviços críticos, dependências e obrigações aplicáveis à resposta são mantidas atualizadas e acessíveis às equipes responsáveis?



TERRITÓRIO 2

PAPÉIS & RESPONSABILIDADES

O QUE ESTE TERRITÓRIO DEVE EXPLORAR

Neste território, você avaliará se está claro quem coordena, quem decide e quem executa as ações de resposta a incidentes.

Cada atribuição deve ser alocada a indivíduos ou equipes com autoridade, recursos e capacitação suficientes para exercê-la, incluindo terceiros que participem da resposta.

POR QUE ESTE TERRITÓRIO É RELEVANTE?

Durante um incidente, decisões precisam ser tomadas rapidamente e por diferentes áreas. Sem atribuições claras, podem ocorrer atrasos, tarefas duplicadas, falhas de comunicação ou decisões sem a autoridade necessária.

Definir previamente quem coordena, quem executa, quem decide e quem comunica facilita uma atuação organizada. Também permite avaliar o desempenho dos envolvidos, identificar lacunas e aprimorar continuamente a capacidade de resposta.

PRINCIPAIS ASPECTOS QUE DEVEM SER CONSIDERADOS:

RESPONSABILIDADE DA LIDERANÇA

Definir o papel da liderança no acionamento do comitê de crise, na aprovação de decisões críticas e na disponibilização de recursos para a resposta. Estabelecer em quais situações a liderança deve ser envolvida e quais decisões dependem de sua aprovação.

DISTRIBUIÇÃO E DOCUMENTAÇÃO DAS ATRIBUIÇÕES

Definir quem é responsável por receber e analisar alertas, classificar incidentes, investigar suas causas e extensão, preservar evidências, executar medidas de contenção e recuperação e realizar comunicações. Documentar as atribuições das áreas envolvidas e dos terceiros independentes nos planos e procedimentos de resposta.

AUTORIDADE PARA AGIR

Estabelecer quem pode determinar ou executar medidas urgentes, como isolar sistemas, bloquear acessos, suspender serviços e contratar apoio externo especializado.

COORDENAÇÃO INTERNA E EXTERNA

Designar um responsável pela coordenação da resposta, com autoridade para mobilizar equipes, distribuir tarefas, acompanhar sua execução e resolver conflitos de prioridade.

RESPONSABILIDADES PELAS COMUNICAÇÕES

Definir quem recebe e encaminha os reportes de incidentes, quem mantém as áreas envolvidas informadas e quem prepara, aprova e realiza comunicações externas. Distinguir o ponto de contato operacional dos responsáveis por notificações e dos porta-vozes autorizados.

DISPONIBILIDADE E CONTINUIDADE DA EQUIPE DE RESPOSTA

Assegurar que os responsáveis possam ser acionados nos prazos necessários, inclusive fora do horário de expediente. Prever substitutos, contatos atualizados, passagem de responsabilidades e acesso aos recursos necessários à execução de suas funções.

CAPACITAÇÃO E EXERCÍCIOS POR FUNÇÃO

Preparar cada participante para suas atribuições na resposta, incluindo a tomada de decisões sob pressão, preservação de evidências, coordenação e comunicação.

TERRITÓRIO 2

PONTOS PRELIMINARES PARA VALIDAÇÃO



01

A responsabilidade da liderança pelos riscos de segurança da informação e pelo apoio à estrutura de resposta a incidentes está formalmente definida e é exercida?

02

Os proprietários dos ativos da informação foram definidos e instruídos sobre seu papel em incidentes cibernéticos, incluindo a avaliação de impactos e a tomada de decisões relacionadas aos ativos sob sua responsabilidade?

03

Os papéis, as responsabilidades e as autoridades para identificar, avaliar eventos e classificá-los como incidentes, coordenar e executar a resposta, aprovar decisões, preservar evidências e comunicar incidentes estão documentados, comunicados e compreendidos pelos envolvidos?

04

Os mecanismos de acionamento e coordenação das equipes internas e dos terceiros estão estabelecidos, incluindo um ponto de contato para comunicações e substitutos para as funções essenciais?

05

Os responsáveis pela resposta e seus substitutos estão disponíveis e podem ser acionados nos prazos necessários, inclusive, sendo o caso, fora do expediente, e dispõem de meios alternativos de comunicação caso os canais habituais estejam comprometidos?

06

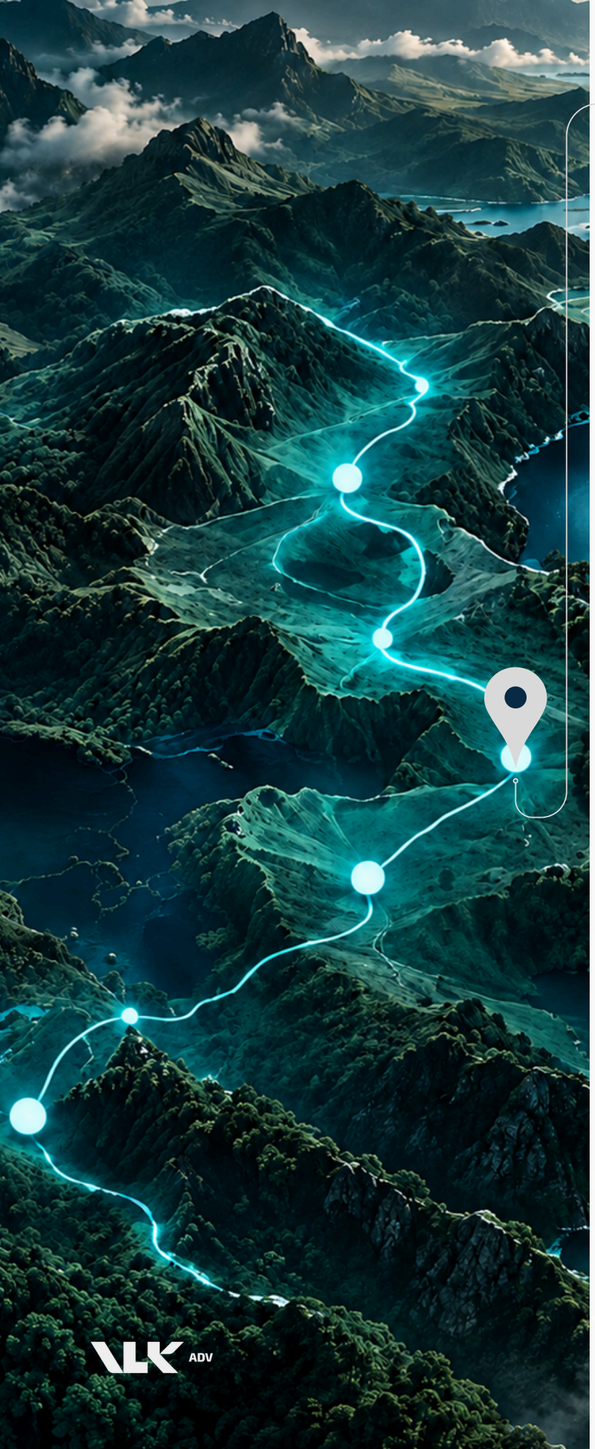
Os recursos humanos, financeiros e técnicos necessários à resposta a incidentes estão disponíveis e são compatíveis com os riscos e as responsabilidades atribuídas?

07

As práticas de gestão de pessoas contemplam treinamento, simulações, certificações pertinentes, desenvolvimento profissional e avaliação dos responsáveis pela resposta, com aplicação das lições aprendidas?

08

Existem critérios para acionar terceiros relevantes, como autoridades policiais, seguradoras e prestadores de serviços, com definição do papel esperado de cada um?



TERRITÓRIO 3

POLÍTICAS, PROCEDIMENTOS & GESTÃO DE RISCOS

O QUE ESTE TERRITÓRIO DEVE EXPLORAR

Este território deve orientar a elaboração e a aplicação de políticas, planos e procedimentos para gerir crises e responder a incidentes de segurança.

A avaliação de riscos deve apoiar a definição dos cenários, das prioridades e das medidas de resposta, continuidade e recuperação, considerando os possíveis impactos sobre a organização e as pessoas afetadas.

POR QUE ESTE TERRITÓRIO É RELEVANTE?

Políticas e procedimentos claros ajudam a organização a agir com rapidez e coordenação. Planos e playbooks transformam essas diretrizes em ações para identificar e avaliar o ocorrido, conter seus efeitos, comunicar as partes relevantes e restabelecer as operações.

A avaliação de riscos e a análise de impacto nos negócios (BIA) ajudam a identificar quais cenários exigem preparação, quais serviços devem ser recuperados primeiro e quais recursos serão necessários. Exercícios, simulações e lições aprendidas permitem verificar se os planos funcionam e como aprimorá-los.

PRINCIPAIS ASPECTOS QUE DEVEM SER CONSIDERADOS:

POLÍTICA DE RESPOSTA A INCIDENTES

Estabelecer diretrizes alinhadas ao contexto e às prioridades da organização, comunicá-las aos envolvidos e assegurar sua aplicação.

PLANOS E PROCEDIMENTOS DE RESPOSTA

Definir ações para identificação, avaliação, contenção, erradicação das causas e dos mecanismos de persistência, recuperação e encerramento, incluindo critérios para acionamento das equipes, tomada de decisão e coordenação com terceiros.

RISCOS E CENÁRIOS DE INCIDENTES E DESASTRES

Considerar ameaças, vulnerabilidades, probabilidade e impacto para selecionar os cenários que exigem preparação e definir prioridades, recursos e medidas de resposta e recuperação.

ANÁLISE DE IMPACTO NOS NEGÓCIOS (BIA)

Identificar as atividades essenciais, suas dependências e os impactos de sua interrupção, orientando a ordem prioritária e os objetivos de recuperação.

CONTINUIDADE E RECUPERAÇÃO DE DESASTRES

Articular os planos com a resposta a incidentes, prevendo alternativas para manter atividades essenciais e restabelecer sistemas, dados e serviços.

PLAYBOOKS

Elaborar instruções práticas para cenários comuns ou previsíveis, com ações, responsáveis, critérios de decisão e condições para encaminhamento a outras equipes ou à liderança.

TERRITÓRIO 3

PONTOS PRELIMINARES PARA VALIDAÇÃO



01

A política de resposta a incidentes está estabelecida, alinhada ao contexto e às prioridades da organização, comunicada aos envolvidos e aplicada?

02

Os planos e procedimentos de resposta estão documentados e contemplam identificação, avaliação, priorização, contenção, erradicação, recuperação e encerramento, incluindo registro, comunicação nos prazos aplicáveis, coordenação interna e externa e cadeia de custódia de evidências?

03

Os principais riscos de segurança da informação foram identificados e mensurados?

04

Os planos de continuidade de negócios e recuperação estão estabelecidos e articulados com a resposta a incidentes, com prioridades e objetivos de recuperação definidos a partir da análise de impacto nos negócios (BIA)?

05

A avaliação de riscos é utilizada para selecionar os cenários de crise e incidentes, elaborar playbooks e definir critérios de decisão, prioridades e recursos para a resposta e a recuperação?

06

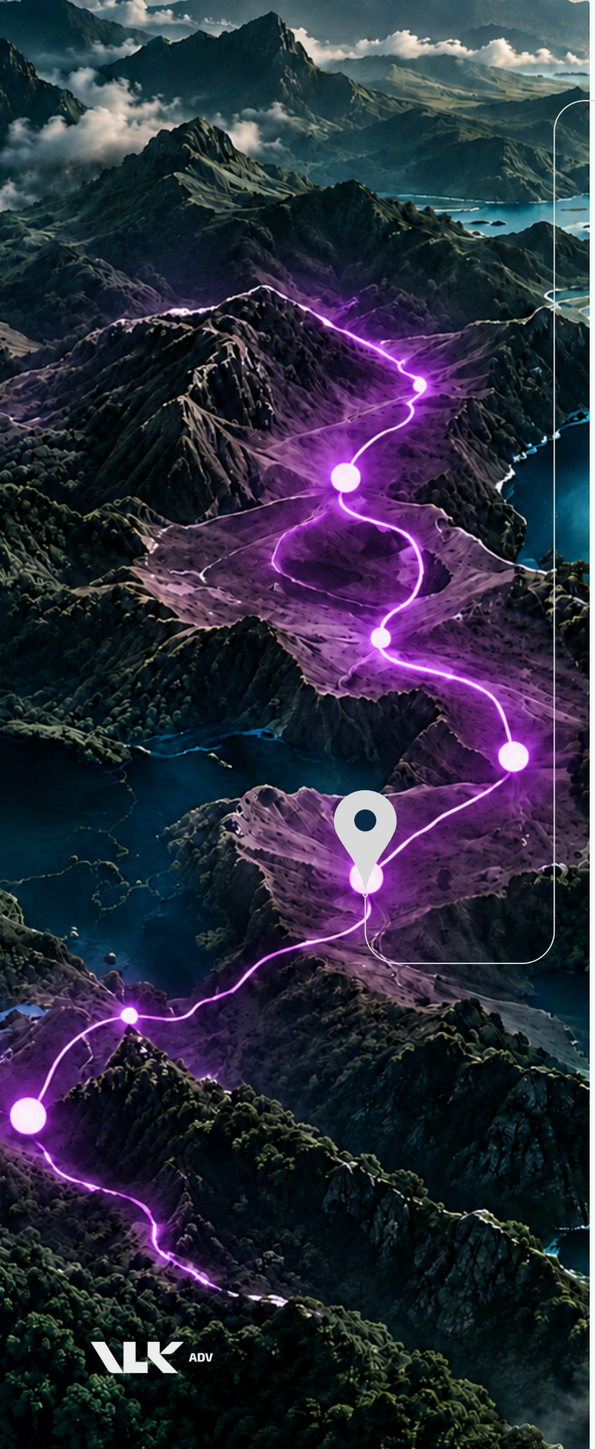
Controles preventivos foram implementados de forma proporcional aos riscos identificados?

07

As políticas, os planos, os procedimentos e os playbooks de gestão de incidentes foram aprovados, comunicados e implementados, e a organização disponibilizou os recursos necessários à sua execução, incluindo ativos da informação como cópias de segurança e recursos de recuperação protegidos contra os cenários de incidentes considerados?

08

As políticas, os planos, os procedimentos e os playbooks são revisados, testados e atualizados considerando mudanças relevantes, resultados dos exercícios e simulações e lições aprendidas?



TERRITÓRIO 4

DETECÇÃO

O QUE ESTE TERRITÓRIO DEVE EXPLORAR

Este território deve orientar a implementação e manutenção de medidas de monitoramento contínuo e a análise de sinais que possam indicar um incidente de segurança. Isso inclui identificar atividades não autorizadas, desvios dos padrões esperados e indícios de comprometimento em redes, sistemas, dados, ambientes físicos e serviços de terceiros.

POR QUE ESTE TERRITÓRIO É RELEVANTE?

A detecção proativa é essencial para garantir que um incidente de segurança seja identificado em seus estágios iniciais, de modo que a resposta seja iniciada a tempo de mitigar os impactos do incidente. Para isso, a organização precisa reconhecer sinais de comprometimento e disponibilizar informações que ajudem as equipes a avaliar o ocorrido e agir de forma célere e eficaz.

O monitoramento deve produzir alertas úteis. Alertas excessivos ou imprecisos podem sobrecarregar as equipes, enquanto falhas de cobertura ou configuração podem deixar incidentes sem identificação tempestiva.

PRINCIPAIS ASPECTOS QUE DEVEM SER CONSIDERADOS:

COBERTURA E CONTINUIDADE DO MONITORAMENTO

Monitorar redes, equipamentos, sistemas, ambientes de execução e dados, considerando sua criticidade e os cenários de incidentes relevantes. Assegurar continuidade e identificar falhas na coleta ou na geração de alertas.

AMBIENTE FÍSICO

Monitorar tentativas de acesso, entrada e saída de pessoas em áreas restritas e sinais de violação dos controles físicos que protegem os ativos.

ATIVIDADES DE USUÁRIOS

Identificar comportamentos anômalos, tentativas de autenticação, acessos indevidos e uso incomum de sistemas, inclusive por contas privilegiadas.

PRESTADORES DE SERVIÇOS EXTERNOS

Estabelecer como serão monitorados os serviços e as atividades de fornecedores, incluindo o acesso a registros, o recebimento de alertas e a comunicação de eventos que possam afetar a organização.

INTELIGÊNCIA DE AMEAÇAS

Utilizar informações sobre ameaças para reconhecer atividades suspeitas e ajustar as regras de detecção.

ANÁLISE E ENCAMINHAMENTO DOS SINAIS DETECTADOS

Definir como os alertas serão recebidos, analisados e encaminhados aos responsáveis pela resposta.

TERRITÓRIO 4

PONTOS PRELIMINARES PARA VALIDAÇÃO



01

Existem canais divulgados para que colaboradores e terceiros relatem suspeitas de incidentes, com critérios definidos para triagem, classificação e acionamento da resposta?

02

As redes e os serviços de rede são monitorados continuamente para identificar comunicações suspeitas, desvios de tráfego e redes ou dispositivos não autorizados?

03

Os registros de eventos (logs) necessários à detecção e à análise são coletados, protegidos contra alteração ou exclusão indevida e mantidos acessíveis pelo período definido pela organização?

04

Os equipamentos, sistemas, ambientes de execução e repositórios de dados são monitorados continuamente para identificar atividades não autorizadas e indícios de comprometimento?

05

Os acessos físicos, as atividades dos usuários e o uso de tecnologia são monitorados para identificar tentativas de acesso indevido, comportamentos anômalos e sinais de violação?

06

Os serviços e as atividades de prestadores externos são acompanhados por mecanismos que permitem identificar e comunicar eventos potencialmente adversos à organização?

07

A organização mantém práticas de inteligência de ameaças e adequa a sua estratégia de monitoramento às novas ameaças?

08

Os alertas são analisados e encaminhados aos responsáveis, e os mecanismos de detecção são periodicamente avaliados e ajustados com base em informações sobre ameaças e falhas identificadas?



TERRITÓRIO 5

TESTES & MELHORIAS

O QUE ESTE TERRITÓRIO DEVE EXPLORAR

Este território deve orientar a avaliação e o aprimoramento da capacidade de gestão de crise e resposta a incidentes. Isso inclui testar planos e procedimentos, avaliar a atuação das equipes e transformar os resultados dos exercícios, simulações e dos incidentes em melhorias concretas.

POR QUE ESTE TERRITÓRIO É RELEVANTE?

A existência de um plano não garante que ele funcionará quando necessário. Exercícios e testes permitem verificar se as equipes sabem como agir, se os recursos estão disponíveis e se a continuidade e a recuperação podem ocorrer nos níveis e prazos definidos.

A análise dos incidentes também permite identificar causas, falhas e medidas eficazes. Incorporar esse aprendizado aos planos, controles e treinamentos ajuda a reduzir a recorrência e os impactos de situações semelhantes.

PRINCIPAIS ASPECTOS QUE DEVEM SER CONSIDERADOS:

AVALIAÇÃO PERIÓDICA DA CAPACIDADE DE RESPOSTA

Realizar autoavaliações, avaliações externas ou auditorias para identificar deficiências nos planos, procedimentos, recursos e na atuação das equipes.

EXERCÍCIOS COM CENÁRIOS RELEVANTES

Realizar simulações e exercícios de mesa (tabletop) que permitam praticar decisões, acionamento, comunicação e coordenação, envolvendo todas as partes necessárias à resposta.

TESTES DE CONTINUIDADE E RECUPERAÇÃO

Verificar a execução dos procedimentos de restauração, a integridade das informações recuperadas, o atendimento ao tempo previsto para restabelecer os serviços (RTO) e ao limite aceitável de perda de dados no tempo (RPO).

SEGURANÇA DURANTE A DISRUPÇÃO

Verificar se os controles de segurança podem ser mantidos durante a operação alternativa e a recuperação. Quando isso não for possível, eleger, implementar e testar controles alternativos.

ANÁLISE PÓS-INCIDENTE

Avaliar as causas, as ações adotadas e sua eficácia, ouvindo os envolvidos. Identificar incidentes recorrentes ou graves e registrar as lições aprendidas.

IMPLEMENTAÇÃO DAS MELHORIAS

Priorizar as ações identificadas, definir responsáveis e prazos e acompanhar sua execução. Atualizar planos, playbooks, controles, avaliações de riscos e treinamentos, verificando se as alterações corrigiram as deficiências.

TERRITÓRIO 5

PONTOS PRELIMINARES PARA VALIDAÇÃO



01

A capacidade de resposta a incidentes e desastres é avaliada periodicamente, com registro das deficiências e oportunidades de melhoria?

02

São realizados exercícios e simulações para praticar os procedimentos de resposta, incluindo acionamento, tomada de decisão, comunicação e coordenação com fornecedores e terceiros relevantes?

03

Os planos de continuidade e recuperação são regularmente testados para verificar a capacidade de restauração de sistemas e informações, sua integridade e o atendimento aos objetivos de tempo de recuperação (RTO) e de ponto de recuperação (RPO)?

04

Os testes verificam se os controles de segurança podem ser mantidos durante a disrupção e a recuperação, incluindo a eficácia dos controles de compensação previstos?

05

Após os incidentes, são realizadas análises das causas, recorrências, eficácia e eficiência da resposta, com participação dos envolvidos e registro das lições aprendidas?

06

Os pontos de melhoria identificados em avaliações, exercícios, testes e incidentes são priorizados, atribuídos a responsáveis, e têm sua implementação acompanhada?

07

Os planos, procedimentos, controles e treinamentos são atualizados com base nas melhorias e mudanças relevantes, mantendo o alinhamento com a continuidade de negócios e a aprovação dos planos de continuidade pela instância responsável?



CONCLUSÃO

Sua organização está preparada para responder a um incidente cibernético?
As respostas deste mapa ajudam a reconhecer o que já funciona e o que ainda precisa de atenção.

O próximo passo é transformar as lacunas identificadas em ações, com prioridades, responsáveis e prazos.
Ter um plano é importante, mas é nos testes e exercícios que a organização verifica se as pessoas sabem como agir e se os recursos disponíveis são suficientes.

Revisite o mapa após mudanças relevantes, exercícios e incidentes.
Use cada aprendizado para ajustar a preparação e melhorar a capacidade de conter os impactos, manter as atividades essenciais e recuperar as operações.

AUTORES



Caio lima
caio@vlklaw.com.br



Nina Pinheiro
nina.pinheiro@vlklaw.com.br



Jean Santana
jean.santana@vlklaw.com.br

2026, VLK Advogados. Todos os direitos reservados.

Para mais informações ou para questões relacionadas à publicação, entre em contato conosco atra ves do e-mail contato@vlklaw.com.br.

CC BY-ND - Esta licença permite cópia e distribuição do material em qualquer meio ou formato apenas de forma não adaptada e apenas desde que a atribuição seja dada ao criador. A licença permite o uso comercial.

VLK Direito, Inovação & Tecnologia

Onde o **Direito** impulsiona a **Inovação**

SOBRE NÓS

No VLK, **o Direito não é barreira**. É impulso para **inovar, viabilizar negócios** e construir uma sociedade mais próspera e justa.

Somos uma **boutique de Direito Digital** movida por **entregas que fazem a diferença.**

Conciliamos:

» Riscos e oportunidades;

» Complexidade e clareza; e

» Proteção e progresso.

Não importa o quão ousado seja o projeto: **faremos acontecer**, com segurança e **quebrando formalismos desnecessários**, nas seguintes áreas:

» Proteção de Dados Pessoais

» Governança Ética e Responsável de IA

» Cibersegurança e Resposta a Incidentes

» Legal Marketing e Propriedade Intelectual

» Regulação de Tecnologia

» Contencioso Estratégico

vlklaw.com.br