GUIA DE REFERÊNCIA

Prevenção e Resposta a Ransomware

Diretrizes, boas práticas e referências para auxiliar na **Capacidade de Resistir à Ransomware** no serviço público.

cpqd Finep gov.br
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO
MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

FICHA TÉCNICA

Guia de Referência de Prevenção e Resposta a Ransomware

REALIZAÇÃO

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

Esther Dweck
Ministra

SECRETARIA DE GOVERNO DIGITAL

Rogério Souza Mascarenhas
Secretário de Governo Digital

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Leonardo Rodrigo Ferreira
Diretor de Privacidade e Segurança da Informação

COORDENAÇÃO-GERAL DE PRIVACIDADE

Marta Juvina de Medeiros
Coordenadora-Geral de Privacidade

COORDENAÇÃO-GERAL DE COMBATE A FRAUDES

Marcus Paulo Barbosa Vasconcelos
Coordenador-Geral de Combate a Fraudes

COORDENAÇÃO-GERAL DE SEGURANÇA DA INFORMAÇÃO

Loriza Andrade Vaz de Melo
Coordenadora-Geral de Segurança da Informação

COORDENAÇÃO DE GOVERNANÇA

Patrícia Araújo de Oliveira
Coordenadora de Governança

EQUIPE TÉCNICA DE ELABORAÇÃO

Patrícia Araújo de Oliveira
Carla Simone Guedes Pires
Sumaid Andrade de Albuquerque
Loriza Andrade Vaz de Melo

EQUIPE TÉCNICA DE REVISÃO

Marcus Paulo Barbosa Vasconcelos
Lázaro Gabriel do Nascimento Alves
Patrícia Araújo de Oliveira
Loriza Andrade Vaz de Melo

EXECUÇÃO TÉCNICA

CPQD — CENTRO DE PESQUISA E DESENVOLVIMENTO EM TELECOMUNICAÇÕES

Sebastião Sahão Junior
Presidente

COMITÊ ESTRATÉGICO

Paulo Curado
Diretor

Alberto Paradise
Diretor

COMITÊ OPERACIONAL M4 — CIBERSEGURANÇA NO CONTEXTO DE IA

Sérgio Ribeiro
Gerente Técnico M4

Olavo Poleto Filho
Gerente Técnico de Cibersegurança

Simone Machado
Gestora de Projeto

Alexandre Braga
Líder Técnico Geral M4

Yuri Arcanjo de Carvalho
Líder Técnico M4.4 — Resiliência Organizacional

EQUIPE TÉCNICA DE ELABORAÇÃO

Andre Santos de Oliveira
Daylon Pardini Sampaio
Douglas Manoel Machado
Gustavo Zoppello Toffoli
Hideki Sakihama
Jéssica Monteiro de Camargos Fernandes
Julio Cesar Sernaglia Gregio
Lilian Suziane Bueno
Marcos Ide
Raissa Sukar de Moura
Yuri Arcanjo de Carvalho

EQUIPE TÉCNICA DE REVISÃO

Douglas Manoel Machado
Jéssica Monteiro de Camargos Fernandes
Lilian Suziane Bueno
Marcos Ide
Yuri Arcanjo de Carvalho

Brasília, junho de 2026 — Versão 1.1

Histórico de versões

Data	Versão	Descrição	Autor
10/06/2026	1.0	Primeira versão	Equipe Técnica de Elaboração
24/06/2026	1.1	Revisão	Equipe Técnica de Revisão

Sumário

Introdução

Capítulo 1.

O presente Guia de Referência para Prevenção e Resposta a Ransomware constitui um instrumento orientador e estratégico, concebido para fornecer informações claras, precisas e abrangentes que subsidiem a atuação dos órgãos e das entidades da administração pública diante de crises decorrentes de incidentes dessa natureza. Seu propósito é apoiar a adoção de medidas preventivas, bem como orientar a resposta, a recuperação e o fortalecimento da resiliência institucional frente a ataques de ransomware.

Esta publicação foi desenvolvida no âmbito do projeto Inteligência Artificial no Serviço Público com Inovação, Responsabilidade e Ética (INSPIRE), iniciativa do Ministério da Gestão e da Inovação em Serviços Públicos (MGI), em parceria com o Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPQD). O projeto resulta de uma encomenda do Fundo Nacional de Desenvolvimento Científico e Tecnológico (FNDCT), com apoio do Ministério da Ciência, Tecnologia e Inovação (MCTI) e gestão da Financiadora de Estudos e Projetos (Finep), tendo como objetivo impulsionar o desenvolvimento e a adoção soberana de soluções nacionais de Inteligência Artificial (IA) na administração pública brasileira.

Nesse contexto, o presente guia foi elaborado em conjunto com a Diretoria de Privacidade e Segurança da Informação (DEPSI), da Secretaria de Governo Digital (SGD) do MGI, como material complementar ao Guia do Framework de Privacidade e Segurança da Informação do Programa de Privacidade e Segurança da Informação (PPSI). Dessa forma, configura-se como uma extensão prática e operacional do framework, oferecendo orientações específicas para a prevenção, a preparação, a resposta e a recuperação de incidentes de ransomware, em consonância com os controles de segurança da informação estabelecidos pelo PPSI.

1.1. Para quem é este guia?

O documento tem como objetivo orientar lideranças na tomada de decisões críticas relacionadas à continuidade dos negócios, à gestão de riscos e passivos legais e à preservação da reputação institucional em um ataque de ransomware. Ao mesmo tempo, oferece uma referência operacional consistente para o Gestor de Segurança da Informação e para a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR).

Em termos gerais, o material foi concebido para atender aos órgãos e entidades que integram o Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), podendo, no entanto, ser facilmente adaptado por qualquer organização que pretenda elevar seu nível de maturidade em segurança cibernética e reforçar sua resiliência organizacional.

1.2. Por que este guia existe?

No contexto da administração pública contemporânea, a resiliência cibernética transcende a esfera da mera conformidade técnica, configurando-se como um pilar essencial para a garantia e a continuidade dos serviços essenciais prestados ao cidadão. Alinhado às diretrizes do Programa de Privacidade e Segurança da Informação (PPSI), este Guia de Referência surge como uma resposta estratégica e pragmática aos desafios diários enfrentados pelos gestores de Tecnologia da Informação (TI) e de Segurança da Informação.

O cenário atual é caracterizado por uma assimetria complexa: de um lado, observa-se o crescimento exponencial e a sofisticação dos incidentes de ransomware; de outro, as instituições públicas deparam-se com restrições orçamentárias severas e limitação de recursos humanos qualificados. Diante desta realidade, este documento estabelece-se não apenas como um manual consultivo, mas como uma ferramenta indispensável de padronização operacional, fundamentada em três vetores principais:

- Redução Crítica do Tempo de Resposta (MTTR): Em situações de crise cibernética, a ausência de diretrizes claras maximiza o impacto sobre os dados e prolonga a interrupção dos serviços públicos. A padronização de procedimentos garante uma reação imediata e coordenada.
- Conformidade Integral com o PPSI: O guia assegura o alinhamento das operações locais com os controles preventivos e as exigências de governação determinadas pelo Ministério da Gestão e da Inovação em Serviços Públicos (MGI).
- Mitigação do Erro Humano: Sob cenários de elevada pressão e stress institucional, este material serve como um plano de ação objetivo, transformando a incerteza numa resposta assertiva, célere e estruturada.

Com o propósito de viabilizar uma execução realista e adaptada, as fontes e dados estruturais refletem o cenário atualizado até janeiro de 2026, ancorando-se de forma rigorosa nos frameworks de referência globais e nacionais mais recentes. O material consolida as diretrizes do PPSI 2.0, CIS Controls v8.1, NIST CSF 2.0, NIST IR 8374, MITRE ATT&CK e o CISA StopRansomware Guide. Longe de ser uma mera transposição de conceitos, essa base metodológica foi integralmente contextualizada e adequada à realidade orçamentária, de infraestrutura e de governança dos órgãos públicos brasileiros.

Desta forma, a presente fundamentação visa converter diretrizes complexas de segurança da informação num roteiro prático e acionável de contenção, erradicação e recuperação face a incidentes de ransomware, fortalecendo a maturidade tecnológica e a segurança do ecossistema público nacional.

1.3. Estruturação do Guia

Este material foi cuidadosamente desenvolvido para traduzir diretrizes estratégicas em ações operacionais de prontidão e resposta rápida. Nossa metodologia segue a consagrada estrutura de gestão de incidentes estabelecida pelo NIST SP 800-61 Rev. 2, integrando-a de forma harmoniosa às funções do NIST CSF 2.0 e às diretrizes fundamentais da PPSI 2.0 v1.

Para facilitar a navegação e garantir a máxima clareza operacional, o guia está dividido em duas grandes macroseções: o Ciclo de Resposta a Incidentes e os Instrumentos de Suporte Operacional.

1.3.1. O Ciclo de Resposta a Incidentes

A essência do guia está estruturada nas quatro fases tradicionais de resposta a incidentes, detalhando como as funções e capacidades de segurança se aplicam na prática em cada momento.

Preparação (Funções CSF: Identificar e Proteger)

Seção 04. Focada na prevenção e na prontidão institucional para ataques de ransomware. Aqui, você encontrará uma Matriz de Priorização com 11 controles preventivos fundamentais, essenciais para reduzir a superfície de ataque e blindar a organização antes que a crise aconteça.

Detecção e Análise (Função CSF: Detectar)

Seção 05. O sistema sensorial da instituição. Esta fase aborda o monitoramento contínuo e a busca proativa por ameaças (Threat Hunting), fornecendo ferramentas como linhas de base de comportamento, listas de sinais de alerta (IoCs) e formulários de registro de incidentes para que nenhuma atividade suspeita passe despercebida.

Contenção, Erradicação e Recuperação (Funções CSF: Responder e Recuperar)

Seção 06. O momento em que a teoria se transforma em prática operacional. Esta seção oferece fluxos de decisão, protocolos estruturados, roteiros de recuperação e templates de comunicação para isolar a ameaça, eliminar o atacante do ambiente e restabelecer os serviços de forma segura.

Atividades Pós-Incidente (Função CSF: Melhoria Contínua)

Seção 07. O fechamento do ciclo de crise. Dedicada ao fortalecimento do órgão através do aprendizado, esta fase traz roteiros e modelos de Relatório de Lições Aprendidas (Post-mortem) para corrigir falhas estruturais, atualizar políticas e evitar a reincidência de ataques.

1.3.2. Material de Apoio

A segunda metade do guia funciona como um acervo prático e customizável, projetado para acelerar a execução das atividades e municiar as equipes com os artefatos necessários para reduzir o atrito administrativo. Ela está dividida em:

Prateleira: modelos prontos para uso

Seção 08. Onde estão consolidados os templates, formulários e checklists estruturados para padronizar as respostas.

Recursos, Ferramentas e Contatos

Seção 09. Um diretório centralizado com referências técnicas, ferramentas operacionais e canais de notificação obrigatórios para acionamento de autoridades competentes (como a ANPD) e parceiros de suporte.

Navegue pelas seções conforme a necessidade da sua instituição e utilize este guia como uma ferramenta viva para elevar a resiliência cibernética e garantir a continuidade dos serviços públicos.

Como usar este guia

Capítulo 2.

O documento funciona como uma referência norteadora e operacional para auxiliar lideranças em decisões críticas (como continuidade de negócios, riscos legais e reputação) e equipes técnicas no tratamento de ransomware. Ele é voltado para os órgãos do SISP, mas pode ser adaptado por qualquer organização. O usuário encontrará checklists acionáveis, fluxos de decisão e uma "Prateleira de Instrumentos", que reúne modelos prontos (templates de comunicação, planos de resposta simplificados, checklists e matriz RACI) para padronizar processos e acelerar a tomada de decisão.

2.1. Sou gestor(a) (Alta Administração / Lideranças), o que devo saber?

O pré-requisito é a compreensão estratégica sobre gestão de riscos, continuidade de negócios e preservação da reputação institucional. Deve conhecer as estruturas de governança do órgão para liderar a tomada de decisões críticas sob extrema pressão e validar a alocação de recursos para os controles preventivos.

2.2. Sou profissional da TI, o que preciso saber?

O pré-requisito é possuir nível de conhecimento intermediário em segurança da informação, com domínio técnico sobre infraestrutura e segmentação de rede, gerenciamento de privilégios de contas, rotinas e testes de backup, além de processos de atualização (patching) e reconstrução de ambientes a partir de imagens limpas (Golden Images).

2.3. Sou profissional de Segurança da Informação (Gestor de SI / ETIR), o que preciso saber?

O pré-requisito é o conhecimento avançado em frameworks de cibersegurança (como NIST e CIS Controls), monitoramento proativo de ameaças (Threat Hunting), análise centralizada de logs e a capacidade operacional para coordenar e executar os protocolos estruturados de contenção forense, erradicação e recuperação segura de incidentes.

2.4. Sou Encarregado pelo Tratamento de Dados Pessoais, o que preciso saber?

O pré-requisito é o domínio regulatório da LGPD e das resoluções da ANPD. Precisa ter capacidade para avaliar prontamente o impacto à privacidade dos cidadãos caso ocorra vazamento ou indisponibilidade de dados

pessoais, conhecendo rigorosamente os prazos e os ritos de notificação obrigatória às autoridades e aos titulares.

2.5. Sou servidor(a) usuário, o que devo saber?

O pré-requisito é o entendimento das práticas básicas de higiene cibernética (como o uso correto do MFA e a identificação de phishing) e a clareza sobre os canais e obrigações de reporte imediato de qualquer anomalia à equipe técnica, sem tentar intervir de forma autônoma nos sistemas.

O que é um ataque de Ransomware

Capítulo 3.

O ransomware é uma modalidade de código malicioso (malware) que utiliza técnicas de criptografia para o sequestro de dados e o bloqueio de ativos computacionais, normalmente condicionando o restabelecimento do acesso ao pagamento de resgate. No âmbito da Administração Pública Federal (APF), o impacto é crítico, a indisponibilidade de sistemas e bases de dados vitais compromete a execução de políticas públicas, a soberania nacional e o atendimento direto ao cidadão.

Conforme reportado pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR.GOV), segundo dados de pesquisa, o ransomware consolidou-se como a principal ameaça às Infraestruturas Críticas no Brasil. A interrupção de serviços essenciais não apenas gera prejuízos financeiros e operacionais, mas pode comprometer a segurança jurídica e a integridade social.

Figura 1 - Infográfico Ransomware: Como acontece
Fonte: CERT.br CC BY-NC-ND 4.0 – https://cert.br/docs/ransomware/entender

3.1. Evolução das Táticas e Extorsão Qualificada

Os agentes de ameaça têm refinado suas táticas de coerção através da dupla extorsão, além do bloqueio dos sistemas, há a exfiltração de dados sensíveis e credenciais de autenticação, sob ameaça de vazamento público para causar danos reputacionais às instituições. É imperativo prever que esses grupos passem a utilizar Inteligência Artificial (IA) para automatizar a exploração de vulnerabilidades e sofisticar as táticas de engenharia social.

Atualmente, observamos um aumento na furtividade operacional. O modus operandi envolve:

Movimentação Lateral
Após o acesso inicial, os atacantes mapeiam a rede em busca de sistemas de missão crítica e dados sigilosos.

Persistência e Monitoramento
Os agentes monitoram as comunicações internas e os planos de contingência da instituição para neutralizar os esforços de resposta e recuperação

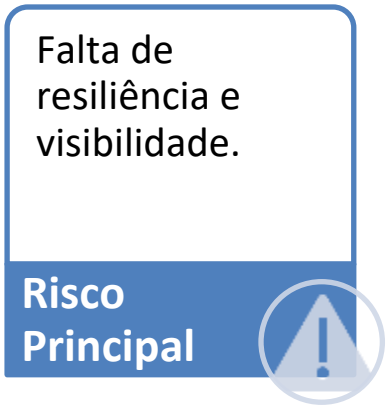
Comprometimento Estratégico
A carga útil (payload) é implantada preferencialmente em ativos de alto valor e sistemas de backup, visando maximizar o poder de negociação do atacante.

A efetiva utilização deste roteiro como eixo orientador é premissa basilar para a consolidação de uma estratégia de defesa em. A complexidade do cenário de ameaças atual exige que as instituições transcendam ações isoladas, adotando este instrumental técnico e operacional de forma integrada. A estrita aplicação destas recomendações traduz-se no alinhamento ao PPSI 2.0, na preservação da integridade dos dados governamentais e na institucionalização de uma capacidade coordenada de resposta a incidentes, salvaguardando o interesse público.

Fortalecendo a instituição para resistir a um ataque

[Identificar e Proteger].

Capítulo 4.



Visão geral

A maioria dos incidentes de segurança da informação, como o ransomware, não decorre de técnicas de invasão sofisticadas, mas sim da falha na execução da higiene cibernética básica. Os ataques exploram controles negligenciados: gestão inadequada de contas e credenciais, instâncias de dados de recuperação (cópias de segurança) não testadas, acesso remoto sem autenticação multifator (MFA) e gestão ineficiente de vulnerabilidades em soluções de software.

As estatísticas globais corroboram que os vetores de acesso inicial mais explorados permanecem sendo:

- Comprometimento de credenciais de contas de usuário e de administrador;
- Exploração de vulnerabilidades conhecidas em ativos expostos;
- Técnicas de engenharia social (ex.: phishing) direcionadas aos agentes públicos.

Isso demonstra que controles fundamentais, quando efetivamente implementados, mitigam a grande maioria dos incidentes. O framework do PPSI 2.0, fundamentado no CIS Controls, estabelece que a adoção integral das medidas do Grupo de Implementação 1 (GI1), considerado o alicerce da higiene cibernética, defende a infraestrutura contra as principais táticas e técnicas adversárias contemporâneas.

A seguir, estruturam-se 11 Iniciativas Estratégicas de alto impacto, priorizadas sob a ótica da gestão de riscos, sensibilidade dos dados, criticidade de sistemas e potencial impacto no negócio, direcionadas a órgãos e entidades da Administração Pública Federal que possuam limitações operacionais ou que não disponham de um Centro de Operações de Segurança (SOC) dedicado.

4.1. Criar um plano de ação para incidentes cibernéticos

Por que esse controle é crítico?

Ter um plano de ação é o que diferencia a capacidade real de resposta de um órgão de uma mera intenção no papel. Protocolos puramente teóricos falham sob as condições de estresse causadas por um ataque de Ransomware. Por isso, é essencial possuir um roteiro escrito e detalhado que dite o caminho para a recuperação institucional.

Esse plano garante que todos saibam como paralisar a ameaça, como manter a comunicação com a sociedade e outras instituições durante a crise e, o mais importante, como retomar a prestação de serviços públicos o mais rápido possível. Um plano de ação robusto evita que o órgão sofra uma paralisação catastrófica, permitindo que os sistemas e dados sejam restaurados dentro de um tempo que não prejudique o cidadão nem a missão do Estado.

Táticas do framework MITRE ATT&CK associadas

Impacto (Impact - MITRE ATT&CK)

Medidas PPSI associadas

0.8 - O órgão instituiu Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR)?

0.14 - O órgão possui um processo de gestão de continuidade de negócios em segurança da informação?

17.2 - O órgão estabelece e mantém informações de contato para notificar incidentes de segurança da informação?

17.4 - O órgão estabelece e mantém um processo de gestão de incidentes de segurança da informação?

17.6 - O órgão define mecanismos de comunicação a serem realizados durante o tratamento de incidentes de segurança da informação?

17.7 - O órgão conduz exercícios de tratamento de incidentes de segurança da informação regularmente?

17.8 - O órgão realiza análises pós-incidente de segurança da informação?

Procedimentos e ferramentas

Instituir e documentar formalmente a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), definindo seus membros titulares, substitutos designados, funções e telefones de contato. Saiba mais no anexo 1

Desenvolver a matriz de severidade e o fluxo para o tratamento dos incidentes, categorizando-os estruturalmente (ex.: Crítico, Alto, Médio). Saiba mais no anexo 2

Estabelecer a árvore de comunicação, determinando os mecanismos primários e secundários que serão usados para a notificação do incidente. Saiba mais no anexo 3

Mapear canais de comunicação alternativos (out-of-band), considerando que a infraestrutura primária (como o correio eletrônico corporativo) pode estar indisponível durante a crise. Saiba mais no anexo 4

Integrar ao plano o inventário de processos de negócio prioritários, definindo métricas claras de Tempo de Recuperação (RTO) e Ponto de Recuperação (RPO). Saiba mais no anexo 5

Consolidar a lista de contatos externos essenciais, incluindo provedores de seguro de cibersegurança, equipe jurídica, empresas de resposta a incidentes contratadas e autoridades governamentais, como o CTIR Gov e o CISC gov.br. Saiba mais no anexo 6

Planejar e conduzir cenários rotineiros de exercícios de mesa (tabletop) com periodicidade regular, garantindo a participação da ETIR e o envolvimento direto da alta administração. Saiba mais no anexo 7

Realizar análises pós-incidente e pós-exercício, documentando as lacunas identificadas e atualizando o plano com as lições aprendidas e ações de acompanhamento. Saiba mais no anexo 8

Papéis e Responsabilidades:

Alta Administração: Apoio estratégico e fornecimento de recursos para a elaboração do plano, além de liderar a tomada de decisões críticas durante a ativação dos protocolos de crise.

Gestor de Tecnologia da Informação e Comunicação: Assegurar que a infraestrutura tecnológica esteja preparada para executar as manobras de recuperação previstas no plano.

Gestor de Segurança da Informação: Planejar e gerenciar a elaboração do Plano de Resposta a Incidentes, garantindo que ele esteja integrado ao Plano de Continuidade de Negócios do órgão.

Encarregado pelo Tratamento de Dados Pessoais: Definir, dentro do plano, os protocolos de notificação em caso de vazamento de dados, conforme as exigências da LGPD e órgãos reguladores.

Responsável Setorial pela Gestão da Integridade: Zelar para que as ações tomadas durante a crise sigam os princípios Éticos e de transparência administrativa.

Responsável pela Unidade de Gestão de Pessoas: Estabelecer fluxos de acionamento das equipes em regimes especiais durante a execução do plano de ação.

Equipe de TI: Implantar os procedimentos técnicos de restauração e suporte descritos no plano, garantindo o funcionamento das ferramentas de emergência.

Equipe de Comunicação: Gerenciar a comunicação oficial durante um incidente, utilizando o plano para informar o público de maneira clara e evitar boatos que prejudiquem a imagem do órgão.

Equipe Jurídica: Analisar o plano para garantir o amparo legal das ações emergenciais e assessorar juridicamente o órgão durante a vigência da crise.

ETIR: Deve ser notificada para ativar formalmente o Plano de Ação; a partir daí, coordena a execução técnica da resposta, distribui tarefas, monitora a evolução da contenção e mantém o registro cronológico de todas as ações para auditoria posterior.

Usuários: Aderir às soluções propostas no plano, seguindo rigorosamente as orientações de uso de sistemas alternativos ou procedimentos manuais caso o plano de contingência seja ativado.

4.2. Preparar a instituição para crise de ransomware

Por que esse controle é crítico?

A forma como a gestão do órgão conduz os primeiros momentos de um ataque define se a instituição sobreviverá ou se sofrerá um colapso total, tanto em suas operações quanto em sua reputação perante a sociedade. Não basta ter tecnologia de ponta; é preciso ter uma gestão de crise organizada, profissional e testada. Seguindo padrões internacionais de excelência (como a ISO 22361), essa preparação garante que a liderança do órgão não seja pega de surpresa. Estar preparado significa ter a capacidade de tomar decisões rápidas sob pressão, manter a confiança dos cidadãos e de outros órgãos governamentais e garantir que a prestação de serviços públicos continue, mesmo diante de um incidente grave. É este controle que transforma o pânico em uma resposta coordenada, técnica e eficiente.

- Tomada de Decisão sob Extrema Pressão: Um ataque de ransomware gera caos imediato, sistemas inoperantes, processos críticos paralisados e pressão extrema pelo pagamento de resgate. A norma estabelece uma estrutura de comando clara (o comitê de crise), definindo quem tem a palavra final e evitando a paralisia por análise ou decisões emocionais (como ceder a extorsões sem amparo legal)
- Visão Estratégica Além da TI

  Diferente de um plano puramente técnico, a gestão de crises trata o incidente como um impacto direto na continuidade da instituição, englobando:

  - Comunicação: Como notificar partes interessadas e autoridades reguladoras (como a ANPD, em conformidade com a LGPD) sem causar pânico desnecessário.
  - Jurídico: Como mapear e mitigar as implicações legais do vazamento de dados.
  - Operacional/Financeiro: Como manter serviços essenciais e processos administrativos (como folha de pagamento e faturamento) rodando em contingência.
- Proteção e Recuperação da Confiança: O maior dano de um ransomware frequentemente não é financeiro, mas a perda de credibilidade. A ISO 22361 orienta a criação de protocolos de comunicação transparentes. Instituições preparadas demonstram resiliência, provando à sociedade, aos parceiros e aos órgãos de controle que o incidente está sendo ativamente gerenciado, e não em estado de descontrole.

Táticas do framework MITRE ATT&CK associadas

Impacto (Impact)

Exfiltração (Exfiltration)

Comando e Controle (Command and Control)

Medidas PPSI associadas

0.1 - A alta administração do órgão estabelece, mantém, monitora e aprimora o sistema de gestão de riscos e controles internos relativos aos temas de privacidade e segurança da informação?

0.6 - O órgão institui Comitê de Segurança da Informação?

0.11 - O órgão possui Política de Segurança da Informação (POSIN)?

0.13 - O órgão possui um processo de gestão de riscos de segurança da informação?

0.14 - O órgão possui um processo de gestão de continuidade de negócios em segurança da informação?

0.15 - O órgão possui um processo de gestão de mudanças dos aspectos de segurança da informação?

11.3 - O órgão protege os dados de recuperação?

11.4 - O órgão estabelece e mantém uma instância isolada de dados de recuperação?

17.2 - O órgão estabelece e mantém informações de contato para notificar incidentes de segurança da informação?

17.3 - O órgão estabelece e mantém informações de contato para notificar incidentes de segurança da informação?

17.4 - O órgão estabelece e mantém um processo de gestão de incidentes de segurança da informação?

17.5 - O órgão atribui funções e responsabilidades para gestão de incidentes de segurança da informação?

17.6 - O órgão define mecanismos de comunicação a serem realizados durante o tratamento de incidentes de segurança da informação?

17.7 - O órgão implementa processo de gestão de incidentes com dados pessoais?

17.8 - O órgão realiza análises pós-incidente de segurança da informação?

20.1 - O órgão implementa processo de gestão de incidentes com dados pessoais?

Procedimentos e ferramentas

Desenvolva um plano de gestão de crises. Saiba mais no anexo 9

Papéis e Responsabilidades:

Alta Administração: Apoio estratégico e fornecimento de recursos para a estrutura de gestão de crises; atua como a autoridade máxima na tomada de decisões políticas e institucionais durante o evento.

Gestor de Tecnologia da Informação e Comunicação: Garantir que a infraestrutura técnica suporte às comunicações de emergência e as manobras necessárias para a sobrevivência do ecossistema digital do órgão.

Gestor de Segurança da Informação: Planejar e gerenciar os protocolos de gestão de crise cibernética, integrando as ações técnicas às decisões administrativas e estratégicas.

Encarregado pelo Tratamento de Dados Pessoais: Orientar o comitê de crise sobre as obrigações legais de notificação à ANPD e às vítimas, caso dados pessoais sejam comprometidos.

Responsável Setorial pela Gestão da Integridade: Zelar pela transparência e conformidade dos atos tomados durante a crise, garantindo que a resposta siga os preceitos da ética pública.

Responsável pela Unidade de Gestão de Pessoas: Coordenar a mobilização das equipes e o suporte psicológico ou operacional aos servidores diretamente envolvidos na resposta ao ataque.

Equipe de TI: Executar as manobras técnicas de contenção e recuperação conforme as prioridades estabelecidas pelo gabinete de crise.

Equipe de Comunicação: Gerenciar a imagem pública do órgão, emitindo notas oficiais e combatendo desinformações (fake news) sobre o incidente.

Equipe Jurídica: Prestar assessoria imediata sobre a legalidade das medidas de exceção tomadas durante a crise e analisar responsabilidades contratuais com terceiros.

ETIR: Deve ser notificada imediatamente no primeiro sinal de um ataque de grande escala; a partir do aviso, assume o comando técnico da resposta, fornece os diagnósticos reais para o gabinete de crise e executa a contenção direta da ameaça no ambiente do órgão.

Usuários: Aderir às soluções propostas e aos canais oficiais de informação, seguindo as diretrizes de "silêncio de rádio" ou comunicação restrita para evitar o vazamento de detalhes estratégicos da resposta.

4.3. Preparar as pessoas para resistir ao ataque

Por que esse controle é crítico?

A maioria das invasões a instituições públicas começa com uma tentativa de enganar alguém — técnica conhecida como “engenharia social” (como os e-mails falsos chamados phishing). O objetivo dos criminosos é explorar a boa-fé, a curiosidade ou a pressa dos servidores para conseguir uma porta de entrada no órgão. No entanto, o que define se um ataque será apenas uma tentativa frustrada ou um desastre total é a capacidade de reação das pessoas.

Um programa de treinamento contínuo, com simulações práticas, transforma cada colaborador em um “sensor vivo” de ameaças. Em vez de serem o ponto vulnerável, os servidores passam a ser os primeiros a identificar e reportar perigos. Ao mesmo tempo, realizar exercícios reais de crise com as equipes técnicas garante que, se um Ransomware aparecer, todos saibam exatamente como agir. Isso reduz drasticamente o tempo de resposta e garante que o órgão continue prestando serviços à sociedade mesmo sob pressão.

Táticas do framework MITRE ATT&CK associadas

Acesso Inicial (Initial Access)

Execução (Execution)

Medidas PPSI associadas

14.1 - O órgão implementa um programa de conscientização em segurança da informação?

14.2 - O órgão conscientiza os agentes públicos para reconhecer ataques de engenharia social??

14.6 - O órgão conscientiza os agentes públicos sobre como reconhecer e notificar incidentes de segurança da informação?

14.9 - O órgão implementa ações para capacitação sobre segurança da informação?

17.3 - O órgão estabelece e mantém um processo institucional para notificar incidentes de segurança da informação?

17.6 - O órgão define mecanismos de comunicação a serem realizados durante o tratamento de incidentes de segurança da informação?

17.7 - O órgão conduz exercícios de tratamento de incidentes de segurança da informação regularmente?

Procedimentos e ferramentas

Conscientização: Estabelecer simulações periódicas de engenharia social (ex.: testes mensais de phishing) para todos os agentes públicos, abordando cenários realistas do contexto organizacional (ex.: notas fiscais falsas ou demandas urgentes forjadas). Utilizar materiais de referência de excelência, como as cartilhas do CERT.br ou do CEPS GOV.BR. Saiba mais no anexo 10

Cultura Educativa: Fomentar uma cultura não punitiva para os agentes públicos que falharem nas simulações, direcionando-os de forma construtiva a ações de reforço de conscientização. Saiba mais no anexo 11

Reporte de Incidentes: Estabelecer, divulgar e manter um processo institucional com um canal de comunicação simples e direto para que os agentes públicos notifiquem tempestivamente qualquer atividade suspeita. Saiba mais no anexo 12

Capacitação Técnica: Incluir, nos instrumentos de desenvolvimento de pessoas da organização (ex.: Plano de Desenvolvimento de Pessoas), treinamentos técnicos específicos para a área de TI e Segurança da Informação, abrangendo competências como resposta a incidentes, análise forense e DevSecOps. Saiba mais no anexo 13

Simulações de Crise: Planejar e conduzir exercícios rotineiros de tratamento de incidentes (como Tabletop Exercises ou simulações Red/Blue Team) envolvendo a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) e a alta administração. Saiba mais no anexo 14

Comunicação de Crise: Determinar e testar mecanismos de comunicação primários e secundários, incluindo canais alternativos (out-of-band), garantindo que a coordenação do tratamento do incidente ocorra de forma ininterrupta, mesmo que os sistemas corporativos (ex.: e-mail institucional) sejam afetados pelo ataque. Saiba mais no anexo 15

Papéis e Responsabilidades:

Alta Administração: Apoio estratégico e fornecimento de recursos para programas de capacitação e exercícios de simulação de crise em larga escala.

Gestor de Tecnologia da Informação e Comunicação: Prover as ferramentas necessárias para as simulações técnicas e garantir que os sistemas de segurança facilitem o reporte de ameaças pelos usuários.

Gestor de Segurança da Informação: Planejar e gerenciar o programa de conscientização, definindo os conteúdos dos treinamentos e o cronograma de exercícios práticos.

Encarregado pelo Tratamento de Dados Pessoais: Orientar sobre como o fator humano impacta na proteção de dados e instruir os servidores sobre o tratamento seguro de informações pessoais.

Responsável Setorial pela Gestão da Integridade: Promover a ética digital e a responsabilidade no uso dos ativos públicos, combatendo a negligência que possa facilitar ataques.

Responsável pela Unidade de Gestão de Pessoas: Integrar os treinamentos de segurança cibernética ao plano de desenvolvimento de pessoas e à integração de novos servidores.

Equipe de TI: Apoiar a execução técnica das simulações de phishing e garantir que os canais de suporte técnico estejam prontos para receber dúvidas e possíveis reportes de phishing real.

Equipe de Comunicação: Criar campanhas educativas criativas e diretas, utilizando linguagem acessível para disseminar a cultura de segurança em todo o órgão.

Equipe Jurídica: Analisar os impactos normativos dos treinamentos e orientar sobre as responsabilidades administrativas em casos de violação das políticas de segurança.

ETIR: Deve ser notificada pela equipe de TI quando identificado e-mail, link ou comportamento suspeito; a partir do aviso, deve analisar a ameaça, emitir alertas para todo o órgão para prevenir novos cliques e utilizar os dados do repórter para aprimorar as defesas técnicas.

Usuários: Aderir às soluções propostas, participar ativamente das capacitações e reportar imediatamente à equipe de TI responsável qualquer suspeita de golpe ou mensagem atípica, funcionando como a primeira linha de defesa do órgão.

4.4. Proteger as credenciais de acesso dos usuários

Por que esse controle é crítico?

Imagine que a rede do órgão possui uma central de comando onde ficam guardadas todas as chaves e permissões de acesso: esse é o serviço de diretório (o “cérebro” da rede). Se um invasor consegue comprometer essa central, ele ganha controle absoluto sobre todo o ambiente institucional. Com esse poder, ele pode desligar qualquer sistema de defesa, acessar processos sigilosos de qualquer área e espalhar o vírus ransomware para todos os computadores do governo ao mesmo tempo.

Proteger essa arquitetura é como reforçar a segurança do cofre principal do órgão. Ao restringir severamente o uso de contas com superpoderes (privilegiadas) e eliminar tecnologias antigas e vulneráveis, criamos barreiras que impedem o criminoso de “subir de nível” dentro do sistema. Sem conseguir essas chaves mestras, o invasor fica preso em uma área limitada, perdendo a capacidade de causar um dano generalizado à prestação de serviços e à imagem da instituição.

Táticas do framework MITRE ATT&CK associadas

Movimentação Lateral (Lateral Movement)

Acesso a Credenciais (Credential Access)

Medidas PPSI associadas

4.6 - O órgão gerencia com segurança os ativos institucionais e soluções de software?

5.4 - O órgão limita os privilégios de administrador às contas de administrador dedicadas?

5.5 - O órgão estabelece e mantém um inventário de contas de serviço?

6.8 - O órgão define e mantém o controle de acesso baseado em funções?

8.5 - O órgão coleta logs de auditoria detalhados?

12.8 - O órgão utiliza e mantém recursos computacionais dedicados para todas as atividades administrativas de TI?

Procedimentos e ferramentas

Limitar rigorosamente os membros de grupos de alto privilégio (como Domain Admins) ao mínimo absoluto (ex.: 2 ou 3 acessos), garantindo que esses privilégios pertençam exclusivamente a contas de administrador dedicadas. Saiba mais no anexo 16

Definir e documentar o controle de acesso baseado em funções, habilitando grupos de segurança restritivos (como o Protected Users Security Group) para contas privilegiadas, a fim de mitigar a exposição e o roubo de credenciais em memória. Saiba mais no anexo 17

Gerenciar os ativos e o diretório de forma segura, desabilitando protocolos de autenticação antigos e inerentemente vulneráveis (como NTLMv1 e Kerberos DES), forçando o uso de protocolos de rede seguros. Saiba mais no anexo 18

Configurar a coleta de logs de auditoria detalhados no serviço de diretório (incluindo origem, data e nome de usuário) para identificar e alertar sobre alterações não autorizadas em grupos e políticas. Saiba mais no anexo 19

Estabelecer inventário e proteção rigorosa para as contas de serviço de infraestrutura (como a conta KRBTGT), estipulando rotinas de rotação periódica de senhas (ex.: duplo reset a cada 180 dias) para invalidar a persistência adversária via forja de tíquetes (Golden Tickets). Saiba mais no anexo 20

Implementar o Modelo de Administração em Camadas (Tiered Administration Model), mantendo recursos de computação dedicados e logicamente separados para garantir que a administração do Tier 0 (Controladores de Domínio e AD) nunca ocorra a partir de equipamentos do Tier 1 (Servidores Gerais) ou Tier 2 (Estações de Trabalho). Saiba mais no anexo 21

Papéis e Responsabilidades:

Alta Administração: Apoio estratégico e fornecimento de recursos para a modernização das tecnologias de diretório e proteção de identidades digitais.

Gestor de Tecnologia da Informação e Comunicação: Prover a infraestrutura necessária para a centralização de acessos e garantir que as ferramentas de diretório estejam sempre atualizadas.

Gestor de Segurança da Informação: Planejar e gerenciar as políticas de endurecimento (hardening) das contas de sistema, definindo critérios rígidos para o uso de credenciais administrativas.

Encarregado pelo Tratamento de Dados Pessoais: Fiscalizar o controle de acesso às credenciais para garantir que apenas pessoas autorizadas possam gerenciar identidades que contenham dados pessoais.

Responsável Setorial pela Gestão da Integridade: Monitorar o uso de contas com altos privilégios para prevenir o uso indevido de autoridade no ambiente digital.

Responsável pela Unidade de Gestão de Pessoas: Colaborar no processo de desligamento ou movimentação de servidores, garantindo que as credenciais e chaves de acesso sejam revogadas no momento exato da mudança.

Equipe de TI: Implantar as configurações de segurança no serviço de diretório, desativar protocolos antigos e proteger fisicamente e logicamente os servidores de comando da rede.

Equipe de Comunicação: Alertar o corpo funcional sobre os riscos de fornecer credenciais em sites não oficiais e a importância da proteção da identidade funcional.

Equipe Jurídica: Assessorar na regulamentação do uso de assinaturas e certificados digitais vinculados às credenciais de acesso do órgão.

ETIR: Deve ser notificada sobre qualquer sinal de comprometimento de contas administrativas ou tentativas de acesso ao controlador de domínio; a partir do aviso, deve isolar o sistema de diretório, realizar a troca emergencial de senhas mestras e auditar todos os acessos recentes para identificar a extensão da invasão.

Usuários: Aderir às soluções propostas, zelando pela guarda de suas senhas e identidades funcionais, compreendendo que sua credencial é a porta de entrada para a segurança de todo o órgão.

4.5. Proteger acessos externos à organização

Por que esse controle é crítico?

Senhas sozinhas não são mais suficientes para proteger as contas de acesso. Atualmente, a perda de controle de uma conta com altos privilégios é um dos riscos mais graves para o serviço público, pois facilita a entrada de vírus que bloqueiam arquivos e roubam dados sigilosos (ransomware).

A melhor defesa para proteger os órgãos e sistemas é o uso da Autenticação de Múltiplos Fatores (MFA). Ele funciona como uma barreira decisiva: além da senha, o sistema exige uma segunda confirmação de identidade (como um código no celular ou uma chave de segurança). Isso impede que invasores e robôs acessem informações mesmo que descubram a senha, diminuindo drasticamente as chances de um ataque bem-sucedido contra a administração pública.

Táticas do framework MITRE ATT&CK associadas

Acesso Inicial (Initial Access - MITRE ATT&CK)

Acesso a Credenciais (Credential Access - MITRE ATT&CK)

Medidas PPSI associadas

6.3 - O órgão exige autenticação multifator (Multi-Factor Authentication, MFA) para soluções de software expostas externamente?

6.4 - O órgão exige autenticação multifator (Multi-Factor Authentication, MFA) para acesso remoto à rede?

6.5 - O órgão exige autenticação multifator (Multi-Factor Authentication, MFA) para acesso administrativo?

14.3 - O órgão conscientiza os agentes públicos nas melhores práticas de autenticação?

Procedimentos e ferramentas

Exigir MFA para todo acesso remoto à infraestrutura de rede, como VPNs. Saiba mais no anexo 22

Implementar MFA em todas as contas de acesso administrativo, abrangendo todos os ativos institucionais e soluções de software (serviços de diretório, infraestrutura de nuvem, firewalls e switches). Saiba mais no anexo 23

Ativar MFA nos sistemas de gerenciamento de cópias de segurança (consoles de backup), isolando-os contra tentativas adversárias de destruição de dados de recuperação. Saiba mais no anexo 24

Exigir MFA para todas as soluções de software expostas externamente, incluindo serviços de correio eletrônico corporativo e plataformas em nuvem (SaaS). Saiba mais no anexo 25

Elevar a maturidade da autenticação substituindo fatores baseados em SMS (vulneráveis a SIM-swapping) por aplicativos autenticadores ou tokens físicos de hardware, instruindo os agentes públicos sobre essa transição. Saiba mais no anexo 26

Papéis e Responsabilidades:

Alta Administração: Apoio estratégico e fornecimento de recursos para a implementação de técnicas de proteção.

Gestor de Tecnologia da Informação e Comunicação: Prover a infraestrutura tecnológica necessária e garantir a integração das soluções de autenticação nos sistemas do órgão.

Gestor de Segurança da Informação: Planejar, implantar e gerenciar tecnologias de proteção de acesso e treinar o time técnico responsável.

Encarregado pelo Tratamento de Dados Pessoais: Zelar para que os métodos de autenticação estejam em conformidade com a proteção de dados dos cidadãos e servidores.

Responsável Setorial pela Gestão da Integridade: Monitorar e mitigar riscos de fraudes ou desvios de conduta relacionados ao uso indevido de acessos.

Responsável pela Unidade de Gestão de Pessoas: Orientar os servidores sobre as normas de acesso e colaborar na sensibilização sobre a importância do uso das ferramentas de segurança.

Equipe de TI: Implantar e gerenciar as tecnologias de MFA e oferecer suporte técnico para a ativação dessas camadas de proteção.

Equipe de Comunicação: Produzir e divulgar campanhas informativas para que todos os colaboradores entendam como e por que utilizar as novas travas de segurança.

Equipe Jurídica: Prestar assessoria normativa sobre a obrigatoriedade do uso de tecnologias de segurança e os impactos legais em caso de descumprimento das políticas de acesso.

ETIR: Após acionado, monitorar tentativas de acessos indevidos, investigar alertas de contas comprometidas e atuar prontamente na contenção caso um acesso externo seja explorado por um atacante.

Usuários: Aderir às soluções propostas, configurando o segundo fator de autenticação em suas contas e zelando pela segurança de suas credenciais de acesso.

4.6. Monitorar a infraestrutura da organização de forma ininterrupta

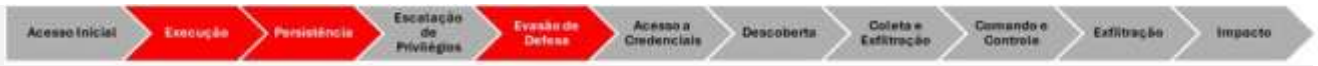
Por que esse controle é crítico?

As ferramentas de proteção só cumprem seu papel se houver alguém vigiando o que elas têm a dizer. Ter visibilidade total sobre como as ameaças tentam entrar é fundamental, mas o diferencial está na agilidade da resposta. Como os ataques de ransomware não respeitam o horário comercial e geralmente acontecem

quando a vigilância está baixa, como madrugadas, feriados e finais de semana, a observação precisa ser constante.

Para garantir essa proteção sem interrupções, o órgão pode contar com serviços especializados de detecção e resposta. Isso garante que, mesmo sem uma equipe interna disponível 24 horas por dia, especialistas externos monitoram os sistemas para identificar e bloquear qualquer atividade suspeita imediatamente. Essa estratégia assegura que uma ameaça seja contida antes mesmo de se tornar um problema real, transferindo a complexidade da vigilância para quem domina o assunto.

Táticas do framework MITRE ATT&CK associadas



Execução (Execution - MITRE ATT&CK)

Persistência (Persistence - MITRE ATT&CK)

Evasão de Defesa (Defense Evasion - MITRE ATT&CK)

Medidas PPSI associadas

13.7 - O órgão implanta soluções para prevenção de intrusão baseada em host?

15.4 - O órgão descreve os requisitos mínimos de segurança da informação nos contratos dos provedores de serviços?

17.4 - O órgão estabelece e mantém um processo de gestão de incidentes de segurança da informação?

17.5 - O órgão atribui funções e responsabilidades para gestão de incidentes de segurança da informação?

Procedimentos e ferramentas

Avaliar a viabilidade e contratar um provedor de serviços de MDR compatível com o porte e a infraestrutura tecnológica do órgão, assegurando monitoramento e análise de ameaças 24/7. Saiba mais no anexo 27

Garantir que o escopo técnico inclua a implantação de soluções de detecção de intrusão baseada em host (como agentes Endpoint Detection and Response - EDR) , que suportem identificação de ameaças, resposta automatizada, isolamento de ativos e coleta forense. Saiba mais no anexo 28

Descrever os requisitos mínimos de segurança da informação no contrato do provedor de serviços, estipulando Acordos de Nível de Serviço (SLA) rigorosos para os tempos de detecção (ex.: <1min), investigação (ex.: <10min) e remediação (ex.: <60min). Saiba mais no anexo 29

Integrar o provedor de serviços ao processo interno de gestão de incidentes de segurança da informação, documentando claramente os papéis e atribuindo as responsabilidades de resposta conjuntas entre a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) do órgão e os analistas do MDR. Saiba mais no anexo 30

Papéis e Responsabilidades:

Alta Administração: Apoio estratégico e fornecimento de recursos para a contratação e manutenção de serviços de monitoramento contínuo (24/7).

Gestor de Tecnologia da Informação e Comunicação: Garantir que a infraestrutura tecnológica do órgão esteja integrada às ferramentas de monitoramento e que os dados fluam corretamente para a análise de segurança.

Gestor de Segurança da Informação: Planejar e gerenciar o escopo do monitoramento, definindo quais ativos são críticos para o órgão e estabelecendo os níveis de serviço esperados.

Encarregado pelo Tratamento de Dados Pessoais: Orientar sobre os limites da coleta de dados de monitoramento para garantir a conformidade com a proteção à privacidade dos servidores e cidadãos.

Responsável Setorial pela Gestão da Integridade: Atuar em conjunto com o monitoramento para identificar acessos atípicos que possam indicar desvios de conduta ou uso indevido de sistemas.

Responsável pela Unidade de Gestão de Pessoas: Colaborar na definição de normas sobre o monitoramento de ativos institucionais e apoiar a comunicação com servidores em casos de incidentes identificados fora do horário comercial.

Equipe de TI: Implantar as ferramentas de monitoramento nos servidores e redes do órgão e apoiar a resolução de problemas técnicos que impeçam a visibilidade dos sistemas.

Equipe de Comunicação: Preparar protocolos de comunicação para informar ao público interno e externo sobre possíveis indisponibilidades preventivas geradas por ações de contenção.

Equipe Jurídica: Analisar os contratos de serviços de monitoramento externo e garantir o amparo legal para as ações de bloqueio e contenção de ameaças em tempo real.

ETIR: Deve ser notificada imediatamente pelo serviço de monitoramento sobre qualquer alerta de alta criticidade detectado; a partir daí, deve coordenar a resposta ao incidente, validar a ameaça, isolar os sistemas afetados e realizar o reporte oficial aos órgãos de controle e segurança cibernética do Governo Federal.

Usuários: Aderir às soluções propostas e reportar imediatamente à ETIR qualquer comportamento anômalo em seus equipamentos, especialmente em períodos fora do horário de expediente.

4.7. Criar, proteger e testar cópias de segurança (Backup)

Por que esse controle é crítico?

Para a segurança de qualquer órgão, garantir que as informações estejam disponíveis é tão importante quanto mantê-las em sigilo. Os ataques modernos de ransomware (vírus de sequestro de dados) evoluíram: hoje, os criminosos não apenas bloqueiam os sistemas, mas tentam ativamente destruir as cópias de segurança para forçar o pagamento do resgate. Manter cópias isoladas e imutáveis — ou seja, protegidas de forma que ninguém, nem mesmo um administrador com acessos totais, consiga alterá-las ou apagá-las — é o que diferencia uma recuperação rápida de uma paralisação catastrófica. Uma estratégia de recuperação sólida e testada reduz drasticamente os impactos no dia a dia e elimina o risco de perda total dos dados críticos pelo órgão.

Para garantir a sobrevivência das informações, a segurança moderna exige que o órgão mantenha pelo menos três cópias dos dados, armazenadas em dois tipos de mídias diferentes. Além disso, é fundamental que uma dessas cópias seja guardada fora do ambiente físico da instituição e outra seja mantida em um formato imutável, que impede qualquer tipo de alteração. Por fim, todo esse processo deve resultar em zero erros, o que é garantido por meio de testes constantes de restauração para confirmar que o serviço público pode ser restabelecido em minutos.

Táticas do framework MITRE ATT&CK associadas

Impacto (Link de acesso: MITRE ATT&CK - Impact)

Medidas PPSI associadas

5.4 - O órgão limita os privilégios de administrador às contas de administrador dedicadas?

6.5 - O órgão exige autenticação multifator (Multi-Factor Authentication, MFA) para acesso administrativo?

11.1 - O órgão estabelece e mantém um processo de realização de cópias de segurança (backup)?

11.3 - O órgão protege os dados de recuperação?

11.4 - O órgão estabelece e mantém uma instância isolada de dados de recuperação?

11.5 - O órgão testa a recuperação dos dados?

Procedimentos e ferramentas

Estabelecer um processo de realização de cópias de segurança, mapeando dados e soluções de software críticas para definir os critérios de priorização de recuperação. Saiba mais no anexo 31

Configurar pelo menos uma cópia imutável (ex.: tecnologias WORM - Write-Once-Read-Many ou Object Lock em nuvem), garantindo proteção dos dados de recuperação com controles rigorosos. Saiba mais no anexo 32

Criar e manter pelo menos uma instância isolada dos dados de recuperação, como um destino em nuvem segregada, cofre digital ou datacenter separado (offsite). Saiba mais no anexo 33

Realizar testes regulares (ex.: trimestrais) de integridade do backup, executando processos práticos de restauração e documentando a eficácia e o tempo de recuperação. Saiba mais no anexo 34

Estruturar um processo de configuração segura, mantendo imagens padronizadas (Golden Images) ou infraestrutura como código (IaC) de servidores e ativos críticos para viabilizar uma reconstrução sistêmica rápida. Saiba mais no anexo 35

Garantir que os consoles de gerenciamento de backup possuam contas de administrador estritamente dedicadas (segregadas do serviço de diretório principal) e protegidas compulsoriamente por autenticação multifator (MFA). Saiba mais no anexo 36

Papéis e Responsabilidades:

Alta Administração: Apoio estratégico e fornecimento de recursos para a implementação de infraestrutura de backup de alta disponibilidade e tecnologias de imutabilidade.

Gestor de Tecnologia da Informação e Comunicação: Prover os recursos de armazenamento e garantir que as políticas de backup estejam integradas ao plano de continuidade de negócios do órgão.

Gestor de Segurança da Informação: Planejar e gerenciar as políticas de proteção de dados, definindo os requisitos de retenção e a frequência das cópias de segurança.

Encarregado pelo Tratamento de Dados Pessoais: Validar se as cópias de segurança cumprem as normas de proteção de dados pessoais e se o descarte de backups antigos segue a legislação vigente.

Responsável Setorial pela Gestão da Integridade: Apoiar a definição de salvaguardas que impeçam a destruição intencional de backups por agentes internos.

Responsável pela Unidade de Gestão de Pessoas: Promover a conscientização sobre a importância de salvar dados institucionais apenas em locais alcançados pelo backup oficial.

Equipe de TI: Implantar e gerenciar as tecnologias de backup, executar as rotinas de cópia e realizar os testes periódicos de restauração para garantir a integridade dos dados.

Equipe de Comunicação: Informar as unidades do órgão sobre janelas de manutenção e os procedimentos de recuperação em caso de necessidade.

Equipe Jurídica: Analisar os contratos de armazenamento (especialmente em nuvem) e garantir que atendam às exigências de soberania e custódia de dados públicos.

ETIR: Deve ser notificada imediatamente caso ocorra qualquer falha crítica nas rotinas de backup ou suspeita de tentativa de deleção de cópias por agentes maliciosos; a partir daí, deve investigar possíveis intrusões e validar a integridade das cópias restantes para suportar a resposta a incidentes.

Usuários: Aderir às soluções propostas, utilizando exclusivamente os sistemas e pastas oficiais do órgão para salvar documentos de trabalho, garantindo que suas informações estejam protegidas pelo backup institucional.

4.8. Implementar segurança em camadas de rede

Por que esse controle é crítico?

Em redes onde todos os computadores e servidores estão conectados sem nenhuma barreira, um único dispositivo infectado pode espalhar um vírus rapidamente por toda a estrutura. Esse fenômeno é conhecido como “movimentação lateral”: o Ransomware entra por uma estação de trabalho comum e, em poucos minutos, consegue alcançar os servidores centrais, sistemas críticos e até as cópias de segurança do órgão.

A solução é organizar a rede em camadas ou compartimentos, como se fossem as salas de um prédio com portas de segurança entre elas. Ao adotar essa arquitetura, o órgão delimita o alcance de um possível ataque.

Se um computador for invadido, o impacto fica isolado naquela “sala”, protegendo os sistemas vitais e garantindo que os serviços essenciais prestados ao cidadão continuem funcionando enquanto o problema é resolvido.

Táticas do framework MITRE ATT&CK associadas

Descoberta (Discovery - MITRE ATT&CK)

Movimentação Lateral (Lateral Movement- MITRE ATT&CK)

Medidas PPSI associadas

3.12 - O órgão segmenta o processamento e o armazenamento de dados com base na criticidade?

4.5 - O órgão implementa e gerencia um firewall em dispositivos do usuário final?

11.4 - O órgão estabelece e mantém uma instância isolada de dados de recuperação?

12.1 - O órgão mantém atualizada a infraestrutura de rede?

12.2 - O órgão estabelece e mantém uma arquitetura de rede segura?

13.4 - O órgão realiza filtragem de tráfego entre os segmentos de rede?

Procedimentos e ferramentas

Projetar e manter uma arquitetura de rede segura abordando segmentação e privilégio mínimo, separando a infraestrutura em VLANs por função específica (ex.: servidores, dispositivos de usuário final, dispositivos IoT e rede de visitantes). Saiba mais no anexo 37

Realizar a filtragem de tráfego entre os segmentos de rede, bloqueando ativamente a comunicação de protocolos de alto risco frequentemente utilizados para movimentação lateral (como RDP, SMB, WMI e PsExec). Saiba mais no anexo 38

Estabelecer e manter uma instância isolada dos dados de recuperação, segregando a rede de cópias de segurança em um segmento próprio com acesso restrito e protegido. Saiba mais no anexo 39

Implementar e gerenciar um firewall baseado em host nos dispositivos de usuário final, com regra de negação padrão, restringindo severamente a comunicação lateral direta entre estações de trabalho. Saiba mais no anexo 40

Isolar ativos institucionais e infraestruturas de rede legadas que não possam ser plenamente atualizados, alocando-os em segmentos de rede altamente restritos para conter a exploração de vulnerabilidades. Saiba mais no anexo 41

Papéis e Responsabilidades:

Alta Administração: Apoio estratégico e fornecimento de recursos para a modernização da infraestrutura de rede e aquisição de equipamentos de proteção.

Gestor de Tecnologia da Informação e Comunicação: Prover os recursos técnicos necessários e assegurar que o desenho da rede suporte às necessidades operacionais do órgão com segurança.

Gestor de Segurança da Informação: Planejar e gerenciar a estratégia de segmentação, definindo quais áreas da rede devem ser isoladas e quem possui permissão para transitar entre elas.

Encarregado pelo Tratamento de Dados Pessoais: Orientar sobre a segregação de ambientes que tratam dados sensíveis, garantindo que o acesso a essas camadas seja restrito e auditável.

Responsável Setorial pela Gestão da Integridade: Apoiar a definição de controles que impeçam o acesso não autorizado a sistemas críticos por usuários com diferentes níveis de responsabilidade.

Responsável pela Unidade de Gestão de Pessoas: Comunicar aos servidores sobre as políticas de uso da rede e a importância de respeitar os limites de acesso entre diferentes setores.

Equipe de TI: Implantar e gerenciar as tecnologias de rede, configurando filtros de tráfego e garantindo que as divisões entre os departamentos estejam operacionais.

Equipe de Comunicação: Divulgar as mudanças na estrutura de acesso à rede para minimizar impactos na percepção dos servidores sobre a agilidade dos sistemas.

Equipe Jurídica: Analisar os impactos normativos da restrição de acesso a sistemas e garantir que as políticas de rede estejam em conformidade com as diretrizes de segurança do governo.

ETIR: Deve ser notificada imediatamente sobre qualquer tentativa de violação de perímetros de rede ou comunicações anômalas entre setores isolados; a partir do aviso, deve realizar a contenção técnica, bloquear os caminhos de movimentação lateral e investigar a origem da tentativa de invasão.

Usuários: Aderir às soluções propostas, utilizando exclusivamente os caminhos de acesso autorizados e compreendendo que a separação de redes é uma medida de proteção institucional.

4.9. Gerenciar contas e acessos administrativos

Por que esse controle é crítico?

A maioria dos ataques digitais começa de forma silenciosa, invadindo a conta de um usuário comum. A partir daí, o criminoso tenta “subir de nível” até conseguir acessos de administrador. Se ele atingir esse objetivo, o impacto é total: o invasor passa a ter o poder de desligar as defesas (como o antivírus), apagar as cópias de segurança (backups) e espalhar o vírus por todos os computadores do órgão.

Para evitar que isso aconteça, é fundamental aplicar o controle rigoroso de quem pode acessar o quê. Ao limitar as permissões para que cada servidor tenha apenas o necessário para realizar seu trabalho (o chamado “privilégio mínimo”), cortamos o caminho do invasor. Sem acessos de superusuário, o criminoso perde a

capacidade de dominar a infraestrutura, impedindo que um incidente isolado se torne um desastre generalizado que interrompa a prestação de serviços públicos.

Táticas do framework MITRE ATT&CK associadas

Escalação de Privilégios (Privilege Escalation - MITRE ATT&CK)

Acesso a Credenciais (Credential Access - MITRE ATT&CK)

Medidas PPSI associadas

4.7 - O órgão gerencia contas padrão?

5.1 - O órgão estabelece e mantém um inventário de contas?

5.3 - O órgão desabilita ou exclui contas inativas?

5.4 - O órgão limita os privilégios de administrador às contas de administrador dedicadas?

5.5 - O órgão estabelece e mantém um inventário de contas de serviço?

6.1 - O órgão estabelece um processo de concessão de acesso?

6.2 - O órgão estabelece um processo de revogação de acesso?

6.8 - O órgão define e mantém o controle de acesso baseado em funções?

12.8 - O órgão utiliza e mantém recursos computacionais dedicados para todas as atividades administrativas de TI?

Procedimentos e ferramentas

Estabelecer e manter o inventário contínuo de contas de usuários e contas de serviço, realizando auditorias regulares para remover acessos administrativos desnecessários ou esquecidos. Saiba mais no anexo 42

Limitar os privilégios de administrador estritamente a contas de administrador dedicadas. Atividades gerais (como navegação na internet e leitura de e-mails corporativos) devem ser realizadas exclusivamente pela conta primária não privilegiada do usuário. Saiba mais no anexo 43

Remover direitos de administrador local nos dispositivos de usuário final, restringindo modificações indevidas no sistema operacional. Saiba mais no anexo 44

Estabelecer processos ágeis de concessão e revogação de acesso lógico aos ativos, preferencialmente automatizando o modelo de acesso Just-In-Time (JIT) para limitar a janela temporal em tarefas administrativas. Saiba mais no anexo 45

Gerenciar adequadamente contas padrão nos ativos institucionais (como administrador local), desabilitando-as ou utilizando soluções de randomização de credenciais. Saiba mais no anexo 46

Estabelecer e manter recursos computacionais dedicados (física ou logicamente isolados da rede primária) para tarefas administrativas, garantindo que contas altamente privilegiadas nunca se autentiquem em estações de trabalho de uso comum. Saiba mais no anexo 47

Papéis e Responsabilidades:

Alta Administração: Apoio estratégico e fornecimento de recursos para a implementação de sistemas de gestão de identidades e ferramentas de controle de acesso privilegiado.

Gestor de Tecnologia da Informação e Comunicação: Prover as ferramentas tecnológicas que permitam a segregação de funções e a administração segura das contas do órgão.

Gestor de Segurança da Informação: Planejar e gerenciar as políticas de acesso, definindo os perfis de usuários e revisando periodicamente quem possui permissões administrativas.

Encarregado pelo Tratamento de Dados Pessoais: Fiscalizar se o acesso a dados pessoais está limitado apenas a quem possui necessidade legal e administrativa para tratá-los.

Responsável Setorial pela Gestão da Integridade: Atuar na prevenção de abusos de autoridade digital e monitorar possíveis conflitos de interesse na concessão de acessos especiais.

Responsável pela Unidade de Gestão de Pessoas: Informar prontamente à TI sobre movimentações de pessoal, como exonerações ou transferências, para a revogação imediata de acessos.

Equipe de TI: Implantar e gerenciar as configurações de contas, garantindo que usuários comuns não possuam privilégios de administrador em suas estações de trabalho.

Equipe de Comunicação: Orientar os servidores sobre a importância de não compartilhar senhas e os riscos de utilizar contas com altos privilégios para tarefas rotineiras.

Equipe Jurídica: Assessorar na elaboração de termos de responsabilidade para detentores de contas administrativas e analisar as implicações legais de acessos indevidos.

ETIR: Deve ser notificada imediatamente sobre qualquer tentativa de “escalada de privilégio” (quando um usuário tenta obter poderes de administrador sem autorização); a partir do aviso, deve suspender a conta suspeita, investigar a atividade e auditar o rastro deixado pelo possível invasor.

Usuários: Aderir às soluções propostas, utilizando exclusivamente suas contas nominais e compreendendo que a limitação de privilégios é uma medida de proteção para o próprio servidor e para o órgão.

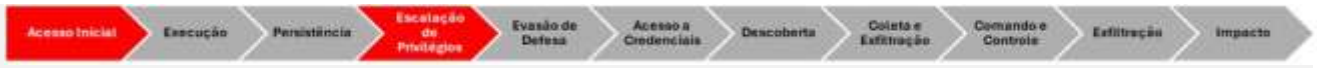
4.10. Gerenciar e corrigir falhas em sistemas

Por que esse controle é crítico?

Na prática, é inviável atualizar todos os sistemas e equipamentos de um órgão simultaneamente. Como os criminosos digitais buscam constantemente brechas (falhas) conhecidas para invadir a administração pública, o segredo do sucesso não é apenas atualizar tudo, mas corrigir as falhas certas com máxima agilidade.

A prioridade deve ser fechar as brechas em sistemas que estão expostos à internet e aquelas que já sabemos que estão sendo exploradas por atacantes no mundo real, como as listadas no catálogo KEV da CISA, que funciona como um alerta global de falhas críticas. Complementarmente, o órgão utiliza técnicas de "blindagem" (o chamado hardening), que configuram os sistemas de forma mais rígida e restringem comandos automáticos. Isso bloqueia a ação de vírus e impede que eles se espalhem pela rede, mesmo antes de o fabricante lançar uma correção definitiva.

Táticas do framework MITRE ATT&CK associadas



Escalação de Privilégios (Privilege Escalation - MITRE ATT&CK)

Acesso Inicial (Initial Access - MITRE ATT&CK)

Medidas PPSI associadas

2.5 - O órgão possui uma lista de soluções de software autorizadas?

2.7 - O órgão possui uma lista de scripts autorizados?

4.1 - O órgão estabelece e mantém um processo de configuração segura?

4.8 - O órgão desinstala ou desativa serviços desnecessários?

7.2 - O órgão estabelece e mantém um processo de remediação?

7.6 - O órgão realiza varreduras automatizadas de vulnerabilidades expostas externamente?

7.7 - O órgão corrige vulnerabilidades detectadas?

8.8 - O órgão coleta logs de auditoria de linha de comando?

Procedimentos e ferramentas

Estabelecer um processo de remediação fundamentado em risco, priorizando a correção de vulnerabilidades em ativos institucionais e soluções de software expostos externamente (como portais web, appliances de VPN e firewalls). Saiba mais no anexo 48

Priorizar a correção de falhas listadas em catálogos de vulnerabilidades ativamente exploradas (ex.: KEV - Known Exploited Vulnerabilities). Saiba mais no anexo 49

Focar na aplicação ágil de atualizações em servidores de correio eletrônico e sistemas que possuam serviços de acesso remoto habilitados (ex.: RDP). Saiba mais no anexo 50

Ações de Mitigação Imediatas (Quick Wins):

Elaborar uma lista de scripts autorizados e implementar controles técnicos para bloquear a execução de macros em arquivos oriundos da internet e de scripts não assinados digitalmente. Saiba mais no anexo 51

Implementar controles técnicos rigorosos (como AppLocker ou listas de soluções de software permitidas) para impedir a execução de softwares e scripts não autorizados, inclusive a partir de pastas temporárias. Saiba mais no anexo 52

Estabelecer um processo de configuração segura e desativar serviços e protocolos de rede desnecessários, legados ou inerentemente inseguros (ex.: SMBv1, LLMNR e NetBIOS). Saiba mais no anexo 53

Atualizar as ferramentas de linha de comando (ex.: PowerShell) e habilitar compulsoriamente a coleta de logs de auditoria sobre a sua utilização, a fim de identificar comportamentos anômalos. Saiba mais no anexo 54

Papéis e Responsabilidades:

Alta Administração: Apoio estratégico e fornecimento de recursos para a substituição de sistemas obsoletos e aquisição de ferramentas de gestão de vulnerabilidades.

Gestor de Tecnologia da Informação e Comunicação: Prover a infraestrutura necessária para a automação de atualizações e assegurar que a manutenção dos sistemas não interrompa a prestação de serviços públicos.

Gestor de Segurança da Informação: Planejar e gerenciar o cronograma de correções, priorizando falhas críticas com base em inteligência de ameaças e no catálogo KEV da CISA.

Encarregado pelo Tratamento de Dados Pessoais: Monitorar se as falhas de segurança corrigidas poderiam ter exposto dados pessoais e avaliar a necessidade de notificações legais.

Responsável Setorial pela Gestão da Integridade: Acompanhar o cumprimento dos prazos de atualização para garantir que a omissão na correção de falhas não se torne um risco à integridade institucional.

Responsável pela Unidade de Gestão de Pessoas: Facilitar a comunicação sobre paradas programadas para manutenção, garantindo que os servidores estejam cientes das atualizações em seus equipamentos.

Equipe de TI: Implantar as correções de software e aplicar as configurações de “blindagem” (hardening) nos servidores e estações de trabalho do órgão.

Equipe de Comunicação: Informar ao público interno e externo sobre janelas de manutenção necessárias para a segurança dos sistemas governamentais.

Equipe Jurídica: Analisar contratos de licenciamento e suporte para garantir que os fornecedores de software cumpram prazos adequados para o envio de correções.

ETIR: Deve ser notificada imediatamente quando uma vulnerabilidade crítica for detectada em sistemas expostos ou quando uma correção falhar; a partir do aviso, deve monitorar sinais de exploração dessa falha e propor medidas de contenção emergencial até que o sistema seja devidamente atualizado.

Usuários: Aderir às soluções propostas, permitindo a instalação de atualizações em seus computadores e reiniciando os dispositivos sempre que solicitado pela equipe técnica para garantir a eficácia da proteção.

4.11. Mapear sistemas críticos e assegurar a continuidade de sua operação

Por que esse controle é crítico?

Para proteger eficazmente o órgão e garantir que ele suporte ataques digitais, é preciso conhecer a fundo quais tecnologias fazem o "coração" da instituição bater. Em um cenário de ataque por ransomware, o caos pode fazer com que a equipe tente restaurar os sistemas na ordem errada — como tentar ligar as luzes de uma sala antes de garantir que o prédio tenha energia. Sem entender como um sistema depende do outro, o processo de recuperação pode falhar e causar uma paralisação ainda mais longa dos serviços públicos. O mapeamento detalhado de todos os ativos e a classificação do que é mais urgente garantem que o órgão tenha um roteiro claro de sobrevivência. Ao definir quais serviços devem voltar primeiro e por quanto tempo a instituição suporta ficar sem eles, criamos uma ponte entre a expectativa da alta administração e a realidade da equipe técnica. Isso evita que um incidente digital se torne uma interrupção definitiva dos serviços prestados ao cidadão.

Táticas do framework MITRE ATT&CK associadas

Reconhecimento (Reconnaissance - MITRE ATT&CK)

Exfiltração (Exfiltration - MITRE ATT&CK)

Medidas PPSI associadas

0.14 - O órgão possui um processo de gestão de continuidade de negócios em segurança da informação?

1.1 - O órgão estabelece e mantém um inventário detalhado de ativos institucionais?

3.7 - O órgão estabelece e mantém um esquema de classificação de dados?

3.8 - O órgão documenta os fluxos de dados?

11.1 - O órgão estabelece e mantém um processo de realização de cópias de segurança (backup)?

11.4 - O órgão estabelece e mantém uma instância isolada de dados de recuperação?

12.4 - O órgão elabora e mantém diagramas de arquitetura?

Procedimentos e ferramentas

Estabelecer e manter o inventário preciso e detalhado de ativos institucionais e soluções de software, identificando claramente os proprietários, as unidades organizacionais e aprovando os sistemas críticos de negócio. Saiba mais no anexo 55

Estabelecer e manter um esquema geral de classificação de dados fundamentado na criticidade para a organização, avaliando o impacto imediato da indisponibilidade sistêmica na operação. Saiba mais no anexo 56

Elaborar e manter diagramas da arquitetura de rede e documentar o fluxo de dados, garantindo a rastreabilidade estrutural para identificar pontos únicos de falha e dependências vitais (ex.: vínculo entre sistemas de gestão, bancos de dados e serviços de resolução de nomes DNS). Saiba mais no anexo 57

Integrar o processo de gestão de continuidade de negócios em segurança da informação, definindo junto às áreas de negócio as métricas de Tempo de Recuperação (RTO) e Ponto de Recuperação (RPO), a fim de estabelecer os critérios de priorização no processo de recuperação de cópias de segurança (backups). Saiba mais no anexo 58

Assegurar que as documentações estratégicas (planos de continuidade, inventários e diagramas) sejam mantidas em uma instância isolada e de acesso restrito (como um sistema off-line ou ambiente segregado em nuvem), garantindo disponibilidade total da informação para a equipe de crise mesmo em caso de comprometimento da rede corporativa principal. Saiba mais no anexo 59

Papéis e Responsabilidades:

Alta Administração: Apoio estratégico e fornecimento de recursos para o mapeamento de processos e validação das prioridades de continuidade do órgão.

Gestor de Tecnologia da Informação e Comunicação: Prover o inventário atualizado de ativos e assegurar que a arquitetura tecnológica suporte a ordem de restauração definida.

Gestor de Segurança da Informação: Planejar e gerenciar a classificação dos sistemas por criticidade, estabelecendo os tempos máximos permitidos para recuperação de cada serviço.

Encarregado pelo Tratamento de Dados Pessoais: Identificar quais sistemas críticos tratam dados pessoais para garantir que sua recuperação priorize também a proteção à privacidade.

Responsável Setorial pela Gestão da Integridade: Zelar para que o mapeamento de sistemas considere os riscos de interrupção em processos sensíveis à integridade pública.

Responsável pela Unidade de Gestão de Pessoas: Auxiliar na identificação das competências e das equipes necessárias para operar os sistemas críticos durante regimes de contingência.

Equipe de TI: Implantar as ferramentas de monitoramento de ativos e executar tecnicamente a ordem de prioridade na restauração dos serviços.

Equipe de Comunicação: Informar à sociedade e aos demais órgãos sobre a previsão de retorno dos serviços, baseando-se no mapeamento de prioridades.

Equipe Jurídica: Analisar os impactos contratuais e legais da indisponibilidade de sistemas críticos e a conformidade dos planos de continuidade.

ETIR: Deve ser notificada imediatamente sobre qualquer indisponibilidade em sistemas classificados como críticos; a partir do aviso, deve avaliar se a falha é fruto de um ataque, orientar a ordem de contenção baseada na criticidade mapeada e monitorar a recuperação para evitar que ameaças persistam nos sistemas restaurados.

Usuários: Aderir às soluções propostas, auxiliando na identificação de sistemas vitais para suas atividades e reportando falhas conforme o impacto percebido no serviço público.

Será que estamos sofrendo um ataque de *Ransomware*?

[Detecção e Análise].

Capítulo 5.

A adoção de uma estratégia de contenção incorreta, tardia ou ineficaz.

Risco Principal

Visão geral

A fase de detecção e análise é um dos momentos mais críticos e desafiadores da resposta a incidentes. Para ser eficaz, ela não deve depender apenas da espera passiva por alertas de sistemas, mas incorporar uma postura proativa de proteção. Isso envolve o monitoramento contínuo e a busca ativa por ameaças (Threat Hunting), visando identificar comportamentos anômalos, credenciais comprometidas e movimentação lateral antes que o ransomware seja executado em larga escala.

Uma vez identificado o evento (seja de forma proativa ou reativa), a análise inicial serve para mensurar de forma correta a magnitude, o vetor de entrada e os impactos reais do incidente. É através dessa inteligência que a equipe obtém as informações necessárias para definir as atividades de contenção e mitigação.

No caso de um ransomware, em que a própria sobrevivência operacional do órgão pode estar em risco, as consequências de uma detecção tardia ou de uma análise inadequada podem levar a:

- **Falha crítica na contenção e agravamento de danos:** As estratégias de contenção de um ransomware podem exigir decisões de alto impacto, como a desativação temporária ou permanente de infraestruturas vitais e o isolamento de redes. Se a análise errar o escopo e não identificar corretamente os sistemas comprometidos, a equipe poderá aplicar a estratégia errada no momento inadequado, causando interrupções de serviço desnecessárias ou, pelo contrário, não agindo a tempo de impedir que a criptografia atinja sistemas essenciais e servidores de backup.

- **Incapacidade de erradicação e recuperação:** Se não for feita uma análise precisa do vetor de ataque e de quais contas, vulnerabilidades ou arquivos foram comprometidos, a fase de erradicação será falha. Resquícios do malware permanecerão na rede, impedindo uma restauração segura dos dados e abrindo brechas para reincidência logo após o restabelecimento do ambiente.
- **Descontrole da crise e dano reputacional:** Os ataques de ransomware modernos frequentemente envolvem dupla extorsão (roubo de dados aliado ao sequestro de sistemas). Se a análise técnica falhar e não confirmar os fatos com precisão para classificar a gravidade, não haverá como tomar decisões proporcionais ao risco. Sem a correta dimensão do problema, as respostas serão confusas, a organização perderá o controle da narrativa perante o público, resultando em danos incalculáveis à reputação e na violação de obrigações legais (LGPD, por exemplo).

A seguir listamos ações imprescindíveis para que a organização detecte e analise os incidentes de forma proativa, ágil e acurada.

5.1. Criar um plano de ação para incidentes

Detecção: Parece que fomos atacados

CONFIRME QUE É REAL!
Nem toda tela estranha é ransomware — e alguns atacantes blefam.

Nem todo problema técnico ou tela estranha no computador significa que o órgão está sob um ataque de ransomware. Existem falhas comuns de sistema e até atacantes que “blefam” para tentar extorquir instituições. A fase de detecção é o filtro que separa um simples erro técnico de uma crise real.

O risco de não possuir um processo de detecção claro é duplo: por um lado, o órgão pode entrar em pânico e paralisar serviços essenciais sem necessidade; por outro, pode ignorar sinais sutis de uma invasão real, permitindo que o vírus se espalhe silenciosamente até que seja tarde demais. Saber identificar os “rastros” corretos garante que a resposta seja proporcional e certeira.

Medidas PPSI associadas
8.5 - O órgão coleta logs de auditoria detalhados?
8.8 - O órgão coleta logs de auditoria de linha de comando?
10.1 - O órgão instala e mantém um software antimalware?
10.7 - O órgão utiliza software antimalware baseado em comportamento?
13.1 - O órgão centraliza alertas de eventos de segurança?

13.6 - O órgão coleta logs de fluxo de tráfego de rede?

17.4 - O órgão estabelece e mantém um processo de gestão de incidentes de segurança da informação?

17.5 - O órgão atribui funções e responsabilidades para gestão de incidentes?

17.9 - O órgão estabelece a diferença entre evento e incidente de segurança da informação?

Verifique os itens abaixo, eles são possíveis indicativos de um ataque de ransomware:

1. Arquivos com extensões alteradas (.crypt, .locked, .encrypted, extensões aleatórias)
2. Notas de resgate em pastas ou na área de trabalho
3. Renomeação em massa de arquivos
4. Shadow copies deletadas (checar: vssadmin list shadows)
5. Logs mostram execução anômala de PowerShell, PsExec ou ferramentas de compressão
6. Tráfego de saída incomum (grandes volumes para IPs desconhecidos)
7. Alertas do EDR/antivírus ignorados ou desabilitados
8. Logins em horários ou locais atípicos

Saiba mais no anexo 60

O acionamento da resposta a incidentes não deve ser uma regra matemática rígida baseada na quantidade de indicadores, mas sim um funil de escalonamento flexível guiado pelo contexto da ameaça, pela criticidade do sistema afetado e pelo julgamento técnico da sua equipe.

Se confirmado, ative o Plano de Resposta a Incidentes imediatamente, observe as Obrigações Legais e acione o Plano de Comunicação.

Papéis e Responsabilidades:

Alta Administração: Apoio estratégico e fornecimento de recursos para a manutenção de ferramentas de detecção e auditoria (logs).

Gestor de Tecnologia da Informação e Comunicação: Garantir que todos os sistemas e redes gerem registros de eventos (logs) detalhados e centralizados, conforme as normas do PPSI (medidas 8.5, 8.8 e 13.6).

Gestor de Segurança da Informação: Planejar e gerenciar os critérios que diferenciam um evento comum de um incidente real (medida 17.9) e garantir que o software antimalware baseado em comportamento esteja ativo (medidas 10.1 e 10.7).

Encarregado pelo Tratamento de Dados Pessoais: Manter-se de prontidão para avaliar se a detecção inicial indica risco de exposição de dados pessoais dos cidadãos.

Responsável Setorial pela Gestão da Integridade: Auxiliar na análise de alertas que possam sugerir o uso indevido de credenciais por colaboradores internos.

Responsável pela Unidade de Gestão de Pessoas: Facilitar o contato com servidores cujos equipamentos apresentem alertas, para validar se a atividade detectada foi legítima ou não.

Equipe de TI: Manter a infraestrutura de detecção operacional, assegurando que os alertas cheguem às centrais de monitoramento sem atrasos.

Equipe de Comunicação: Preparar-se para agir caso a detecção seja confirmada como incidente, seguindo o Plano de Comunicação pré-estabelecido.

Equipe Jurídica: Assessorar na verificação das obrigações legais que surgem no exato momento em que um incidente de segurança é confirmado.

ETIR: Deve ser notificada imediatamente assim que qualquer servidor ou sistema de monitoramento detectar um sinal de alerta; a partir daí, deve realizar a triagem técnica, verificar a veracidade do ataque (usando ferramentas como o vssadmin para checar cópias de sombra ou analisando tráfego de rede) e, se confirmado, ativar formalmente o Plano de Resposta a Incidentes (PPSI 17.4).

Usuários: Reportar imediatamente à ETIR qualquer comportamento estranho em seu computador (como arquivos que mudaram de ícone ou nome), abstendo-se de tentar resolver o problema ou desligar o equipamento sem orientação.

4.1. Há algo errado, o que fazer?

Análise

Após detectar que algo está errado, o próximo passo crucial é a análise. Tentar resolver um problema sem entender sua origem ou extensão é como tentar apagar um incêndio sem saber o que está queimando. Se o órgão pular esta etapa, pode acabar restaurando sistemas que ainda contêm o vírus, causando uma nova infecção, ou pior: pode não perceber que dados sensíveis de cidadãos foram roubados, gerando graves consequências legais.

A análise permite identificar o “Vetor de Entrada” (como o invasor entrou), quais sistemas foram afetados e, principalmente, se houve a saída de dados (exfiltração). Além disso, verificar a variante do vírus pode revelar que já existe uma “vacina” (ferramenta de descriptografia gratuita), economizando dias de trabalho e evitando o colapso dos serviços.

Medidas PPSI associadas
1.1 - O órgão estabelece e mantém um inventário detalhado de ativos institucionais?
8.8 - O órgão coleta logs de auditoria de linha de comando?
8.11 - O órgão conduz revisões de logs de auditoria?
13.6 - O órgão coleta logs de fluxo de tráfego de rede?
17.4 - O órgão estabelece e mantém um processo de gestão de incidentes de segurança da informação?

17.5 - O órgão atribui funções e responsabilidades para gestão de incidentes?

19.4 - O órgão inclui no registro das operações de tratamento de dados pessoais os tipos de dados tratados e as categorias de titulares?

20.1 - O órgão implementa processo de gestão de incidentes com dados pessoais?

Verifique os itens abaixo, eles são possíveis indicativos de um ataque de ransomware:

1. Determinar quais sistemas foram criptografados e quais estão intactos (Checagem dupla). Importante: Identificar qual o backup mais recente íntegro.
2. Verificar se houve exfiltração de dados (logs de tráfego de saída, ferramentas como rclone, WinSCP, megacmd)
3. Identificar o vetor de entrada provável (phishing, VPN comprometida, RDP exposto, vulnerabilidade explorada)
4. Entendimento e registro da linha do tempo do incidente
5. Verificar se dados pessoais foram comprometidos (aciona obrigações da LGPD) (Guia de resposta a incidentes com dados pessoais)
6. Identificar a variante do ransomware:

   ID Ransomware: https://id-ransomware.malwarehunterteam.com/

   No More Ransom / Crypto Sheriff: https://www.nomoreransom.org/crypto-sheriff.php
7. Verificar se existe ferramenta de descriptografia gratuita disponível

5.2. Notificações obrigatórias

A transparência e o dever de informar não são apenas boas práticas, são obrigações legais rigorosas. Um ataque de ransomware não é um problema isolado da TI; ele gera um dever de resposta perante órgãos de controle e, principalmente, perante o cidadão.

O risco de omitir ou atrasar essas notificações é altíssimo: o órgão pode sofrer sanções administrativas pesadas da ANPD (multas e suspensão de sistemas), além de enfrentar danos irreparáveis à reputação institucional e possíveis processos judiciais por parte dos titulares dos dados. Notificar corretamente e dentro dos prazos demonstra que a instituição possui governança e responsabilidade com o patrimônio público e a privacidade.

Medidas PPSI associadas

17.2 - O órgão estabelece e mantém informações de contato para notificar incidentes?

17.4 - O órgão estabelece e mantém um processo de gestão de incidentes de segurança da informação?

17.5 - O órgão atribui funções e responsabilidades para gestão de incidentes?

19.4 - O órgão inclui no registro das operações de tratamento de dados pessoais os tipos de dados tratados e as categorias de titulares?

20.1 - O órgão implementa processo de gestão de incidentes com dados pessoais?

21.1 - O órgão provê os meios necessários para que o encarregado exerça suas atividades e atribuições?

21.2 - O órgão disponibiliza meios céleres, eficazes e adequados para viabilizar a comunicação dos titulares com o encarregado e o exercício de direitos?

Órgãos para Notificação obrigatória:

CISC gov.br - notificar de forma célere o órgão através do site https://www.gov.br/cisc/pt-br/notificar-incidente-cibernetico ou através do e-mail **cisc@gestao.gov.br.**

CTIR Gov - Formulário eletrônico no portal do CTIR Gov (https://gov.br/ctir) ou, em casos de indisponibilidade, através do e-mail oficial **ctir@ctir.gov.br** (Requer envio de artefatos e IoCs).

Polícia Federal - para crimes de jurisdição federal (https://apps.pf.gov.br/r/comunicapf/)

Após analisar a extensão do incidente, verificar as obrigações legais atreladas.

Órgãos para Notificação obrigatória:

Se dados pessoais foram comprometidos (acessados, exfiltrados ou tornados indisponíveis), a LGPD exige notificação.

Prazo: 3 dias úteis a partir da ciência de que dados pessoais foram afetados. Agentes de pequeno porte: 6 dias úteis. (Resolução CD/ANPD nº 15/2024)

Para quem notificar:

- ANPD — via formulário de CIS no sistema SEI! (https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis)
- Titulares de dados afetados — comunicação individualizada e direta

O que a notificação deve conter:

- Natureza dos dados pessoais afetados
- Número de titulares impactados (ou estimativa)
- Medidas técnicas e de segurança utilizadas
- Riscos e impactos potenciais aos titulares
- Medidas para mitigar os efeitos
- Informações complementares: até 20 dias úteis

Órgãos para Notificação obrigatória:

Multa simples de até **2% do faturamento** (teto de **R$ 50 milhões por infração**), multa diária, publicização da infração, bloqueio ou eliminação de dados, suspensão de atividades de tratamento.

Após a análise e compreensão da extensão do impacto é hora de iniciar a contenção

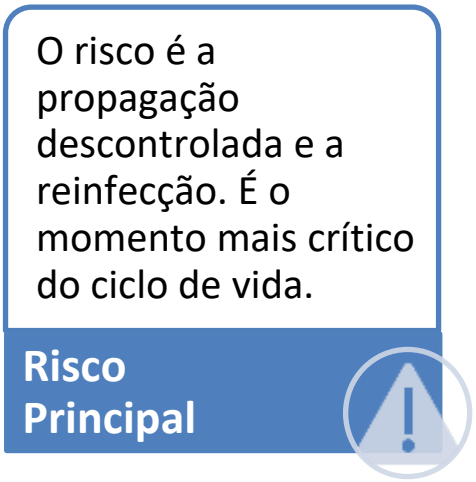
Dica prática: prepare os formulários de notificação ANTES de precisar deles. Mantenha-os no kit de resposta, com dados pré-preenchidos (razão social, CNPJ, contatos do Encarregado).

Papéis e Responsabilidades:
Alta Administração: Apoio estratégico para garantir que o órgão cumpra seu dever de transparência e fornecimento de recursos para que as comunicações aos titulares e órgãos de controle sejam realizadas sem entraves.
Gestor de Tecnologia da Informação e Comunicação: Fornecer os dados técnicos necessários para preencher os formulários de notificação, garantindo que as informações sobre as medidas de segurança adotadas sejam precisas.
Gestor de Segurança da Informação: Coordenar a notificação junto ao CISC gov.br e ao CTIR Gov, enviando os artefatos técnicos e indicadores de invasão (IoCs) coletados (medidas 17.2 e 17.4).
Encarregado pelo Tratamento de Dados Pessoais: Liderar o processo de notificação à ANPD e aos titulares de dados (medida 21.1), avaliando o risco e a natureza dos dados afetados com base no registro de operações (medida 19.4).
Responsável Setorial pela Gestão da Integridade: Acompanhar as notificações para assegurar que a comunicação oficial reflita a realidade dos fatos e mantenha a integridade da imagem do órgão.
Responsável pela Unidade de Gestão de Pessoas: Auxiliar na comunicação individualizada caso os dados afetados pertençam ao corpo funcional do órgão.
Equipe de TI: Manter os meios técnicos (e-mails, sistemas e acessos) operacionais para que as notificações possam ser enviadas de forma célere e segura.
Equipe de Comunicação: Redigir as mensagens direcionadas aos titulares de dados e à sociedade, garantindo que o tom seja adequado, transparente e siga as orientações do Encarregado e da área Jurídica.
Equipe Jurídica: Analisar o conteúdo das notificações para garantir o cumprimento das resoluções da ANPD (como a nº 15/2024) e orientar sobre as possíveis sanções e medidas de mitigação de danos legais.
ETIR: Deve ser notificada imediatamente assim que a análise confirmar o incidente; a partir daí, deve fornecer ao Encarregado e ao Gestor de SI todos os detalhes técnicos (natureza dos dados, número de impactados e riscos potenciais) para o preenchimento imediato dos comunicados de incidente.
Usuários: Cooperar com o fornecimento de informações caso sejam solicitados pela ETIR ou pelo Encarregado durante a fase de apuração do impacto para as notificações.

Fomos atacados! Como agir?

[Conter, Responder e Recuperar].

Capítulo 6.



Princípio central: Cada minuto conta.

Visão geral

Após a confirmação de um incidente, o foco passa a ser a limitação de danos e a restauração dos serviços. O objetivo é equilibrar o rigor técnico com a necessidade de manter o negócio funcionando, garantindo que as decisões de contenção reduzam os prejuízos imediatos e fortaleçam a resiliência da Administração Pública Federal a longo prazo.

Não existe um padrão universal ou guia oficial que estabeleça tempos exatos para a contenção e resolução de um incidente de segurança. Um ataque de ransomware complexo e um alerta falso de antivírus levam tempos drasticamente diferentes para serem resolvidos. O que segue é um protocolo estruturado e acionável. **Adapte ao seu contexto, respeitando a sequência lógica**.

Durante o incidente utilize o checklist (Modelo 7 — Checklist para resposta a incidentes) que está na prateleira de instrumentos.

6.1. Comunicação necessária

Comunicação durante o incidente

Para a equipe interna:

Atualizações factuais a cada 2 horas. Deve-se informar o que aconteceu (no nível adequado), o que está sendo feito, o que cada área deve fazer ou evitar.

Modelo 1 — Comunicação interna durante incidente

Instruções claras:

- Não discutir o incidente em redes sociais
- Não tentar “resolver” por conta própria
- Reportar qualquer comportamento anormal
- Usar canais de comunicação alternativos conforme orientação da equipe de RI

Para clientes, parceiros e fornecedores: Comunicar apenas quando houver informação concreta sobre impacto. Ser factual, breve e demonstrar controle da situação. Modelos de comunicação disponíveis na seção de Templates deste playbook.

6.2. Contendo o incidente

Contenção

A contenção é o momento de “isolar o incêndio” para que ele não destrua o prédio inteiro. Em um ataque de Ransomware, a velocidade é tudo: cada segundo em que o vírus permanece conectado à rede, ele pode estar sequestrando novos arquivos ou enviando dados sigilosos para fora do país. O objetivo aqui é limitar o alcance do invasor e impedir que ele continue sua destruição.

Um aviso crítico para a Alta Gestão: No pânico, a reação natural é querer “puxar a tomada” ou desligar os computadores. Isso é um erro grave. Desligar as máquinas apaga provas fundamentais que estão na memória temporária e pode destruir as únicas chaves que permitiriam recuperar os dados sem pagar resgate. A regra de ouro é: isole da rede, mas mantenha o equipamento ligado.

Esta ação deve ser executada em paralelo com as ações Análise e Preservação de Evidências.

Não desligue as máquinas: A memória volátil contém chaves de criptografia e evidências forenses que serão perdidas. Desconecte da rede, mas as mantenha ligadas.

Medidas PPSI associadas
6.2 - O órgão estabelece um processo de revogação de acesso?
9.2 - O órgão usa serviços de filtragem de Sistema de Nomes de Domínio (Domain Name System, DNS)?
12.2 - O órgão estabelece e mantém uma arquitetura de rede segura?
13.3 - O órgão implanta soluções de detecção de intrusão de rede?
13.4 - O órgão realiza filtragem de tráfego entre os segmentos de rede?
13.8 - O órgão implanta soluções para prevenção de intrusão de rede?
17.2 - O órgão estabelece e mantém informações de contato para notificar incidentes de segurança da informação?
17.3 - O órgão estabelece e mantém um processo institucional para notificar incidentes de segurança da informação?
17.5 - O órgão atribui funções e responsabilidades para gestão de incidentes?

Ações imediatas de contenção
Executar em paralelo:
Desconectar sistemas infectados da rede (cabo ethernet, desabilitar Wi-Fi, isolamento via ferramenta de segurança)
Matar túneis VPN e conexões de acesso remoto
Se múltiplos segmentos estiverem comprometidos, isolar no nível do switch
Desabilitar contas de serviço suspeitas e resetar senhas de contas administrativas
Isolar sistemas críticos que ainda não foram afetados (desconectar preventivamente)
Bloquear IPs e domínios maliciosos conhecidos, ou descobertos, no firewall
Correção de emergência de vulnerabilidades ativamente exploradas
Saiba mais no anexo 61

Comunicação imediata (canais FORA da rede corporativa):
Acionar a equipe de resposta pelos canais secundários (ex.: Ligação pela operadora, ferramentas de mensagens instantâneas)
Registrar o horário exato da detecção (o relógio regulatório da LGPD começa a contar)
Acionar o porta-voz único pré-estabelecido, ninguém mais fala sobre o incidente externamente

Papéis e Responsabilidades:

Alta Administração: Autorizar medidas emergenciais de interrupção de serviços, caso o isolamento preventivo de sistemas críticos seja necessário para proteger o órgão, e garantir que apenas o porta-voz oficial se comunique externamente.

Gestor de Tecnologia da Informação e Comunicação: Supervisionar o isolamento físico e lógico da rede e garantir que a arquitetura de segurança (firewalls e switches) seja utilizada para bloquear o tráfego malicioso (medidas 12.2 e 13.4).

Gestor de Segurança da Informação: Coordenar as ações de contenção técnica e garantir que a revogação de acessos e o reset de senhas administrativas sejam executados imediatamente (medida 6.2).

Encarregado pelo Tratamento de Dados Pessoais: Registrar o horário exato da detecção para fins de conformidade com a LGPD e orientar o comitê de crise sobre os limites da comunicação durante a fase de contenção.

Responsável Setorial pela Gestão da Integridade: Monitorar as ações de contenção para assegurar que o isolamento de sistemas não prejudique evidências de possíveis desvios internos.

Responsável pela Unidade de Gestão de Pessoas: Auxiliar na comunicação imediata com as equipes afetadas através de canais secundários, garantindo que todos saibam como proceder com seus equipamentos.

Equipe de TI: Executar a desconexão física e lógica dos sistemas, bloquear túneis de acesso remoto e aplicar correções de emergência em vulnerabilidades exploradas (medidas 13.3 e 13.8).

Equipe de Comunicação: Acionar o plano de comunicação de crise, garantindo que o porta-voz único centralize todas as informações para evitar pânico ou informações desencontradas.

Equipe Jurídica: Validar as medidas de contenção sob a ótica contratual e legal, assegurando o amparo para suspensões temporárias de serviços públicos.

ETIR: Deve ser notificada imediatamente para liderar as ações de contenção; a partir do aviso, a ETIR deve identificar quais IPs e domínios bloquear, decidir quais contas devem ser desativadas e coordenar o isolamento dos segmentos de rede afetados.

Usuários: Seguir rigorosamente a instrução de não desligar o computador, apenas desconectar o cabo de rede ou desligar o Wi-Fi se solicitado, e utilizar exclusivamente os canais de comunicação secundários informados pelo órgão.

6.3. Preservar as evidências

Preservação de evidências

Em um incidente cibernético, as evidências são o “DNA” do crime. Elas são fundamentais para entender como o invasor agiu, para cumprir as obrigações de transparência da LGPD e para possibilitar que os órgãos de segurança pública e investigação identifiquem os criminosos. Uma evidência perdida ou mal manuseada é irrecuperável e pode levar ao arquivamento de investigações importantes.

Além disso, preservar amostras de arquivos criptografados é uma estratégia de longo prazo. Em grandes operações policiais internacionais, chaves de recuperação são frequentemente recuperadas e disponibilizadas para órgãos que guardaram suas evidências, permitindo restaurar dados que pareciam perdidos para sempre.

Esta ação deve ser executada em paralelo com as ações Análise e Contenção.
Não pule esta etapa. Evidências são necessárias para investigação forense, cumprimento da LGPD e eventual processo criminal. Uma vez perdidas, não voltam.

Medidas PPSI associadas
8.5 - O órgão coleta logs de auditoria detalhados?
8.8 - O órgão coleta logs de auditoria de linha de comando?
8.9 - O órgão centraliza os logs de auditoria?
8.11 - O órgão conduz revisões de logs de auditoria?
17.2 - O órgão estabelece e mantém informações de contato para notificar incidentes?
17.4 - O órgão estabelece e mantém um processo de gestão de incidentes de segurança da informação?
17.5 - O órgão atribui funções e responsabilidades para gestão de incidentes?

Ações recomendadas para preservar evidências
Capturar imagens de memória (RAM) dos sistemas infectados. Possível ferramenta: FTK Imager, Volatility (gratuitas)
Criar imagens forenses dos discos. (cópias bit-a-bit)
Exportar e armazenar logs imediatamente. (Windows Event Logs, firewall, VPN, e-mail, proxy, DNS, PowerShell)
Preservar notas de resgate (screenshots + cópias dos arquivos)
Documentar: extensões dos arquivos criptografados, timestamps, IPs/MACs afetados
Guardar amostras de arquivos criptografados (descriptores podem surgir depois, a Operação Cronos recuperou 7.000+ chaves do LockBit em 2024)
Manter cadeia de custódia: calcular hashes SHA-256 de todas as evidências
Se não há expertise forense interna: acione o órgão responsável de resposta a incidentes ou provedor MDR. Não tente “limpar” os sistemas antes da análise forense.
Saiba mais no anexo 62

Papéis e Responsabilidades:
Alta Administração: Apoio estratégico para garantir que as evidências sejam preservadas mesmo que isso atrase levemente a restauração total, assegurando que o órgão cumpra seu papel na persecução penal.
Gestor de Tecnologia da Informação e Comunicação: Garantir a disponibilidade de espaço em disco e mídias seguras para o armazenamento das imagens forenses e logs exportados (medidas 8.5 e 8.9).
Gestor de Segurança da Informação: Coordenar o processo de coleta de evidências e garantir que a revisão dos logs (medida 8.11) seja documentada conforme o processo de gestão de incidentes (medida 17.4).
Encarregado pelo Tratamento de Dados Pessoais: Acompanhar a coleta de evidências para assegurar que as provas necessárias para a defesa do órgão junto à ANPD estejam sendo devidamente guardadas.
Responsável Setorial pela Gestão da Integridade: Apoiar a guarda das evidências caso haja necessidade de abertura de processos administrativos internos.
Responsável pela Unidade de Gestão de Pessoas: Facilitar o acesso a equipamentos de servidores que precisem ser periciados, garantindo a transparência do processo.
Equipe de TI: Executar a exportação imediata de logs e a captura de notas de resgate, prints de telas e arquivos de amostra sem alterar os metadados dos arquivos.
Equipe de Comunicação: Abster-se de divulgar detalhes técnicos que possam comprometer a investigação ou alertar os criminosos sobre as evidências coletadas.
Equipe Jurídica: Orientar sobre os procedimentos de Cadeia de Custódia para garantir que as provas tenham validade junto aos órgãos de segurança pública e investigação.
ETIR: Deve ser notificada imediatamente para coordenar a coleta forense; a partir do aviso, a ETIR deve capturar a memória RAM (usando ferramentas especializadas), calcular o hash SHA-256 das evidências e acionar o CTIR Gov para suporte técnico especializado se necessário.
Usuários: Não tentar apagar arquivos, desinstalar programas ou “limpar” o computador após detectar o incidente, permitindo que a equipe técnica encontre os rastros deixados pelo invasor.

6.4. Nada de resgate!

Recomendação sobre resgate

Medidas PPSI associadas
17.5 - O órgão atribui funções e responsabilidades para gestão de incidentes?

A orientação é o **NÃO PAGAMENTO**. O pagamento implica em infração de leis e regulamentos da APF, bem como a possibilidade o financiamento de cibercrime.

Princípio da Legalidade e Interesse Público (Constituição Federal/Lei 14.133/2021)

O administrador público só pode gastar dinheiro público com autorização legal e para finalidades de interesse público. Pagamentos a criminosos (extorsão) são ilegais e não possuem amparo no orçamento ou finalidade pública.

Lei de Responsabilidade Fiscal (LRF - LC 101/2000)

Qualquer saída de recursos federais exige licitação ou justificativa legal rigorosa. O pagamento de resgate não se enquadra em despesas públicas legítimas.

Política Nacional de Cibersegurança (Decreto 11.856/2023)

Instituída para aumentar a resiliência das infraestruturas nacionais, orienta que a resposta a incidentes deve focar na recuperação de dados e soberania digital, não na negociação com agentes maliciosos.

Convenção de Budapeste (Decreto 11.491/2023)

O Brasil ratificou este tratado internacional, que define crimes cibernéticos e estabelece diretrizes para que países combatam a criminalidade cibernética, o que inclui a não validação de ações de grupos criminosos.

Conteúdo para conhecimento

A ideia de que o pagamento resolve o problema é um mito. As estatísticas demonstram a baixa eficácia dessa tomada de decisão.

O cenário atual de pagamentos

- Recuperação Parcial: Quem paga recupera, em média, apenas 65% dos dados.
- Falha Total: Apenas 4% das organizações conseguem recuperar 100% dos dados após o pagamento.
- Recuperação Alternativa: 97% das instituições conseguem reaver seus dados através de backups ou outros métodos técnicos.
- Risco de Reincidência: o pagamento sinaliza vulnerabilidade, incentivando novos ataques à mesma instituição.

Por que o não pagamento é a única via?

- Integridade do Backup: a prioridade deve ser a recuperação via backups e o cumprimento do Recovery Time Objective (RTO).
- Descriptografia Gratuita: muitas variantes possuem chaves de descriptografia já disponibilizadas por órgãos de segurança.

- Falta de Garantia: grupos atacantes frequentemente não entregam as chaves ou já publicaram os dados antes mesmo da negociação.
- Financiamento do Crime: conforme legislação e melhores práticas apontam, o dinheiro do resgate sustenta atividades ilegais e novas extorsões.

Ações Prioritárias em Vez de Negociar

- Acionamento Jurídico (AGU): Formalizar o incidente e os riscos de lavagem de dinheiro caso houvesse qualquer transação.
- Restauração Técnica: Focar 100% dos esforços na reconstrução dos sistemas a partir de pontos íntegros.
- Transparência: Notificar os órgãos de controle e, se necessário, os titulares de dados pessoais sensíveis sobre o incidente.

Posição do CERT.br: “O pagamento de resgate não impede novas tentativas de extorsão, nem garante recuperação total ou confidencialidade dos dados. Além disso, o dinheiro do resgate pode financiar e incentivar atividades ilegais.

6.5. Hora de limpar a casa

Erradicação

A erradicação é a fase de “limpeza profunda”. Se o órgão tentar restaurar os sistemas (Recuperação) sem antes

Não pule esta etapa!
Evidências são necessárias para investigação forense, cumprimento da LGPD e eventual processo criminal. Uma vez perdidas, não voltam.

eliminar completamente todos os vestígios do invasor, o ransomware voltará a atacar em questão de minutos. O risco de pular esta etapa é cair em um ciclo infinito de reinfecção, o que esgota as equipes e amplia o tempo de interrupção dos serviços ao cidadão.

Nesta fase, o objetivo não é apenas apagar o vírus, mas fechar as portas que ele deixou abertas. Os criminosos costumam criar “contas fantasmagóricas” ou tarefas agendadas para garantir que possam voltar mesmo após a senha ser trocada. Erradicar significa garantir que o ambiente está estéril e seguro para ser reconstruído.

Medidas PPSI associadas
5.3 - O órgão desabilita ou excluí contas inativas?
6.2 - O órgão estabelece um processo de revogação de acesso?
7.7 - O órgão corrige vulnerabilidades detectadas?
10.1 - O órgão instala e mantém um software antimalware?

10.6 - O órgão gerencia o software antimalware de forma centralizada?

10.7 - O órgão utiliza software antimalware baseado em comportamento?

17.4 - O órgão estabelece e mantém um processo de gestão de incidentes de segurança da informação?

17.5 - O órgão atribui funções e responsabilidades para gestão de incidentes?

Ações Recomendadas

Identifique, ou revalide, todos os dispositivos e serviços afetados dentro da organização para garantir que nenhuma falha ou fraqueza seja esquecida.

Identifique e mitigue todas as vulnerabilidades exploradas, o que inclui corrigir falhas de software, erros de configuração ou problemas de design.

Remova malwares e scripts maliciosos de todos os sistemas identificados.

Desabilite todas as contas de usuário violadas ou criadas pelo atacante.

Remova mecanismos de persistência e pontos de entrada, como backdoors ou tarefas agendadas que possam ser maliciosas.

Configure tecnologias de segurança para realizar ações de erradicação de forma automatizada onde for possível.

Garanta que os responsáveis pela resposta a incidentes tenham autoridade para realizar ações de erradicação manuais quando a precisão for necessária.

Acione provedores de serviços para que eles atuem na erradicação em ambientes fora do seu controle direto, se aplicável. (Nuvem, ISPs, dentre outros)

Se durante o processo de erradicação for identificado que a contenção não foi efetiva, repita as ações 2, 3 e 4. **Somente após a certeza do sucesso do processo de erradicação**, avance para RECUPERAÇÃO.

Saiba mais no anexo 63

Papeis e Responsabilidades:

Alta Administração: Apoio estratégico para assegurar que a equipe técnica tenha autoridade total para realizar intervenções manuais profundas e autorizar correções de emergência em sistemas críticos (medida 7.7).

Gestor de Tecnologia da Informação e Comunicação: Supervisionar a remoção de malwares e garantir que o software antimalware esteja operando de forma centralizada e baseada em comportamento em todo o órgão (medidas 10.6 e 10.7).

Gestor de Segurança da Informação: Coordenar a identificação de contas violadas e garantir a execução rigorosa do processo de revogação de acessos (medidas 5.3 e 6.2).

Encarregado pelo Tratamento de Dados Pessoais: Validar se as ações de erradicação não impactam a integridade de bancos de dados que contenham informações pessoais sensíveis.

Responsável Setorial pela Gestão da Integridade: Acompanhar a desabilitação de contas para garantir que nenhum acesso legítimo seja removido sem justificativa e que acessos ilícitos sejam devidamente registrados.

Responsável pela Unidade de Gestão de Pessoas: Informar aos servidores sobre a necessidade de reset de senhas em massa ou indisponibilidade temporária de perfis durante a limpeza.

Equipe de TI: Executar a remoção técnica de vírus e scripts, fechar brechas de segurança e limpar tarefas agendadas ou entradas de registro criadas pelo invasor (medida 10.1).

Equipe de Comunicação: Manter o público interno atualizado sobre o progresso da limpeza, preparando o terreno para o anúncio da futura fase de recuperação.

Equipe Jurídica: Analisar responsabilidades de provedores de serviços (nuvem e ISPs) caso a erradicação dependa da atuação técnica desses parceiros externos.

ETIR: Deve ser notificada imediatamente se for detectado que o invasor ainda possui acesso após as medidas de contenção; a partir daí, deve liderar a caça por ameaças (threat hunting), identificar as "portas dos fundos" deixadas pelo criminoso e certificar que o ambiente está limpo antes de autorizar a fase de Recuperação.

Usuários: Colaborar com a equipe técnica caso seus equipamentos precisem ser formatados ou reinstalados do zero para garantir que nenhum resquício da ameaça permaneça no dispositivo.

6.6. De volta ao normal

Recuperação

A recuperação é a fase mais delicada e aguardada, mas não deve ser guiada pelo pânico ou apenas pela pressa. O maior erro nesta etapa é restaurar sistemas exatamente como estavam antes do ataque: se a porta que o invasor usou continuar aberta, o órgão será reinfectado em poucos minutos.

Recuperar não é apenas "voltar o backup". É reconstruir a confiança na rede. A estratégia moderna prioriza a reconstrução (instalar sistemas novos e limpos) em vez da simples restauração (copiar o que estava infectado). Ao utilizar modelos pré-configurados e seguros (as chamadas Golden Images), o órgão garante que o serviço público retorne sobre uma base sólida, atualizada e livre de "bombas lógicas" deixadas pelos criminosos.

Medidas PPSI associadas
4.1 - O órgão estabelece e mantém um processo de configuração segura?
4.2 - O órgão estabelece e mantém um processo de configuração segura para a infraestrutura de rede?
5.1 - O órgão mantém um inventário de contas?
5.3 - O órgão desabilita ou excluí contas inativas?
5.6 - O órgão centraliza a gestão de contas?

6.2 - O órgão estabelece um processo de revogação de acesso?

6.4 - O órgão exige autenticação multifator (Multi-Factor Authentication, MFA) para acesso remoto à rede?

6.7 - O órgão centraliza o controle de acesso?

7.2 - O órgão estabelece e mantém um processo de remediação?

7.7 - O órgão corrige vulnerabilidades detectadas?

11.1 - O órgão estabelece e mantém um processo de realização de cópias de segurança (backup)?

11.2 - O órgão executa backups automatizados?

11.3 - O órgão protege os dados de recuperação?

11.4 - O órgão estabelece e mantém uma instância isolada de dados de recuperação?

11.5 - O órgão testa a recuperação de dados?

17.4 - O órgão estabelece e mantém um processo de gestão de incidentes de segurança da informação?

17.5 - O órgão atribui funções e responsabilidades para gestão de incidentes?

Ordem de recuperação

A recuperação deve seguir uma sequência lógica de dependências, não de urgência percebida. Deve-se utilizar uma metodologia como a das joias da coroa. A lista já deve estar previamente definida e revisada periodicamente.

Reconstruir é mais seguro do que restaurar. Limpar e reconstruir sistemas a partir de imagens limpas é preferível a tentar desinfetar sistemas comprometidos. Malware pode persistir em locais de difícil detecção (firmware, WMI, partição de boot).

Princípios de recuperação segura Golden Images

Corrigir a vulnerabilidade de entrada ANTES de reconectar sistemas. O risco de reinfecção imediata é altíssimo (ex: VPNs vulneráveis ou credenciais vazadas).

Ambientes Limpos: Se um servidor for comprometido, a equipe de segurança pode simplesmente “destruir” a instância infectada e subir uma nova a partir da golden image, garantindo que o novo sistema esteja livre de malwares e com todas as patches de segurança atualizadas. Se todas as máquinas recuperadas partem do mesmo modelo, fica mais fácil identificar comportamentos anômalos que fogem do padrão da imagem original. Elas ajudam a reduzir drasticamente o Tempo de Recuperação Objetivado (RTO), minimizando o impacto financeiro da indisponibilidade.

Criar sub-rede de recuperação isolada, e adicionar apenas sistemas verificados como limpos.

Testar cada sistema restaurado antes de reintegrá-lo à rede de produção.

MFA (Multi-factor Authentication) é obrigatório, deve-se reabilitar e validar o segundo fator de autenticação em todos os acessos.

Monitoramento intensivo por no mínimo 30 dias (atacantes frequentemente implantam bombas lógicas nos sistemas infectados).

Ações Recomendadas

Passo 1 — Infraestrutura de identidade (primeiro, sempre)

Restaurar Active Directory (AD) e servidores DNS — pré-requisitos fundamentais.

Resetar TODAS as senhas do domínio (incluindo KRBTGT — duas vezes, com intervalo de 10-12h entre os resets para propagação).

Rotacionar senhas de Contas de Serviço (MSAs/gMSAs) e verificar privilégios delegados.

Revogar todos os tickets Kerberos e sessões ativas (OAuth/Cloud) se houver ambiente híbrido.

Auditoria de persistência: Verificar contas criadas, Políticas de Grupos (GPOs) alteradas, certificados instalados e tarefas agendadas suspeitas.

Saiba mais no anexo 64

Passo 2 — Serviços núcleo (core) de rede

Restaurar DHCP, firewalls, switches core.

Validar regras de firewall: Remover exceções temporárias e bloquear tráfego SMB entre estações de trabalho (segmentação horizontal).

Revisar acessos administrativos: Garantir que apenas IPs da VLAN de gerenciamento acessem a console dos equipamentos.

Saiba mais no anexo 65

Passo 3 — Sistemas críticos de negócio

Restaurar por ordem de RTO (Recovery Time Objective) definido no plano de continuidade.

Sanitização de Backups: Montar os backups em ambiente isolado (Sandbox) e realizar varredura completa com EDR antes da promoção para produção.

Validar a integridade e consistência dos dados antes de liberar o acesso aos usuários.

Saiba mais no anexo 66

Passo 4 — Sistemas de Comunicação

Restaurar e-mail e sistemas de comunicação.

Validar regras de encaminhamento: Verificar se o atacante criou regras ocultas de “forwarding” de e-mails para exfiltração de dados.

Saiba mais no anexo 67

Passo 5 — Servidores de arquivo e aplicações secundárias

Restaurar e validar cada aplicação antes de reintegrar.

Limpeza de arquivos: Verificar macros em documentos Office e scripts em pastas públicas que possam servir de “trigger” para reinfecção.

Saiba mais no anexo 68

Passo 6 — Endpoints de usuário

Reinstalar a partir de Golden Images (altamente preferível à restauração de backup de máquinas infectadas).

Instalação imediata de patches, garantindo que o sistema operacional suba com todas as atualizações críticas de segurança.

Saiba mais no anexo 69

Monitoramento pós-recuperação

Escaneamento de GPOs e Scripts de Logon diariamente por 2+ semanas.

Verificar chaves autorun, tarefas agendadas e serviços recém-criados

Monitorar criação de novas contas de usuário/admin e alterações em grupos sensíveis.

Atenção especial a tráfego de saída (Egress) para IPs incomuns ou países fora do escopo de operação.

Manter alertas máximos no EDR/SIEM

Verificar persistência via WMI events, DLL hijacking ou scheduled tasks

Papeis e Responsabilidades:

Alta Administração: Apoio estratégico para sustentar a ordem de prioridade técnica (mesmo sob pressão por urgência), validar o retorno dos serviços críticos e garantir recursos para o monitoramento intensivo pós-incidente.

Gestor de Tecnologia da Informação e Comunicação: Supervisionar a reconstrução da infraestrutura de rede e garantir que as configurações seguras (medidas 4.1 e 4.2) sejam aplicadas antes da reconexão.

Gestor de Segurança da Informação: Coordenar a centralização da gestão de contas e garantir que a autenticação multifator (MFA) seja validada em todos os acessos remotos (medidas 5.6 e 6.4).

Encarregado pelo Tratamento de Dados Pessoais: Validar a integridade e a consistência dos dados pessoais restaurados antes da liberação oficial dos sistemas para uso.

Responsável Setorial pela Gestão da Integridade: Acompanhar a auditoria de persistência para garantir que nenhuma conta ilícita ou alteração de privilégio permaneça no diretório de usuários.

Responsável pela Unidade de Gestão de Pessoas: Coordenar o reset em massa de senhas e orientar os servidores sobre os novos procedimentos de segurança no retorno às atividades.

Equipe de TI: Executar tecnicamente os 6 passos da recuperação:** desde o Active Directory e DNS até os endpoints dos usuários, priorizando o uso de Golden Images e a instalação imediata de correções (medidas 7.2 e 11.2).

Equipe de Comunicação: Informar gradualmente os servidores e cidadãos sobre o cronograma de retorno dos serviços, gerenciando as expectativas de acordo com a ordem técnica de recuperação.

Equipe Jurídica: Analisar se a recuperação cumpre os requisitos de continuidade pactuados em contratos e normas vigentes.

ETIR: Deve ser notificada para validar cada sistema antes de sua reintegração à rede de produção; a partir do aviso, a ETIR deve realizar varreduras de segurança (sanitização) nos backups, monitorar tráfego de saída suspeito e conduzir o monitoramento intensivo de 30 dias para detectar tentativas de reinfecção.

Usuários: Cooperar com o reset de suas credenciais, adotar o MFA obrigatoriamente e manter vigilância redobrada, reportando qualquer comportamento atípico nos primeiros dias de retorno ao trabalho.

Pós incidente: o que é importante ser feito?

[Atividades Pós-Incidente].

Capítulo 7.

A reincidência de crises por falha na correção da causa raiz e a consequente erosão da confiança nas camadas de proteção.

Risco Principal

Visão Geral

Esta etapa constitui o mecanismo de inteligência que impede a organização de pagar, repetidamente, o preço da mesma vulnerabilidade. A experiência demonstra que grandes incidentes raramente são fruto de tecnologias insuperáveis, mas sim do colapso da higiene cibernética básica. Ao negligenciar as lições aprendidas, o gestor permite que lacunas em identidades, acessos remotos sem autenticação multifator e vulnerabilidades já mapeadas permaneçam como convites abertos a novos ataques.

O valor estratégico desta fase reside na conversão do prejuízo operacional em um ativo de governança. Através de um diagnóstico honesto, é possível validar investimentos e redirecionar esforços para as medidas de implementação do PPSI de forma estruturada. Em última análise, documentar o que aprendemos é o que diferencia uma gestão que apenas apaga incêndios de uma liderança que edifica uma infraestrutura genuinamente resiliente.

7.1. Avaliação Coletiva e Documentação

Após o fim de uma crise, a tendência natural é que as equipes queiram esquecer o ocorrido e voltar à rotina. No entanto, ignorar a etapa de avaliação é o que condena um órgão a sofrer o mesmo ataque novamente. A avaliação coletiva não serve para apontar culpados, mas para identificar falhas sistêmicas e pontos cegos na defesa do órgão.

Esta etapa transforma um evento traumático em conhecimento estratégico. Ao documentar formalmente o que aconteceu e por que as defesas falharam, a instituição cumpre seu dever de prestação de contas (accountability) e fortalece sua resiliência. Sem essa análise crítica e honesta, o órgão continua vulnerável às mesmas táticas, técnicas e procedimentos usados pelos criminosos.

Medidas PPSI associadas

0.1 - A alta administração do órgão estabelece, mantém, monitora e aprimora o sistema de gestão de riscos e controles internos relativos aos temas de privacidade e segurança?

0.13 - O órgão possui um processo de gestão de riscos de segurança da informação?

0.14 - O órgão possui um processo de gestão de continuidade de negócios em segurança da informação?

14.1 - O órgão implementa um programa de conscientização em segurança da informação?

14.6 - O órgão conscientiza os agentes públicos sobre como reconhecer e notificar incidentes de segurança da informação?

14.9 - O órgão implementa ações para capacitação sobre segurança da informação?

17.4 - O órgão estabelece e mantém um processo de gestão de incidentes de segurança da informação?

17.8 - O órgão realiza análises pós-incidentes de segurança da informação?

Deve ocorrer em até 7 dias após o fechamento do incidente, mantendo o foco em processos e não em culpados:

Realizar um encontro com todos os envolvidos, para revisar o que funcionou e o que falhou.

Mapear desde o acesso inicial e movimentação lateral até a detecção e recuperação total.

Determinar o vetor exato de entrada e os motivos sistêmicos pelos quais os controles falharam.

Calcular o Tempo Médio de Detecção (MTTD), o Tempo Médio de Recuperação (MTTR) e o Impacto financeiro e operacional real.

Documentar formalmente o incidente, as evidências coletadas e o plano de ações corretivas. Utilize o checklist (Modelo 6 – Modelo de Registro de Incidente de Segurança) que está na prateleira de instrumentos.

Papeis e Responsabilidades:

Alta Administração: Liderar a cultura de aprendizado, garantindo que o foco da avaliação seja a melhoria dos processos e não a punição, além de aprovar o sistema de gestão de riscos e controles internos (medidas 0.1 e 0.13).

Gestor de Tecnologia da Informação e Comunicação: Fornecer os dados técnicos para o cálculo do Tempo Médio de Recuperação (MTTR) e garantir que as falhas de infraestrutura mapeadas sejam priorizadas no plano de continuidade (medida 0.14).

Gestor de Segurança da Informação: Coordenar o encontro de lições aprendidas e garantir que a análise pós-incidente seja documentada e arquivada conforme as normas (medidas 17.4 e 17.8).

Encarregado pelo Tratamento de Dados Pessoais: Avaliar se as lições aprendidas exigem mudanças nos processos de tratamento de dados para evitar novos incidentes de privacidade.

Responsável Setorial pela Gestão da Integridade: Participar da avaliação para identificar se falhas na integridade institucional contribuíram para o sucesso do ataque.

Responsável pela Unidade de Gestão de Pessoas: Utilizar os resultados da avaliação para atualizar o programa de conscientização e os planos de capacitação dos servidores (medidas 14.1, 14.6 e 14.9).

Equipe de TI: Apresentar o mapeamento técnico da movimentação lateral do invasor e sugerir melhorias práticas nas configurações de rede e sistemas.

Equipe de Comunicação: Revisar a eficácia do plano de comunicação de crise utilizado e propor ajustes para melhorar a transparência em eventos futuros.

Equipe Jurídica: Analisar o relatório final do incidente para subsidiar defesas administrativas ou ações judiciais futuras, garantindo a preservação do interesse público.

ETIR: Deve ser notificada para apresentar o relatório técnico detalhado; a partir do aviso, a ETIR deve detalhar o vetor de entrada, os indicadores de comprometimento encontrados e os motivos técnicos pelos quais os controles de detecção ou contenção falharam.

Usuários: Participar ativamente fornecendo feedbacks sobre as dificuldades encontradas durante a interrupção dos sistemas, auxiliando a tornar os planos de resposta mais práticos e eficazes.

7.2. Governança e Ajustes Estratégicos

A governança é o que garante que o aprendizado obtido na fase de “Lições Aprendidas” não se perca com o passar do tempo. Se as falhas identificadas não forem transformadas em mudanças permanentes nas normas, processos e tecnologias do órgão, a instituição permanecerá vulnerável.

Ajustar a estratégia significa alinhar a expectativa da alta gestão com a realidade técnica. Se o incidente mostrou que um sistema leva 48 horas para ser recuperado, e o plano antigo previa apenas 4 horas, o Plano de Continuidade deve ser corrigido imediatamente. Governança eficaz é usar o incidente como um catalisador para modernizar políticas, fechar lacunas de visibilidade e garantir que o investimento em segurança seja aplicado onde realmente importa.

Medidas PPSI associadas
0.1 - A alta administração do órgão estabelece, mantém, monitora e aprimora o sistema de gestão de riscos e controles internos relativos aos temas de privacidade e segurança?
0.13 - O órgão possui um processo de gestão de riscos de segurança da informação?
0.14 - O órgão possui um processo de gestão de continuidade de negócios em segurança da informação?

14.1 - O órgão implementa um programa de conscientização em segurança da informação?

14.6 - O órgão conscientiza os agentes públicos sobre como reconhecer e notificar incidentes de segurança da informação?

14.9 - O órgão implementa ações para capacitação sobre segurança da informação?

17.4 - O órgão estabelece e mantém um processo de gestão de incidentes de segurança da informação?

17.8 - O órgão realiza análises pós-incidentes de segurança da informação?

Deve-se transformar o aprendizado advindo das lições aprendidas em mudanças permanentes de segurança para o órgão:

Revisar o Plano de Resposta a Incidentes e as Políticas de cibersegurança e privacidade com base nas lacunas de visibilidade identificadas.

Ajustar o Plano de Continuidade de Negócios para refletir os tempos reais de restauração observados.

Atualizar inventários de ativos caso o incidente tenha revelado novos sistemas ou ativos.

Realizar treinamentos focados nas falhas humanas ou técnicas que permitiram o incidente.

Papeis e Responsabilidades:

Alta Administração: Liderar a revisão estratégica, assegurando que as mudanças nas políticas de segurança e privacidade sejam priorizadas e que os recursos necessários para os ajustes estruturais sejam alocados (medida 0.1).

Gestor de Tecnologia da Informação e Comunicação: Ajustar o Plano de Continuidade de Negócios (PCN) para refletir os tempos reais de restauração e atualizar o inventário de ativos com base nos novos sistemas identificados durante a crise (medidas 0.14 e 1.1).

Gestor de Segurança da Informação: Planejar e gerenciar a atualização das Políticas de Segurança e do Processo de Gestão de Incidentes, fechando as brechas de visibilidade reveladas pelo ataque (medidas 0.13 e 17.4).

Encarregado pelo Tratamento de Dados Pessoais: Revisar as políticas de privacidade e proteção de dados, garantindo que as mudanças estratégicas estejam em conformidade com a LGPD e as orientações da ANPD.

Responsável Setorial pela Gestão da Integridade: Propor ajustes nos códigos de conduta e nos controles internos para mitigar riscos de integridade que possam ter sido explorados no incidente.

Responsável pela Unidade de Gestão de Pessoas: Implementar ações de capacitação e treinamentos focados especificamente nas falhas humanas identificadas na análise pós-incidente (medidas 14.1 e 14.9).

Equipe de TI: Aplicar as mudanças técnicas permanentes nas configurações de rede, sistemas e ferramentas de segurança conforme as novas diretrizes estratégicas.

Equipe de Comunicação: Atualizar os manuais de comunicação de crise e disseminar as novas diretrizes de segurança para todo o órgão de forma clara e acessível.

Equipe Jurídica: Assessorar na atualização das normas internas e revisar contratos com prestadores de serviço para incluir novas exigências de segurança detectadas como necessárias.

ETIR: Deve ser notificada para validar se os novos ajustes estratégicos cobrem tecnicamente os vetores de ataque identificados; a partir do aviso, a ETIR deve sugerir indicadores de desempenho para monitorar se as mudanças estão sendo eficazes na prevenção de novos incidentes.

Usuários: Aderir às novas normas e participar dos treinamentos de reciclagem, compreendendo que as mudanças estratégicas visam a proteção do seu ambiente de trabalho e dos dados do cidadão.

7.3. Colaboração e Comunicação

A segurança cibernética no setor público funciona como um sistema de "imunidade coletiva". Quando um órgão compartilha o que aprendeu com um ataque, ele impede que outras instituições sofram o mesmo dano. A colaboração não é apenas uma gentileza, é uma estratégia de defesa nacional que fortalece a soberania dos dados do Estado.

Além disso, esta fase final assegura que o órgão esteja juridicamente protegido. Validar se todas as notificações obrigatórias foram concluídas e se os titulares de dados foram devidamente informados evita que o incidente gere "pendências" legais ou administrativas que poderiam resultar em sanções futuras. É o momento de transformar a crise em um argumento sólido para investimentos prioritários, mostrando à gestão exatamente onde o órgão precisa ser reforçado.

Medidas PPSI associadas

0.1 - A alta administração do órgão estabelece, mantém, monitora e aprimora o sistema de gestão de riscos e controles internos relativos aos temas de privacidade e segurança?

0.14 - O órgão possui um processo de gestão de continuidade de negócios em segurança da informação?

17.8 - O órgão realiza análises pós-incidentes de segurança da informação?

Deve-se validar se as obrigações legais foram cumpridas, aconselha-se contribuir para a imunidade coletiva do setor:

Validar as notificações ao CISC gov.br, CTIR Gov e a Polícia Federal, se necessário complementar as informações já enviadas.

Confirmar o cumprimento de leis, decretos, e instruções normativas quanto ao reporte de brechas a autoridades e titulares.

Apresentar à gestão do órgão as melhorias necessárias e os investimentos em segurança que devem ser priorizados após o incidente.

Papeis e Responsabilidades:

Alta Administração: Validar o cumprimento das obrigações legais e institucionais do órgão e aprovar o plano de investimentos e melhorias prioritárias sugeridas após o incidente (medida 0.1).

Gestor de Tecnologia da Informação e Comunicação: Assegurar que as lições técnicas aprendidas sejam compartilhadas com a rede de TI do governo federal, contribuindo para a continuidade de negócios do setor público (medida 0.14).

Gestor de Segurança da Informação: Finalizar os reportes técnicos aos órgãos centrais (CISC gov.br e CTIR Gov), garantindo que todos os indicadores de invasão (IoCs) descobertos tenham sido enviados para ajudar outros órgãos.

Encarregado pelo Tratamento de Dados Pessoais: Confirmar se todas as comunicações aos titulares e à ANPD foram encerradas conforme os ritos legais, documentando o encerramento do incidente de privacidade.

Responsável Setorial pela Gestão da Integridade: Promover a transparência dos resultados da análise pós-incidente (resguardando o sigilo técnico necessário) para reforçar a confiança na governança do órgão.

Responsável pela Unidade de Gestão de Pessoas: Comunicar ao corpo funcional o encerramento oficial do incidente e as melhorias implementadas para garantir a segurança de todos.

Equipe de TI: Organizar os artefatos técnicos finais e os dados de desempenho para subsidiar os pedidos de investimento em novas tecnologias de defesa.

Equipe de Comunicação: Elaborar o comunicado final de encerramento da crise para o público externo, reafirmando o compromisso do órgão com a transparência e a segurança da informação.

Equipe Jurídica: Emitir parecer final atestando que todas as leis, decretos e instruções normativas de reporte de brechas foram rigorosamente cumpridos.

ETIR: Deve ser notificada para consolidar o dossiê técnico final do incidente; a partir do aviso, a ETIR deve complementar as notificações ao CTIR Gov com dados detalhados e participar de fóruns de colaboração para disseminar o conhecimento técnico adquirido durante a resposta.

Usuários: Manter a postura colaborativa, reportando qualquer dúvida residual sobre a segurança de seus sistemas e participando da cultura de vigilância contínua que deve permanecer após a crise.

Prateleira: modelos prontos para uso

[Material complementar].

Capítulo 8.

8.1. Modelo 1 — Comunicação interna durante incidente

Adapte os campos entre [colchetes] ao seu contexto. Envie por canais fora da rede corporativa.

COMUNICADO INTERNO — INCIDENTE DE SEGURANÇA

Data/hora: [DATA E HORA]

Classificação: [CRÍTICO / ALTO / MÉDIO]

Atualização número: [N]

1. O que aconteceu

Na [data], às [hora], foi identificada atividade anômala em nossos sistemas consistente com um ataque de ransomware. A equipe de resposta a incidentes foi ativada imediatamente.

2. O que sabemos até agora

Sistemas afetados: [listar ou "em investigação"]

Sistemas operacionais: [listar sistemas que continuam funcionando]

Dados comprometidos: [em investigação / não há indícios / confirmado — especificar]

3. O que estamos fazendo

[Descrever ações em andamento: isolamento, investigação, restauração]

[Informar se firma especializada foi acionada]

[Informar se seguradora e autoridades foram notificadas]

4. O que precisamos de vocês

Não tente acessar sistemas que estejam indisponíveis.

Não discuta este incidente em redes sociais ou com pessoas externas à organização.

Reporte qualquer comportamento anormal observado para [CONTATO].

Use [CANAL ALTERNATIVO] para comunicação de trabalho até novo aviso.

5. Próxima atualização: [DATA/HORA prevista]

6. Ponto de contato: [NOME] — [TELEFONE PESSOAL]

8.2. Modelo 2 — Comunicação externa para clientes e parceiros

Adapte os campos entre [colchetes] ao seu contexto. Envie por canais fora da rede corporativa.

COMUNICADO EXTERNO — INCIDENTE DE SEGURANÇA

Prezado(a) [NOME/ÓRGÃO-INSTITUIÇÃO],

Informamos que a [NOME DO ÓRGÃO/INSTITUIÇÃO] identificou e está respondendo a um incidente de segurança cibernética em seus sistemas.

1. O que aconteceu:

Na data de [DATA], nosso monitoramento detectou atividade não autorizada em parte de nossa infraestrutura de TI. Ativamos imediatamente nosso protocolo de resposta a incidentes e estamos trabalhando com [especialistas em segurança cibernética / firma de resposta a incidentes] para investigar e resolver a situação.

2. Impacto para sua organização

[Opção A — sem impacto confirmado] até o momento, não identificamos comprometimento de dados ou serviços relacionados ao seu contrato/relacionamento conosco. Seguimos monitorando e informaremos caso esta avaliação mude.

[Opção B — com impacto] Nossa investigação indica que [descrever natureza do impacto de forma objetiva]. Estamos tomando as seguintes medidas para mitigar os efeitos: [listar medidas].

3. O que estamos fazendo

Investigação forense em andamento com apoio de especialistas.

Autoridades competentes foram notificadas conforme legislação vigente.

Medidas de contenção e recuperação em execução.

4. Recomendações:

[Se aplicável: alterar senhas, monitorar contas etc.]

5. Próxima comunicação: Enviaremos atualização até [DATA] ou antes, caso haja informações relevantes.

Para dúvidas: [CONTATO DESIGNADO — e-mail e telefone]

Atenciosamente,

[NOME DO PORTA-VOZ]

[CARGO]

[ÓRGÃO/INSTITUIÇÃO]

8.3. Modelo 3 — Notificação à ANPD (estrutura de conteúdo)

Este modelo organiza as informações exigidas pela Resolução CD/ANPD nº 15/2024. A submissão formal deve ser feita via sistema SEI! da ANPD.

1. Identificação do controlador

Razão social, CNPJ, endereço

Nome e contato do Encarregado pelo Tratamento de Dados Pessoais

2. Descrição do incidente
Data e hora do incidente
Data e hora da ciência pelo controlador
Natureza do incidente (ransomware / acesso não autorizado / exfiltração / outro)
Duração do incidente
Localização dos dados afetados

3. Dados pessoais afetados
Tipos de dados (identificação, financeiros, saúde, etc.)
Categorias de titulares (clientes, funcionários, fornecedores)
Número de titulares afetados (ou estimativa)

4. Riscos e impactos
Possíveis consequências para os titulares
Probabilidade de materialização dos riscos

5. Medidas de segurança antes do incidente

Controles técnicos e administrativos em vigor

6. Medidas adotadas após o incidente
Ações de contenção e mitigação
Comunicação realizada ou planejada aos titulares
Medidas para evitar recorrência

7. Informações complementares

Se houver necessidade de prazo adicional (20 dias úteis)

8.4. Modelo 4 — Modelo simplificado de plano de resposta a incidentes

Modelo mínimo viável. Adapte ao contexto da sua instituição.

1. Plano de Resposta a Incidentes de Segurança — [ÓRGÃO/INSTITUIÇÃO]

Versão: [N] | Data: [DATA] | Responsável: [NOME]

2. Equipe de Resposta a Incidentes

Função	Nome	Telefone pessoal	E-mail alternativo
Coordenador da ETIR (ou Agente Responsável pela ETIR)			
Coordenador Substituto (ou Suplente da ETIR)			
Gestor de Segurança da Informação (GSI) / Alta Administração			
Consultoria Jurídica (CONJUR) ou Procuradoria Jurídica			
Encarregado pelo Tratamento de Dados Pessoais			
Equipe de TIC			

3. Canal de Comunicação de Emergência

- **Primário:** [Grupo Mensagem instantânea dedicado — Link]
- **Secundário:** [chamada telefônica direta]
- *O e-mail corporativo NÃO deve ser usado durante um incidente.*

4. Classificação de Severidade

Nível	Critério	Exemplo	Resposta
P1 — Crítico	Sistemas indisponíveis ou dados criptografados	Ransomware em produção	Resposta imediata 24/7
P2 — Alto	Sistemas parcialmente afetados	Malware em estações	Resposta em até 1h

Nível	Critério	Exemplo	Resposta
P3 — Médio	Alerta sem impacto operacional confirmado	Tentativa de phishing identificada	Análise pelo líder de SI em horário comercial

5. Inventário de Ativos Críticos

Sistema	Função	RTO	RPO	Responsável
Serviço de diretório (ou sistema de gerenciamento de identidade e acesso)	Autenticação	[X]h	[X]h	
ERP / Sistema Principal	Operação	[X]h	[X]h	
E-mail	Comunicação	[X]h	[X]h	
[Servidor de arquivos]	Operação	[X]h	[X]h	
[Sistemas financeiros]	Operação	[X]h	[X]h	

6. Protocolo Resumido por Fase

Detecção → Contenção → Erradicação → Recuperação → Lições Aprendidas

8. Contatos de Autoridades e Recursos

Em caso de incidente cibernético de qualquer natureza, acesse a página de notificação do CISC gov.br para obter orientações e informações sobre os procedimentos de comunicação do incidente: Notificar Incidente Cibernético – CISC gov.br.

Entidade	Contato	Quando Acionar
CISC gov.br	cisc@gestao.gov.br	Sempre
CTIR Gov	ctir@ctir.gov.br	Sempre
ANPD	https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis	Se dados pessoais expostos
Polícia Federal	https://apps.pf.gov.br/r/comunicapf/comunicapf/comunicar-ocorrencia	Crimes federais

9. Outros Contatos

Entidade	Contato	Quando Acionar
CERT.br	cert@cert.br	Quando envolver outras instituições
No More Ransom	https://www.nomoreransom.org/	Identificar variante e buscar descriptografia
ID Ransomware	https://id-ransomware.malwarehunterteam.com/	Identificar variante

10. Registro de Exercícios de Mesa (Tabletop)

Data	Cenário Simulado	Principais Gaps
--/--/--	Ataque de Ransomware	

11. Histórico de versões

Versão atual: 1.0

8.5. Modelo 5 — Modelo de Relatório de Teste de Integridade

Este modelo serve para evidenciar a eficácia do backup aos auditores.

Data do Teste: [DD/MM/AAAA]

Responsável: [Nome do Analista]

1. Ativos testados

● [ ] Banco de Dados Principal

● [ ] Servidor de Arquivos (File Server)

● [ ] Controlador de Domínio (AD)

* Devem ser acrescentados os todos os ativos testados

2. Checklist de validação

Critério	Resultado (OK/Falha)	Observações
Integridade do arquivo de backup	[ ]	Hash verificado?
Tempo de restauração (RTO) dentro do limite?	[ ]	Tempo gasto:
Sistema operacional iniciou (Boot)?	[ ]	Erros de tela azul?
Aplicação conectou ao banco de dados?	[ ]	Teste de query OK?

*O check list acima é um exemplo e os critérios devem ser adicionados e adaptados conforme contexto.

3. Conclusão

( ) O backup é confiável para recuperação imediata.

( ) Foram encontradas falhas. Ação corretiva necessária: [descrever]

8.6. Modelo 6 — Modelo de Registro de Incidente de Segurança

Este modelo serve para descrever todo procedimento executado durante o ciclo de vida do incidente e deve ser adaptado de acordo com as características específicas de cada incidente e da organização.

1. Descrição geral do incidente

Resumo executivo das informações coletadas e dos exames realizados: apresentação resumida do incidente, incluindo a data de ocorrência, os sistemas afetados e a natureza do evento (ex.: violação de dados, ransomware, interrupção de serviços - DDoS), indicação do time responsável por coordenar o incidente, ações tomadas para tratar o incidente tais como isolamento, investigação, recuperação de sistemas, comunicação, os resultados obtidos, como causas identificadas, vulnerabilidades corrigidas e medidas de mitigação implementadas.

Síntese sobre dever de comunicação: resultado da avaliação de risco do incidente e decisão sobre comunicação aos titulares e à ANPD.

2. Introdução

Apresentação: breve descrição da organização, do sistema afetado e do incidente.

Nível de prioridade, escalonamento e elevação: indicação do nível de prioridade atribuído ao incidente (ex: Crítico, Alto, Médio, Baixo) e documentação de quaisquer decisões de escalonamento (aumento de recursos) ou elevação (envolvimento da alta gestão) tomadas durante a resposta. **FONTE**: (NIST SP 800-61r3, RS.MA-03; RS.MA-04)

Objetivos: definir os objetivos do relatório, como:

· Documentar o incidente e as ações tomadas. **FONTE**: (NIST SP 800-61 Revision 2, Seção 7 - (NIST SP 800-61r3, RS.AN-06)

· Analisar as causas do incidente e identificar vulnerabilidades. **FONTE:** (NIST SP 800-61 Revision 2, Seção 6 - NIST SP 800-61r3, RS.AN-03)

· Desenvolver recomendações para evitar incidentes futuros. **FONTE:** (NIST SP 800-61 Revision 2, Seção 6 - NIST SP 800-61r3, ID.IM-03)

· Cumprir com os requisitos legais e regulamentares, como a LGPD. **FONTE:** (Lei Geral de Proteção de Dados) e (NIST SP 800-171, Seção 3.5.1 - NIST SP 800-61r3, GV.OC-03)

· Público-alvo (Constituency). Adaptar o relatório ao público-alvo (ex.: alta gerência, equipe técnica, clientes, ANPD) garante a clareza da comunicação e a compreensão das informações. **FONTE:** (ISO/IEC 27035-2:2023, 6.7)

RECOMENDAÇÃO ADICIONAL: manter um histórico cronológico (changelog) de todas as modificações realizadas neste documento, registrando para cada uma: a data e hora, o autor, e uma descrição clara da alteração efetuada. O objetivo é assegurar a rastreabilidade, a integridade e a transparência das informações

ao longo da evolução do relatório do incidente, sendo também recomendável incluir a justificativa para a mudança e a(s) seção(ões) específica(s) que foram afetadas.

3. Metodologia de investigação

Limitação do trabalho (se houver): descrever quaisquer limitações na investigação, como falta de acesso a dados específicos ou dificuldades na análise forense.

Ferramentas utilizadas: listar as ferramentas e tecnologias empregadas na investigação do incidente, incluindo as ferramentas forenses e a sua versão. **FONTE**: (NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response e ISO/IEC 27041:2018, 5.2.1)

4. Cronologia do incidente

Data de ocorrência do incidente: especificar a data e hora precisas do incidente, conforme logs de sistema e outros registros. **FONTE**: (NIST SP 800-61 Revision 2, Seção 4.1, - NIST SP 800- 61r3, DE.AE - Adverse Event Analysis - Resolução CD/ANPD nº 15 de 24 de abril de 2024)

RECOMENDAÇÃO ADICIONAL: utilizar um formato para registrar a data e hora (ex.: ISO 8601: YYYY-MM-DD hh:mm:ss), incluindo o fuso horário para evitar ambiguidades em casos de equipes ou sistemas distribuídos em diferentes localidades. **FONTE**: (ISO/IEC 27035-2:2023, B.3.1)

Data de conhecimento do incidente: especificar a data e hora em que a organização teve conhecimento do incidente. **FONTE**: (NIST SP 800-61 Revision 2, Seção 4.2 - NIST SP 800-61r3, **DE.AE-08 e Resolução CD/ANPD nº 15 de 24 de abril de 2024)**

Datas e atividades realizadas desde a detecção do incidente: documentar todas as ações tomadas desde a detecção, incluindo isolamento de sistemas, análise forense, recuperação de dados, notificação de autoridades e comunicação com stakeholders. **FONTE**: (NIST SP 800-61 Revision 2, Seção 5 - NIST SP 800-61r3, RS - Respond, RC - Recover, e Resolução CD/ANPD nº 15 de 24 de abril de 2024)

Critérios para Início da Recuperação: documentar o momento e a justificativa para a transição das fases de contenção/erradicação para a fase de recuperação, com base nos critérios definidos no plano de resposta a incidentes. **FONTE**: (NIST SP 800-61r3, RS.MA-05)

RECOMENDAÇÃO ADICIONAL: incluir o tempo de resposta para cada atividade realizada (ex.: tempo para isolar os sistemas, tempo para análise forense). A medição do tempo de resposta permite a identificação de gargalos no processo, a otimização das ações e a avaliação da eficiência da equipe, contribuindo para a avaliação de desempenho do programa. **FONTE**: (NIST SP 800-61r2, 4.1.1 - NIST SP 800-61r3, GV.OV-03)

5. Evidências do incidente

Cadeia de custódia: documentar a cadeia de custódia das evidências, descrevendo detalhadamente o processo de coleta, armazenamento, acesso e transferência das informações, incluindo os responsáveis por cada etapa. A documentação da cadeia de custódia garante a integridade e a admissibilidade legal das evidências, protegendo-as contra adulteração e questionamentos em eventuais processos legais. **FONTE**: (NIST SP 800-61r3, RS.AN-07; e ISO/IEC 27037:2015, 5.3)

Indicação dos documentos e informações relevantes para descrição do incidente: listar todos os documentos, registros e informações relevantes ao incidente, incluindo logs de sistema (SIEM), logs de firewall, relatórios

de análise forense, mensagens de e-mail etc. **FONTE**: (NIST SP 800-86, LGPD e Art. 10 da Resolução CD/ANPD nº 15 de 24 de abril de 2024)

RECOMENDAÇÃO ADICIONAL: incluir capturas de tela ou outras representações visuais das evidências para complementar a descrição textual. **FONTE**: (ISO/IEC 27042:2015, 6.3.2)

Resultado da análise: detalhar as evidências examinadas e os métodos de coleta utilizados. Descrever também a investigação conduzida no ambiente, como, por exemplo, a análise de um endereço IP desconhecido, e explicar o processo que levou aos resultados. **FONTE**: (NIST SP 800-86 - NIST SP 800-61r3, RS.AN - Incident Analysis;)

Descrição das circunstâncias em que o incidente ocorreu e de como tomou conhecimento: fornecer um relato detalhado das circunstâncias do incidente e como a organização tomou conhecimento dele, incluindo a fonte da notificação. **FONTE**: (NIST SP 800-61 Revision 2, Seção 4.2 - NIST SP 800-61r3, DE.AE - Adverse Event Analysis; RS.MA-02)

Descrição do impacto do incidente nos sistemas, dados e operações: descrever o impacto do incidente, incluindo sistemas afetados, dados comprometidos, interrupções de serviço e eventuais custos financeiros. **FONTE**: (NIST SP 800-61 Revision 2, Seção 4.4 - NIST SP 800-61r3, RS.AN-08)

Causa-raiz e vetor de ataque: identificar a causa raiz do incidente, o vetor de ataque e as vulnerabilidades exploradas. Fornecer evidências, como mensagens de resgate, alertas de segurança e logs de firewall, para apoiar a análise. **FONTE**: (NIST SP 800-61 Revision 2, Seção 6.1-NIST SP 800-61r3, RS.AN-03 eArt. 10 da Resolução CD/ANPD nº 15 de 24 de abril de 2024)

Descrição dos ambientes/servidores afetados: especificar os ambientes, servidores e aplicativos afetados pelo incidente. A documentação deve se basear nos inventários de ativos da organização. **FONTE**: (NIST SP 800-61 Revision 2, Seção 4.4 - NIST SP 800-61r3, ID.AM-Asset Management)

RECOMENDAÇÃO ADICIONAL: para cada ativo afetado listado, indicar sua criticidade para a organização e o impacto direto na missão ou nos processos de negócio que ele suporta, conforme a priorização de ativos. **FONTE**: (NIST SP 800-61r3, ID.AM-05)

Descrição da exfiltração ou da ausência de evidência de exfiltração: determinar se houve exfiltração e apresentar evidências para sustentar a conclusão, com base na análise de tráfego de rede (NetFlow) e logs. **FONTE**: (NIST SP 800-61 Revision 2, Seção 4.5 - NIST SP 800- 61r3, DE.CM-09. R1 e Art. 10 da Resolução CD/ANPD nº 15 de 24 de abril de 2024)

Natureza e categoria dos dados afetados: classificar os dados afetados pelo incidente, incluindo informações pessoais, dados financeiros, dados de saúde etc. **FONTE**: (NIST SP 800-171, Seção 3.5.1 - NIST SP 800-61r3, ID.AM-07 e Art. 10 da Resolução CD/ANPD nº 15 de 24 de abril de 2024)

Número de titulares afetados: identificar o número de pessoas cujos dados foram potencialmente comprometidos. **FONTE**: (NIST SP 800-171, Seção 3.5.1 e Art. 10 da Resolução CD/ANPD nº 15 de 24 de abril de 2024)

Análise de violação das propriedades da informação envolvendo dados pessoais: realizar uma avaliação das possíveis violações das propriedades da segurança da informação, envolvendo dados pessoais: confidencialidade, disponibilidade, integridade e autenticidade. **FONTE**: (NIST SP 800-171, Seção 3.5.1 e Art. 10 da Resolução CD/ANPD nº 15 de 24 de abril de 2024)

6. Medidas técnicas e administrativas de segurança adotadas

Ações adotadas para tratamento do incidente: descrever as ações de contenção (para evitar a expansão do incidente) e erradicação (para eliminar a causa) tomadas, como isolamento de sistemas, remoção de malware, restauração de dados, aplicação de patches e correções. **FONTE**: (NIST SP 800-61 Revision 2, Seção 5 - NIST SP 800-61r3, RS.MI - Incident Mitigation e Art. 10 da Resolução CD/ANPD nº 15 de 24 de abril de 2024)

RECOMENDAÇÃO ADICIONAL: detalhar e distinguir explicitamente as ações tomadas em cada uma das fases:

· Contenção: medidas para impedir a expansão do incidente (ex: isolar segmento de rede, colocar endpoint em quarentena). **FONTE**: (NIST SP 800-61r3, RS.MI-01)

· Erradicação: medidas para eliminar a causa raiz e os componentes do incidente (ex: remover malware, desabilitar contas comprometidas, aplicar patches). **FONTE**: (NIST SP 800-61r3, RS.MI-02)

· Recuperação: medidas para restaurar os sistemas à operação normal e confirmar sua integridade (ex: restaurar de backup limpo, validar funcionalidades, monitoramento pós-incidente). **FONTE**: (NIST SP 800-61r3, RC.RP-05)

Medidas de segurança técnica e administrativas adotadas antes do incidente: descrever as medidas implementadas antes do incidente, como políticas de segurança, controle de acesso, firewalls, antivírus, criptografia e treinamento de funcionários. **FONTE**: (NIST SP 800-61r3, PR – Protect e Art. 10 da Resolução CD/ANPD nº 15 de 24 de abril de 2024)

Novas medidas de segurança técnica e administrativas adotadas após o incidente: descrever as novas medidas de segurança implementadas em resposta ao incidente, incluindo a atualização de políticas, a implementação de novas tecnologias, a revisão de processos e o treinamento adicional de funcionários. **FONTE**: (NIST SP 800-61r3, ID.IM - Improvement e Art. 10 da Resolução CD/ANPD nº 15 de 24 de abril de 2024)

Medidas de correção e de mitigação dos efeitos do incidente para os titulares: descrever as medidas tomadas para corrigir os efeitos do incidente e minimizar os danos aos titulares, incluindo a recuperação de dados, a notificação dos titulares afetados e a assistência à recuperação e a oferta de serviços. **FONTE**: (NIST SP 800-171, Seção 3.5.2 e Art. 10 da Resolução CD/ANPD nº 15 de 24 de abril de 2024)

RECOMENDAÇÃO ADICIONAL: documentar se, e quais, informações técnicas (ex: Indicadores de Comprometimento - IoCs, Táticas, Técnicas e Procedimentos - TTPs) foram compartilhadas com partes externas confiáveis (ex: ISACs setoriais, parceiros, governo) para benefício mútuo e fortalecimento do ecossistema de segurança. A documentação deve assegurar que nenhum dado pessoal foi compartilhado. **FONTE**: (NIST SP 800-61r3, RS.CO-03)

RECOMENDAÇÃO ADICIONAL (apenas para relatórios internos): detalhar o processo de comunicação com stakeholders (internos e externos), especificando os canais de comunicação utilizados, o conteúdo das mensagens e a frequência dos updates. A comunicação transparente e eficiente com stakeholders é fundamental para a gestão de crises, a manutenção da confiança e o alinhamento das expectativas. Além disso, documentar como a comunicação e as ações conjuntas foram gerenciadas é fundamental para incidentes em cadeia de suprimento **FONTE**: (NIST SP 800-61r3, GV.SC-08 e ISO/IEC 27035- 1:2023, 4.6).

7. Conclusão sobre comunicação à anpd e aos titulares

Avaliação do risco e possíveis danos aos titulares: realizar uma avaliação do risco e dos possíveis danos aos titulares, incluindo perda financeira, danos à reputação, violação da privacidade, entre outros. A análise deve conectar o incidente ao contexto geral de risco da organização, inclusive das medidas de mitigação adotadas. **FONTE**: (ISO/IEC 27035-2:2023, A.11, NIST SP 800-171 - NIST SP 800-61r3, GV.RM-03, Seção 3.5.1 e Art. 10 da Resolução CD/ANPD nº 15 de 24 de abril de 2024)

Se for comunicado: descrever a forma e o conteúdo da comunicação à ANPD (Autoridade Nacional de Proteção de Dados) e aos titulares, de acordo com os requisitos da LGPD e Art. 10 da Resolução CD/ANPD nº 15 de 24 de abril de 2024. **FONTE**: (NIST SP 800-61r3, RS.CO - Incident Response Reporting and Communication)

Se não for comunicado: justificar a decisão de não comunicar, apresentando as razões e as evidências que justificam a decisão. Detalhar o processo de coordenação da comunicação. **FONTE**: (LGPD, Art. 48 e Resolução CD/ANPD nº 15 de 24 de abril de 2024 e Art. 10 da Resolução CD/ANPD nº 15 de 24 de abril de 2024)

8. Lições apreendidas

Lições apreendidas: indicar quais foram as principais lições aprendidas com o incidente, não apenas no final, mas também durante o processo de resposta. **FONTE**: (NIST SP 800-61 Revision 2, Seção 4.1.1 - NIST SP 800-61r3, ID.IM - Improvement)

Prevenção de incidentes: identificar e comunicar as melhorias necessárias assim que forem descobertas, mesmo que a resposta ao incidente ainda esteja em andamento. A melhoria contínua não deve esperar pelo fim do incidente para ser iniciada. **FONTE**: (NIST SP 800- 61r3, Figure 2, ID.IM - ISO/IEC 27035-1:2023, 5.6).

Prevenção de incidentes (Plano de Ação): relacionar as lições aprendidas com as melhorias propostas no plano de ação para garantir a efetividade do aprendizado e a prevenção de incidentes futuros. O plano deve ser sincronizado com os planos de continuidade de negócios. **FONTE**: (NIST SP 800-61r3, ID.IM-04; ISO/IEC 27035-1:2023, 5.6)

RECOMENDAÇÃO ADICIONAL: avaliar e documentar o papel de fornecedores ou terceiros no incidente (seja como vetor de ataque ou como parte da resposta). Descrever como a colaboração com esses parceiros ocorreu durante o planejamento, resposta e recuperação, e identificar melhorias necessárias nos contratos ou processos de gestão de risco de fornecedores. **FONTE**: (NIST SP 800-61r3, GV.SC-08)

RECOMENDAÇÃO ADICIONAL: descrever como as descobertas deste incidente (ex: vetores de ataque não previstos, falhas em controles) impactam a estratégia geral de gestão de riscos de cibersegurança da organização. Indicar se o incidente alterou a percepção sobre o apetite a risco ou a direção estratégica da segurança. **FONTE**: (NIST SP 800- 61r3, GV.OV-01; GV.OV-02)

9. Assinaturas e controle

Data e Assinatura: importante que o relatório seja datado e assinado pelo menos pelo Encarregado pelo Tratamento de Dados Pessoais ou responsável designado do CSIRT/segurança da informação. **FONTE**: (ISO/IEC 27035-1:2023, 4.7.4)

REFERÊNCIAS PARA ELABORAÇÃO DESTE DOCUMENTO:

NIST SP 800-61 Revision 2: Computer Security Incident Handling Guide:

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.80061r2.pdf

NIST Special Publication 800 NIST SP 800-61r3 Incident Response Recommendations and Considerations for Cybersecurity Risfi Management A CSF 2.0 Community Profile: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf

NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response:

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-86.pdf

NIST Cybersecurity Frameworfi (CSF):

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.80053r5.pdf

ABNT NBR ISO/IEC 27035-1, 27035-2 e 27035-3:

https://www.normas.com.br/produto/normas-brasileiras- emercosul/pesquisar/27035

Lei Geral de Proteção de Dados (LGPD): https://www.gov.br/anpd/ptbr/assuntos/legislacao/lei-geral-de-protecao- de-dados

Resolução CD/ANPD nº 15 de 24 de abril de 2024: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24- deabril-de-2024-556243024

8.7. Modelo 7 — Checklist para resposta a incidentes

Este modelo serve para a criação de um checklist para utilização durante a ocorrência de um incidente.

CHECKLIST DE RESPOSTA A RANSOMWARE PARA O TIME TÉCNICO

Ação		Realizado?
Detecção (tempo máximo recomendado < 10 minutos)		
1.	Determinar se ocorreu um incidente	
1.1	Verifique os itens abaixo, eles são possíveis indicativos de um ataque de ransomware: ● Arquivos com extensões alteradas (.crypt, .locked, .encrypted, extensões aleatórias) ● Notas de resgate em pastas ou na área de trabalho ● Renomeação em massa de arquivos ● Shadow copies deletadas (checar: vssadmin list shadows) ● Logs mostram execução anômala de PowerShell, PsExec ou ferramentas de compressão ● Tráfego de saída incomum (grandes volumes para IPs desconhecidos) ● Alertas do EDR/antivírus ignorados ou desabilitados ● Logins em horários ou locais atípicos	
1.2	**Se confirmado, ative o Plano de Resposta a Incidentes imediatamente, observe as Obrigações Legais e acione o Plano de Comunicação** ● Acione o ETIR/Equipe técnica da instituição ● Acione a cadeia de gestão ● Destaque uma pessoa para começar o registro de ações: Registrar o horário exato da detecção (o relógio regulatório da LGPD começa a contar) ● Comunicação imediata (canais FORA da rede corporativa): Acionar a equipe de resposta pelos canais secundários (ex.: Ligação pela operadora, ferramentas de mensagens instantâneas) ● Acionar o porta-voz único pré-estabelecido, ninguém mais fala sobre o incidente externamente	
Análise (tempo máximo recomendado < 60 minutos)		
2.	Análise e compreensão da extensão do impacto	
2.1	Determinar quais sistemas foram criptografados e quais estão intactos (Checagem dupla). **Importante**: Identificar qual o backup mais recente íntegro para os sistemas criptografados	
2.2	Verificar se houve exfiltração de dados (logs de tráfego de saída, ferramentas como rclone, WinSCP, megacmd)	
2.3	Identificar o vetor de entrada provável (phishing, VPN comprometida, RDP exposto, vulnerabilidade explorada)	
2.4	Entendimento e registro da linha do tempo do incidente	

2.5	Verificar se dados pessoais foram comprometidos (aciona obrigações da LGPD) (guia de resposta a incidentes com dados pessoais)	
2.6	Identificar a variante do ransomware: ● ID Ransomware: https://id-ransomware.malwarehunterteam.com/	

Ação		Realizado?
	● No More Ransom / Crypto Sheriff: https://www.nomoreransom.org/crypto-sheriff.php	
2.7	Verificar se existe ferramenta de descriptografia gratuita disponível	
Contenção **NÃO DESLIGUE AS MÁQUINAS: A preservação de evidências depende disso**		
3.	Desconectar, desabilitar, isolar, bloquear, corrigir	
3.1	Desconectar sistemas infectados da rede (cabo ethernet, desabilitar Wi-Fi, isolamento via ferramenta de segurança)	
3.2	Matar túneis VPN e conexões de acesso remoto	
3.3	Se múltiplos segmentos estiverem comprometidos, isolar no nível do switch	
3.4	Desabilitar contas de serviço suspeitas e resetar senhas de contas administrativas	
3.5	Isolar sistemas críticos que ainda não foram afetados (desconectar preventivamente)	
3.6	Bloquear IPs e domínios maliciosos conhecidos, ou descobertos, no firewall	
3.7	Correção de emergência de vulnerabilidades ativamente exploradas	
Preservação de Evidências **Se não há expertise forense interna: acione o órgão responsável de resposta a incidentes ou provedor MDR. Não tente "limpar" os sistemas antes da análise forense.**		
4.	Coletar e preservar evidências: ● Capturar imagens de memória (RAM) dos sistemas infectados. Possível ferramenta: FTK Imager, Volatility (gratuitas) ● Criar imagens forenses dos discos. (cópias bit-a-bit) ● Exportar e armazenar logs imediatamente. (Windows Event Logs, firewall, VPN, e-mail, proxy, DNS, PowerShell) ● Preservar notas de resgate (screenshots + cópias dos arquivos) ● Documentar: extensões dos arquivos criptografados, timestamps, IPs/MACs afetados ● Guardar amostras de arquivos criptografados (descriptores podem surgir depois, a Operação Cronos recuperou 7.000+ chaves do LockBit em 2024) ● Manter cadeia de custódia: calcular hashes SHA-256 de todas as evidências	

Erradicação		
5.	Execute as sub tarefas a seguir	
5.1	Identifique, ou revalide, todos os dispositivos e serviços afetados dentro da organização para garantir que nenhuma falha ou fraqueza seja esquecida	

Ação		Realizado?
5.2	Identifique e mitigue todas as vulnerabilidades exploradas, o que inclui corrigir falhas de software, erros de configuração ou problemas de design	
5.3	Remova malwares e scripts maliciosos de todos os sistemas identificados	
5.4	Desabilite todas as contas de usuário violadas ou criadas pelo atacante	
5.5	Remova mecanismos de persistência e pontos de entrada, como backdoors ou tarefas agendadas que possam ser maliciosas	
5.6	Configure tecnologias de segurança para realizar ações de erradicação de forma automatizada onde for possível	
5.7	Garanta que os responsáveis pela resposta a incidentes tenham autoridade para realizar ações de erradicação manuais quando a precisão for necessária	
5.8	Acione provedores de serviços para que eles atuem na erradicação em ambientes fora do seu controle direto, se aplicável. (Nuvem, ISPs, dentre outros)	
5.9	Se durante o processo de erradicação for identificado que a contenção não foi efetiva, repita as ações 2, 3 e 4. Somente após a certeza do sucesso do processo de erradicação, avance para RECUPERAÇÃO.	
Recuperação		

6.	Recuperar sistemas afetados: ● Ordem de recuperação ○ A recuperação deve seguir uma sequência lógica de dependências, não de urgência percebida. ○ Reconstruir é mais seguro do que restaurar. Limpar e reconstruir sistemas a partir de imagens limpas é preferível a tentar desinfetar sistemas comprometidos. Malware pode persistir em locais de difícil detecção (firmware, WMI, partição de boot). ● Princípios de recuperação segura Golden Images ○ Corrigir a vulnerabilidade de entrada ANTES de reconectar sistemas. O risco de reinfecção imediata é altíssimo (ex: VPNs vulneráveis ou credenciais vazadas). ○ Criar VLAN de recuperação isolada, e adicionar apenas sistemas verificados como limpos. ○ Testar cada sistema restaurado antes de reintegrá-lo à rede de produção. ○ MFA é obrigatório, deve-se reabilitar e validar o segundo fator de autenticação em todos os acessos. ● Monitoramento intensivo por no mínimo **30 dias** (atacantes frequentemente implantam “bombas relógio” nos ambientes).	
6.1	Passo 1 — Infraestrutura de identidade (primeiro, sempre) ● Restaurar Active Directory (AD) e servidores DNS — pré-requisitos fundamentais. ● Resetar TODAS as senhas do domínio (incluindo KRBTGT — duas vezes, com intervalo de 10-12h entre os resets para propagação).	

	Ação	Realizado?
	• Rotacionar senhas de Contas de Serviço (MSAs/gMSAs) e verificar privilégios delegados. • Revogar todos os tickets Kerberos e sessões ativas (OAuth/Cloud) se houver ambiente híbrido. • Auditoria de persistência: Verificar contas criadas, Políticas de Grupos (GPOs) alteradas, certificados instalados e tarefas agendadas suspeitas.	
6.2	Passo 2 — Serviços core de rede • Restaurar DHCP, firewalls, switches core. • Validar regras de firewall: Remover exceções temporárias e bloquear tráfego SMB entre estações de trabalho (segmentação horizontal). • Revisar acessos administrativos: Garantir que apenas IPs da VLAN de gerenciamento acessem a console dos equipamentos.	
6.3	Passo 3 — Sistemas críticos de negócio • Restaurar por ordem de RTO (Recovery Time Objective) definido no plano de continuidade. • Sanitização de Backups: Montar os backups em ambiente isolado (Sandbox) e realizar varredura completa com EDR antes da promoção para produção. • Validar a integridade e consistência dos dados antes de liberar o acesso aos usuários.	
6.4	Passo 4 — Serviços de Comunicação • Restaurar e-mail e sistemas de comunicação. • Validar regras de encaminhamento: Verificar se o atacante criou regras ocultas de "forwarding" de e-mails para exfiltração de dados.	
6.5	Passo 5 — Servidores de arquivo e aplicações secundárias • Restaurar e validar cada aplicação antes de reintegrar. • Limpeza de arquivos: Verificar macros em documentos Office e scripts em pastas públicas que possam servir de "trigger" para reinfecção.	
6.6	Passo 6 — Endpoints de usuário • Reinstalar a partir de Golden Images (altamente preferível à restauração de backup de máquinas infectadas). • Instalação imediata de patches, garantindo que o sistema operacional suba com todas as atualizações críticas de segurança.	
7.	Monitoramento pós-recuperação • Escaneamento de GPOs e Scripts de Logon diariamente por 2+ semanas. • Verificar chaves autorun, tarefas agendadas e serviços recém-criados • Monitorar criação de novas contas de usuário/admin e alterações em grupos sensíveis. • Atenção especial a tráfego de saída (Egress) para IPs incomuns ou países fora do escopo de operação. • Manter alertas máximos no EDR/SIEM • Verificar persistência via WMI events, DLL hijacking ou scheduled tasks	

8.8. Modelo 8 — Matriz RACI para Resposta a Incidentes Cibernéticos

Matriz RACI: Resposta a Incidentes Cibernéticos

Esta matriz define os papéis da **ETIR** interna e a interação com os *stakeholders* críticos.

Legenda:

- **R (Responsible):** Quem executa a tarefa.
- **A (Accountable):** Quem aprova e possui a responsabilidade final (apenas um por tarefa).
- **C (Consulted):** Quem deve ser consultado antes da ação.
- **I (Informed):** Quem deve ser informado após a execução.

Atividade / Processo	ETIR (Interna)	Alta Administração / Comitê de Crise	CISC gov.br / CTIR Gov	ANPD (Dados Pessoais)	Polícia Federal / Civil
Detecção	R / A	I	I	I	I
Análise	R / A	I	I / C	I	I
Contenção	R	A	I / C	I	I
Preservação de Evidências	R / A	I	C	I	C
Decisão de Não Pagamento de Resgate	C	A	I	I	I
Notificação de Incidente Crítico	R	A	R (Recebe)	I	I

Comunicado de Incidente (LGPD)	C	R / A	I	R (Recebe)	I
Erradicação e Limpeza	R / A	I	C	I	I
Recuperação de Sistemas (Restore)	R	A	I	I	I
Análise Forense	R	C	C	I	I
Registro de B.O. / Notificação Crime	C	R / A	I	I	R (Recebe)
Relatório de Lições Aprendidas	R	A	I	I	I

Atribuições Detalhadas dos Stakeholders

1. ETIR (Interna)

- **Execução Técnica:** Responsável por tratar o incidente desde a contenção até a execução das atividades pós incidente.
- **Custódia:** Deve garantir a cadeia de custódia das evidências para futuras investigações criminais ou auditorias.

2. Alta Administração / Comitê de Crise (CCC)

- **Autoridade Decisória:** Possui o papel de *Accountable* para decisões de alto impacto, como desligar o Data Center da internet ou autorizar a reconstrução do ambiente do zero.
- **Comunicação:** Gerencia a narrativa pública e o posicionamento oficial contra o pagamento de resgate.

3. CTIR Gov e CISC gov.br

- **Coordenação Nacional:** O **CTIR Gov** atua na triagem e coordenação sistêmica para mitigar riscos ao governo.
- **Apoio Operacional:** O **CISC gov.br** oferece suporte técnico especializado ("ETIR as a Service") para ajudar na resposta rápida das instituições afetadas.

4. ANPD, Órgãos Reguladores, Polícias

- **Conformidade Legal:** ANPD deve ser notificada em até **3 dias úteis** caso o incidente envolva riscos aos dados pessoais (LGPD).
- **Órgãos Reguladores, Polícias:** Deve-se analisar caso a caso.

Recursos, ferramentas e contatos

[Material complementar].

Capítulo 9.

9.1. Programa de Privacidade e Segurança da Informação (PPSI)

O Programa de Privacidade e Segurança da Informação (PPSI) consiste em um conjunto estratégico de ações em governança, maturidade, metodologia, pessoas e tecnologia, com o objetivo de elevar a resiliência e o nível de maturidade em privacidade e segurança da informação nos órgãos e entidades da administração pública federal direta, autárquica e fundacional integrantes do SISP.

PPSI 2.0

No âmbito do Programa de Privacidade e Segurança da Informação (PPSI), e em conformidade com o art. 14 da Portaria SGD/MGI nº 9.511/2025, a Secretaria de Governo Digital (SGD/MGI) publica diretrizes e normas voltadas a apoiar os órgãos do SISP na implementação do Framework de Privacidade e Segurança da Informação; essa iniciativa, cuja gestão cabe à estrutura de governança do PPSI, visa disseminar um conjunto de controles essenciais para elevar a maturidade e a resiliência institucional nesses aspectos. A Secretaria de Governo Digital (SGD) disponibiliza materiais de suporte e ferramenta para apoiar a implementação do PPSI 2.0.

Material disponíveis no CEPS

O Centro de Excelência em Privacidade e Segurança da Informação do Governo Digital (CEPS GOV.BR) tem como missão promover a cultura de privacidade e segurança da informação nos órgãos e entidades da administração pública federal direta, autárquica e fundacional integrantes do SISP, conforme previsto no Art. 21 da Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025.

Guias e modelos disponibilizados pelo PPSI

No âmbito do Programa de Privacidade e Segurança da Informação (PPSI), estas publicações visam à efetiva implementação das melhores práticas de segurança da informação e proteção de dados, promovendo-as por meio da disponibilização de guias, processos, modelos e procedimentos.

Guias, Modelos e Cartilhas

9.2. Outros frameworks e guias de referência

- **Guia de Resposta a Incidentes - PPSI:** https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_resposta_incidentes.pdf
- **NISTIR 8374 — Ransomware Risk Management:** https://csrc.nist.gov/pubs/ir/8374/final
- **NIST CSF 2.0:** https://csf.tools/reference/nist-cybersecurity-framework/v2-0/
- **CIS Controls v8.1:** https://www.cisecurity.org/controls/v8-1
- **Blueprint for ransomware Defence:** https://securityandtechnology.org/wp-content/uploads/2025/11/Blueprint-for-Ransomware-Defense-Mapped-to-NIST-CSF-2.0-2.pdf
- **CISA #StopRansomware Guide:** https://www.cisa.gov/stopransomware/ransomware-guide
- **CISA CPGs 2.0:** https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
- **CERT.br — Ransomware: Como se Proteger:** https://cert.br/docs/ransomware/
- **Cartilha CERT.br:** https://cartilha.cert.br/ransomware/

9.3. Relatórios anuais para acompanhamento

Estes relatórios estão entre as melhores fontes de dados atualizados sobre ransomware. Vale acompanhar anualmente.

Sophos State of Ransomware: https://www.sophos.com/en-us/content/state-of-ransomware

Verizon DBIR: https://www.verizon.com/business/resources/reports/dbir/

IBM Cost of a Data Breach: https://www.ibm.com/reports/data-breach

Coveware Quarterly Reports: https://www.coveware.com/ransomware-quarterly-reports

9.4. Ferramentas gratuitas de resposta

Ferramenta	Finalidade	Link
No More Ransom	Descriptografia (100+ decryptors)	https://www.nomoreransom.org/
ID Ransomware	Identificação de variante	https://id-ransomware.malwarehunterteam.com/
FTK Imager	Captura de memória e imagem forense	https://www.exterro.com/digital-forensics-software/ftk-imager
CISA RRA	Autoavaliação de prontidão	GitHub (CSET)
MITRE ATT&CK Calculator	Priorização de técnicas	https://ctid.mitre.org/projects/top-attack-techniques/

9.5. Templates e playbooks gratuitos

Recurso	Descrição	Link
Counteractive IR Plan	Template open-source completo	Repositório GitHub
Rapid7 Ransomware Playbook	Playbook focado em ransomware	Baixar PDF
NMFTA Template	Template para transporte e logística	Baixar PDF
CRI Decision Tree	Árvore de decisão para ransomware	Baixar PDF

9.6. Outras fontes

Outras fontes de notificações não obrigatórias em caso de incidentes.

- **CERT.br (cert@cert.br)** - voluntário mais fortemente recomendado
- **Boletim de Ocorrência** - Delegacia de Crimes Cibernéticos https://new.safernet.org.br/content/delegacias-cibercrimes
- **CAIS RNP** - se for uma instituição pertencente à rede RNP é necessária a comunicação.
- **CVM** - se forem sociedades de economia mista com capital aberto (com ações na bolsa) e o incidente constituir fato relevante.
- **BACEN** - se instituição financeira regulada (Resolução CMN 4.893/2021)
- **ANEEL** - se instituição geradora, transmissora e distribuidora de energia elétrica.
- **ONS** - se instituição geradora, transmissora e distribuidora de energia elétrica.
- **ANATEL** - se instituição de telecomunicação.
- **ANAC** - se instituição operadora de aeródromos e organizações de serviços auxiliares.
- **ANTAQ** - se instituição operadora de portos e serviços aquaviários.
- **ANTT** - se instituição operadora de ferrovias e rodovias concessionadas.
- **ANP** - se instituição que explora, produz, refina e distribui petróleo e gás.
- **ANVISA** - se instituição operadora de hospitais, laboratórios e fabricantes de dispositivos médicos.

9.7. Contatos no Brasil

Entidade	Contato	Finalidade
CISC gov.br	cisc@gestao.gov.br.	coordenação operacional das ações de prevenção, tratamento e resposta a incidentes cibernéticos no âmbito do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP.
CTIR Gov	ctir@ctir.gov.br	Atender aos incidentes na Administração Pública Federal (APF)
ANPD	Site Oficial	Notificação obrigatória (dados pessoais)
CERT.br	cert@cert.br / Reportar	O centro presta serviços da área de Gestão de Incidentes de Segurança da Informação para qualquer rede que utilize recursos administrados pelo NIC.br
Delegacias de Cibercrimes	Diretório por Estado	Denúncia e registro de ocorrência
Polícia Federal	Comunica PF	Crimes de jurisdição federal
SaferNet Brasil	Acessar Recursos	Recursos e orientação

Termos e definições

Capítulo 10.

Glossário de referência destinado a padronizar a linguagem técnica e normativa entre as equipes de TI, segurança e alta gestão. Tem como objetivo garantir o nivelamento conceitual, alinhar o vocabulário aos frameworks oficiais e evitar ambiguidades de comunicação durante momentos críticos de resposta a incidentes.

Os termos a seguir consolidam e harmonizam conceitos do CIS Controls v8.1, NIST CSF 2.0, NIST SP 800-61 e orientações da CISA, devidamente adaptados à realidade da Administração Pública Federal. Para definições complementares legais, recomenda-se a consulta à Portaria SGD/MGI nº 9.511/2025 e ao Glossário de Segurança da Informação do GSI/PR (Portaria GSI/PR nº 93/2021).

A

Aplicações: Programas ou grupos de programas que rodam sobre um sistema operacional em ativos institucionais (ex.: aplicações web, móveis, bancos de dados e serviços em nuvem).

Arquitetura de rede: Desenho físico e lógico de uma rede que define sua organização estrutural, as conexões entre dispositivos e softwares, e o fluxo dos dados transmitidos. Deve ser documentada por meio de diagramas de arquitetura e segurança.

Ativos institucionais: Equipamentos físicos ou virtuais com capacidade de processar, armazenar ou transmitir dados. Incluem servidores, dispositivos de rede, equipamentos de usuário final e dispositivos IoT, operando em ambientes locais (on-premise) ou em nuvem.

B

Biblioteca: Base de código pré-compilada e compartilhável (contendo classes, procedimentos e scripts) projetada para otimizar o desenvolvimento e a execução padronizada de *softwares*.

C

Contas de administrador: Identidades atribuídas a usuários com privilégios elevados, destinadas ao gerenciamento de sistemas, domínios ou infraestrutura de TI. Devem ser estritamente vinculadas a um usuário único (ex.: *root, admin* local, *admin* de domínio).

Contas de serviço: Identidades criadas exclusivamente para a execução de aplicações, serviços e tarefas automatizadas no sistema operacional. Possuem um responsável técnico definido e não devem, sob nenhuma hipótese, ser utilizadas para navegação ou computação geral.

Contas de usuário: Identidades padrão, compostas por credenciais (usuário e senha), com privilégios limitados e destinadas à execução de atividades operacionais rotineiras.

D

Dados: Conjunto de informações (físicas ou digitais) processadas, transferidas ou arm

azenadas pela instituição para apoiar a tomada de decisão e a execução de serviços.

Dados críticos: Informações digitais ou físicas que exigem rigoroso controle de privacidade, integridade e disponibilidade. O vazamento, alteração ou destruição indevida desses dados pode causar severos danos operacionais, legais ou reputacionais à organização.

Dados físicos: Informações armazenadas em meios não digitais (ex.: documentos em papel) ou mídias removíveis físicas mantidas *off-line* (ex.: fitas de *backup*).

Dispositivos de rede: Equipamentos eletrônicos essenciais para a conectividade e interação estrutural em uma rede de computadores (física, virtual ou em nuvem). Incluem *switches*, roteadores, *firewalls*, *gateways* e pontos de acesso sem fio.

Dispositivos de usuário final: Equipamentos utilizados por agentes públicos para a execução de suas atividades corporativas, como *desktops*, *notebooks*, *smartphones* e *tablets*.

Documentação: Acervo consolidado de informações escritas, físicas ou digitais, que formalizam as diretrizes da organização. Inclui políticas, normas, planos, processos, procedimentos e diagramas arquiteturais.

F

Firmware: *Software* de baixo nível armazenado em memória não volátil (como ROM ou flash) que controla diretamente o hardware e permite sua comunicação com o sistema operacional. Sua atualização geralmente ocorre isolada das atualizações comuns de sistema.

I

Infraestrutura de rede: Conjunto de recursos (físicos, virtuais ou em nuvem) que fornece conectividade, gerenciamento e suporte à operação do negócio, permitindo a comunicação entre usuários, serviços e aplicações.

Interface de Programação de Aplicação (API): Conjunto de regras, protocolos e interfaces que permite a integração e a comunicação padronizada entre diferentes sistemas e componentes de *software*.

Internet das Coisas (IoT) e dispositivos não computacionais: Equipamentos com sensores e softwares integrados capazes de conectar e trocar dados com outros sistemas. Incluem câmeras de segurança, catracas biométricas, impressoras, *smartwatches* e sistemas de controle industrial.

L

Log (Registro de Eventos): Coleção cronológica de registros gerados por sistemas, redes ou aplicações. Podem ser persistentes (arquivos armazenados em disco) ou transitórios. São a base para rastreabilidade, análise de incidentes e auditoria.

Logs de auditoria: Registros focados em eventos de segurança e ações em nível de usuário (ex.: logins, acessos a pastas, escalonamento de privilégios). Exigem planejamento estratégico para configuração e retenção adequadas.

Logs de sistema: Registros nativos de sistemas operacionais e aplicações que documentam o funcionamento interno das máquinas (ex.: inicialização e parada de serviços, falhas, *crashes*).

M

Mídias removíveis: Dispositivos de armazenamento portáteis que podem ser desconectados de um computador em funcionamento, permitindo a movimentação de dados entre sistemas (ex.: *drives* USB, discos rígidos externos, cartões SD).

P

Plano: Documento estratégico e estrutural que consolida e orienta a implementação de políticas, normas e procedimentos para um fim específico (ex.: Plano de Resposta a Incidentes).

Política: Declaração oficial e mandatória de governança da alta gestão que define os objetivos, princípios e regras fundamentais de um programa institucional.

Prestadores de serviço: Entidades externas que fornecem plataformas, *softwares* ou serviços (gerenciados ou em nuvem) para a organização. Incluem provedores de TI, fornecedores de SaaS e consultorias.

Procedimento: Roteiro operacional tático ou passo a passo detalhado que define a maneira correta, segura e aprovada de executar uma tarefa específica.

Processo: Conjunto estruturado de atividades inter-relacionadas que transformam insumos em resultados práticos para alcançar objetivos de gestão ou segurança.

R

Rede: Conjunto global de dispositivos interconectados que trocam dados entre si. O conceito de rede engloba, de forma ampla, tanto a infraestrutura quanto a arquitetura lógica.

S

Serviços: Programas especializados executados em segundo plano (*background*) que realizam funções críticas vitais para o sistema operacional, como gerenciamento de comunicações e controle de permissões.

Servidores: Equipamentos ou sistemas (físicos, virtuais, em datacenters ou nuvem) dedicados a fornecer recursos, dados e aplicações para outros dispositivos em uma rede (ex.: servidores web, servidores de arquivos, servidores de e-mail).

Sistemas operacionais: Softwares de base responsáveis por gerenciar os recursos de hardware e fornecer o ambiente comum necessário para a execução de aplicações (ex.: Windows, Linux, macOS).

Soluções de software: Conjunto lógico de instruções e dados que direcionam o computador a realizar tarefas. O termo abrange sistemas operacionais, aplicações, bibliotecas e APIs.

T

Threat Hunting (Busca Ativa de Ameaças): Investigação proativa de redes e sistemas para identificar atividades maliciosas que não foram detectadas pelas ferramentas automatizadas de segurança. O objetivo é antecipar a descoberta de invasores e interromper o ataque antes que o impacto final se concretize.

U

Usuários: Indivíduos (agentes públicos, terceirizados, prestadores de serviços ou consultores) autorizados a interagir e acessar os ativos institucionais mediante o uso de credenciais formais.

Termos e referências complementares

Glossário de Segurança da Informação (GSI) - https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/glossario-de-seguranca-da-informacao-1

Glossário de Termos de Dados - Infraestrutura Nacional de Dados - https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/governancadedados/glossario-de-termos-de-dados

Referências

ABNT NBR ISO/IEC 27002:2023: Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação. Rio de Janeiro, 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001:2023: Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro, 2023.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. **Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025**: Institui o Programa de Privacidade e Segurança da Informação (PPSI 2.0). Brasília, DF: MGI, 2025. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-9.511-de-28-de-outubro-de-2025-665815455. Acesso em: 23 de junho de 2026.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021. Processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal. Brasília, DF: GSI/PR, 2021. Disponível em: https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/legislacao/copy_of_IN03_consolidada.pdf. Acesso em: 23 de junho de 2026.

BRASIL. Ministério da Justiça e Segurança Pública. Agência Nacional de Proteção de Dados. Resolução CD/ANPD nº 15, de 24 de abril de 2024. Regulamento de Comunicação de Incidente de Segurança. Brasília, DF: ANPD, 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Acesso em: 23 de junho de 2026.

CENTER FOR INTERNET SECURITY (CIS). **CIS Critical Security Controls Version 8.1**. East Greenbush, NY: CIS, 2024. Disponível em: https://www.cisecurity.org/controls/. Acesso em: 23 de junho de 2026.

CERT.BR (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil). **Fascículo Ransomware**: Recomendações para prevenir infecções e reduzir o impacto de ataques. São Paulo: NIC.br, 2021. Disponível em: https://cert.br/docs/ransomware/. Acesso em: 23 jun. 2026.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA). **#StopRansomware Guide**. Washington, DC: CISA/FBI/NSA/MS-ISAC, 2023. Disponível em: https://www.cisa.gov/stopransomware/mitigation-guide. Acesso em: 23 de junho de 2026.

International Organization for Standardization. ISO/IEC 27701:2025 – Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. ISO; 2025.

MITRE CORPORATION. **MITRE ATT&CK®**. McLean, VA: MITRE, [Ano Atual]. Disponível em: https://attack.mitre.org/. Acesso em: 23 de junho de 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **The NIST Cybersecurity Framework (CSF) 2.0**. NIST Special Publication (SP) 1299. Gaithersburg, MD: NIST, 2024. DOI: https://doi.org/10.6028/NIST.SP.1299. Disponível em: https://csrc.nist.gov/pubs/sp/1299/final. Acesso em: 23 de junho de 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **Ransomware Risk Management: A Cybersecurity Framework 2.0 Community Profile**. NIST IR 8374 Rev. 1. Gaithersburg, MD: NIST, 2026. DOI: https://doi.org/10.6028/NIST.IR.8374r1. Disponível em: https://csrc.nist.gov/pubs/ir/8374/r1/final. Acesso em: 23 de junho de 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **Computer Security Incident Handling Guide**. NIST Special Publication (SP) 800-61 Rev. 2. Gaithersburg, MD: NIST, 2012. DOI: https://doi.org/10.6028/NIST.SP.800-61r2. Disponível em: https://csrc.nist.gov/pubs/sp/800/61/r2/final. Acesso em: 23 de junho de 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile**. NIST Special Publication (SP) 800-61 Rev. 3. Gaithersburg, MD: NIST, 2025. DOI: https://doi.org/10.6028/NIST.SP.800-61r3. Disponível em: https://csrc.nist.gov/pubs/sp/800/61/r3/ipd. Acesso em: 23 de junho de 2026.

Resolução CD/ANPD nº 18, de 16 de julho de 2024. Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais. Brasília, DF: ANPD, 2024.

Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074. Acesso em: 23 de junho de 2026.

Anexos

[Documento de apoio referenciado na seção 5].

Capítulo 12.

Anexo 1

Instituir e documentar formalmente a Equipe de Prevenção

Instituir e documentar formalmente a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), definindo seus membros titulares, substitutos designados, funções e telefones de contato.

Muitas organizações cometem o erro de tratar a resposta a incidentes cibernéticos como uma atividade improvisada, reunindo técnicos de TI apenas quando um ataque ocorre. A institucionalização da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) significa transformar esse grupo informal em uma entidade oficial dentro do organograma, dotada de autoridade formal, orçamento próprio, processos documentados e independência de atuação. O objetivo destas diretrizes é estabelecer a ETIR não apenas como um grupo operacional, mas como um pilar estratégico de governança contínua.

1. Escolha do Modelo de Institucionalização da ETIR

A estrutura ideal depende do tamanho da organização, do orçamento disponível e do volume de ameaças enfrentadas. Os modelos mais comuns são:

- **Equipe Ad-Hoc / Virtual:** Formada por colaboradores de TI que possuem outras funções principais e são convocados apenas durante crises (Baixo custo, mas gera sobrecarga e lentidão na resposta).
- **Equipe Híbrida (Core + Especialistas):** Um núcleo pequeno e dedicado exclusivamente à segurança, que aciona especialistas de outras áreas (redes, banco de dados) apenas quando a resposta exige (Excelente equilíbrio e alto nível técnico).
- **Equipe Dedicada:** Um grupo integral de analistas (SOC/CSIRT) focado 100% na monitoração e resposta a incidentes (Alta maturidade, recomendável para organizações de grande porte ou criticidade).
- **Equipe Terceirizada (MSSP):** A operação técnica é repassada a um provedor externo, mas a governança e a tomada de decisão permanecem com um gestor interno (Ideal para superar a falta imediata de talentos internos).

2. Arquitetura de Governança e Reporte

A posição da ETIR no organograma dita a sua eficácia e independência. Os cenários de reporte mais comuns são:

- **Cenário A: Subordinação à TI (CIO/Diretor de TI)** A ETIR responde diretamente à liderança de tecnologia. Embora facilite o alinhamento técnico diário, pode gerar conflitos de interesse: a TI tradicional busca disponibilidade a todo custo, enquanto a segurança pode precisar desligar sistemas para conter um vazamento.

- **Cenário B: Subordinação à Alta Gestão (Comitê de Risco / CISO / Presidência)** A ETIR tem um canal de reporte direto (ou via Comitê de Segurança) à diretoria executiva, separada da operação de TI. Este cenário garante autoridade irrestrita para auditar processos, investigar falhas internas e tomar ações de contenção drásticas sem interferência operacional.

3. Passos Práticos para Implementação

Passo 1: O Mandato Oficial (Ato Normativo)

- Publique uma Portaria, Resolução ou documento executivo oficializando a criação da ETIR.

- O mandato **deve** outorgar à equipe a autoridade explícita para isolar ativos da rede, bloquear contas de usuários (incluindo da alta gestão) e confiscar equipamentos temporariamente durante uma investigação de incidente.

Passo 2: Definição de Papéis e Matriz RACI

- Especifique quem é o Coordenador da ETIR e defina os papéis dos membros técnicos (Triagem, Análise Forense, Comunicação).

- Formalize a ponte da ETIR com agentes externos fundamentais: o Encarregado pelo Tratamento de Dados Pessoais e a Assessoria Jurídica.

Passo 3: Orçamento e Ferramental Dedicado

- Desvincule o orçamento de segurança do orçamento geral de TI. A ETIR deve ter rubricas próprias para aquisição de ferramentas (como EDR, SIEM, cofres de senhas) e financiamento das capacitações técnicas contínuas abordadas anteriormente.

Passo 4: Elaboração da Carta de Serviços (RFC - Request for Comments)

- Escreva e publique o documento que descreve detalhadamente para o resto do órgão o que a ETIR faz (ex: tratamento de malware, análise de vulnerabilidades, educação) e, mais importante, o que ela **não faz** (ex: redefinir senha esquecida ou consertar impressora).

Passo 5: Integração em Redes de Confiança

- Institucionalize o cadastro da sua ETIR em fóruns e centros de coordenação nacionais e internacionais (como o CTIR Gov, no caso da administração pública federal brasileira, ou o CERT.br), permitindo a troca antecipada de indicadores de ameaças.

4. Considerações de Contingência e Adoção

- **Sobrecarga e Rotação (Burnout):** A atuação em resposta a incidentes é altamente estressante. Se a equipe for híbrida ou ad-hoc (sob demanda), crie políticas de compensação para sobreaviso (plantões) e promova o rodízio de funções para evitar a exaustão física e mental dos agentes.

- **Conflitos de Autoridade no "Dia Zero":** Durante o primeiro grande incidente após a criação da ETIR, é comum que gerentes de outras áreas tentem intervir ou "dar carteiradas" para não terem seus sistemas desligados. O apoio incondicional da Alta Administração à ETIR neste momento é vital para consolidar a autoridade da equipe.

Fonte: Baseado nas diretrizes do NIST (publicação SP 800-61 Rev. 2: Computer Security Incident Handling Guide - Seção de Organização), nas normas do CERT.br para criação de CSIRTs, e nos normativos do GSI/PR (como a NC 04/IN01, que orienta a criação de ETIRs na Administração Pública Federal).

Anexo 2

Desenvolver a matriz de severidade

Desenvolver a matriz de severidade e o fluxo para o tratamento dos incidentes, categorizando-os estruturalmente (ex.: Crítico, Alto, Médio).

Tratar todo alerta de segurança com a mesma prioridade é o caminho mais rápido para a exaustão da equipe e para o colapso operacional. Sem uma matriz de severidade clara, incidentes catastróficos podem aguardar em uma fila de chamados enquanto a equipe resolve problemas triviais. O objetivo destas diretrizes é estabelecer um sistema de triagem objetivo e um fluxo de escalonamento previsível, garantindo que a Equipe de Tratamento de Incidentes (ETIR) concentre seu poder de fogo imediato nas ameaças que realmente podem paralisar a instituição ou comprometer dados sensíveis.

1. Escolha do Modelo de Triagem

A forma como a organização classifica um incidente dita a velocidade e o custo da resposta. A escolha do modelo deve refletir a maturidade operacional da TI:

- **Matriz Qualitativa Simples (Urgência x Impacto):** Cruza a importância do serviço afetado com a velocidade de propagação do ataque. (Ideal para organizações em fase inicial de estruturação da ETIR).
- **Matriz Quantitativa (Scoring):** Atribui pesos numéricos a fatores como volume de dados em risco, exigências legais e impacto financeiro, gerando uma nota final. (Recomendado para organizações com alta maturidade e processos automatizados).
- **Matriz Orientada a Serviços Críticos (Business-Driven):** A severidade é automaticamente herdada do catálogo de serviços. Se um sistema classificado como “Tier 1” (ex: Folha de Pagamento ou Portal do Cidadão) for afetado, o incidente é automaticamente “Alto” ou “Crítico”, independentemente da técnica do ataque.

2. Arquitetura do Fluxo de Tratamento

O caminho que a informação percorre desde a detecção até a resolução precisa ser desenhado para evitar gargalos:

- **Cenário A: Escalonamento em Camadas (Tiered Support)** O fluxo clássico e estruturado. O Nível 1 (Service Desk) faz a triagem inicial e bloqueios básicos. Se a ameaça for complexa (Severidade Média/Alta), o ticket é passado ao Nível 2 (Segurança Operacional). Em caso de crise (Severidade Crítica), aciona-se o Nível 3 (ETIR Especializada e Alta Gestão).
- **Cenário B: Modelo de “Swarming” (Enxame)** Utilizado para incidentes de severidade Alta ou Crítica. Em vez de passar um ticket de uma equipe para outra (o que perde tempo), um alerta central convoca instantaneamente especialistas de várias áreas (Segurança, Redes, Banco de Dados) para uma Sala de Guerra (virtual ou física), onde todos trabalham simultaneamente na contenção até a estabilização.

3. Passos Práticos para Implementação

Passo 1: Definição Estrutural das Severidades

- **Crítico (P1):** Interrupção total de serviços essenciais, vazamento ativo de dados sensíveis ou comprometimento profundo da rede (ex: Ransomware, invasão do Active Directory). *Ação: *Acionamento imediato do Comitê de Crise e ETIR, 24/7*.

- **Alto (P2):** Degradação severa de sistemas importantes ou infecção contida que ameaça se espalhar (ex: malware em servidores secundários, roubo de credenciais de administradores). *Ação: Prioridade máxima da equipe de segurança no horário comercial ou sobreaviso*.

- **Médio (P3):** Ameaça isolada e sem impacto sistêmico imediato (ex: estação de trabalho de usuário comum infectada e isolada, tentativa de phishing relatada). *Ação: Tratamento dentro do SLA padrão de TI*.

- **Baixo (P4):** Anomalias, falsos positivos ou atividades suspeitas bloqueadas pelas ferramentas automatizadas (ex: scan de portas no firewall). *Ação: Apenas monitoramento e registro nos logs*.

Passo 2: Documentação do Fluxo de Ciclo de Vida (PICERL)

Para cada nível de severidade, formalize o fluxo baseado no padrão internacional de resposta:

1. **Preparação:** Ter a matriz documentada e as ferramentas configuradas.
2. **Identificação:** Quem detectou e como o alerta foi gerado.
3. **Contenção:** Ação imediata para estancar o sangramento (ex: isolar a máquina da rede).
4. **Erradicação:** Remoção da causa raiz (ex: deletar o malware, aplicar o patch).
5. **Recuperação:** Retorno seguro das operações (ex: restaurar backup limpo).
6. **Lições Aprendidas:** Reunião pós-incidente para evitar a repetição.

Passo 3: Estabelecimento de SLAs (Acordos de Nível de Serviço)

- Defina métricas rigorosas para as fases críticas. Por exemplo, para um incidente "Alto": Tempo para Triagem Inicial (15 min), Tempo para Contenção (2 horas), Tempo para Recuperação (8 horas).

Passo 4: Integração com a Ferramenta de ITSM

- Configure o sistema de chamados (ServiceNow, GLPI, Jira) para que ele force o analista a escolher a urgência e o impacto, calculando a severidade automaticamente e roteando o chamado para a fila da ETIR sem intervenção manual.

4. Considerações de Contingência e Adoção

- **A "Inflação" de Severidade:** É comum que usuários ou diretores exijam que seus chamados sejam classificados como "Críticos" por conveniência ou pânico. A política deve deixar claro que a **ETIR tem a palavra final** sobre a classificação técnica da severidade do incidente, baseada em evidências, e não na pressão hierárquica.

- **Alertas Fora de Expediente:** Para incidentes Críticos ou Altos que ocorram na madrugada ou finais de semana, o fluxo deve prever a integração com ferramentas de paging (como PagerDuty ou

acionamento via SMS/Call Tree automatizada) para acordar a equipe de sobreaviso, pois um e-mail de alerta não será lido a tempo.

Fonte: Baseado nas diretrizes do NIST (publicação SP 800-61 Rev. 2: Computer Security Incident Handling Guide), na norma ISO/IEC 27035 (Gestão de Incidentes de Segurança da Informação) e nos preceitos de priorização de serviços do ITIL v4 e do PPSI.

Anexo 3

Estabelecer a árvore de comunicação

Estabelecer a árvore de comunicação, determinando os mecanismos primários e secundários que serão usados para a notificação do incidente.

Em um incidente cibernético de alta severidade, a confusão sobre quem deve ser notificado, por quem e através de qual canal pode atrasar a resposta em horas críticas. A ausência de um fluxo de acionamento claro resulta em executivos descobrindo crises pela imprensa ou técnicos paralisados aguardando ordens que nunca chegam. O objetivo destas diretrizes é estabelecer uma Árvore de Comunicação (Call Tree) estruturada, garantindo que as notificações fluam de forma rápida, ordenada e resiliente, mesmo em cenários de indisponibilidade tecnológica.

1. Escolha dos Mecanismos de Notificação

Os canais devem ser pré-definidos com base na gravidade do incidente e na disponibilidade da infraestrutura. A matriz de mecanismos inclui:

- **Notificação Automatizada (Primária para TI/ETIR):** Ferramentas de paging e alertas (ex: PagerDuty, Opsgenie) integradas ao monitoramento de segurança, que disparam SMS ou ligações automáticas para a equipe de plantão.
- **Comunicação Corporativa Padrão (Primária Geral):** E-mail institucional e plataformas de colaboração (Teams, Slack, Google Chat). Utilizados apenas quando há certeza de que a rede principal é segura e o incidente é de baixa/média severidade.
- **Comunicação Out-of-Band (Secundária/Emergência):** Aplicativos com criptografia de ponta a ponta (Signal, WhatsApp) instalados em dispositivos móveis, operando fora da rede corporativa. Acionados imediatamente em casos de comprometimento de e-mail (BEC) ou Ransomware.
- **Comunicação Analógica (Último Recurso):** Ligações telefônicas convencionais diretas (voz) e SMS manual. Essencial para cenários de apagão total de conectividade ou indisponibilidade de nuvem.

2. Arquitetura da Árvore de Comunicação

A estrutura define como a informação se propaga para evitar que uma única pessoa fique sobrecarregada tendo que avisar dezenas de envolvidos:

- **Cenário A: Modelo Hierárquico (Top-Down/Cascata)** Ideal para escalar a equipe técnica. O analista que detecta a ameaça notifica o Líder da ETIR. O Líder aciona os Coordenadores de Infraestrutura, Redes e Banco de Dados. Cada Coordenador, por sua vez, aciona os membros de suas respectivas equipes.
- **Cenário B: Modelo Hub-and-Spoke (Centralizado no Comitê)** Ideal para o acionamento executivo durante crises críticas. O Líder da ETIR (Hub) atua como ponto central e notifica simultaneamente um representante focal de cada área estratégica de negócio (Spokes: Jurídico, Encarregado pelo Tratamento de Dados Pessoais, Relações Públicas, Alta Administração), garantindo que todos recebam a mesma versão dos fatos ao mesmo tempo.

3. Passos Práticos para Implementação

Passo 1: Mapeamento de Stakeholders e Gatilhos

- Identifique quem precisa ser notificado com base na matriz de severidade (ex: Incidentes Médios ficam na TI; Incidentes Críticos acionam o Encarregado pelo Tratamento de Dados Pessoais e a Presidência).
- Estabeleça limites de tempo (ex: A Presidência deve ser notificada em até 60 minutos após a confirmação de um incidente Crítico).

Passo 2: Construção da Tabela de Contatos

- Documente nome, cargo, e os mecanismos de contato primário (ex: ramal/e-mail corporativo) e secundário (ex: celular pessoal/Signal).
- **Regra de Ouro:** Para cada cargo crítico na árvore (CISO, Encarregado pelo Tratamento de Dados Pessoais, Diretor de TI), defina e documente obrigatoriamente um "Substituto Imediato" (Backup) caso o titular esteja incomunicável, em férias ou em voo.

Passo 3: Distribuição e Armazenamento Resiliente

- A árvore de comunicação não pode residir apenas na intranet corporativa, pois ela será inacessível caso a rede caia.
- Distribua a Call Tree em formato PDF criptografado para os dispositivos móveis dos membros chave e mantenha cópias físicas (impressas e guardadas em locais seguros/cofres) na sala de operações e com a diretoria.

Passo 4: Protocolo de Acionamento (Handshake)

- Defina que toda notificação crítica exige confirmação de recebimento (ex: "Recebi a mensagem e estou entrando na sala de guerra"). Se não houver confirmação em 10 minutos, o fluxo dita que se deve ligar para o canal secundário ou para o substituto.

Passo 5: Exercícios de Verificação (Drills)

- Realize um "Teste de Call Tree" a cada seis meses. Dispare uma mensagem ("Isto é um teste do plano de resposta. Responda OK em até 15 minutos") e meça quanto tempo leva para toda a árvore confirmar o recebimento.

4. Considerações de Contingência e Adoção

- **A Obsolescência Silenciosa:** O maior risco de uma árvore de comunicação é a desatualização de dados. Pessoas mudam de número de celular, são demitidas ou mudam de cargo. Vincule a atualização da Call Tree aos processos de admissão/demissão (Onboarding/Offboarding) do RH para garantir precisão contínua.
- **Contenção de Informação (Need-to-Know):** A comunicação inicial de um incidente crítico deve ser restrita apenas aos indivíduos listados na árvore. Vazamentos internos para grupos de WhatsApp não oficiais da organização geram pânico, rumores e podem alertar os criminosos (caso tenham acesso aos dispositivos de funcionários) de que foram descobertos.

Fonte: Baseado nas diretrizes do NIST (National Institute of Standards and Technology) (publicação SP 800-61 Rev. 2: Computer Security Incident Handling Guide), SANS Institute (Incident Response Guidelines - Call Trees) e nas boas práticas de Continuidade de Negócios do PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 4

Mapear canais de comunicação alternativos

Mapear canais de comunicação alternativos (out-of-band), considerando que a infraestrutura primária (como o correio eletrônico corporativo) pode estar indisponível durante a crise

Durante um incidente cibernético severo, como um ataque de Ransomware ou o comprometimento do servidor de e-mails (BEC - *Business Email Compromise*), a infraestrutura primária de TI torna-se inoperante ou, pior, passa a ser monitorada pelo atacante. Utilizar o e-mail corporativo ou o chat interno para coordenar a defesa nessas condições é o equivalente a entregar o seu plano de batalha ao inimigo. O objetivo destas diretrizes é mapear e implementar canais de comunicação alternativos (*Out-of-Band* - OOB), criando uma infraestrutura paralela e isolada que garanta a coordenação ininterrupta e sigilosa da crise.

1. Escolha dos Canais Alternativos (Out-of-Band)

A seleção das ferramentas OOB deve basear-se na premissa de "Zero Dependência" da rede corporativa principal. Os canais recomendados incluem:

- **Aplicativos de Mensageria com Criptografia Fim-a-Fim:** Soluções como Signal, Threema ou WhatsApp Business, instalados em dispositivos móveis que utilizem redes de dados celulares (4G/5G), ignorando o Wi-Fi corporativo. (O Signal é o padrão-ouro técnico devido à sua forte postura de privacidade).
- **Plataforma de Colaboração em Nuvem Isolada (*Shadow Tenant*):** Um ambiente de chat e videoconferência totalmente separados (ex: um Workspace do Slack ou do Google Meet pago com um cartão de crédito corporativo independente). **Regra fundamental:** Este ambiente não pode estar integrado ao Active Directory (SSO) da organização.
- **Telefonia Celular Convencional (Voz e SMS):** Aparelhos celulares corporativos ou lista de números pessoais pré-autorizados. (Vital caso os links de internet do órgão sejam cortados para conter o vazamento de dados).
- **Sistemas de Conferência Web Secundários:** Contas de Zoom ou Webex registradas com e-mails alternativos de emergência, utilizadas estritamente para montar a "Sala de Guerra Virtual".

2. Arquitetura de Isolamento (Governança do OOB)

Para que o canal alternativo seja seguro, sua arquitetura lógica deve ser compartimentada e isolada do ambiente padrão:

- **Cenário A: "Air-Gapped" Lógico (Desacoplamento de Identidade)** A autenticação no canal OOB não pode depender da infraestrutura de identidade primária. Se o servidor de autenticação (IdP/AD) for derrubado pelo ataque, os usuários ainda devem conseguir acessar o canal secundário através de credenciais específicas de emergência e MFA (Múltiplo Fator de Autenticação) nativo da plataforma OOB.
- **Cenário B: Compartimentação da Informação (Need-to-Know)** Devem existir, no mínimo, dois canais OOB distintos: um **Canal Tático** (exclusivo para a ETIR compartilhar IPs maliciosos, hashes de malware

e scripts de contenção) e um **Canal Estratégico** (para a Alta Gestão, Encarregado pelo Tratamento de Dados Pessoais e Jurídico debaterem impactos legais, notificações e comunicação externa).

3. Passos Práticos para Implementação

Passo 1: Seleção e Homologação Técnica

- Escolha formalmente quais serão as ferramentas primária e secundária de comunicação *Out-of-Band*.
- Garanta que o uso dessas ferramentas (especialmente se instaladas em celulares pessoais dos gestores de TI) esteja coberto por uma política formal de uso aceitável para emergências.

Passo 2: Pré-Provisionamento (Pre-staging)

- Crie os grupos, canais e *workspaces* alternativos **agora**, durante o período de normalidade.
- Adicione os membros essenciais e configure as permissões. Nomeie os canais de forma inequívoca.

Passo 3: Criação de Diretórios Offline

- A lista com os links de acesso ao *tenant* secundário, bem como os números de telefone das lideranças, deve ser distribuída em formato físico (impresso) ou em arquivos digitais criptografados armazenados localmente nos dispositivos dos respondentes, pois a intranet não estará acessível.

Passo 4: Protocolo de Virada (Failover Trigger)

- Defina o gatilho exato para a migração de canal. Exemplo prático: “Diante de qualquer suspeita de invasão no software editor de texto, a ETIR disparará um SMS com a palavra-código para o Comitê de Crise, ordenando a migração imediata para o canal [*especificar canal*]”.

Passo 5: Regras de Engajamento no OOB

- Estabeleça regras claras sobre o que pode transitar no canal alternativo. Por exemplo, proíba o envio de bancos de dados completos ou listas de senhas nos aplicativos de mensageria, limitando o uso a comandos, coordenação e status de operações.

4. Considerações de Contingência e Adoção

- **O Perigo do Dispositivo Comprometido:** Treine a equipe para não acessar o canal *Out-of-Band* (ex: abrir o Slack secundário via navegador ou WhatsApp Web) a partir de um notebook corporativo que seja suspeito de infecção. Se houver um *keylogger* (rastreador de teclado) na máquina, o atacante roubará o acesso ao OOB. O acesso deve ser feito preferencialmente via dispositivos móveis (celulares/tablets).
- **Manutenção do Canal (Keep-Alive):** Canais e contas não utilizados por muito tempo podem ser suspensos por inatividade pelas plataformas de nuvem. Realize testes trimestrais (ex: uma reunião rápida do comitê de crise conduzida inteiramente pela plataforma OOB) para garantir que as contas estão ativas, as senhas funcionam e o aplicativo está atualizado nos celulares de todos.

Fonte: Baseado nas diretrizes da CISA (Cybersecurity and Infrastructure Security Agency) sobre Comunicações Resilientes de Resposta a Incidentes, no NIST (SP 800-61 Rev. 2) e nas boas práticas de gestão de crises e continuidade de negócios do PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 5

Integrar ao plano o inventário de processos de negócio prioritários

Integrar ao plano o inventário de processos de negócio prioritários, definindo métricas claras de Tempo de Recuperação (RTO) e Ponto de Recuperação (RPO).

Em um cenário de ataque cibernético massivo (como um Ransomware que paralisa todo o data center), a equipe de TI não pode tentar restaurar todos os sistemas ao mesmo tempo. Sem um mapa claro do que é vital para o órgão, os técnicos podem gastar horas restaurando o sistema de catracas ou a intranet administrativa, enquanto a folha de pagamento ou o portal de serviços ao cidadão continuam fora do ar. O objetivo destas diretrizes é integrar a visão de negócios à resposta técnica, definindo métricas precisas de RTO e RPO, para que a Equipe de Tratamento de Incidentes (ETIR) saiba exatamente o que deve ser salvo primeiro.

1. Definição das Métricas de Recuperação (RTO e RPO)

Antes de mapear os processos, as áreas de negócio e a TI precisam ter um entendimento nivelado sobre os dois conceitos fundamentais que guiam a continuidade de serviços:

- **RPO (Recovery Point Objective - Ponto de Recuperação):** Define a tolerância máxima à perda de dados. Responde à pergunta: “Quantas horas ou dias de dados inseridos no sistema podemos perder e recadastrar manualmente sem causar um desastre administrativo?”. **Isso dita a frequência dos backups**.

- **RTO (Recovery Time Objective - Tempo de Recuperação):** Define o tempo máximo tolerável em que o sistema pode ficar fora do ar após o incidente. Responde à pergunta: “Em quantas horas a TI precisa devolver este sistema funcionando?”. **Isso dita a estratégia de redundância e alta disponibilidade**.

2. Arquitetura de Priorização (Business Impact)

A classificação dos sistemas não é baseada em qual tecnologia é mais moderna, mas sim no impacto que sua indisponibilidade causa à missão da instituição. Os cenários de categorização (Tiers) são:

- **Cenário A: Processos Essenciais (Tier 1 - Missão Crítica)** Serviços que, se paralisados, causam risco à vida, paralisação da arrecadação, impacto direto em massa ao cidadão ou multas regulatórias imediatas. Exigem **RTO baixo** (ex: 2 a 4 horas) e **RPO baixo** (ex: perda máxima de 1 hora de dados). Requerem backups contínuos e infraestrutura replicada (Ativo/Ativo).

- **Cenário B: Processos de Suporte (Tier 2 e 3)** Sistemas administrativos internos, portais de comunicação ou processos que podem ser executados no papel por alguns dias. Permitem **RTO alto** (ex: 48 a 72 horas) e **RPO moderado** (ex: perda de 24 horas aceitável). Podem depender de backups diários e restauração sequencial (Ativo/Passivo).

3. Passos Práticos para Implementação

Passo 1: Análise de Impacto nos Negócios (BIA - Business Impact Analysis)

- Convoque os diretores de cada área de negócio (não apenas a TI) para identificar quais são os processos-chave de seus departamentos.

- Questione qual o impacto financeiro, legal e de imagem se aquele processo parar por 1 hora, 1 dia ou 1 semana.

Passo 2: Negociação de RTO e RPO (Choque de Realidade)

- As áreas de negócio tendem a pedir RTO zero e RPO zero para tudo. A TI deve apresentar o custo disso.
- Defina RTOs e RPOs realistas baseados na infraestrutura atual. Se o negócio exige um RPO de 1 hora, mas o backup só é feito uma vez à noite, gere um plano de ação para corrigir essa lacuna.

Passo 3: Mapeamento de Dependências Técnicas

- Uma vez que o processo prioritário (ex: “Emissão de Notas”) foi definido, a TI deve mapear todas as dependências que o sustentam: o banco de dados principal, o servidor de autenticação (Active Directory), o link de internet e o firewall.
- O RTO da dependência técnica deve ser igual ou menor que o RTO do processo de negócio.

Passo 4: Integração ao Playbook da ETIR

- Documente a lista priorizada (Tier 1 a 3) e insira-a na primeira página do Plano de Resposta a Incidentes.
- Em caso de crise, a ordem do Comitê deve ser explícita: “A ETIR está focada 100% em restaurar os sistemas Tier 1 listados no inventário. O Tier 2 só será abordado amanhã”.

Passo 5: Alinhamento de Rotinas de Backup

- Ajuste as políticas da sua ferramenta de backup para espelhar as definições do RPO. Sistemas Tier 1 devem ter snapshots ou replicação de logs frequentes, enquanto o Tier 3 segue na rotina noturna padrão.

4. Considerações de Contingência e Adoção

- **A Falácia do “Tudo é Crítico”:** Se a diretoria afirmar que todos os 50 sistemas do órgão são “Tier 1”, significa que nada é prioridade. Exija um limite (ex: no máximo 15% dos processos podem ser Tier 1). A classificação força a tomada de decisões difíceis antes que o desastre ocorra.
- **Teste do RTO na Prática:** O papel aceita qualquer prazo. Um RTO de 4 horas é uma teoria até que a equipe de infraestrutura seja obrigada a restaurar 2 Terabytes de um servidor de banco de dados a partir do backup em fita ou nuvem. Realize testes de restauração periódicos para validar se a velocidade de rede/leitura permite cumprir o RTO estipulado em contrato.

Fonte: Baseado nas diretrizes do NIST (publicação SP 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems), na norma ISO 22301 (Segurança e resiliência — Sistemas de gestão de continuidade de negócios) e nas práticas de Gestão de Riscos do PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 6

Consolidar a lista de contatos externos essenciais

Consolidar a lista de contatos externos essenciais, incluindo provedores de seguro de cibersegurança, equipe jurídica, empresas de resposta a incidentes contratadas e autoridades governamentais, como o CTIR Gov e o CISC gov.br.

Quando um incidente de proporções severas atinge a infraestrutura, é comum que a complexidade da ameaça ou as exigências legais ultrapassem a capacidade de resposta exclusiva da equipe interna. Atrasar o acionamento de suporte externo por não saber a quem recorrer, ou perder horas procurando números de apólices e contatos de plantão, pode agravar o impacto financeiro e regulatório do ataque. O objetivo destas diretrizes é consolidar uma rede de contatos externos essenciais, estabelecendo protocolos claros sobre quando e como acionar especialistas, autoridades governamentais e provedores de serviços durante uma crise.

1. Categorização dos Contatos Externos

A lista de parceiros externos deve ser segmentada pelo papel que desempenham na resolução da crise. As categorias fundamentais incluem:

- **Autoridades Governamentais e Reguladores:** Entidades que devem ser notificadas por exigência legal ou para coordenação nacional. Inclui o **CTIR Gov** (Centro de Tratamento de Incidentes de Redes do Governo), o **CISC gov.br** (Centro Integrado de Segurança Cibernética do Governo Federal), a **ANPD** (Autoridade Nacional de Proteção de Dados) e delegacias especializadas em crimes cibernéticos.

- **Suporte de Resposta Técnico (IR Retainer / MSSP):** Empresas terceirizadas de Resposta a Incidentes e Análise Forense Digital, contratadas preventivamente para fornecer especialistas “sob demanda” (hands-on) em caso de ataques complexos como Ransomware.

- **Suporte Legal e Financeiro:** Provedores de Seguro de Cibersegurança (Cyber Insurance), assessorias jurídicas externas especializadas em direito digital e empresas de Relações Públicas especializadas em gestão de crises corporativas.

- **Fornecedores Críticos (Supply Chain):** Contatos de emergência (Nível 2/Nível 3) de Provedores de Nuvem (AWS, Azure, Google Cloud), Provedores de Link de Internet (ISPs) e desenvolvedores dos sistemas mais críticos do órgão.

2. Arquitetura do Fluxo de Acionamento

A decisão de chamar um ente externo não deve ser aleatória. A arquitetura de acionamento deve separar o fluxo técnico do fluxo legal/institucional:

- **Cenário A: Acionamento Técnico (Coordenação e Contenção)** Executado pelo Coordenador da ETIR ou Líder Técnico. O foco é compartilhar Indicadores de Comprometimento (IoCs) e solicitar bloqueios. Aciona-se rapidamente o CISC gov.br e o CTIR Gov para verificar se outros órgãos estão sofrendo o mesmo ataque e os Fornecedores Críticos/ISPs para aplicar filtros contra-ataques DDoS, por exemplo.

- **Cenário B: Acionamento Executivo e Legal (Compliance e Risco)** executado pela Alta Administração, Encarregado pelo Tratamento de Dados Pessoais ou Jurídico. O foco é a proteção de responsabilidade. Aciona-se a Seguradora Cibernética (para ativar a apólice) e a ANPD (para cumprir o prazo legal de notificação de vazamento de dados).

3. Passos Práticos para Implementação

Passo 1: Levantamento e Consolidação do Diretório

- Crie uma matriz contendo: Nome da Instituição/organização, Nome do Ponto de Contato (se houver), Telefone de Plantão (24/7), E-mail de emergência, e **Número do Contrato/Apólice**.
- Sem o número do contrato/apólice em mãos, o atendimento em empresas privadas pode ser negado ou colocado no final da fila.

Passo 2: Estabelecimento de Contratos de Retenção (IR Retainers)

- Não espere o ataque acontecer para procurar no mercado uma empresa de resposta a incidentes. A negociação de preços, escopo e Acordos de Confidencialidade (NDA) leva semanas.
- Celebre contratos de Retainer (horas pré-pagas ou taxa de prontidão) com antecedência, garantindo um SLA de resposta de poucas horas em caso de crise.

Passo 3: Mapeamento dos Gatilhos do Seguro Cibernético

- Revise a apólice do seguro cibernético com o Jurídico. Muitas apólices exigem notificação em prazos exíguos (ex: 24 a 72 horas após a descoberta) e ditam que a instituição **não pode** contratar serviços forenses sem a aprovação prévia da seguradora, sob pena de perda da cobertura.

Passo 4: Matriz de Autorização (Quem liga para quem?)

- Defina explicitamente no Plano de Resposta a Incidentes quem tem a autoridade para acionar cada contato externo.
- Exemplo: Um analista Nível 1 não deve ligar para a Polícia Federal ou para a Imprensa; isso é responsabilidade exclusiva do Comitê de Crise ou da área de Comunicação. No entanto, o analista deve ter autoridade para abrir um chamado crítico no provedor de nuvem.

Passo 5: Integração com o Governo

- Formalize o cadastro da sua instituição e dos contatos da sua ETIR junto ao CTIR Gov e CISC gov.br. Mantenha as chaves criptográficas (PGP/GPG) atualizadas para a troca segura de informações sobre vulnerabilidades e ameaças ativas na administração pública.

4. Considerações de Contingência e Adoção

- **Armazenamento Seguro e Offline:** Assim como a árvore de comunicação interna, a lista de contatos externos deve estar disponível *out-of-band* (impressa e armazenada em dispositivos móveis seguros). Se o Active Directory e os servidores de arquivos forem criptografados, o contato da seguradora não pode ser perdido.

- **Preservação de Evidências vs. Recuperação:** Antes de permitir que a TI interna formate servidores para restaurar os serviços (RTO), é obrigatório consultar a equipe jurídica, forense externa ou a seguradora. A formatação apaga os rastros do atacante (destruição de provas), o que inviabiliza investigações legais e pode invalidar o pagamento do seguro.

Fonte: Baseado nas diretrizes do NIST (SP 800-61 Rev. 2: Computer Security Incident Handling Guide - Seção 2.3.2 Interacting with Outside Parties), CIS Controls (Controle 17: Incident Response Management), exigências da LGPD (Lei Geral de Proteção de Dados) referentes à ANPD, e manuais de notificação de incidentes do CTIR Gov.

Anexo 7

Planejar e conduzir cenários rotineiros de exercícios de mesa (tabletop)

Planejar e conduzir cenários rotineiros de exercícios de mesa (tabletop) com periodicidade regular, garantindo a participação da ETIR e o envolvimento direto da alta administração.

Um plano de resposta a incidentes que existe apenas no papel proporciona uma falsa sensação de segurança. Durante um ataque real, a falta de familiaridade com os processos leva ao pânico, decisões precipitadas e falhas de comunicação entre a equipe técnica e a diretoria. O objetivo destas diretrizes é instituir um programa contínuo de Exercícios de Mesa (*Tabletop Exercises* - TTX), criando um ambiente de simulação falada, livre de riscos tecnológicos, onde a ETIR e a Alta Administração possam testar a coordenação, alinhar expectativas e identificar gargalos antes que a crise verdadeira ocorra.

1. Escolha do Foco do Cenário (Tabletop)

Os exercícios de mesa devem variar em escopo para não se tornarem repetitivos e para testarem diferentes partes do plano de resposta. Os formatos ideais para rodízio são:

- **TTX Operacional (Foco Técnico):** Direcionado primariamente à ETIR e TI. Testa playbooks específicos (ex: isolamento de VLANs, acionamento de backups). A alta administração participa apenas como observadora ou em momentos pontuais de aprovação.
- **TTX Executivo (Foco Estratégico):** Direcionado à Alta Gestão, Jurídico e Comunicação. A ameaça cibernética é apenas o pano de fundo; o foco real é testar o gerenciamento de crise da instituição (ex: decidir se paga ou não um resgate de ransomware, aprovar notas para a imprensa, lidar com a ANPD).
- **TTX Integrado (Foco em Coordenação):** O cenário mais completo. Une a sala de máquinas (ETIR) e a diretoria na mesma dinâmica. Testa especificamente o fluxo de comunicação e a tradução do "tecniquês" para o risco de negócio em tempo real.

2. Arquitetura do Programa Contínuo (Periodicidade)

Um exercício isolado gera um pico de conscientização que logo se dissipa. A institucionalização exige um calendário estruturado (Programa de Exercícios):

- **Ciclo Semestral Recomendado:** Realizar um TTX a cada seis meses.
    - *Semestre 1*: Foco em ameaças de indisponibilidade (ex: Ransomware, Ataques DDoS).
    - *Semestre 2*: Foco em quebra de confidencialidade (ex: Vazamento de banco de dados, Insider Threat / ameaça interna).
- **Maturidade Progressiva:** O primeiro TTX do ano deve ser simples e linear. O subsequente deve introduzir cenários mais caóticos e injeções de informações simultâneas para estressar a capacidade de multitarefa do comitê.

3. Passos Práticos para Implementação

Passo 1: Planejamento e Engajamento da Diretoria

- Com pelo menos 60 dias de antecedência, bloqueie as agendas dos diretores. Para garantir o comparecimento, posicione o TTX não como um "treinamento de TI", mas como um "Exercício de Continuidade de Negócios e Mitigação de Risco Executivo".

Passo 2: Construção do Cenário e Injeções (Threat Modeling)

- Desenvolva um cenário altamente plausível para a realidade do órgão (ex: "Uma credencial de um funcionário do RH foi vendida na dark web").
- Prepare "Injeções" (novas informações entregues a cada 15-20 minutos) para evoluir a crise. Exemplo de Injeção: *"A imprensa acaba de ligar perguntando sobre o vazamento. O portal do cidadão também parou de responder."*

Passo 3: Definição das Regras do Jogo

- No início da sessão, o Facilitador deve declarar: "Este é um ambiente seguro (*blame-free*). O objetivo é quebrar o plano de resposta aqui na sala, não as pessoas. Joguem com os recursos que temos hoje, não com o que gostaríamos de ter amanhã."

Passo 4: Execução Baseada no Plano (Playbook)

- Evite que as respostas sejam apenas "achismos". O facilitador deve cobrar: "De acordo com o nosso plano atualizado, quem deve aprovar essa decisão de desligar o datacenter principal?". Se o plano não disser, anota-se a falha.

Passo 5: Sessão de Hotwash (Debriefing Imediato)

- Separe os últimos 30 minutos do encontro para um debate aberto. Quais foram as maiores dificuldades? Onde a comunicação falhou? O que precisamos comprar ou ajustar emergencialmente?

Passo 6: Relatório Pós-Ação (After Action Report - AAR)

- Em até duas semanas, emita um relatório documentando as lacunas descobertas e gere um Plano de Ação (ex: "O Jurídico não sabia o prazo de notificação da LGPD; ação: revisar fluxo jurídico").

4. Considerações de Contingência e Adoção

- **A Síndrome da Resposta Perfeita:** Membros da equipe de TI frequentemente tentam "vencer" o exercício, afirmando que suas ferramentas (antivírus, firewall) bloqueariam o ataque antes dele começar. O facilitador deve usar o "Cenário Magicamente Efetuado" (ex: "Entendo que temos firewall, mas para fins do exercício, considere que ele já foi burlado. O que fazemos agora?").
- **A Delegação Executiva:** É comum que diretores tentem mandar gerentes substitutos para o TTX por "falta de agenda". Isso deve ser desencorajado fortemente pelo patrocinador do programa (Presidência/CISO), pois a dinâmica testa a autoridade de tomada de decisão, algo que não pode ser facilmente delegado durante uma crise real.

O CISA (Cybersecurity and Infrastructure Security Agency) tem um guia bastante completo (https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages). A Agência de

segurança do Reino Unido (NCSC) também possui um (https://www.ncsc.gov.uk/section/exercise-in-a-box/overview) similar.

Fonte: Baseado nas diretrizes do NIST (SP 800-84: Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities), no manual do CISA (Tabletop Exercise Package - CISA CTEC) e nas boas práticas de avaliação de governança do PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 8

Realizar análises pós-incidente e pós-exercício

Realizar análises pós-incidente e pós-exercício, documentando as lacunas identificadas e atualizando o plano com as lições aprendidas e ações de acompanhamento.

A fase mais valiosa de um incidente cibernético ou de uma simulação de crise ocorre imediatamente após o seu fim. Omitir a fase de "Lições Aprendidas" significa desperdiçar a oportunidade de corrigir falhas sistêmicas, condenando a organização a cometer os mesmos erros no futuro. O objetivo destas diretrizes é estabelecer um processo formal e contínuo de análise pós-evento, transformando o caos de um incidente ou as falhas de um exercício de mesa (Tabletop) em melhorias concretas de governança, processos e tecnologias.

1. Escolha do Método de Análise

A profundidade da investigação deve ser proporcional à gravidade do incidente ou à complexidade do exercício. Os métodos recomendados variam em formalidade e tempo de execução:

- **Debriefing Imediato (Hotwash):** Reunião informal de 30 a 60 minutos realizada logo após o fim da contenção do incidente ou do término do exercício. (Captura impressões "a quente", enquanto a memória dos envolvidos está fresca).
- **Análise de Causa Raiz (RCA - Root Cause Analysis):** Investigação técnica aprofundada utilizando metodologias como os "5 Porquês" ou Diagrama de Ishikawa. (Ideal para incidentes de alta severidade, buscando entender como a vulnerabilidade inicial foi explorada).
- **Auditoria de Conformidade (Compliance Review):** Análise focada em validar se as exigências legais e regulatórias (como prazos de notificação da LGPD/ANPD) foram cumpridas durante a crise. (Essencial para mitigar riscos de multas pós-incidente).

2. Arquitetura da Documentação Pós-Evento

O conhecimento adquirido não pode ficar restrito à memória da Equipe de Tratamento de Incidentes (ETIR). Ele deve ser formalizado em um Relatório Pós-Ação (AAR - After Action Report), cuja arquitetura deve atender a dois públicos:

- **Cenário A: Registro Técnico (Para a ETIR e TI)** Foca no "Como". Detalha a linha do tempo técnica (ex: hora exata em que o firewall falhou), os Indicadores de Comprometimento (IoCs) mapeados, logs analisados e falhas específicas de configuração de segurança.
- **Cenário B: Registro Executivo (Para a Alta Administração)** Foca no "Impacto e Risco". Resume o impacto financeiro/operacional, o tempo total de indisponibilidade (RTO real vs. planejado), os custos de recuperação e as necessidades orçamentárias urgentes para que o problema não se repita.

3. Passos Práticos para Implementação

Passo 1: Convocação da Reunião de Lições Aprendidas

- Agende a reunião em, no máximo, **48 a 72 horas** após a resolução do incidente ou a conclusão do exercício. Atrasar esse encontro resulta em perda de detalhes cruciais.

- Convoque representantes de todas as áreas envolvidas (TI, ETIR, Jurídico, Comunicação, áreas de negócio afetadas).

Passo 2: Reconstrução da Linha do Tempo (Timeline)

- Compare a linha do tempo ideal (o que o Plano de Resposta dizia que deveria acontecer) com a linha do tempo real (o que efetivamente aconteceu).
- Documente atrasos (ex: "Levamos 4 horas para acionar o backup porque a documentação da senha estava desatualizada").

Passo 3: Identificação de Lacunas (Gap Analysis)

- Categorize as falhas descobertas no tripé de segurança:
    - **Pessoas:** Houve falta de treinamento? Alguém não sabia quem acionar?
    - **Processos:** O playbook estava desatualizado? A comunicação falhou?
    - **Tecnologia:** Faltou visibilidade de logs? O antivírus não detectou a ameaça?

Passo 4: Elaboração do Plano de Ação (CAPA)

- Converta as lacunas em um plano de Ações Corretivas e Preventivas (CAPA).
- **Regra de Ouro:** Nenhuma ação corretiva deve ser registrada sem um **Responsável (Owner)** e um **Prazo (Deadline)**. (Ex: "Atualizar lista de contatos do comitê" - Responsável: João / Prazo: 5 dias).

Passo 5: Atualização dos Playbooks e Procedimentos

- Modifique ativamente os Planos de Resposta a Incidentes (PRI) e os Playbooks com base nas descobertas. Se o exercício provou que a etapa 3 do plano não funciona na prática, reescreva-a imediatamente.

4. Considerações de Contingência e Adoção

- **Cultura Não Punitiva (Blame-Free Culture):** A reunião de lições aprendidas **não é um tribunal**. Se os colaboradores sentirem que o objetivo é caçar culpados ou aplicar demissões, eles esconderão falhas sistêmicas (ex: uso de senhas fracas por falta de um gerenciador). O foco deve ser estritamente na melhoria do processo.
- **Fadiga de Acompanhamento (Ações Órfãs):** O maior risco desta fase é o engavetamento do relatório. É comum gerar dezenas de tarefas de melhoria que morrem no backlog da TI por falta de tempo. É responsabilidade do CISO (ou Líder da ETIR) cobrar periodicamente o andamento do Plano de Ação e escalar para a Alta Administração caso tarefas críticas (como a compra de um link redundante) fiquem travadas.

Fonte: Baseado nas diretrizes do NIST (National Institute of Standards and Technology) (especificamente SP 800-61 Rev. 2, Seção 3.4 - Post-Incident Activity), no manual de Lessons Learned do SANS Institute, e nas práticas de melhoria contínua do PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 9

Ações para proteger a instituição contra-ataques de ransomware

Apesar do **Plano de Resposta a Incidentes (PRI)** e o **Plano de Gestão de Crises (PGC)** parecerem similares, a diferença reside no escopo de atuação, nos objetivos de controle e nas camadas do modelo de governança envolvidas.

O PRI é um conjunto de procedimentos operacionais e técnicos destinados a detectar, analisar, conter e recuperar a infraestrutura de TI de um evento adverso.

- **Foco Principal:** Triagem, contenção técnica e erradicação da ameaça.
- **Escopo:** Ativos de informação, redes, sistemas e dados.
- **Métricas (KPIs):** Tempo Médio de Detecção (MTTD) e Tempo Médio de Resposta (MTTR).
- **Fluxo de Trabalho:** Baseia-se em playbooks técnicos (ex: resposta a Ransomware, ataque DDoS ou Injeção de SQL).
- **Equipe:** CSIRT (Computer Security Incident Response Team) e SOC (Security Operations Center).

O PGC é um framework estratégico que lida com os impactos extra-técnicos resultantes de um incidente que ultrapassa a capacidade de contenção operacional ou que afeta a viabilidade do negócio.

- **Foco Principal:** Gestão de stakeholders, conformidade legal, comunicação externa e preservação da continuidade de negócios.
- **Escopo:** Reputação da marca, passivos jurídicos, impacto financeiro e relações governamentais/regulatórias.
- **Objetivo:** Gerenciar a incerteza e garantir a sobrevivência da organização perante o mercado e órgãos reguladores (como a ANPD em casos de LGPD).
- **Equipe:** Comitê de Crise (Alta Administração, Jurídico, Relações Públicas, Encarregado pelo Tratamento de Dados Pessoais e RH).

Ponto de acionamento entre planos

No gerenciamento de incidentes, ocorre o **escalonamento vertical**. Quando o incidente técnico atinge um limite crítico (ex: comprometimento total de um banco de dados de produção ou exfiltração de PII de alto volume), o PRI suspende a autonomia puramente técnica para reportar ao PGC. A partir desse ponto, as decisões técnicas (como desligar um serviço crítico para conter o ataque) passam a ser validadas pelo Comitê de Crise devido ao impacto financeiro/negocial envolvido.

Convém que a gestão de crises inclua

- O reconhecimento de situações que exijam ativação da gestão de crises;
- As pessoas competentes e responsáveis por analisar rapidamente as situações, definir estratégias, determinar opções, tomar decisões e avaliar o seu potencial impacto;

- Um entendimento comum dos princípios subjacentes à gestão de crises;
- As estruturas e os processos para traduzir decisões em ações, atribuir atividades e avaliar os resultados;
- O pessoal capaz de compartilhar, apoiar e implementar a visão, as intenções e as políticas da Alta Administração;
- A capacidade de apoiar soluções aplicando os recursos apropriados em tempo hábil;
- Uma estrutura organizacional que apoie e mantenha a capacidade de resposta a crises em curso;
- Uma cultura que suporte os princípios de gestão de crises.

Fonte: ISO/IEC 22361 (Segurança e resiliência — Gestão de crises — Diretrizes)

Anexo 10

Conscientização

Estabelecer simulações periódicas de engenharia social (ex.: testes mensais de phishing) para todos os agentes públicos, abordando cenários realistas do contexto organizacional ex.: notas fiscais falsas ou demandas urgentes forjadas

A conscientização em segurança da informação exige mais do que treinamentos teóricos anuais; ela demanda a construção de um "firewall humano" resiliente. Estabelecer simulações periódicas de engenharia social é fundamental para condicionar os agentes públicos a identificar e reportar ameaças de forma reflexa, reduzindo drasticamente a superfície de ataque da organização.

1. Escolha da Plataforma e Ferramental

Antes de iniciar os testes, defina qual solução técnica será utilizada para orquestrar e medir as campanhas. As opções variam em custo e complexidade:

- **Plataformas Nativas/Integradas:** Ferramentas de Treinamento de Simulação de Ataque podem ser utilizadas.
- **Plataformas Especializadas (SaaS):** Soluções de mercado como KnowBe4 ou PhishLine (Rica biblioteca de templates e alta facilidade de gestão).
- **Soluções Open-Source:** Ferramentas como GoPhish (Baixo custo, porém exigem infraestrutura própria, gestão de SMTP e maior esforço de configuração).

2. Arquitetura de Cenários e Vetores de Ataque

Para que o teste seja efetivo, os cenários devem refletir o dia a dia e as pressões do setor público:

- **Ameaças Financeiras/Administrativas:** Simulações de envio de notas fiscais falsas com links maliciosos, boletos em atraso ou comunicados de pregões eletrônicos forjados.
- **Demandas Urgentes e Autoridade (Spear Phishing):** E-mails simulando ordens de superiores, demandas jurídicas com prazos curtos ou solicitações urgentes do suporte de TI (ex.: "Atualize sua senha em 2 horas ou sua conta será bloqueada").
- **Ameaças Multicanal:** Expansão futura para *Smishing* (SMS malicioso) ou Vishing (ligações telefônicas falsas), refletindo abordagens modernas de atacantes.

3. Passos Práticos para Implementação

Passo 1: Planejamento e Preparação Técnica

- Defina o escopo de usuários e obtenha apoio da alta gestão e do RH/Jurídico.
- Configure *Whitelists* (listas de permissão) nos firewalls, gateways de e-mail e sistemas antispam para garantir que os e-mails de simulação não sejam bloqueados pelas soluções de segurança antes de chegarem aos usuários.

Passo 2: Definição da Linha de Base (Baseline)

- Realize um “teste cego” inicial sem aviso prévio para a organização (exceto para a gestão do projeto).
- Meça a taxa de cliques (Click Rate) e a taxa de comprometimento (quantos inseriram credenciais) para estabelecer o marco zero da instituição.

Passo 3: Configuração e Execução de Campanhas

- Desenvolva um calendário de testes mensais, variando o nível de dificuldade (identificação fácil vs. altamente sofisticada).
- Programe disparos aleatorizados (distribua os e-mails ao longo de dias e horários diferentes para evitar que um usuário avise os outros no corredor).

Passo 4: Resposta e Educação Imediata (Just-in-Time)

- Configure a “Página de Pouso” (Landing Page) para exibir uma mensagem educativa instantânea assim que o usuário cair no teste.
- Explique claramente quais foram as “bandeiras vermelhas” (red flags) do e-mail que o usuário deixou passar (ex.: domínio do remetente incorreto, senso de urgência falso).

Passo 5: Métricas e Monitoramento Contínuo

- Monitore não apenas a redução na taxa de cliques, mas principalmente o aumento na **Taxa de Reporte** (quantos usuários denunciaram o e-mail ativamente para a TI).
- Mapeie departamentos ou grupos de usuários de alto risco para direcionar treinamentos específicos.

4. Considerações de Contingência e Cultura

- **Cultura “No-Blame” (Não Punitiva):** O objetivo é educar, não punir. Evite expor publicamente ou aplicar sanções a usuários que caem nas simulações, pois isso gera medo e inibe a comunicação em incidentes reais de segurança.
- **Canal de Denúncia Simplificado:** Implemente um botão de “Reportar Phishing” diretamente no cliente de e-mail (Outlook/Gmail) para facilitar a notificação rápida de simulações e ameaças reais.
- **Alinhamento de Comunicação (Help Desk):** O suporte de TI deve estar preparado para o aumento de chamados durante os dias de campanha e orientado sobre como acolher o usuário que está em dúvida sobre a veracidade de um e-mail.

Fonte: NIST (National Institute of Standards and Technology) - SP 800-50 (Building an Information Technology Security Awareness and Training Program), CIS Controls (Controle 14: Conscientização e Treinamento de Segurança) e o PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 11

Cultura Educativa

Fomentar uma cultura não punitiva para os agentes públicos que falharem nas simulações, direcionando-os de forma construtiva a ações de reforço de conscientização

A implementação de simulações de cibersegurança (como campanhas de phishing simulado) é uma ferramenta essencial para fortalecer a proteção de dados na administração pública. No entanto, punir servidores que caem nessas armadilhas gera um ambiente de medo, ocultação de incidentes (subnotificação) e desengajamento. O objetivo destas diretrizes é estabelecer uma cultura de segurança positiva, onde o erro na simulação seja tratado como uma oportunidade de aprendizado, transformando o agente público em uma linha de defesa ativa.

1. Escolha das Ações de Reforço de Conscientização

Antes de iniciar as simulações, defina quais métodos educacionais serão acionados quando um agente público falhar no teste. As abordagens variam em formato e engajamento:

- **Just-in-Time Training (Treinamento Imediato):** Uma página de alerta amigável que se abre imediatamente após o clique, explicando o que era o teste e quais foram os sinais de alerta ignorados (Alto impacto pedagógico).
- **Microlearning:** Pílulas de conhecimento interativas de 3 a 5 minutos enviadas por e-mail nos dias seguintes à falha (Alta conveniência e retenção).
- **Gamificação e Reforço Positivo:** Pontuação e reconhecimento formal para usuários que identificam e reportam a simulação, em vez de focar apenas em quem clicou (Engajamento máximo).
- **Treinamento Departamental:** Workshops direcionados para áreas específicas se uma vulnerabilidade em massa for detectada, sem expor indivíduos (Abordagem colaborativa).

2. Arquitetura do Fluxo de Aprendizado

Para que a plataforma de simulação “converse” com os objetivos educacionais, é necessário estruturar o fluxo da informação:

- **Cenário A: Integração com o LMS (Learning Management System)** A plataforma de simulação de phishing é integrada (via API ou SCORM) ao portal de educação corporativa do órgão. Quando o agente clica no link simulado, ele é automaticamente matriculado em um curso de reciclagem curto no LMS, que o notifica de forma automatizada e confidencial.
- **Cenário B: Intervenção Direta na Plataforma de Segurança** Utilização dos módulos de treinamento nativos da própria ferramenta de simulação. O processo ocorre totalmente dentro do ambiente de e-mail e navegador do usuário, com relatórios gerenciais consolidados para o Encarregado pelo Tratamento de Dados Pessoais ou equipe de Segurança da Informação, garantindo o anonimato perante os pares.

3. Passos Práticos para Implementação

Passo 1: Comunicação de Transparência (Pre-launch)

- Divulgue amplamente o início do programa de conscientização para todos os servidores.
- Deixe explicitamente claro em normativas internas que as simulações não têm caráter punitivo, não afetarão avaliações de desempenho e não gerarão sanções administrativas.

Passo 2: Execução Ética das Simulações

- Crie cenários realistas, mas evite iscas emocionais antiéticas ou prejudiciais (ex: falsos comunicados sobre "demissões", "cortes salariais" ou "benefícios de saúde"). Foque em rotinas administrativas (ex: "atualização de senha", "documento do Office compartilhado").

Passo 3: Acolhimento Imediato (Just-in-Time)

- Se o usuário clicar no link malicioso simulado, redirecione-o para uma Landing Page neutra e educativa.
- **Mensagem sugerida:** "Ops! Este foi um teste de segurança. Se isso fosse um ataque real, nossos sistemas poderiam ter sido comprometidos. Veja abaixo as pistas que você poderia ter notado neste e-mail."

Passo 4: Trilha de Aprendizado Automatizada

- Configure a plataforma para enviar, 24 ou 48 horas após a falha, um e-mail confidencial ao servidor com um link para um vídeo de microlearning focado especificamente no tipo de ataque em que ele caiu (ex: Ransomware, Engenharia Social, Clonagem de Credenciais).

Passo 5: Acompanhamento de Reincidentes Crônicos

- Defina um limite técnico (ex: falhar em 3 simulações consecutivas).
- Para esses casos, não escale para advertências de RH. Em vez disso, a equipe de TI/Segurança deve realizar uma abordagem consultiva (ex: "Notamos que você recebe muitos e-mails externos, quer ajuda para configurar filtros melhores ou um treinamento rápido 1:1?").

Passo 6: Mudança nas Métricas de Sucesso (KPIs)

- Passe a medir e celebrar a **Taxa de Reporte** (quantos usuários clicaram no botão "Reportar Phishing"), em vez de focar apenas na redução da **Taxa de Cliques** (quantos caíram na isca).

4. Considerações de Contingência e Adoção

- **Apoio Técnico ao Invés de Cobrança:** Tenha em mente que usuários que caem repetidamente em phishing podem estar sobrecarregados de trabalho ou necessitar de controles técnicos compensatórios (ex: implementação obrigatória de MFA ou restrição de macros), e não apenas de mais treinamentos.

Botão de Reporte (Phish Alert Button): Garanta que os usuários tenham um botão visível e de fácil acesso no cliente de e-mail (Outlook, Gmail, Zimbra) para reportar mensagens suspeitas com apenas um clique. Isso capacita o usuário a agir corretamente.

Fonte: Baseado nas diretrizes do NIST (National Institute of Standards and Technology) (especificamente a publicação SP 800-50: Building an Information Technology Security Awareness and Training Program), CIS Controls (Controle 14: Security Awareness and Skills Training) e as diretrizes do PPSI (Programa de Privacidade e Segurança da Informação) focadas no fator humano e na cultura organizacional.

Anexo 12

Reporte de Incidentes

Estabelecer, divulgar e manter um processo institucional com um canal de comunicação simples e direto para que os agentes públicos notifiquem tempestivamente qualquer atividade suspeita

A capacidade de detectar e conter uma ameaça cibernética rapidamente depende diretamente da agilidade com que os usuários notificam a equipe de segurança. Processos burocráticos, formulários longos ou o medo de punição desestimulam o reporte, dando aos atacantes o tempo necessário para se infiltrarem na rede. Estas orientações técnicas visam estruturar um fluxo de trabalho eficiente para o reporte de incidentes e atividades suspeitas, garantindo que a instituição reaja com a celeridade necessária para mitigar riscos.

1. Escolha do Canal de Comunicação

Antes de desenhar o fluxo, defina por onde o agente público fará a notificação. Os canais devem priorizar a facilidade de uso e a disponibilidade:

- **Botão de Reporte no E-mail (Phish Alert Button):** Um suplemento no cliente de e-mail (Outlook, Zimbra, Google Workspace) que permite reportar mensagens suspeitas com um único clique (Conveniência máxima e envio automático de cabeçalhos/anexos originais).
- **Portal de Serviços (ITSM / Help Desk):** Um catálogo de serviços com um botão de destaque “Reportar Incidente de Segurança” na página inicial da intranet, com um formulário extremamente enxuto (Ideal para roubo/perda de dispositivos ou sistemas lentos).
- **Canal de Comunicação Direta (Hotline/Chat):** Um número de telefone de emergência ou canal específico no comunicador corporativo (Teams, Slack, WhatsApp Business) (Essencial para incidentes críticos e imediatos, como telas de ransomware).
- **E-mail Dedicado (ex: seguranca@orgao.gov.br):** Método tradicional e de fácil memorização, embora exija triagem mais manual por parte da equipe técnica.

2. Arquitetura do Fluxo de Atendimento

Para que os chamados não se percam no volume diário do suporte de TI, é necessário estruturar como a notificação será roteada:

- **Cenário A: Automação e Triagem Direta (SOAR/SIEM)** Se houver maturidade técnica, os reportes (especialmente do Botão de E-mail) vão direto para a ferramenta de segurança da informação. Sistemas automatizados examinam links e anexos (sandbox) e já classificam a ameaça, alertando o Centro de Resposta a Incidentes (CSIRT/SOC) apenas em caso de perigo real, reduzindo o esforço humano.
- **Cenário B: Triagem em Camadas (Help Desk Nível 1)** Todos os reportes chegam ao Service Desk comum. Cria-se um procedimento padrão (SOP) rápido para que os atendentes de Nível 1 saibam separar dúvidas comuns (falsos positivos) de potenciais incidentes de segurança, escalando imediatamente estes últimos para a equipe especializada, “furando a fila” dos chamados convencionais.

3. Passos Práticos para Implementação

Passo 1: Definição da Matriz de Incidentes e SLAs

- Catalogue o que é considerado um incidente para o usuário comum (ex: e-mail de phishing, perda de notebook, senha exposta, computador bloqueado).
- Defina Acordos de Nível de Serviço (SLA) específicos e agressivos para chamados classificados como segurança (ex: tempo de resposta inicial de 15 minutos).

Passo 2: Estabelecimento de um "Safe Harbor" (Política de Não Retaliação)

- Documente e divulgue que agentes públicos que reportarem incidentes não sofrerão sanções administrativas, mesmo que eles próprios tenham causado o incidente acidentalmente (ex: clicou no link antes de perceber o erro). A honestidade e a tempestividade devem ser premiadas.

Passo 3: Implantação da Tecnologia e Canais

- Instale o botão de reporte nos clientes de e-mail institucionais.
- Crie a categoria de segurança no sistema de chamados.
- Disponibilize o número de telefone de emergência em adesivos nos equipamentos ou na assinatura de tela dos computadores.

Passo 4: Campanha de Lançamento e Letramento

- Não basta criar o canal; os servidores precisam conhecê-lo. Lance campanhas curtas explicando: "Viu algo estranho? Não tente resolver sozinho e não tenha medo. Avise a TI pelo canal X".
- Ensine a diferença entre um problema de TI (ex: impressora não funciona) e um incidente de segurança (ex: impressora imprimindo mensagens estranhas).

Passo 5: Estabelecimento do "Loop de Retorno" (Feedback ao Usuário)

- Ação Crítica: Quando um usuário reportar algo, nunca deixe o chamado terminar sem resposta. Configure respostas automáticas de agradecimento e, após a análise técnica, informe o resultado (ex: "Muito obrigado! Sua denúncia confirmou um ataque de phishing que já foi bloqueado para toda a instituição."). Isso valida a atitude do servidor e garante engajamento futuro.

4. Considerações de Contingência e Adoção

- **Fadiga de Falsos Positivos:** No início do programa, é esperado que os servidores reportem e-mails legítimos (como newsletters ou comunicações de RH). A equipe técnica deve estar dimensionada e preparada para acolher esses reportes sem hostilidade, usando-os como oportunidades de micro-educação.
- **Canais Out-of-Band (Comunicação Fora de Banda):** Tenha um plano de contingência caso a infraestrutura principal (Rede e E-mail) caia ou seja sequestrada. Como o usuário avisa a TI se o computador nem sequer liga? Telefone físico, grupos de WhatsApp pré-aprovados ou comunicação via chefias imediatas devem estar mapeados.

Fonte: Baseado nas diretrizes do NIST (National Institute of Standards and Technology) (especificamente a publicação SP 800-61 Rev. 2: Computer Security Incident Handling Guide), CIS Controls (Controle 17: Incident Response Management) e as diretrizes do PPSI (Programa de Privacidade e Segurança da Informação) referentes à gestão de incidentes corporativos.

Anexo 13

Capacitação Técnica

Incluir, nos instrumentos de desenvolvimento de pessoas da organização (ex.: Plano de Desenvolvimento de Pessoas), treinamentos técnicos específicos para a área de TI e Segurança da Informação, abrangendo competências como resposta a incidentes, análise forense e DevSecOps

A evolução constante das ameaças cibernéticas exige que as equipes de Tecnologia da Informação (TI) e Segurança da Informação atuem sempre um passo à frente. Depender apenas de conhecimentos generalistas ou obsoletos deixa a instituição vulnerável a ataques complexos. O objetivo destas diretrizes é formalizar a capacitação técnica avançada nos instrumentos de gestão de pessoas (como o Plano de Desenvolvimento de Pessoas - PDP), garantindo orçamento e tempo para que os agentes técnicos dominem disciplinas críticas como DevSecOps, Resposta a Incidentes e Análise Forense, transformando a TI de um centro reativo em uma força de defesa proativa.

1. Escolha do Modelo de Capacitação

Antes de alocar recursos, defina quais formatos de treinamento melhor atendem à rotina e aos objetivos técnicos da equipe. Os modelos variam em custo, profundidade e aplicação prática:

- **Laboratórios Práticos e Cyber Ranges:** Plataformas de simulação de ataque e defesa em tempo real (ex: Hack The Box, TryHackMe). (Excelente custo-benefício, aprendizado contínuo e prático).
- **Certificações Profissionais Reconhecidas:** Financiamento de cursos e vouchers para exames de mercado (ex: CompTIA Security+, SANS/GIAC, CISSP, AWS Certified Security). (Alto custo, mas estabelece um padrão de excelência e nivela o conhecimento técnico).
- **Treinamentos *In-Company* / Bootcamps:** Contratação de especialistas para imersões de alguns dias com toda a equipe sobre tecnologias específicas utilizadas no órgão (Ideal para alinhamento rápido em novas ferramentas ou frameworks).
- **Participação em Conferências Técnicas:** Envio de servidores para fóruns e eventos de cibersegurança e infraestrutura. (Foco em tendências de mercado, networking e *threat intelligence*).

2. Arquitetura das Trilhas de Conhecimento

A capacitação não deve ser “tamanho único”. É necessário dividir os esforços educacionais de acordo com o papel do servidor na arquitetura de TI:

- **Cenário A: Integração de Segurança (Foco em Desenvolvedores e Infraestrutura)** A trilha de **DevSecOps** é voltada para quem constrói e mantém os sistemas. O foco aqui não é transformar o desenvolvedor em um analista de segurança, mas ensiná-lo a programar de forma segura (framework OWASP), utilizar ferramentas de análise de código (SAST/DAST) no pipeline de CI/CD e aplicar conceitos de Infraestrutura como Código (IaC) e segurança em contêineres.
- **Cenário B: Especialização de Defesa (Foco em Blue Team / SOC / CSIRT)** A trilha de **Resposta e Análise** é voltada para a equipe de segurança dedicada. Abrange treinamentos densos em triagem de malwares, contenção de ataques (Ransomware/DDoS), caça a ameaças (*Threat Hunting*) e Análise Forense Digital (coleta e preservação de evidências para investigações legais ou administrativas).

3. Passos Práticos para Implementação

Passo 1: Mapeamento de Lacunas de Competências (Skills Gap Analysis)

- Faça um levantamento das tecnologias críticas do órgão e cruze com os conhecimentos atuais da equipe.
- Identifique os pontos cegos (ex: "Temos muitos sistemas na nuvem, mas ninguém com treinamento formal em segurança de *Cloud"*).

Passo 2: Inclusão Estratégica no PDP

- Utilize o levantamento do Passo 1 para justificar a inclusão dessas capacitações no Plano de Desenvolvimento de Pessoas (PDP) do ano seguinte, garantindo o empenho orçamentário.
- Desvincule a capacitação de segurança do orçamento geral de TI; ela deve ter uma rubrica dedicada para não ser canibalizada por urgências operacionais.

Passo 3: Definição de Metas de Estudo no Horário de Trabalho

- O aprendizado técnico complexo exige foco. Estabeleça políticas que permitam aos servidores dedicar algumas horas de sua jornada semanal (ex: sexta-feira à tarde) exclusivamente para consumir as plataformas de *Cyber Range* ou cursos oficiais, sem interrupções do *Help Desk*.

Passo 4: Criação do "ROI Educacional" (Retorno sobre Investimento)

- Condicione o pagamento de treinamentos e certificações caras a um compromisso de repasse de conhecimento.
- O servidor que retornar do treinamento deverá conduzir um *Workshop* interno ou escrever documentações técnicas para disseminar o que aprendeu com o restante da equipe.

Passo 5: Simulações de Mesa (Tabletop Exercises)

- Utilize as capacitações teóricas para rodar exercícios práticos trimestrais. Reúna a equipe de TI e simule um ataque real (ex: "O servidor de banco de dados principal foi criptografado. Como aplicamos o que aprendemos no curso de Resposta a Incidentes agora?").

4. Considerações de Contingência e Adoção

- **Risco de Fuga de Talentos (Turnover):** Existe o receio comum de capacitar o agente público e ele deixar o órgão para a iniciativa privada. No entanto, o custo de não treiná-lo e sofrer um ataque é infinitamente maior. Para mitigar, vincule certificações de alto custo a contrapartidas legais de permanência mínima no órgão ou invista na melhoria do ambiente de trabalho e plano de carreira.
- **Obsolescência Rápida:** O conhecimento em cibersegurança "vence" rapidamente. Prefira assinar plataformas de acesso contínuo e atualizado do que comprar cursos estáticos que em um ano estarão defasados.

Fonte: Baseado nas diretrizes do NIST (especificamente o NICE Workforce Framework for Cybersecurity - SP 800-181, que padroniza papéis e competências), CIS Controls (Controle 2: Inventory and Control of Software Assets / Treinamento de Desenvolvedores) e as diretrizes de governança do PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 14

Simulações de Crise

Planejar e conduzir exercícios rotineiros de tratamento de incidentes (como Tabletop Exercises ou simulações Red/Blue Team) envolvendo a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) e a alta administração>

Ter um Plano de Resposta a Incidentes documentado é fundamental, mas a verdadeira resiliência cibernética só é testada quando o plano é colocado em prática. Em uma crise real de cibersegurança, o pânico e a falta de coordenação podem causar mais danos do que o próprio ataque. O objetivo destas diretrizes é instituir uma cultura de simulações de crise recorrentes, garantindo que a Equipe de Tratamento de Incidentes (ETIR) desenvolva "memória muscular" técnica e que a Alta Administração saiba tomar decisões estratégicas sob pressão.

1. Escolha do Modelo de Simulação

A complexidade do exercício deve acompanhar a maturidade de segurança da organização. Os formatos variam em impacto operacional e objetivos:

- **Tabletop Exercises (TTX - Exercícios de Mesa):** Reuniões de discussão guiadas por um facilitador, onde a equipe técnica e os executivos debatem verbalmente como reagiriam a um cenário hipotético em evolução (Baixo custo, sem impacto na infraestrutura, alto valor estratégico).

- **Purple Teaming (Exercícios Colaborativos):** A equipe de ataque (Red Team) executa técnicas reais lado a lado com a equipe de defesa (Blue Team/ETIR), validando em tempo real se os alertas do sistema funcionam e ajustando as configurações imediatamente (Alto valor de aprendizado técnico mútuo).

- **Simulações Red/Blue Team (Combate Cego):** Testes não anunciados onde uma equipe ataca a infraestrutura e a ETIR deve detectar e conter a ameaça como se fosse real. (Alta complexidade, exige maturidade para não gerar interrupção de serviços reais).

2. Arquitetura dos Cenários de Crise

Os exercícios não devem ser aleatórios; eles precisam ser desenhados para testar camadas específicas da governança e da tecnologia do órgão:

- **Cenário A: Foco Operacional (ETIR / SOC)** Avalia a capacidade de detecção, contenção e erradicação. Exemplo: *Simulação de movimentação lateral de um malware a partir de uma credencial comprometida de um terceirizado*. O teste valida se a equipe consegue isolar a máquina da rede rapidamente e se os logs de auditoria são suficientes para a análise forense.

- **Cenário B: Foco Estratégico e de Negócios (Comitê de Crise / Alta Administração)** Avalia o gerenciamento de crise, comunicação e obrigações legais. Exemplo: *Simulação de um ataque de Ransomware com duplo impacto (criptografia + roubo de dados sensíveis dos cidadãos)*. O teste valida o tempo de acionamento jurídico, quando notificar a ANPD (Autoridade Nacional de Proteção de Dados), como lidar com a imprensa e a tomada de decisão sobre restaurar backups versus impacto no negócio.

3. Passos Práticos para Implementação

Passo 1: Definição do Escopo e Regras de Engajamento (RoE)

- Determine o que será testado (ex: apenas o plano de comunicação ou a restauração de um banco de dados?).
- Se houver testes técnicos, defina explicitamente as "Regras de Engajamento" para garantir que nenhum sistema crítico real seja derrubado durante a simulação.

Passo 2: Elaboração do Cenário de Ameaça (Threat Modeling)

- Crie histórias realistas baseadas em ameaças que o setor público enfrenta (ex: ataque de negação de serviço - DDoS durante período de arrecadação de impostos).
- Prepare "Injeções" (novas informações introduzidas no meio do exercício para aumentar a tensão, ex: "O backup primário também estava corrompido, o que fazemos agora?").

Passo 3: Engajamento Executivo pré-exercício

- Garanta que os diretores e líderes (Jurídico, Comunicação, RH e Alta Gestão) estejam com a agenda bloqueada. O engajamento deles é inegociável, pois as crises não são problemas exclusivos da TI.

Passo 4: Condução do Exercício (Facilitação)

- O facilitador apresenta o cenário passo a passo.
- Deixe que os participantes usem os planos documentados (Playbooks) para embasar suas respostas. Se o plano falhar ou faltar informação, isso deve ser anotado, não punido.

Passo 5: Sessão de "Hotwash" (Debriefing Imediato)

- Imediatamente após o fim da simulação, faça uma reunião de 30 minutos para capturar as impressões a quente. Pergunte: "O que funcionou bem?", "Onde hesitamos?", "O que faríamos diferente?".

Passo 6: Emissão do Relatório Pós-Ação (After Action Report - AAR)

- Documente formalmente as falhas descobertas e transforme-as em um Plano de Ação com prazos e responsáveis (ex: "Atualizar a lista telefônica do Comitê de Crise", "Contratar link de internet redundante").

4. Considerações de Contingência e Adoção

- **Cultura Não Punitiva (Blame-Free):** O objetivo do exercício de crise é "quebrar" o processo na sala de reunião para que ele não quebre na vida real. Se a equipe descobrir que o plano de resposta falhou miseravelmente, a simulação foi um sucesso absoluto. Ninguém deve ser repreendido por decisões erradas tomadas durante o exercício.
- **Fadiga de Simulação:** Evite exercícios excessivamente longos ou muito frequentes a ponto de desgastar as equipes. Um Tabletop Exercise (Exercício de mesa) profundo por semestre ou trimestre é geralmente o ideal para manter o engajamento sem esgotar a operação.

Fonte: Baseado nas diretrizes do NIST (National Institute of Standards and Technology) (especificamente a publicação SP 800-84: Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities), CIS Controls (Controle 17: Incident Response Management) e as diretrizes de resposta do PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 15

Comunicação de Crise

Determinar e testar mecanismos de comunicação primários e secundários, incluindo canais alternativos (out-of-band), garantindo que a coordenação do tratamento do incidente ocorra de forma ininterrupta, mesmo que os sistemas corporativos (ex.: e-mail institucional) sejam afetados pelo ataque

Durante um incidente cibernético de alta gravidade, como um ataque de ransomware, é comum que a primeira ação do invasor seja comprometer ou derrubar a infraestrutura de comunicação da instituição (E-mail corporativo, Serviço de diretório, Plataforma de comunicação e colaboração, etc.). Se a equipe de resposta depender desses sistemas para coordenar a defesa, o invasor não apenas impedirá a reação, mas também poderá ler as estratégias de contenção em tempo real. O objetivo destas diretrizes é estruturar uma rede de comunicação resiliente e paralela (Out-of-Band - OOB), garantindo que a governança da crise não seja interrompida mesmo no pior cenário técnico possível.

1. Escolha dos Canais de Comunicação

Antes de uma crise acontecer, a organização deve mapear e oficializar quais ferramentas serão usadas em cada nível de gravidade do incidente:

- **Comunicação Primária (In-Band):** E-mail corporativo institucional, Plataforma de trabalho e comunicação corporativa ou ramais VoIP da rede interna. (Uso: Incidentes de baixo impacto, onde há certeza de que o ambiente corporativo não foi totalmente comprometido).
- **Comunicação Secundária Criptografada (Out-of-Band):** Aplicativos de mensagens de ponta a ponta independentes da infraestrutura da organização, como Signal, Threema ou WhatsApp. (Uso: Crises severas e indisponibilidade de serviços internos. O Signal é altamente recomendado pela privacidade).
- **Comunicação Baseada em Nuvem Alternativa:** Um “tenant” (ambiente) isolado em outra nuvem, pago pela organização, mas que não compartilha senhas com a rede principal (ex: um workspace do Slack externo ou Google Meet isolado). (Uso: Coordenação centralizada (War Room virtual) livre de interceptação).
- **Comunicação Analógica e Física:** Telefonia celular convencional (ligações de voz), SMS e uma “War Room” (Sala de Guerra) física pré-determinada. (Uso: Cenários catastróficos ou de apagão total de conectividade).

2. Arquitetura da Governança de Comunicação

A comunicação de crise precisa de canais específicos para públicos específicos. Não se coloca toda a organização no mesmo canal. A arquitetura recomendada divide-se em:

- **Cenário A: Canal Tático/Técnico (Sala de Operações)** Grupo fechado de comunicação out-of-Band (ex: grupo no Signal) contendo estritamente a equipe da ETIR (Equipe de Tratamento de Incidentes), administradores de rede e provedores de segurança gerenciada (SOC/MSSP). O foco é o compartilhamento rápido de indicadores de comprometimento (IoCs) e comandos técnicos.
- **Cenário B: Canal Estratégico (Comitê de Crise)** Grupo separado contendo a Alta Administração, Encarregado pelo Tratamento de Dados Pessoais, Jurídico, RH e o líder da ETIR. O foco é a tomada de

decisão executiva (ex: aprovar a notificação à ANPD, desligar servidores críticos, aprovar comunicados de imprensa).

3. Passos Práticos para Implementação

Passo 1: Criação da "Call Tree" (Árvore de Acionamento)

- Documente quem deve ligar para quem nos primeiros 15 minutos de uma crise crítica.
- Defina substitutos imediatos (ex: "Se o Diretor de TI não atender em 5 minutos, ligue para o Gerente de Infraestrutura").

Passo 2: Provisionamento Prévio (Pre-staging)

- Não espere o incidente ocorrer para criar os grupos de WhatsApp ou Signal.
- Crie os grupos hoje, nomeie-os de forma clara e adicione os membros essenciais. Mantenha os grupos silenciados até que sejam necessários.

Passo 3: Criação de Diretórios Offline

- A lista de contatos da Call Tree (com números de telefone pessoais ou corporativos alternativos) deve ser impressa em papel ou salva localmente (em formato PDF criptografado) nos celulares e notebooks da equipe. Se o Active Directory cair, a lista de ramais da intranet estará inacessível.

Passo 4: Protocolos de Migração de Canal

- Estabeleça um gatilho claro de quando abandonar a comunicação Primária.
- **Regra de Ouro:** Em qualquer suspeita de comprometimento de e-mail corporativo (Business Email Compromise - BEC) ou movimentação de um invasor na rede, assume que o invasor está lendo seus e-mails e mude imediatamente para o canal Out-of-Band.

Passo 5: Alinhamento de Comunicação Externa

- Defina previamente modelos (templates) de comunicados para a imprensa, servidores e cidadãos, aprovados pelo setor Jurídico, para que precisem apenas ser preenchidos com os detalhes do incidente e disparados rapidamente via redes sociais ou canais de contingência.

4. Considerações de Contingência e Adoção

- **Risco de Vazamento Acidental:** Lembre as equipes de que, ao usar canais alternativos (especialmente dispositivos pessoais de forma contingencial), devem evitar enviar prints de telas contendo dados sensíveis ou senhas em texto claro, pois esses dispositivos podem não ter as políticas de segurança (MDM) da instituição.
- **Acesso à Sala de Guerra Física:** Se a estratégia envolver uma sala de reunião física de emergência, certifique-se de que ela não dependa de catracas eletrônicas que precisem da rede do órgão para validar o crachá.

Fonte: Baseado nas diretrizes do NIST (National Institute of Standards and Technology) (publicação SP 800-61 Rev. 2, seção de Comunicações), CIS Controls (Controle 17: Incident Response Management) e as boas práticas de Continuidade de Negócios do PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 16

Limitar rigorosamente os membros de grupos de alto privilégio

Limitar rigorosamente os membros de grupos de alto privilégio (como Domain Admins) ao mínimo absoluto (ex.: 2 ou 3 acessos), garantindo que esses privilégios pertençam exclusivamente a contas de administrador dedicadas.

A restrição rigorosa de membros em grupos de alto privilégio mitiga drasticamente a superfície de ataque lateral e o risco de comprometimento de credenciais em cenários de *Pass-the-Hash (ataque de repetição de hash)*. Ao isolar essas funções em contas administrativas dedicadas, implementa-se o princípio do menor privilégio e a segregação de funções, essenciais para a integridade do diretório. Abaixo, apresentamos as orientações técnicas para implementar o modelo de **Privilégio Mínimo** e a segregação de contas.

1. Definição da Estrutura de Contas

O erro mais comum é utilizar a mesma conta para ler e-mails e administrar o domínio. A arquitetura deve separar as identidades:

- **Contas de Usuário Padrão:** Utilizadas para tarefas do dia a dia (E-mail, Office, Navegação). Nunca possuem privilégios administrativos.
- **Contas de Administração Dedicadas:** Contas exclusivas (ex: adm_joao) utilizadas apenas para tarefas de infraestrutura. Elas não possuem caixa de e-mail e não acessam a internet.

2. Higiene de Grupos de Alto Privilégio

Para limitar o acesso ao mínimo absoluto (2 ou 3 membros), siga estes critérios:

- **Domain Admins / Enterprise Admins:** Devem ser reservados apenas para modificações no nível da floresta ou do domínio.
- **Uso de Grupos Locais:** Em vez de tornar um usuário "Domain Admin" para gerenciar um servidor específico, adicione a conta de administração dele ao grupo de **Administradores Locais** daquela máquina.
- **Contas de Serviço:** Jamais adicione contas de serviço (usadas por softwares) aos grupos de Domain Admins. Utilize *Managed Service Accounts* (gMSA).

3. Passos Práticos para Implementação

Passo 1: Auditoria de Direitos e Permissões

- Realize uma varredura em grupos de "Super Usuários" (Ex: *Global Admins, Domain Admins, Root*).
- Identifique contas inativas ou "contas de serviço" (bots/scripts) que possuam privilégios excessivos e remova-as imediatamente.

Passo 2: Implementação do Privilégio Mínimo (PoLP)

- Substitua o acesso total por **Permissões Granulares**. Em vez de tornar alguém administrador do sistema inteiro, conceda permissão apenas para o serviço que ele gerencia (ex: apenas gestão de DNS ou apenas gestão de usuários).

Passo 3: Fluxo de Acesso Just-in-Time (JIT)

- Para os 2 ou 3 acessos remanescentes, utilize o conceito de **Elevação Temporária**. O usuário permanece com privilégios baixos e, quando necessário, solicita a elevação por um tempo determinado (ex: 4 horas), com justificativa e aprovação registrada.

Passo 4: Isolamento de Sessão

- A gestão do diretório central deve ocorrer apenas a partir de dispositivos ou ambientes isolados (como máquinas de salto ou *bastion hosts*), garantindo que credenciais de alto nível nunca transitem por máquinas comuns.

4. Governança e Resiliência

- **Revisão Periódica:** Estabeleça uma revisão trimestral obrigatória para confirmar se os 2 ou 3 detentores de privilégios ainda necessitam dessa função.

Cofre de Contingência (Break-glass): Mantenha uma conta de emergência altamente protegida e monitorada. O uso desta conta deve disparar alertas críticos para toda a diretoria de TI/Segurança.

Monitoramento de Comportamento: Implemente alertas para qualquer criação de nova conta com privilégios elevados, garantindo que o limite de 2 ou 3 acessos não seja burlado.

Fonte: NIST SP 800-53 (AC-6: Least Privilege), NIST Cybersecurity Framework (PR.AC-4) e CIS Control 5 (Account Management).

Anexo 17

Definir e documentar o controle de acesso baseado em funções

Definir e documentar o controle de acesso baseado em funções, habilitando grupos de segurança restritivos (como o Protected Users Security Group) para contas privilegiadas, a fim de mitigar a exposição e o roubo de credenciais em memória.

A implementação de **Role-Based Access Control (RBAC)** e o uso de grupos como o **Protected Users (Usuários protegidos)** mitigam o movimento lateral ao restringir o cache de credenciais e delegar permissões mínimas necessárias. Essa arquitetura reduz a superfície de ataque em memória (LSASS), impedindo que hashes e tickets sensíveis sejam expostos a técnicas de roubo como o Pass-the-Hash. O objetivo é transformar a estrutura de acessos de um modelo permissivo para um modelo defensivo, onde a função determina o acesso e a tecnologia protege o segredo.

1. Implementação do RBAC (Controle de Acesso Baseado em Funções)

Antes da tecnologia, a organização precisa definir "quem faz o quê". O RBAC reduz o erro humano e a concessão excessiva de privilégios.

- **Mapeamento de Funções:** Identifique perfis claros (ex: Administrador de Rede, Gestor de Identidades, Auditor de Segurança).
- **Atribuição por Grupos:** Nunca atribua permissões diretamente a um indivíduo. As permissões são dadas ao **Grupo de Segurança**, e o usuário é inserido no grupo.
- **Documentação de Matriz de Acessos:** Mantenha um registro formal que correlacione cada função às suas permissões específicas, facilitando auditorias e revogação de acessos.

2. Grupos de Segurança Restritivos (Hardening)

Para contas de alto privilégio, apenas a senha não basta. É necessário ativar proteções nativas que limitem como o sistema operacional lida com essas credenciais.

- **Isolamento de Credenciais:** Utilize grupos especiais (como o *Protected Users* ou equivalentes em ambientes Cloud/Unix) que forçam métodos de autenticação mais seguros.
- **Desativação de Protocolos Legados:** Estes grupos impedem o uso de protocolos fracos (como NTLM ou digest authentication) que deixam "rastros" fáceis de capturar na memória (RAM).
- **Restrição de Cache:** Contas nesses grupos não têm suas credenciais armazenadas em cache local. Se o administrador deslogar, a credencial desaparece, impedindo ataques de *Pass-the-Hash*.

3. Passos Práticos para Implementação

Passo 1: Classificação de Contas

- Separe as contas em "Comuns" e "Sensíveis".
- Identifique as contas que possuem poder de alteração em configurações globais ou acesso a dados críticos.

Passo 2: Configuração de Políticas de Segurança

- Configure o sistema para exigir autenticação baseada em certificados ou chaves modernas para os grupos restritivos.
- Limite o **Tempo de Vida do Ticket (TTL)**: Reduza o tempo de validade dos tokens de autenticação para contas privilegiadas.

Passo 3: Ativação dos Grupos Restritivos

- Mova gradualmente as contas de administração para o grupo de segurança restritivo.
- **Aviso:** Teste antes em laboratório, pois esses grupos podem impedir o login se o ambiente utilizar protocolos muito antigos ou não suportar criptografia moderna (como AES).

Passo 4: Proteção contra Roubo em Memória

- Habilite proteções de integridade de código e isolamento de processos (como o LSA Protection).
- Garanta que administradores nunca façam login em máquinas de nível de segurança inferior ao da sua conta.

4. Considerações de Segurança e Monitoramento

- **Monitoramento de Processos:** Utilize ferramentas para detectar tentativas de leitura da memória do processo de autenticação (ex: tentativas de acesso ao lsass.exe).
- **Higiene de Sessão:** Force o encerramento de sessões administrativas inativas. O roubo de credenciais em memória geralmente ocorre em sessões “esquecidas” no servidor.
- **Revisão de RBAC:** Sempre que um colaborador mudar de função, sua conta deve ser movida entre os grupos de segurança, garantindo que ele não acumule privilégios de cargos anteriores.

Fonte: NIST SP 800-207 (Zero Trust Architecture), Microsoft Security Best Practices (Protected Users Security Group) e MITRE ATT&CK (Mitigação para técnicas de OS Credential Dumping).

Anexo 18

Gerenciar os ativos e o diretório de forma segura

Gerenciar os ativos e o diretório de forma segura, desabilitando protocolos de autenticação antigos e inerentemente vulneráveis (como NTLMv1 e Kerberos DES), forçando o uso de protocolos de rede seguros.

A gestão centralizada de ativos e identidades permite o controle granular da superfície de ataque, mitigando movimentações laterais indesejadas na infraestrutura. Desabilitar protocolos legados (como NTLMv1 ou SMBv1) elimina vetores de exploração por força bruta (*brute force*) e revezamento (*relay*), garantindo que apenas métodos de autenticação modernos e criptograficamente robustos sejam aceitos. A segurança de um serviço de diretório é tão forte quanto o seu protocolo mais fraco. Manter retrocompatibilidade com sistemas legados cria "portas dos fundos" que atacantes exploram para capturar hashes e realizar movimentos laterais.

1. Identificação de Protocolos Inerentemente Vulneráveis

A segurança do ambiente é limitada pelo protocolo mais fraco permitido. Protocolos antigos carecem de criptografia robusta e integridade, facilitando ataques de interceptação.

- **Autenticação de Baixa Segurança:** Métodos que usam hashes obsoletos ou que não protegem contra ataques de "replay".
    - *Exemplo AD:* **NTLMv1**, que pode ter suas credenciais capturadas e quebradas rapidamente.
- **Criptografia Legada:** Uso de algoritmos com chaves curtas e vulneráveis a força bruta.
    - *Exemplo AD:* **Kerberos com criptografia DES ou RC4**.
- **Comunicação em Texto Claro:** Serviços que transmitem dados sem cifragem de transporte.
    - *Exemplo AD:* Consultas **LDAP via porta 389** (sem StartTLS) ou o uso de **SMBv1**.

2. Inventário e Análise de Impacto

Antes de desativar protocolos, é necessário mapear a dependência de sistemas legados para evitar interrupções de serviço.

- **Habilitação de Auditoria:** Ative logs específicos para identificar quem ainda utiliza métodos antigos.
    - *Exemplo AD:* Logs de eventos de logon para identificar tráfego NTLM ou criptografia Kerberos fraca.
- **Mapeamento de Dispositivos de Rede:** Identifique ativos como impressoras, storages antigos ou sistemas de CFTV que podem não suportar padrões modernos.
- **Plano de Atualização/Isolamento:** Ativos que não suportam protocolos seguros devem ser atualizados ou movidos para redes isoladas (VLANs) com controles compensatórios.

3. Passos Práticos para Implementação

Passo 1: Imposição de Criptografia de Camada de Transporte

- **Forçar Canais Seguros:** Desative o tráfego de diretório não cifrado em favor de conexões protegidas por TLS.
    - *Exemplo AD:* Exigir **LDAPS (porta 636)** ou **LDAP Signing**.
- **Desativar Cifras Fracas:** Remova o suporte a protocolos como SSL 2.0/3.0 e TLS 1.0/1.1.

Passo 2: Endurecimento da Autenticação (Hardening)

- **Elevação do Nível de Autenticação:** Force o uso das versões mais recentes e seguras de cada protocolo de rede.
    - *Exemplo AD:* Configurar o nível de autenticação LAN Manager para **"Enviar apenas NTLMv2"** e recusar versões anteriores.
- **Criptografia de Ticket Robusta:** Garanta que a troca de chaves utilize algoritmos de última geração.
    - *Exemplo AD:* Configurar o domínio para exigir apenas **AES-128 e AES-256** para tickets Kerberos.

Passo 3: Proteção de Integridade e Canal

- **Assinatura de Pacotes:** Implemente a assinatura digital em todas as comunicações de rede para impedir ataques de *Man-in-the-Middle*.
    - *Exemplo AD:* Exigir **SMB Signing** para todos os servidores e estações.
- **Channel Binding:** Utilize técnicas que vinculam a autenticação ao túnel TLS, impedindo que tokens sejam desviados.

4. Governança e Sustentabilidade

- **Baseline de Segurança:** Novas implementações de servidores e ativos devem seguir uma configuração padrão (Golden Image) com protocolos legados já desativados.
- **Monitoramento de Downgrade:** Configure alertas para detectar quando um cliente tenta forçar o uso de um protocolo inferior, o que pode indicar uma tentativa de exploração ativa.
- **Ciclo de Vida de Ativos:** Estabeleça como requisito de compras que qualquer novo hardware ou software suporte padrões modernos (como OAuth2, SAML ou Kerberos AES).

Fonte: ISO/IEC 27002 (Segurança em Redes), NIST SP 800-175B (Padrões Criptográficos) e CIS Controls v8 (Controle 4: Configuração Segura).

Anexo 19

Configurar a coleta de logs de auditoria detalhados no serviço de diretório

Configurar a coleta de logs de auditoria detalhados no serviço de diretório (incluindo origem, data e nome de usuário) para identificar e alertar sobre alterações não autorizadas em grupos e políticas.

A configuração de logs detalhados é vital para garantir a **rastreabilidade e a integridade** do serviço de diretório, permitindo a correlação precisa entre eventos e atores. Através do monitoramento de origem, data e usuário, estabelece-se uma **trilha de auditoria forense** essencial para a detecção precoce de escalada de privilégios e desvios de conformidade. Aqui estão as orientações técnicas para implementar essa coleta de forma eficaz:

1. Pilares da Auditoria Detalhada

Para que um log seja útil em uma investigação forense ou em um alerta de segurança, ele deve conter, no mínimo:

- **Quem (Identidade):** O nome da conta de usuário ou serviço que realizou a ação.
- **O quê (Ação):** O valor anterior e o novo valor (ex: quem foi adicionado e de qual grupo foi removido).
- **Quando (Timestamp):** Data e hora precisas, sincronizadas via protocolo NTP para garantir a ordem dos fatos.
- **Onde (Origem):** O endereço IP ou o nome da estação de trabalho de onde partiu a requisição.
- **Resultado:** Se a tentativa foi bem-sucedida ou falhou (tentativas de alteração negadas são fortes indicadores de ataque).

2. Eventos Críticos para Monitoramento

Nem todo log tem a mesma importância. O foco deve estar nos eventos de alto impacto:

- **Gestão de Grupos Privilegiados:** Adição ou remoção de membros em grupos com poderes administrativos.
    - *Exemplo AD*: Monitoramento dos grupos *Domain Admins*, *Enterprise Admins* ou *Schema Admins*.
- **Alterações de Políticas de Segurança:** Mudanças em políticas de senha, bloqueio de conta ou direitos de logon.
    - *Exemplo AD*: Modificações em **GPOs (Group Policy Objects)**.
- **Criação e Deleção de Objetos:** Monitoramento de novas contas de usuários, especialmente se criadas fora dos processos padrão de RH.
- **Acesso a Objetos Sensíveis:** Tentativas de acesso a chaves de criptografia ou modificação de permissões de ACL (Access Control List).

3. Passos Práticos para Implementação

Passo 1: Configuração da Política de Auditoria

- Ative a auditoria detalhada (Auditoria Avançada) em vez da auditoria simples para evitar ruído e excesso de logs irrelevantes.
- Configure o sistema para registrar “Sucesso” e “Falha” para categorias de gerenciamento de contas e modificação de diretório.

Passo 2: Centralização e Retenção

- **Encaminhamento de Eventos:** Não armazene logs apenas localmente no servidor de diretório. É recomendado enviá-los para um repositório centralizado, como um **SIEM (Security Information and Event Management)** ou um coletor de logs (Syslog/WEF).
- **Política de Retenção:** Defina um período mínimo de retenção (ex: 90 dias a 1 ano) para atender a requisitos regulatórios e permitir investigações retroativas.

Passo 3: Criação de Alertas em Tempo Real

- Configure gatilhos automáticos para eventos de criticidade máxima.
- *Exemplo de Alerta:* “Notificar equipe de SOC via e-mail/Teams sempre que um usuário for adicionado ao grupo de administradores globais”.

Passo 4: Proteção da Integridade dos Logs

- Garanta que nem mesmo os administradores de domínio possam apagar ou modificar os logs de auditoria (princípio do “Write Once, Read Many”).

4. Governança e Resiliência

- **Revisão de Dashboards:** Estabeleça uma rotina semanal de revisão de relatórios de auditoria para identificar padrões anômalos que não dispararam alertas automáticos.
- **Sincronização de Horário (NTP):** Certifique-se de que todos os ativos da rede utilizam a mesma fonte de tempo confiável. Logs com horários divergentes inviabilizam a correlação de eventos durante um incidente.
- **Teste de Alertas:** Realize simulações periódicas para validar se o sistema de auditoria está capturando e alertando as alterações conforme configurado.

Fonte: Referências: ISO/IEC 27001 (Controle A.12.4 - Registro e Monitoramento), NIST SP 800-92 (Guide to Computer Security Log Management) e PCI DSS (Requisito 10: Rastrear e monitorar todos os acessos).

Anexo 20

Estabelecer inventário e proteção rigorosa para as contas de serviço de infraestrutura

Estabelecer inventário e proteção rigorosa para as contas de serviço de infraestrutura (como a conta KRBTGT), estipulando rotinas de rotação periódica de senhas (ex.: duplo reset a cada 180 dias) para invalidar a persistência adversária via forja de tíquetes (Golden Tickets).

A rotação periódica de credenciais é técnica fundamental para invalidar o ciclo de vida de **Golden Tickets**, eliminando a persistência de longo prazo baseada em tokens de autenticação forjados. A segurança de um Controlador de Domínio depende da integridade das contas de serviço que sustentam o protocolo de autenticação. A mais crítica delas é a conta emissora de tickets (frequentemente identificada como **KRBTGT**), que funciona como o selo de autenticidade para toda a rede.

1. Identificação e Inventário de Chaves Críticas

O primeiro passo é mapear quais contas ou chaves são responsáveis por assinar e validar tokens de acesso em todo o ambiente:

- **Contas de Emissão de Tokens:** Contas que geram o material criptográfico para autenticação (ex.: a conta **KRBTGT** em ambientes Kerberos/AD).
- **Identidades de Sincronização e Replicação:** Contas utilizadas para replicar a base de dados de identidades entre servidores ou para sincronizar dados com a nuvem (ex.: contas de AD Sync).
- **Contas de Serviço de Terceiros:** Aplicações de backup ou segurança que possuem privilégios de leitura/escrita em nível de sistema no diretório.

2. Estratégia de Higiene e Rotação

A persistência adversária baseia-se no fato de que essas senhas raramente são alteradas. A rotação quebra o ciclo de validade de tickets forjados:

- **O Conceito do Duplo Reset:** Em muitos protocolos (como Kerberos), o sistema mantém o histórico da senha anterior para evitar interrupções. Para invalidar totalmente um ticket forjado antigo, é necessário resetar a senha **duas vezes**, garantindo que o novo segredo sobrescreva tanto a senha atual quanto a histórica.
- **Periodicidade Recomendada:** Recomenda-se um ciclo de 180 dias. Isso equilibra a segurança com o tempo necessário para que a nova chave seja propagada por toda a infraestrutura sem causar quedas de serviço.
- **Automação:** Sempre que possível, utilize identidades gerenciadas pelo sistema (como *Managed Service Accounts*) que realizam a troca de senhas sem intervenção humana.

3. Passos Práticos para Implementação

Passo 1: Inventário de Dependências

- Identifique todos os serviços que dependem das contas de infraestrutura.
- Certifique-se de que o ambiente de replicação está saudável antes de iniciar qualquer alteração de senha crítica.

Passo 2: Execução do Reset Controlado

- **Reset 1:** Altere a senha da conta mestra. Aguarde o tempo de convergência (geralmente 8 a 24 horas) para garantir que todos os servidores do domínio reconheçam a nova chave.
- **Reset 2:** Realize o segundo reset para expurgar definitivamente o material criptográfico antigo da memória e dos bancos de dados.

Passo 3: Proteção de Acesso (Hardening)

- Impeça que essas contas sejam utilizadas para login interativo (RDP, Console).
- Restrinja que essas contas só possam ser acessadas por processos específicos e máquinas de alta confiança.

Passo 4: Monitoramento de Uso

- Configure alertas para qualquer tentativa de logon falha ou bem-sucedida vinda de contas de infraestrutura, já que elas devem operar apenas em segundo plano e de forma automatizada.

4. Considerações de Contingência

- **Janela de Manutenção:** Nunca realize o reset de contas de infraestrutura (especialmente o KRBTGT) em horários de pico ou logo antes de feriados, devido ao risco de desautenticação de sessões ativas.
- **Scripts de Verificação:** Utilize ferramentas de validação de saúde do diretório para garantir que a propagação da nova senha ocorreu com sucesso em todos os nós da rede.
- **Plano de Reversão:** Embora o duplo reset seja destrutivo para tickets forjados, tenha um backup do estado do sistema anterior à operação caso ocorra uma falha crítica de replicação.

Fonte: NIST SP 800-53 (IA-5: Authenticator Management), CIS Controls (Control 5: Account Management) e MITRE ATT&CK (T1558.001 - Golden Ticket).

Anexo 21

Implementar o Modelo de Administração em Camadas

Implementar o Modelo de Administração em Camadas (Tiered Administration Model), mantendo recursos de computação dedicados e logicamente separados para garantir que a administração do Tier 0 (Controladores de Domínio e AD) nunca ocorra a partir de equipamentos do Tier 1 (Servidores Gerais) ou Tier 2 (Estações de Trabalho).

O Modelo de Administração em Camadas é essencial para mitigar o escalonamento de privilégios e o movimento lateral, isolando identidades de alta prioridade em zonas de confiança restritas. Essa separação lógica e física impede que credenciais do **Tier 0** sejam expostas em sistemas menos seguros, garantindo que o controle da infraestrutura crítica permaneça inatingível a partir de vetores de comprometimento periféricos. O objetivo central é criar fronteiras de isolamento onde as credenciais de alta hierarquia nunca toquem sistemas de menor segurança.

1. Definição das Camadas de Administração

O modelo organiza os ativos e as identidades em níveis de confiança, onde o nível superior nunca deve confiar ou processar credenciais de um nível inferior:

- **Tier 0 (Célula de Segurança):** Inclui o "coração" da identidade da organização (Controladores de Domínio, PKI, Servidores de Identidade em Nuvem). É o nível mais alto de privilégio.
- **Tier 1 (Plano de Aplicação):** Servidores de arquivos, bancos de dados, aplicações de negócio e serviços de infraestrutura geral.
- **Tier 2 (Plano do Usuário):** Estações de trabalho, laptops e dispositivos móveis dos colaboradores finais.

2. Regras de Isolamento e Fluxo de Credenciais A regra de ouro do modelo é: Credenciais de um nível superior nunca devem ser inseridas ou armazenadas em um nível inferior.

- **Bloqueio de Logon:** Um administrador do Tier 0 nunca realiza login em um servidor do Tier 1 ou em uma estação do Tier 2. Isso evita que sua senha ou hash seja capturado na memória desses dispositivos.
- **Restrição de Gerenciamento:** O gerenciamento do Tier 0 deve ocorrer exclusivamente a partir de ativos dedicados (como *Privileged Access Workstations* - PAWs) que não acessam a internet ou e-mail.
- **Separação de Contas:** Cada administrador deve possuir contas distintas para cada nível que gerencia (ex: joao_t0 para o AD e joao_t1 para servidores).
- **3. Passos Práticos para Implementação**

Passo 1: Inventário e Classificação de Ativos

- Mapeie todos os servidores e identifique quais pertencem ao Tier 0 (quaisquer sistemas que, se comprometidos, dão controle total sobre as identidades).
- Organize os objetos no serviço de diretório em Unidades Organizacionais (OUs) separadas por Tier.

Passo 2: Configuração de Restrições de Logon

- Aplique políticas que proíbam tecnicamente contas do Tier 0 de logar em máquinas de camadas inferiores.
- Configure os servidores de Tier 0 para aceitar conexões apenas de IPs específicos (as máquinas de salto ou PAWs do Tier 0).

Passo 3: Implementação de Estações Dedicadas (PAWs/Jump Servers)

- Estabeleça equipamentos de hardware dedicados ou sistemas virtuais isolados para a administração de cada camada.
- Garanta que esses recursos de computação não compartilham infraestrutura vulnerável com o Tier 2.

Passo 4: Migração e Aplicação

- Mova os administradores para o uso das novas contas nominais por nível.
- Desabilite o uso de contas genéricas de administração em toda a rede.

4. Considerações de Sustentabilidade e Governança

- **Auditoria de Violação de Camada:** Configure alertas para detectar se uma conta de Tier 0 tentar realizar logon em um recurso de Tier 2. Isso é um indicador crítico de comprometimento ou erro de processo.
- **Manutenção de Limites:** Durante a criação de novos serviços, classifique-os imediatamente no Tier correto para evitar o "desvio de função" (drift) do modelo.
- **Resiliência de Hardware:** No Tier 0, prefira o uso de hardware físico ou virtualização altamente isolada para evitar ataques de movimentação lateral via hipervisor.

Fonte: Microsoft Security Best Practices (Privileged Access Strategy), NIST SP 800-207 (Zero Trust Architecture) e ESAE (Enhanced Security Administrative Environment).

Anexo 22

Exigir MFA para todo acesso remoto

Exigir MFA para todo acesso remoto à infraestrutura de rede, como VPNs

A implementação de MFA em acessos remotos é a barreira mais eficaz contra o sequestro de credenciais, impedindo que senhas vazadas resultem em invasões. Em ambientes de VPN, essa camada extra valida a identidade real do usuário, neutralizando ataques de força bruta e phishing.

1. Escolha do Método de Autenticação

Antes de configurar a tecnologia, defina como o usuário vai confirmar a identidade. Os métodos variam em segurança e conveniência:

- **Aplicativos de Autenticação (TOTP):** Google Authenticator ou Microsoft Authenticator (Equilíbrio ideal).
- **Push Notifications:** O usuário apenas clica em "Aprovar" no celular (Alta conveniência).
- **Tokens de Hardware:** Chaves físicas como YubiKey (Segurança máxima, custo mais alto).
- **SMS/E-mail:** Menos seguros devido a ataques de SIM swapping ou interceptação (Evite, se possível).

2. Arquitetura de Integração

Para que sua VPN "converse" com o sistema de MFA, geralmente utiliza-se um protocolo intermediário. Os cenários mais comuns são:

Cenário A: RADIUS Proxy

A maioria dos Firewalls e VPNs (Fortinet, Cisco, Palo Alto) utiliza o protocolo **RADIUS**. Você instala um "Agente" ou "Proxy" do provedor de MFA (como Duo Security ou Azure MFA Console) no seu servidor.

Cenário B: SAML / Modern Auth

Se você usa uma VPN moderna que suporta SAML 2.0, pode integrar diretamente com seu Provedor de Identidade (IdP) como Okta, Azure AD (Entra ID) ou Google Workspace. O login da VPN redireciona para a página de login da nuvem, que já exige o MFA.

3. Passos Práticos para Implementação

Passo 1: Inventário e Preparação

- Identifique todos os pontos de entrada (VPN Client-to-Site, Portais Web, RDP Gateway).
- Garanta que sua base de usuários (Active Directory ou LDAP) esteja limpa e organizada.

Passo 2: Configuração do Provedor de MFA

- Configure as políticas de acesso no painel do provedor (ex: "Exigir MFA apenas fora da rede da organização").

- Gere as chaves de integração (Secret Keys/API Hostnames).

Passo 3: Configuração no Gateway/VPN

- No console da sua VPN, crie um novo Authentication Server.
- Aponte para o IP do seu Proxy MFA ou URL do Provedor SAML.
- Altere o grupo de usuários para utilizar este novo servidor como método primário ou secundário.

Passo 4: Fase de Implementação

Não ative para todos de uma vez.

- Piloto: Ative para a equipe de TI.
- Auto-enrolment (Inscrição automática): Envie um guia para os usuários cadastrarem seus celulares antes da ativação obrigatória.
- Enforcement (Aplicação): Ative a obrigatoriedade por departamentos.

4. Considerações de Contingência

- **Break-glass accounts (Contas quebradas):** Tenha contas de administrador de emergência que não dependam do MFA (guardadas em cofre físico), para o caso do serviço de autenticação ficar offline.
- **Suporte:** Prepare o Help Desk para “Reset de MFA” (usuários que trocam de celular e perdem o acesso são o chamado #1 após a implementação).

Fonte: NIST (National Institute of Standards and Technology): Especificamente a publicação SP 800-63, CIS Controls (Center for Internet Security) e o PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 23

Implementar MFA em todas as contas de acesso administrativo.

Implementar MFA em todas as contas de acesso administrativo, abrangendo todos os ativos institucionais e soluções de software (serviços de diretório, infraestrutura de nuvem, firewalls e switches).

A implementação de MFA em contas administrativas mitiga o risco de comprometimento de credenciais, impedindo que ataques de phishing ou força bruta escalem privilégios em ativos críticos. Ao abranger serviços de diretório, nuvem e infraestrutura de rede, estabelece-se uma camada de segurança adaptativa que valida a identidade em todo o perímetro lógico. Essa prática é fundamental para garantir a integridade da governança de acessos e a resiliência operacional contra invasões persistentes.

1. Inventário de Ativos

Para garantir a cobertura total, orientamos segmentar os ativos institucionais em quatro pilares principais:

- **Identidade Centralizada:** ferramentas de Gerenciamento de Identidade e Acesso (IAM).
- **Infraestrutura e Rede:** Acessos SSH a servidores, consoles de virtualização (VMware/Proxmox), painéis de firewall e VPNs.
- **Aplicações SaaS e Cloud:** Portais de provedores de nuvem (AWS, Azure, GCP) e sistemas críticos de negócio.
- **Bancos de Dados:** Acessos administrativos a instâncias de SQL, NoSQL e ferramentas de gerenciamento.

2. Seleção de Métodos de Autenticação

Priorize métodos resistentes a phishing e fadiga de MFA:

Método	Recomendação	Uso Sugerido
FIDO2 / Chaves Físicas	Altíssima Segurança	Administradores de Domínio e Infraestrutura Crítica.
Certificados Digitais	Alta Segurança	Acessos via VPN e máquinas corporativas.
Authenticator App (Push)	Alta Segurança	Uso geral para colaboradores e administradores.

Método	Recomendação	Uso Sugerido
SMS / E-mail	Evitar	Apenas como última alternativa (vulnerável a SIM Swap).

3. Diretrizes de Configuração Técnica

A. Políticas de Acesso Condicional

Configure regras que exijam o segundo fator baseado em:

- **Localização:** IP de origem fora da rede corporativa ou de países não operantes.
- **Estado do Dispositivo:** Exigir que o dispositivo seja gerenciado (MDM) ou esteja em conformidade.
- **Risco do Usuário:** Gatilhos automáticos caso as credenciais tenham vazado na internet.

B. Proteção de Protocolos Legados

- **Desative a Autenticação Legada:** Bloqueie protocolos como POP3, IMAP e SMTP que não suportam MFA nativo. Eles são alvos primários para ataques de password spraying (pulverização de senha).

C. Contas de Emergência ("Break-glass")

- Mantenha 1 ou 2 contas de alta hierarquia fora do MFA padrão (usando senhas extremamente longas e armazenadas fisicamente) para evitar o bloqueio total do sistema em caso de falha no provedor de identidade.

4. Etapas de Implementação (Roadmap)

- **Registro Prévio:** Force os administradores a cadastrarem seus métodos de MFA antes da aplicação da política.
- **Habilitação por Grupos:** Comece pelos administradores de TI e expanda para os usuários com privilégios de aplicação.
- **Monitoramento:** Acompanhe logs de falha de login para identificar dificuldades técnicas ou tentativas de ataque reais.
- **Auditoria:** Revise trimestralmente se novos ativos ou softwares foram integrados ao fluxo de MFA.

Dica: Para ativos que não suportam MFA nativamente (ex: servidores legados), utilize um Proxy de Identidade ou um PAM (Privileged Access Management) como camada intermediária de autenticação.

Fonte: NIST (National Institute of Standards and Technology): Especificamente a publicação SP 800-63B (Digital Identity Guidelines), CIS Controls (Center for Internet Security), OWASP, PPSI (Programa de Privacidade e Segurança da Informação) e ISO/IEC 27001.

Anexo 24

Ativar MFA nos sistemas de gerenciamento de cópias de segurança

Ativar MFA nos sistemas de gerenciamento de cópias de segurança (consoles de backup), isolando-os contra tentativas adversárias de destruição de dados de recuperação.

A implementação do MFA (Autenticação de Múltiplos Fatores) nos consoles de backup é a última linha de defesa contra-ataques de ransomware moderno, que visam destruir cópias de segurança para forçar o pagamento do resgate. Ao exigir uma verificação adicional, isola-se o plano de controle de credenciais administrativas comprometidas, impedindo que adversários executem comandos críticos de deleção ou modificação de políticas. Essa camada de segurança lógica é essencial para garantir a imutabilidade operacional e a integridade do último recurso de recuperação da organização.

1. Hardening de Acesso à Console

- **Isolamento de Rede:** A console de backup deve residir em uma VLAN restrita (Zona de Gerenciamento), sem acesso direto à internet ou à rede de usuários comum.
- **MFA Obrigatório:** Exija MFA para todos os níveis de acesso (Admin, Operador, Restore), sem exceções para “redes internas confiáveis”.
- **Contas de “Break-Glass”:** Mantenha uma conta de emergência com uma senha extremamente complexa guardada em cofre físico, também protegida por MFA via hardware (ex: YubiKey).

2. Implementação Técnica do MFA

- **Integração via Provedor de Identidade (IdP):** Sempre que possível, integre a console com uma solução de gerenciamento de identidade, segurança de acesso e autenticação via SAML 2.0 ou OIDC. Isso centraliza as políticas de acesso e permite o uso de Acesso Condicional.
- **Push-Notification vs. TOTP:** Priorize aplicativos de autenticação (Push com verificação de número) ou tokens de hardware. Evite SMS, que é vulnerável a SIM Swapping (Troca de SIM).
- **MFA para Operações Críticas:** Configure a console para exigir uma re-autenticação (MFA adicional) especificamente antes de permitir a exclusão de repositórios ou alteração de políticas de retenção.

3. Proteção Contra Destruição Adversária

- **Imutabilidade (WORM):** O MFA protege o acesso, mas a Imutabilidade protege o dado. Utilize repositórios Linux Hardened ou S3 Object Lock para impedir que mesmo um administrador autenticado apague os dados antes do prazo.
- **RBAC (Controle de Acesso Baseado em Função):** Aplique o princípio do privilégio mínimo. Por exemplo: Quem realiza o backup não deve, necessariamente, ter permissão para apagar backups antigos.
- **Log de Auditoria Externo:** Sempre que possível, envie os logs de acesso da console para um SIEM externo em tempo real. Alertas devem ser disparados em caso de múltiplas falhas de MFA ou tentativas de desativação do recurso.

Fonte: ISO/IEC 27031 (Prontidão de TIC para Continuidade de Negócios), NIST SP 800-34 (Contingency Planning Guide) e CERT.br (Práticas de Gestão de Incidentes).

Anexo 25

Exigir MFA para todas as soluções

Exigir MFA para todas as soluções de software expostas externamente, incluindo serviços de correio eletrônico corporativo e plataformas em nuvem (SaaS)

A implementação de Multi-Factor Authentication (MFA) em superfícies de ataque expostas neutraliza grande parte dos riscos baseados em identidade, impedindo o uso de credenciais vazadas em vetores críticos como SaaS e e-mail. Ao exigir uma prova de posse ou fator biométrico adicional, estabelece-se uma barreira técnica essencial contra-ataques de Credential Stuffing e Account Takeover. Essa camada é o alicerce de uma arquitetura Zero Trust, garantindo que o perímetro lógico permaneça resiliente mesmo diante do comprometimento de senhas estáticas.

1. Centralização via Provedor de Identidade (IdP)

Não configure o MFA individualmente em cada software. Utilize um IdP central (como Microsoft Entra ID, Okta ou Google Workspace) para gerenciar o acesso.

- **Integração SaaS:** Utilize protocolos SAML 2.0 ou OpenID Connect (OIDC) para federar todas as aplicações SaaS ao IdP.
- **Acesso Unificado:** Uma vez que o usuário autentica no IdP com MFA, ele ganha acesso às aplicações autorizadas (Single Sign-On).

2. Configuração de Políticas de Acesso Condicional

Implemente regras automatizadas que exijam o MFA com base no contexto do acesso:

- **Localização e Rede:** Exigir MFA obrigatoriamente para qualquer conexão originada fora da rede corporativa (IPs não confiáveis).
- **Risco do Usuário:** Gatilho de MFA imediato se houver detecção de login anômalo (ex: local de origem suspeito, impossível ou fora do comum).
- **Dispositivos Gerenciados:** Diferenciar níveis de exigência para dispositivos integrados ao MDM (Mobile Device Management).

3. Proteção Específica para Correio Eletrônico

O e-mail é o principal vetor de ataque. Medidas críticas:

- **Desativar Autenticação Legada:** Bloqueie protocolos antigos (POP3, IMAP, SMTP Auth) que não suportam telas de MFA modernas.
- **Modern Auth (Autenticação moderna):** Garanta que todos os clientes de e-mail (Outlook, apps mobile) utilizem Modern Authentication.

4. Métodos de Segundo Fator

Priorize métodos resistentes a phishing:

- **Recomendado:** Aplicativos de autenticação (Push notification com verificação de número) ou chaves físicas (FIDO2/WebAuthn).
- **Evitar:** SMS e chamadas de voz, devido à vulnerabilidade de SIM Swap e interceptação.

Fonte: NIST (National Institute of Standards and Technology): Especificamente a publicação SP 800-63 (Digital Identity Guidelines), CIS Controls (Center for Internet Security), CISA (Cybersecurity & Infrastructure Security Agency) e PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 26

Elevar a maturidade da autenticação substituindo fatores baseados em SMS

Elevar a maturidade da autenticação substituindo fatores baseados em SMS (vulneráveis a SIM-swapping) por aplicativos autenticadores ou tokens físicos de hardware, instruindo os agentes públicos sobre essa transição

A transição de fatores baseados em SMS para aplicativos autenticadores ou tokens físicos visa reduzir significativamente vulnerabilidades críticas, como o SIM-swapping e a interceptação de redes de telefonia. Ao adotar padrões de criptografia assimétrica e protocolos robustos (ex: FIDO2), busca-se elevar o nível de integridade do acesso e fortalecer a validação da posse física do dispositivo. É recomendável que os agentes públicos migrem para essas tecnologias para reforçar a resiliência dos sistemas governamentais e ampliar a proteção de dados sensíveis contra acessos não autorizados.

1. Migração para Aplicativos Autenticadores (TOTP)

Substitua o SMS por algoritmos de senha de uso único baseados em tempo (Time-based One-Time Password - TOTP).

- **Protocolo:** Utilize o padrão RFC 6238.
- **Funcionamento:** O segredo (seed) é compartilhado via QR Code e armazenado localmente no dispositivo do usuário, gerando códigos offline a cada 30 segundos.
- **Vantagem:** Não depende da rede de telefonia; o ataque precisaria de acesso físico ao smartphone ou comprometimento do kernel do aparelho.
- **Sugestões:** Google Authenticator, Microsoft Authenticator ou Authy (com backup em nuvem protegido por senha forte).

2. Implementação de Tokens de Hardware (FIDO2/WebAuthn)

O nível máximo de segurança (resistente a phishing e SIM-swap) é o uso de chaves físicas.

- **Padrão:** Adote chaves compatíveis com FIDO2 / U2F (ex: YubiKey, Google Titan).
- **Criptografia:** Utiliza criptografia de chave pública. O site desafia o token, que assina a resposta localmente.
- **Resiliência:** Como a chave física valida a origem do site (domínio), ela impede ataques de phishing em tempo real, onde o invasor tenta interceptar o código TOTP.

3. Estratégia de Transição e Desativação

A segurança de um sistema é definida pelo seu elo mais fraco. Não basta adicionar novos métodos; é preciso remover os antigos.

- **Cadastramento:** Force o registro do novo fator (App ou Chave).

- **Remoção de Legado:** Após o registro do novo método, desabilite o SMS como opção de recuperação ou segundo fator nas configurações de segurança.
- **Códigos de Backup:** Forneça códigos de recuperação únicos (estáticos) para que o usuário armazene fisicamente, evitando que ele volte ao SMS em caso de perda do dispositivo.

Fonte: NIST (National Institute of Standards and Technology), OWASP (Open Web Application Security Project), FIDO Alliance em conjunto com o World Wide Web Consortium (W3C) e PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 27

Avaliar a viabilidade e contratar um provedor de serviços de MDR

Avaliar a viabilidade e contratar um provedor de serviços de MDR compatível com o porte e a infraestrutura tecnológica do órgão, assegurando monitoramento e análise de ameaças 24/7

A avaliação de viabilidade e a contratação de um serviço de MDR (Managed Detection and Response) garantem que o monitoramento 24/7 e a análise de ameaças sejam tecnicamente compatíveis com a volumetria de dados e a complexidade da infraestrutura do órgão. Essa estratégia otimiza a triagem de incidentes e a resposta a ataques avançados, suprindo lacunas de expertise especializada e capacidade computacional interna. Ao alinhar o provedor ao porte da instituição, assegura-se a resiliência operacional e a conformidade normativa por meio de uma visibilidade contínua de todo o ecossistema digital. Abaixo, as orientações técnicas sucintas para balizar a avaliação e contratação:

1. Diagnóstico e Compatibilidade Técnica

É fundamental mapear a superfície de ataque para garantir que o MDR não tenha “pontos cegos”.

- **Inventário de Ativos:** Liste servidores, endpoints, dispositivos de rede e serviços em nuvem (SaaS/PaaS).
- **Integração de Log:** Verifique se o provedor suporta nativamente suas ferramentas atuais (Firewalls, EDR, SIEM, Identidade).
- **Modelo de Implantação:** Avalie se a coleta de dados será via agente (agent-based) ou via API/Rede, considerando o impacto na performance da infraestrutura.

2. Critérios de Avaliação de Viabilidade

O MDR deve ser proporcional à maturidade da equipe interna de TI.

Critério	Requisito Mínimo
Escopo de Monitoramento	Cobertura 24/7/365 com analistas humanos (não apenas automação).
Capacidade de Resposta	O provedor deve realizar contenção ativa (ex: isolar host infectado) e não apenas enviar alertas.
SLA de Detecção/Resposta	Tempo máximo de detecção (MTTD) e resposta (MTTR) definidos em contrato.

Critério	Requisito Mínimo
Threath Hunting (Caça a ameaças)	Busca proativa por ameaças que evadem defesas padrão, baseada em inteligência de ameaças atualizada.

3. Requisitos para Contratação

Ao elaborar o Termo de Referência (TR) ou Edital, exija os seguintes diferenciais:

- **Visibilidade Unificada:** Painel (Dashboard) único para visualização de incidentes em tempo real.
- **Relatórios Consultivos:** Entrega de relatórios mensais com recomendações de melhoria na postura de segurança (Hardening).
- **Conformidade Local:** Garantia de que o tratamento de dados respeita a LGPD e que os logs são armazenados de forma íntegra.
- **Suporte a Incidentes Graves:** Previsão de apoio especializado em caso de ataques de larga escala (Ransomware).
- **Nível de Serviço (SLA):** Definição clara de tempo de resposta a incidentes (MTTR) e monitoramento 24x7.
- **Amostra do Objeto/Prova de Conceito (PoC):** Com base na IN SGD/ME nº 31/2021, o TR pode exigir testes técnicos para verificar a capacidade de detecção antes da contratação definitiva.
- **Segurança da Informação:** Conformidade com a Política Nacional de Cibersegurança (Decreto nº 11.856/2023).
- **Capacitação da Equipe:** Exigência de certificações técnicas da equipe da contratada (SOC).

4. Gestão e Governança

A contratação de um MDR não exime o órgão de responsabilidade. A Lei nº 14.133/2021 (art. 117) estabelece a necessidade de designar fiscais técnicos e administrativos para acompanhar o contrato.

- **Ponto de Contato Único:** Defina quem no órgão receberá as escalações críticas.
- **Reuniões de Alinhamento:** Estabeleça ciclos trimestrais para revisar a evolução das ameaças detectadas.
- **Prova de Conceito (PoC):** Sempre que possível, realize um teste de 15 a 30 dias para validar a facilidade de integração e a qualidade dos alertas gerados.

Nota de Atenção: Um erro comum é contratar MDR esperando que ele gerencie vulnerabilidades ou para Patch Management. O MDR foca em detecção e resposta a invasões, e não necessariamente na correção preventiva de softwares desatualizados, embora as duas áreas se complementem.

Fonte: NIST Cybersecurity Framework (CSF), ISO/IEC 27001 e 27035, PPSI (Programa de Privacidade e Segurança da Informação) e Instrução Normativa GSI/PR nº 09/2026, Estratégia Nacional de Cibersegurança (E-Ciber) e Lei nº 14.133/2021 (Nova Lei de Licitações).

Anexo 28

Garantir que o escopo técnico inclua a implantação de soluções de detecção de intrusão

Garantir que o escopo técnico inclua a implantação de soluções de detecção de intrusão baseada em host (como agentes Endpoint Detection and Response - EDR) , que suportem identificação de ameaças, resposta automatizada, isolamento de ativos e coleta forense.

A inclusão de soluções de EDR no escopo técnico é vital para garantir a visibilidade granular e a rastreabilidade de eventos diretamente no host, permitindo a detecção de ameaças sofisticadas que evadem perímetros tradicionais. Através da automação de resposta e isolamento de ativos, mitiga-se o movimento lateral e o impacto de incidentes em tempo real, reduzindo drasticamente o Tempo Médio para Remediação (MTTR). Além disso, a capacidade de coleta forense contínua preserva evidências críticas para análise pós-incidente, assegurando a conformidade e o contínuo fortalecimento da resiliência cibernética da infraestrutura. Abaixo, apresento as orientações técnicas estruturadas para compor o seu Escopo de Trabalho.

1. Requisitos de Identificação e Detecção

A solução deve transcender a busca por assinaturas básicas (antivírus comum), focando em comportamento e telemetria avançada.

- **Análise Comportamental:** Capacidade de detectar táticas, técnicas e procedimentos (TTPs) alinhados à matriz MITRE ATT&CK.
- **Visibilidade de Processos:** Registro de execução de comandos, modificações de registro, conexões de rede originadas pelo host e integridade de arquivos.
- **IoCs e IoAs:** Suporte à ingestão automática de Indicadores de Comprometimento (IoCs) e detecção de Indicadores de Ataque (IoAs) em tempo real.

2. Resposta Automatizada e Isolamento

O tempo de resposta (MTTR) é crítico. O escopo deve exigir ações que ocorram sem intervenção humana imediata para conter danos.

- **Playbooks de Remediação:** Configuração de regras para encerramento automático de processos suspeitos e deleção de artefatos maliciosos.
- **Isolamento de Rede:** Capacidade de isolar o ativo logicamente da rede corporativa, mantendo apenas o canal de comunicação entre o agente e o console de gerenciamento para fins de investigação.
- **Rollback (Reversão de Estado):** (Desejável) Funcionalidade de reverter alterações feitas por ransomware ou malware para um estado íntegro anterior.

3. Coleta Forense e Investigação

A solução deve servir como a “caixa-preta” do incidente, permitindo auditoria posterior.

- **Timeline de Eventos:** Histórico detalhado das ações que antecederam o alerta (quem, quando, onde e como).
- **Snapshot de Memória e Disco:** Ferramentas integradas para coleta remota de evidências (dumps de memória ou arquivos específicos) para análise profunda em sandbox ou laboratório.
- **Retenção de Dados:** Garantir que a telemetria seja armazenada em nuvem ou repositório seguro por um período mínimo (ex: 30 a 90 dias), mesmo que o host seja destruído ou formatado.

4. Gerenciamento e Compatibilidade

- **Multiplataforma:** Suporte nativo para Windows, Linux, macOS e ambientes de nuvem/containers.
- **Baixo Impacto:** O agente não deve exceder limites específicos de consumo de CPU e RAM para não degradar a experiência do usuário final.
- **Integração SIEM/SOAR:** Exportação nativa de logs e alertas para centralização em Centros de Operações de Segurança (SOC).

Nota Estratégica: Ao redigir o escopo, certifique-se de que a responsabilidade pela atualização de políticas e ajuste de falsos positivos esteja claramente definida entre o fornecedor e a equipe interna.

Fonte: Framework NIST (Special Publication 800-209 e 800-61), Matriz MITRE ATT&CK, Modelo SANS Institute (Incidência e Forense) e PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 29

Descrever os requisitos mínimos de segurança da informação

Descrever os requisitos mínimos de segurança da informação no contrato do provedor de serviços, estipulando Acordos de Nível de Serviço (SLA) rigorosos para os tempos de detecção (ex.: <1min), investigação (ex.: <10min) e remediação (ex.: <60min).

A formalização técnica de requisitos de segurança e SLAs (Service Level Agreements) em contratos de outsourcing mitiga o risco operacional ao transferir a responsabilidade direta pelo desempenho da defesa cibernética ao provedor. A estipulação de métricas rigorosas de MTTD (Detecção), MTTI (Investigação) e MTTR (Remediação) garante a previsibilidade do tempo de exposição a ameaças, essencial para manter a resiliência do negócio. Estruturalmente, essas cláusulas transformam a segurança de uma "melhor prática" em uma obrigação auditável, permitindo a aplicação de sanções em caso de descumprimento dos patamares críticos de proteção.

1. Gestão de Incidentes e SLAs de Resposta

Os contratos devem detalhar as responsabilidades do Provedor de Serviço em Nuvem (CSP) quanto à notificação e mitigação de incidentes. Recomenda-se estipular métricas rigorosas para garantir a prontidão operacional:

- **Detecção (MTTD):** O CSP deve prover mecanismos para geração e monitoramento de registros de auditoria em tempo real para permitir a detecção rápida.
- **Investigação e Notificação:** O contrato deve prever tempos claros para a notificação de incidentes pela contratada.
- **Remediação e Recuperação:** Devem ser estabelecidos SLAs para a restauração dos serviços para um estado confiável e pré-incidente.
- **Análise Pós-Incidente:** É obrigatória a realização de análises após incidentes de segurança.

EXEMPLO de parâmetros para incidentes de **Alta Criticidade**:

Métrica	Descrição	Meta Sugerida
MTTD (Time to Detect)	Tempo entre o início do evento e o alerta gerado pelo SOC.	**< 1 minuto**
MTTI (Time to Investigate)	Tempo para triagem, análise de escopo e confirmação do incidente.	**< 10 minutos**

Métrica	Descrição	Meta Sugerida
MTTR (Time to Remediate)	Tempo para contenção total e erradicação da ameaça.	**< 60 minutos**

Nota: O descumprimento recorrente destes prazos deve estar atrelado a multas pecuniárias (Service Credits) e cláusulas de rescisão.

2. Requisitos Mínimos de Segurança (Hardening e Governança)

Além dos prazos, o provedor deve comprovar a adoção de controles técnicos rigorosos. A Portaria 5.950/2023 e o Guia PPSI 2.0 estabelecem controles que devem ser exigidos contratualmente, adaptados ao modelo de serviço (IaaS, PaaS ou SaaS):

- **Gestão de Identidades e Acesso:** Exigência de **Autenticação Multifator** (MFA) para acessos administrativos e para aplicações expostas externamente.
- **Proteção de Dados:** Implementação de criptografia ou tokenização para dados críticos em repouso (at rest) e em trânsito (in transit) devem utilizar algoritmos robustos (ex: AES-256 e TLS 1.3).
- **Gestão de Registros de Auditoria:** O CSP deve disponibilizar logs de auditoria detalhados(logs brutos sem filtragem prejudicial), que devem ser retidos por, no mínimo, 90 dias.
- **Configuração Segura:** Aplicação de linhas de base (benchmarks) de segurança e desativação de serviços desnecessários.
- **Defesa contra Malware:** Prevenção da execução de códigos maliciosos, com responsabilidade variando conforme o modelo (ex: no SaaS, a defesa é do CSP).
- **Segregação de Dados:** Garantia lógica (ou física, se aplicável) de que os dados do contratante não se misturam aos de outros clientes do provedor.

3. Auditoria e Conformidade

- **Acesso a Documentação:** O órgão deve ter o direito de solicitar documentação que descreva como o CSP protege a infraestrutura sob sua responsabilidade. Incluindo cláusula que permite auditorias presenciais ou remotas, realizadas pelo contratante ou por terceiros, com aviso prévio mínimo.
- **Relatórios de Terceiros:** Exigência de certificações atualizadas (ex: **ISO/IEC 27001**, **SOC2 Tipo II** ou **PCI-DSS** para pagamentos).
- **Vulnerability Management:** O programa de testes de intrusão deve ser mantido, porém sua execução em ambiente de nuvem exige autorização formal e coordenação prévia com o provedor (CSP) para definir datas, escopo e endereços IP, evitando impactos na disponibilidade. Podendo realizar scans de vulnerabilidades (ex.: diários, semanais, quizenais, mensai, anuais) e testes de invasão (pentests) (ex.: diários, semanais, quizenais, mensai, anuais), compartilhando o sumário executivo dos resultados.

4. Continuidade de Negócios e Disaster Recovery (DR)

- **RPO (Recovery Point Objective):** Tempo máximo de perda de dados aceitável (ex.: < 15 minutos).
- **RTO (Recovery Time Objective):** Tempo máximo para restabelecimento do serviço após falha (ex.: < 4 horas).
- **Backups Automatizados:** Exigência de cópias de segurança automatizadas e instâncias isoladas para dados de recuperação.
- **Testes de Recuperação:** O processo de restauração deve ser testado regularmente para garantir a integridade dos dados.
- **Portabilidade:** O contrato deve prever o encerramento seguro, garantindo a exportação dos dados e a devida retenção conforme requisitos legais.

5. Proteção de Dados (LGPD)

- **Notificação de Vazamento:** Obrigação de notificar o contratante sobre qualquer suspeita de violação de dados pessoais em até **X horas** (recomenda-se um prazo inferior ao legal, ex.: 24 horas), independentemente da confirmação da extensão do dano.

Fonte: NIST Cybersecurity Framework (CSF) 2.0, CIS Controls (Center for Internet Security), NIST SP 800-61 Rev. 2 (Computer Security Incident Handling Guide), SANS Institute, ISO/IEC 27001 e 27002:2022, LGPD (Lei Geral de Proteção de Dados - Brasil), Portaria SGD/MGI nº 5.950/2023 e o Guia Complementar de Segurança da Informação para Computação em Nuvem (PPSI 2.0).

Anexo 30

Integrar o provedor de serviços ao processo interno de gestão de incidentes de segurança da informação

Integrar o provedor de serviços ao processo interno de gestão de incidentes de segurança da informação , documentando claramente os papéis e atribuindo as responsabilidades de resposta conjuntas entre a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) do órgão e os analistas do MDR7

A integração técnica entre a ETIR e o provedor de MDR otimiza o Tempo Médio de Resposta (MTTR) ao eliminar silos operacionais, garantindo que o fluxo de telemetria e contenção seja fluido. A definição precisa de uma Matriz RACI é vital para evitar lacunas de execução ou sobreposição de ações durante crises, permitindo que a inteligência de ameaças externa acione defesas locais de forma orquestrada. Essa sinergia transforma a relação contratual em uma capacidade defensiva unificada, onde a responsabilidade compartilhada assegura a resiliência e a conformidade dos ativos críticos do órgão. O objetivo é eliminar "zonas cinzentas" de responsabilidade, garantindo que o tempo de resposta (MTTR) seja minimizado através de um fluxo de trabalho colaborativo.

1. Fluxo de Integração e Governança

A integração deve basear-se no modelo de Responsabilidade Compartilhada, onde o MDR atua como braço operacional de monitoramento e a ETIR como autoridade de decisão e coordenação interna.

- **Ponto de Contato Único (SPOC - Single Point of Contact):** Estabelecer canal de comunicação 24x7 entre o SOC/MDR e a ETIR.

Crie uma tabela de "Quem chamar e quando", por exemplo.

  - **Nível 1 (Operacional):** Analista do MDR fala com o Técnico da ETIR (via Ticket/Chat).
  - **Nível 2 (Crítico):** Gerente do SOC fala com o Coordenador da ETIR (via Telefone).
  - **Nível 3 (Crise):** Diretoria do Provedor fala com o CIO/CISO do Órgão (Decisões de desligar a rede inteira).

- **Acesso a Dados:** Garantir que o MDR tenha visibilidade sobre logs e ativos críticos.
- **Alinhamento com a ReGIC:** Toda vulnerabilidade ou incidentes de segurança cibernética que impactem ou que possam impactar os serviços prestados ou contratados, detectado pelo MDR deve ser reportado pela ETIR ao CTIR Gov,
- **Responsabilidade Conjunta:** Em casos de incidentes de alta relevância, o MDR atua na frente de "Monitoramento e Resposta Técnica", enquanto a ETIR atua na "Gestão da Resposta", garantindo que as ações técnicas não firam a continuidade do negócio.

2. Requisitos de Contratação e SLA

Para que a integração seja eficaz, o contrato de MDR deve prever:

- **Tempo de Resposta (MTTR):** Prazos máximos para início da contenção.

Não use apenas os SLAs de “atendimento de ticket”. Use SLAs de **segurança**:

- **Tempo de Triagem:** Quanto tempo o MDR leva para ver o alerta? (Recomendado: < 15 min).
- **Tempo de Contenção:** Quanto tempo até o vírus ser bloqueado? (Recomendado: < 60 min).

- **Transferência de Conhecimento:** Relatórios mensais de tendências e melhorias de segurança.
- **Interoperabilidade:** O provedor deve integrar suas ferramentas (SIEM/XDR) com o ecossistema tecnológico do órgão.

Documente quais ferramentas serão compartilhadas.

- A ETIR terá acesso ao console do EDR/MDR para visualizar os incidentes em tempo real?
- Haverá integração entre o sistema de chamados do órgão e o do provedor?

3. Matriz RACI: Resposta a Incidentes (ETIR vs. MDR)

Esta matriz serve como EXEMPLO e foca na divisão entre a **execução técnica (MDR)** e a **responsabilidade institucional (ETIR)**, conforme exigido pela Administração Pública Federal.

Legenda RACI:

- **R (Responsible):** Quem executa a tarefa.
- **A (Accountable):** Quem aprova e é o responsável final pela entrega (apenas um por tarefa).
- **C (Consulted):** Quem deve ser consultado antes da decisão ou ação.
- **I (Informed):** Quem deve ser informado após a execução.

Atividade / Processo	ETIR (Órgão)	Analistas MDR	Gestor de TI/SI (Órgão)	CTIR.Gov
Monitoramento e Detecção de Ameaças 24/7	C	R / A	I	I
Triagem e Classificação Inicial do Incidente	A	R	I	I
Notificação de Incidente Crítico	R / A	C	I	I

Atividade / Processo	ETIR (Órgão)	Analistas MDR	Gestor de TI/SI (Órgão)	CTIR.Gov
Contenção Imediata (Bloqueios de Rede/Contas)	A	R	C	I
Análise Forense e Investigação de Causa Raiz	C	R	I	I
Erradicação da Ameaça e Limpeza de Sistemas	R / A	C	I	I
Recuperação de Serviços (Restore/Backup)	R / A	C	C	I
Elaboração do Relatório de Incidente	A	R	I	I
Comunicação Institucional (Crise)	R / A	I	C	C
Lições Aprendidas e Melhoria do Plano	R / A	C	C	I

Detalhamento das Atribuições por Perfil

1. **Analistas de MDR (Parceiro de Execução)**
    - **Execução Técnica:** É o "braço operacional". Responsável por configurar as ferramentas de detecção, analisar alertas em tempo real e executar ações de contenção pré-aprovadas.
    - **Suporte Especializado:** Fornece a inteligência de ameaças (Threat Intelligence) e os artefatos técnicos para que a ETIR possa tomar decisões baseadas em dados.

2. **ETIR do Órgão (Autoridade de Governança)**
    - **Tomada de Decisão:** A ETIR detém o papel de **Accountable**. Embora o MDR detecte, a decisão final de desligar um sistema crítico ou declarar um estado de crise é da ETIR.
    - **Articulação Interna:** Cabe à ETIR a interface com a alta administração e as áreas de negócio do órgão.
    - **Cumprimento Legal:** Responsável por garantir que as notificações ao CTIR.Gov e à ANPD (se houver dados pessoais envolvidos) sejam realizadas nos prazos regulamentares.
3. **Gestor de TI/SI**
    - **Prover Recursos:** Garantir que tanto a ETIR quanto o contrato de MDR tenham as ferramentas e acessos necessários para atuar.
    - **Supervisão:** Monitorar o desempenho da resposta aos incidentes como parte da governança de TI.

Procedimento Operacional Padrão (POP): Resposta a Incidentes Cibernéticos

EXEMPLO de um POP de Resposta Conjunta a Incidentes Críticos (ETIR + MDR):

O POP tem o objetivo de padronizar as ações de detecção, contenção e comunicação de incidentes cibernéticos, delimitando as fronteiras de atuação entre os analistas de MDR e a equipe interna (ETIR).

1. Fluxo de Execução

Fase 1: Detecção e Triagem (Responsável: MDR)

- **Monitoramento:** O MDR monitora os ativos 24/7 através de ferramentas (SIEM/EDR).
- **Qualificação:** Ao detectar um comportamento anômalo, o analista MDR deve classificar o incidente por severidade (Ex.: Baixa, Média, Alta, Crítica).
- **Abertura de Chamado:** O MDR registra o incidente no sistema oficial e notifica a ETIR em até **X minutos** (Ex.: **15 minutos**) para casos críticos.

Fase 2: Contenção Imediata (Responsável: MDR com Supervisão da ETIR)

- **Ações Pré-Aprovadas:** O MDR executa protocolos de contenção automática (ex: isolar um host infectado da rede) para evitar a propagação (lateral movement).
- **Validação:** O analista MDR informa à ETIR sobre a ação tomada. Se a contenção exigir o desligamento de serviços críticos de negócio, o MDR deve solicitar autorização expressa da ETIR.

Fase 3: Análise e Erradicação (Responsável Conjunto)

- **Coleta de Evidências:** O MDR coleta logs e artefatos (malwares, dumps de memória) para garantir a cadeia de custódia.
- **Remediação:** A ETIR coordena com as equipes de infraestrutura a aplicação de patches ou restauração de sistemas, enquanto o MDR valida se a ameaça foi totalmente removida.

Fase 4: Notificação e Reporte (Responsável: ETIR)

- **CTIR Gov:** A ETIR realiza a notificação oficial ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo.
- **Relatório Final:** O MDR entrega o relatório técnico de análise forense e a ETIR consolida o Relatório de Gestão de Incidente.

Dica: Para que este POP seja eficaz, é recomendável realizar **Exercícios de Simulação (Tabletop Exercises)** semestrais, envolvendo tanto os analistas do MDR quanto os membros da ETIR

Fonte: NIST Special Publication 800-61 Rev.3, Framework MITRE ATT&CK, Instrução Normativa GSI/PR nº 01/2020, Glossário e Manuais do CTIR Gov, Decreto nº 12.572/2025, Decreto nº 10.748/2021, Instrução Normativa nº 94/2022 (SGD/MGI), Instrução Normativa nº 1 (27 de maio de 2020), NC 05/IN01/DSIC/GSIPR, NC 08/IN01/DSIC/GSIPR, Portaria SGD/MGI nº 9.511 (28 de outubro de 2025), PLANGIC (Plano de Gestão de Incidentes Cibernéticos) e o PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 31

Estabelecer um processo de realização de cópias de segurança

Estabelecer um processo de realização de cópias de segurança, mapeando dados e soluções de software críticas para definir os critérios de priorização de recuperação

A implementação de uma política de backup estruturada visa fortalecer a resiliência operacional, buscando mitigar riscos à integridade e disponibilidade dos ativos contra falhas ou ataques. Por meio do mapeamento de dependências, o processo auxilia na definição de uma hierarquia de restauração, o que pode otimizar o RTO e o RPO conforme a criticidade identificada. Essa abordagem estratégica permite que a recuperação de desastres seja mais coordenada, aumentando as chances de manter a continuidade dos serviços essenciais em cenários adversos.

1. Mapeamento e Classificação (Inventário)

Antes de copiar dados, é preciso entender o que eles representam.

- **Inventário de Ativos:** Liste todos os servidores, bancos de dados e aplicações.
- **Análise de Impacto (BIA):** Identifique quais sistemas interrompem a operação se ficarem offline.
- **Mapeamento de Dependências:** Entenda que o Software A só funciona se o Banco de Dados B estiver ativo.

2. Critérios de Priorização (RTO e RPO)

A priorização é definida por duas métricas fundamentais:

- **RPO (Recovery Point Objective):** Qual a perda tolerável de dados? (Ex: 1 hora de transações, 24 horas de arquivos). Define a frequência do backup.
- **RTO (Recovery Time Objective):** Quanto tempo a organização suporta ficar parada? Define a velocidade da restauração e a infraestrutura necessária.

3. Estratégia de Execução: Regra 3-2-1-1-0

Para implementar este nível de segurança, a arquitetura deve ser desenhada da seguinte forma:

- **3 Cópias de dados:** Mantenha os dados originais e, no mínimo, duas cópias de segurança.
- **2 Mídias diferentes:** Armazene as cópias em tecnologias distintas (ex: Discos/NAS e Nuvem ou Fita) para evitar falhas de hardware simultâneas.
- **1 Cópia Off-site:** Uma das cópias deve estar fisicamente fora da sua infraestrutura principal (Data Center secundário ou Nuvem pública).
- **1 Cópia Offline (Air-Gapped) ou Imutável:**
    - **Air-Gapped:** Uma cópia fisicamente desconectada de qualquer rede (ex: Fita LTO ou disco removível).

- **Imutabilidade:** Usar tecnologias de proteção de dados, por exemplo o Object Lock (S3) ou Immutable Repositories (Linux Hardened Repository), onde os dados não podem ser deletados ou alterados por um período definido, mesmo com credenciais de admin.

- **0 Erros após verificação:** Implementação de testes automatizados de integridade (Data Labs/Sandbox) para garantir que o backup não apenas exista, mas seja funcional e livre de malwares.

4. Matriz de Priorização e Recuperação

Com a regra 3-2-1-1-0 estabelecida, os critérios de recuperação devem focar na **ordem de restauração**:

Prioridade	Categoria	Tipo de Recuperação	Local de Origem
P0 - Imediata	Identidade e Rede (AD, DNS, Firewall)	Instant Recovery (Snapshot)	On-site (Disco rápido)
P1 - Crítica	Bancos de Dados e ERP	Restauração de Logs / Pontos PITR	On-site / Off-site
P2 - Operacional	Servidores de Aplicação e Middleware	Reinstalação via Script/Backup	Off-site (Cloud)
P3 - Suporte	Arquivos de usuários e Legados	Restauração em lote	Off-site / Offline

Verificação Técnica (O "Zero" da Regra)

Para garantir o "Zero Erros", o processo deve incluir:

- **Check de Consistência:** Verificação de somas de verificação (checksums) durante a gravação.
- **Restauração de Teste (SureBackup):** Subir as VMs em ambiente isolado automaticamente para checar se o SO inicia e o serviço responde.
- **Scan de Antivírus:** Escanear o conteúdo do backup antes da restauração para evitar a reinfecção por ameaças latentes.

Próximos Passos

- **Validação:** Realize um teste de restauração total (Dry Run) semestralmente. Backup que não restaura é apenas despesa.
- **Segurança:** Implemente criptografia em repouso e em trânsito.

Nota de Segurança: A cópia Imutável (1) é a sua última linha de defesa contra-ataques que tentam apagar seus backups antes de criptografar a rede.

Fonte: NIST Cybersecurity Framework (CSF), ISO/IEC 27001 e 27031, PPSI (Programa de Privacidade e Segurança da Informação) e CISA (Cybersecurity & Infrastructure Security Agency).

Anexo 32

Configurar pelo menos uma cópia imutável

Configurar pelo menos uma cópia imutável (ex.: tecnologias WORM - Write-Once-Read-Many ou Object Lock em nuvem), garantindo proteção dos dados de recuperação com controles rigorosos

Configurar cópias imutáveis é essencial para mitigar riscos de ransomware e deleção acidental, pois impede que os dados sejam alterados ou removidos durante um período definido, mesmo com privilégios de administrador. Essa técnica utiliza o modelo WORM (Write Once, Read Many), criando uma última linha de defesa que assegura a integridade do backup contra ataques de criptografia. Ao associar a imutabilidade a controles de acesso rigorosos, a organização garante a disponibilidade de um ponto de restauração confiável para a continuidade de negócios.

1. Implementação em Nuvem (Object Lock)

A maioria dos provedores de nuvem (AWS S3, Azure Blob, Google Cloud Storage, Serpro e a Dataprev) utiliza o conceito de **Object Lock (Bloqueio de objeto)**.

- **Habilite o Versionamento:** O bucket de destino deve ter o versionamento ativado obrigatoriamente.

Modo de Retenção:

  - **Compliance Mode (Recomendado):** Ninguém, nem o usuário raiz, pode alterar ou excluir os dados até o fim do prazo.
  - **Governance Mode:** Protege contra a maioria dos usuários, mas permite que identidades específicas com permissões especiais removam a trava.

- **Políticas de IAM:** Aplique o princípio do privilégio mínimo. Remova permissões de s3:DeleteObject e s3:PutBucketObjectLockConfiguration das contas de serviço de backup usuais.

2. Implementação On-Premises (Local)

Tecnologia WORM

Para infraestruturas locais, o foco é o endurecimento (hardening) do hardware e do sistema de arquivos.

- **Linux Hardened Repository:** Utilize sistemas de arquivos como **XFS** com atributos de imutabilidade (chattr +i). O software de backup (ex: Veeam) utiliza um serviço de transporte que perde a permissão de escrita após a conclusão do job.
- **Sistemas de Fita (LTO):** Utilize cartuchos **LTO-WORM**. Fisicamente, o hardware da fita impede a sobrescrita de dados já gravados.
- **Appliances Dedicados:** Utilize storages (armazenamentos) que suportam Snapshots (cópia instantânea) imutáveis integrados ao nível do controlador (ex: Dell PowerProtect, Pure Storage SafeMode).

3. Controles Rigorosos e Governança

A imutabilidade técnica é inútil se o acesso ao console de gerenciamento estiver vulnerável.

- **MFA (Autenticação de Múltiplos Fatores):** Exija MFA para qualquer alteração em políticas de retenção ou acesso ao console de armazenamento.
- **Air-Gap Lógico:** Garanta que o repositório imutável esteja em uma rede isolada ou em uma conta de nuvem separada (VPC/Subscription distinta) da rede de produção.
- **Monitoramento de Alarmes:** Configure alertas para tentativas falhas de deleção de objetos imutáveis, o que geralmente é um indicador precoce de ataque.

Fonte: NIST Cybersecurity Framework (CSF), Instrução Normativa GSI nº 5/2021, Instrução Normativa GSI nº 8/2025 e PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 33

Criar e manter pelo menos uma instância isolada

Criar e manter pelo menos uma instância isolada dos dados de recuperação, como um destino em nuvem segregada, cofre digital ou datacenter separado (offsite)

A implementação de uma instância isolada, como um cofre digital ou nuvem segregada, estabelece uma lacuna de segurança (air gap lógico ou físico) essencial para mitigar riscos de movimentação lateral e ataques de ransomware. Essa redundância offsite (externa) garante a integridade dos dados contra desastres geográficos e falhas catastróficas na infraestrutura primária, assegurando a disponibilidade resiliente. Ao desvincular o destino de recuperação do domínio administrativo principal, a organização protege a última linha de defesa contra-ataques ou exclusão acidental de backups críticos.

1. Segregação e Isolamento (Air-Gap ou Imutabilidade)

- **Isolamento Lógico/Físico:** Manter pelo menos uma cópia dos dados em um ambiente que não esteja permanentemente ligado à rede de produção.
- **Cofre Digital (Cyber Vault):** Utilizar soluções de armazenamento com retenção imutável (WORM - *Write Once, Read Many*), onde os dados não podem ser apagados ou alterados por um período predefinido, mesmo com credenciais de administrador.
- **Destino Offsite:** A cópia de segurança deve residir em um datacenter geograficamente separado do principal para mitigar riscos de desastres naturais ou falhas regionais de infraestrutura.

2. Armazenamento em Nuvem Segregada

- **Soberania de Dados:** Conforme a IN GSI nº 8/2025, para dados sensíveis ou classificados da Administração Pública, a nuvem deve ser **privada ou comunitária**, com datacenters obrigatoriamente localizados em território nacional.
- **Independência de Provedor:** Avalie o uso de um provedor de nuvem diferente do utilizado na produção para evitar pontos únicos de falha sistêmica (estratégia Multi-Cloud).
- **Criptografia:** Implementar criptografia de Estado (algoritmos aprovados pelo GSI) para dados em repouso e em trânsito, com a gestão das chaves mantida exclusivamente pelo detentor dos dados.

Fonte: NIST (National Institute of Standards and Technology), CIS Controls (Center for Internet Security), Instrução Normativa GSI/PR nº 8/2025, Decreto nº 12.572/2025, ISO/IEC 27002 e PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 34

Realizar testes regulares de integridade do backup

Realizar testes regulares (ex.: trimestrais) de integridade do backup, executando processos práticos de restauração e documentando a eficácia e o tempo de recuperação

Testes trimestrais de restauração validam a consistência lógica dos dados e a funcionalidade das cadeias de custódia, prevenindo a corrupção silenciosa (bit rot) que ferramentas de monitoramento passivo podem ignorar. A execução prática permite mensurar com precisão o RTO (Recovery Time Objective) real, garantindo que o tempo de inatividade em um desastre esteja alinhado aos SLAs críticos do negócio.

A documentação sistemática desses processos estabelece uma trilha de auditoria e conformidade, assegurando que os scripts de automação e procedimentos de failover (transferência em caso de falha) permaneçam operacionais frente a mudanças na infraestrutura.

1. Critérios de Seleção (Amostragem)

Não é necessário restaurar o ambiente completo em todos os testes, mas a amostra deve ser estratégica:

- **Dados Críticos:** Priorize bancos de dados SQL/NoSQL e arquivos de configuração.
- **Aleatoriedade:** Selecione pastas ou volumes aleatórios para garantir que diferentes partes da fita ou do storage de nuvem sejam lidas.
- **Ponto de Recuperação:** Alterne entre o backup mais recente (Incremental) e um backup mais antigo (Full).

2. Execução do Processo de Restauração

O teste deve ser realizado em um ambiente de sandbox (isolado da produção) para evitar conflitos de IP ou sobrescrita de dados reais.

- **Montagem/Extração:** Inicie o processo de restore através do software de gerenciamento.
- **Validação de Checksum:** Verifique se os hashes dos arquivos restaurados coincidem com os originais.
- **Verificação de Funcionalidade:**
    - **Arquivos simples:** Tente abrir uma amostra de documentos (PDF, XLSX).
    - **Bancos de Dados:** Execute uma query básica para validar a consistência das tabelas.
    - **VMs:** Realize o boot e verifique se o sistema operacional inicia sem erros de sistema de arquivos.

3. Cada teste deve gerar um relatório curto contendo:

- **RTO Real (Recovery Time Objective):** Cronometre quanto tempo levou desde o início do comando até a disponibilidade total do dado. Compare com o RTO definido na política da organização.
- **Integridade:** Os dados estão 100% legíveis? (Sim/Não).
- **Localização:** O backup foi restaurado do armazenamento local ou da nuvem?
- **Responsável:** Assinatura do técnico que executou o teste.

Data do Teste	Sistema Testado	RTO Previsto	RTO Real	Status Final
26/03/2026	DB Produção	X horas	Abaixo do tempo	✅ Sucesso
26/03/2026	Servidor Arquivos	X horas	Acima do tempo	⚠️ Alerta (Gargalo Rede)

4. Recomendações de Melhoria

- **Regra 3-2-1:** Certifique-se de que o teste valide pelo menos uma das cópias *offsite* (externa).
- **Automação:** Sempre que possível, utilize scripts de *Auto-Recovery* (Recuperação automática) que restauram e validam o banco de dados semanalmente, enviando um alerta apenas em caso de falha.

Fonte: Framework NIST (National Institute of Standards and Technology),ITIL (Information Technology Infrastructure Library), ISO/IEC 27001, 27002 e o PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 35

Estruturar um processo de configuração segura

Estruturar um processo de configuração segura, mantendo imagens padronizadas (Golden Images) ou infraestrutura como código (IaC) de servidores e ativos críticos para viabilizar uma reconstrução sistêmica rápida

1. Padronização com Golden Images (Imutabilidade)

- **Hardening Nativo:** Aplique benchmarks (como o CIS Benchmarks) diretamente na imagem base, removendo serviços desnecessários e fechando portas vulneráveis.
- **Pipeline de Build:** Utilize ferramentas para automatizar a criação de imagens em múltiplos ambientes (Serpro, Dataprev, AWS, Azure, VMware).
- **Ciclo de Vida (Patching):** Não atualize servidores em execução. Em vez disso, atualize a Golden Image, teste-a e faça o deploy de novas instâncias (estratégia de **Blue/Green Deployment**).

2. Infraestrutura como Código (IaC) e Orquestração

A IaC garante que a rede, o armazenamento e as permissões sejam reconstruídos exatamente da mesma forma em minutos.

- **Provisionamento Declarativo:** Use soluções para definir o estado desejado da infraestrutura. Isso evita o "desvio de configuração" (configuration drift).
- **Gerenciamento de Configuração:** Para ajustes finos pós-boot (como instalar agentes de monitoramento ou políticas locais),
- **Repositório Centralizado:** Mantenha todo o código de infraestrutura em um sistema de controle de versão (Git), com revisões de código (Pull Requests) para garantir a segurança.

3. Gestão Segura de Segredos

A reconstrução rápida falha se as credenciais estiverem "hardcoded" ou perdidas.

- **Externalização de Segredos:** Nunca armazene senhas, certificados ou chaves de API no código ou na imagem.
- **Cofres Dinâmicos:** Utilize soluções para injetar credenciais em tempo de execução.

Fonte: NIST Special Publication 800-123, CIS Benchmarks (Center for Internet Security), ISO/IEC 27001 e o PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 36

Garantir que os consoles de gerenciamento de backup possuam contas de administrador

Garantir que os consoles de gerenciamento de backup possuam contas de administrador estritamente dedicadas (segregadas do serviço de diretório principal) e protegidas compulsoriamente por autenticação multifator (MFA)

1. Segregação de Identidade (Contas Dedicadas)

O comprometimento do seu Domínio (AD/Entra ID) não deve comprometer o seu Backup.

- **Contas Locais ou Workgroup:** Crie contas de administrador exclusivas na base de dados local do software de backup ou em um grupo de trabalho (Workgroup) isolado.
- **Proibição de Contas de Domínio:** Jamais utilize contas como DOMAIN\Administrator ou usuários do grupo Domain Admins para gerenciar o console.
- **Princípio do Privilégio Mínimo:** Crie contas nominais para cada operador. Evite o uso de contas genéricas como “admin_backup”.

2. Implementação de MFA Compulsório

- **MFA Out-of-Band:** Utilize métodos que não dependam do serviço de diretório principal (ex: aplicativos autenticadores como Google/Microsoft Authenticator, ou tokens de hardware via TOTP).
- **Aplicação no Login do Console:** Configure o software de backup para solicitar o token MFA imediatamente após a inserção da senha, tanto para acesso via interface gráfica (GUI) quanto via linha de comando (CLI).
- **Proteção de Funções Sensíveis:** Garanta que o MFA seja exigido especialmente para ações de “Destructive Operations” (exclusão de repositórios ou alteração de políticas de retenção).

3. Endurecimento do Acesso (Hardening)

- **Lista Branca de IPs (Allowlist):** Restrinja o acesso ao console de gerenciamento apenas a partir de IPs específicos ou de uma **Jump Station** (bastion host) dedicada e segura.
- **Restauração “Break-Glass”:** Mantenha uma conta de emergência offline (em cofre físico) com credenciais altamente complexas para casos de falha total do sistema de MFA.

Fonte: NIST Cybersecurity Framework (NIST CSF 2.0), Guia NIST SP 800-209 (Security Guidelines for Storage Infrastructure), CIS Controls (Center for Internet Security), CISA (Cybersecurity & Infrastructure Security Agency), ISO/IEC 27001:2022 e o PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 37

Projetar e manter uma arquitetura de rede segura

Projetar e manter uma arquitetura de rede segura abordando segmentação e privilégio mínimo, separando a infraestrutura em VLANs por função específica (ex.: servidores, dispositivos de usuário final, dispositivos IoT e rede de visitantes)

Projetar uma rede segura não é apenas sobre colocar um firewall na borda; é sobre garantir que, se um invasor entrar, ele não consiga se mover. Abaixo, segue as orientações técnicas para implementar uma arquitetura baseada em **Segmentação de Rede** e no **Princípio do Privilégio Mínimo (PoLP)**.

1. Planejamento de VLANs por Função

A segmentação lógica via VLANs (IEEE 802.1Q) isola o tráfego de transmissão e limita o raio de alcance de um eventual ataque.

VLAN	Segmento	Descrição e Política de Acesso
10	**Servidores**	Apenas portas específicas abertas (ex: 443, 80). Sem acesso direto à internet, exceto via Proxy/WSUS.
20	**Usuários Finais**	Acesso à VLAN de Servidores e Internet. Bloqueio de comunicação peer-to-peer entre estações.
30	**Dispositivos IoT**	**Isolamento Total.** Acesso apenas aos servidores de gerência. Sem saída para a internet (ou via Gateway inspecionado).
40	**Visitantes**	Acesso apenas à Internet (Portas 80/443). Isolamento total de qualquer recurso interno.
99	**Gerenciamento**	Acesso restrito via VPN/SSH aos switches, firewalls e APs. Nunca use a VLAN 1 (padrão).

2. Implementação do Privilégio Mínimo (PoLP)

O privilégio mínimo dita que cada sistema ou usuário deve acessar apenas o estritamente necessário para sua função.

- **Micro-segmentação:** Além das VLANs, utilize Firewalls de Próxima Geração (NGFW) ou Listas de Controle de Acesso (ACLs) para filtrar o tráfego **Leste-Oeste** (dentro da rede local).
- **Controle de Admissão de Rede (NAC):** Implemente o protocolo **802.1X**. Dispositivos só ganham acesso à respectiva VLAN após autenticação via certificado ou credencial.
- **Políticas de Firewall:** Substitua a regra padrão “Permitir Tudo” por “Negar Tudo” (Default Deny). Libere apenas fluxos documentados.

3. Segurança em Dispositivos IoT e Visitantes

Estes são os elos mais fracos da cadeia.

- **IoT:** Dispositivos IoT raramente recebem atualizações. Eles devem residir em uma rede “sandbox” (área restrita). Se um sensor de temperatura for comprometido, ele não deve conseguir “pingar” o servidor de banco de dados.
- **Rede de Visitantes:** Deve utilizar **Client Isolation** (Isolamento de Cliente) no Ponto de Acesso (AP), impedindo que um visitante veja o notebook de outro visitante.

4. Manutenção e Monitoramento Contínuo

Uma arquitetura segura é um processo, não um estado permanente.

Auditoria de Regras

Revise as ACLs e regras de firewall trimestralmente. Remova acessos temporários que não foram revogados.

Monitoramento de Tráfego

Utilize ferramentas de **IDS/IPS** (Sistema de Detecção/Prevenção de Intrusão) para identificar comportamentos anômalos, como um dispositivo IoT tentando realizar varredura de portas (port scanning) na rede de servidores.

Gestão de Vulnerabilidades

- **VLAN de Quarentena:** Configure o NAC para mover dispositivos que não cumprem os requisitos de segurança (antivírus desatualizado, patches críticos ausentes) para uma VLAN de remediação automática.

Nota de Segurança: Nunca utilize a VLAN 1 para tráfego de dados. Ela é o alvo primário para ataques de VLAN Hopping. Mova todo o gerenciamento para uma VLAN nativa específica e desative portas de switch não utilizadas.

Fonte: National Institute of Standards and Technology (NIST SP 800-125B), CIS Controls (Center for Internet Security), Padrão IEEE 802.1Q e 802.1X, OWASP (Internet of Things Security Project) e o PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 38

Realizar a filtragem de tráfego entre os segmentos de rede

Realizar a filtragem de tráfego entre os segmentos de rede, bloqueando ativamente a comunicação de protocolos de alto risco frequentemente utilizados para movimentação lateral (como RDP, SMB, WMI e PsExec)

A filtragem de tráfego entre segmentos de rede é essencial para implementar o modelo de **Zero Trust**, impedindo que um atacante se desloque livremente após uma brecha inicial. Ao bloquear protocolos de alto risco (como SMB, RDP e RPC) em rotas não essenciais, reduz-se drasticamente a **superfície de ataque** e a eficácia de ferramentas de exploração automatizadas. Essa prática estabelece perímetros de controle granulares que isolam ativos críticos, transformando uma rede plana em uma arquitetura resiliente contra a propagação de malwares e ransomwares. Abaixo, estão descritas as orientações técnicas para implementar esse bloqueio de forma estruturada.

1. Diretrizes de Bloqueio por Protocolo

Abaixo estão as orientações específicas para os protocolos citados, visando restringir o tráfego “Leste-Oeste” (entre estações e servidores do mesmo nível):

RDP (Remote Desktop Protocol - Porta TCP 3389)

- **Ação:** Bloquear comunicações RDP diretas entre estações de trabalho (Endpoint para Endpoint).
- **Exceção:** Permitir apenas a partir de **Jump Servers** (Bastion Hosts) ou redes de gerenciamento seguras com autenticação multifator (MFA).

SMB (Server Message Block - Portas TCP 445 e UDP 137-139)

- **Ação:** Bloquear o tráfego SMB entre estações de trabalho. Este é o principal vetor para disseminação de Ransomware.
- **Exceção:** Permitir apenas tráfego direcionado a File Servers ou Domain Controllers específicos.

WMI e PsExec (Portas RPC/135 e Ephemerals)

- **Ação:** Bloquear RPC (Remote Procedure Call) e portas dinâmicas entre zonas de usuários. O PsExec utiliza SMB (porta 445) e compartilhamentos administrativos (Admin$).
- **Configuração:** Desabilitar o serviço de Gerenciamento Remoto (Ex.: no Windows: WinRM - portas 5985/5986) onde não for estritamente necessário.

2. Implementação Técnica em Camadas

A filtragem deve ocorrer em múltiplos níveis para garantir a defesa em profundidade:

A. Perímetro e Core (Firewall Interno)

Utilize firewalls de próxima geração (NGFW) para segmentar a rede em VLANs distintas (ex: Usuários, Servidores, DMZ, IoT).

- Implemente regras **Stateful Inspection (Inspeção com Estado)**.
- Utilize **Filtro de Aplicação (L7)** em vez de apenas portas, para evitar que protocolos de risco "tunelizados" em portas comuns (como HTTPS) passem despercebidos.

B. Host-Based Firewall (Windows Firewall / IPtables)

Configurar via políticas de grupo (Ex.: No windows via GPO (Group Policy Object) para que as máquinas bloqueiem conexões de entrada de outras estações.

C. Isolamento de Credenciais

Como ferramentas de execução remota (como PsExec, WMI ou SSH) dependem de privilégios elevados, utilize soluções de gerenciamento de senhas de administrador local — como o LAPS para Windows ou cofres de senhas (PAM/Vaults) para contas com privilégios de root/sudo no Linux. Isso garante que cada máquina tenha uma credencial única, impedindo que a captura de um hash ou chave permita o movimento lateral por todo o parque tecnológico.

3. Monitoramento e Resposta

A filtragem ativa deve ser acompanhada de **Logging (registro)**:

- Habilitar logs de "Conexão Negada" no Firewall e SIEM.
- Monitorar o evento **4624** (Logon bem-sucedido) e **4625** (Falha de logon) para identificar tentativas de força bruta via RDP ou SMB.

Regra de Ouro: "Negar por padrão, permitir por exceção."

Fonte: NIST SP 800-207 (Zero Trust Architecture), Matriz MITRE ATT&CK, Guia de Segmentação da NSA (National Security Agency), CIS Controls (Center for Internet Security) e PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 39

Estabelecer e manter uma instância isolada dos dados de recuperação

Estabelecer e manter uma instância isolada dos dados de recuperação, segregando a rede de cópias de segurança em um segmento próprio com acesso restrito e protegido

A segregação de dados de recuperação em uma instância isolada mitiga o risco de movimentação lateral durante ataques de ransomware, garantindo a integridade dos backups através do conceito de air-gap lógico. Essa arquitetura utiliza segmentação de rede e controles de acesso rigorosos (como o modelo Zero Trust) para criar uma zona de segurança que impede a contaminação cruzada entre o ambiente de produção e o repositório de desastre.

Ao manter o tráfego de cópias em um segmento restrito e protegido, a organização assegura a disponibilidade de uma "última linha de defesa" confiável, essencial para a continuidade de negócios sob incidentes cibernéticos críticos. As orientações técnicas a seguir descrevem como estabelecer e proteger esta instância isolada.

1. Segregação e Microsegmentação de Rede

A rede de backup não deve ser uma extensão da rede de produção.

- **VLANs Dedicadas:** Crie um segmento de rede exclusivo para o tráfego de backup e gerenciamento de dados.
- **Firewall de Camada 7:** Implemente um firewall (Barreira de segurança) entre a rede de produção e a rede de backup, permitindo apenas portas específicas (ex: TCP/UDP do software de backup) e bloqueando todo o restante por padrão (*deny all*).
- **Acesso Restrito:** Utilize Listas de Controle de Acesso (ACLs) para garantir que apenas os servidores de origem e o servidor de backup se comuniquem.

2. Implementação do Air Gap (Lógico ou Físico)

O isolamento é a última linha de defesa contra Ransomware.

- **Air Gap Lógico:** Utilize controles de rede para ter acesso a replicação apenas durante a janela de backup, fechando-o imediatamente após a conclusão.
- **Imutabilidade:** Utilize repositórios de dados com suporte a **WORM** (*Write Once, Read Many*) ou instâncias de armazenamento com bloqueio de exclusão (Object Lock ou sistemas de arquivos imutáveis).

3. Controle de Acesso e Identidade (IAM)

- **Autenticação Multifator (MFA):** Torne obrigatório o uso de MFA para qualquer acesso administrativo ao console de backup ou à infraestrutura de armazenamento.

- **Privilégio Mínimo:** Separe as funções. Quem administra a produção não deve ter credenciais administrativas para excluir backups.
- **Contas Locais Isoladas:** Evite integrar o servidor de backup ao serviço de diretório de produção (como Active Directory, LDAP ou FreeIPA). Se ele for comprometido, o atacante não terá acesso imediato aos backups.

4. Monitoramento e Integridade

- **Detecção de Anomalias:** Monitore picos incomuns de alteração de dados ou redução drástica na taxa de desduplicação (sinais comuns de criptografia por ransomware).
- **Varredura de Malware:** Integre o ambiente de recuperação com ferramentas de antivírus/EDR para escanear os dados antes da restauração.
- **Testes de Recuperação Automatizados:** Realize testes periódicos de Restore em ambiente isolado (Sandbox) para garantir que os dados não apenas existam, mas sejam funcionais.

Fonte: NIST SP 800-209 (Security Guidelines for Storage Infrastructure), CIS Controls (Center for Internet Security), ISO/IEC 27001 e 27002:2022, Isolated Recovery Environment (IRE), CISA (Cybersecurity & Infrastructure Security Agency), Instrução Normativa nº 05/2021 e o PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 40

Implementar e gerenciar um firewall

Implementar e gerenciar um firewall baseado em host nos dispositivos de usuário final, com regra de negação padrão, restringindo severamente a comunicação lateral direta entre estações de trabalho

A implementação de firewalls baseados em host com política default-deny (Negação por Padrão) é crucial para estabelecer uma arquitetura de Zero Trust (Confiança Zero) no endpoint (dispositivo final), eliminando a superfície de ataque residual deixada por defesas de perímetro. Ao restringir severamente a comunicação lateral, mitiga-se a propagação de malwares e movimentações de adversários (East-West traffic), isolando comprometimentos ao dispositivo de origem. Esse controle granular transforma cada estação de trabalho em um segmento de rede único, garantindo que apenas fluxos explicitamente autorizados e necessários ao negócio sejam processados. Aqui estão as orientações técnicas para estruturar essa implementação:

1. Arquitetura e Estratégia de Regras

A base da segurança em hosts é o modelo Zero Trust aplicado à interface de rede.

- **Política de Negação Padrão (Default Drop):** Bloqueie todo o tráfego de entrada e saída que não tenha uma permissão explícita.
- **Isolamento de Estação para Estação (Microsegmentação):**
    - Proibir explicitamente qualquer comunicação direta entre IPs de estações de trabalho (ex: Subnet A não fala com Subnet A).
    - Permitir apenas tráfego para **Gargalos Controlados** (ex.: Servidores de arquivos, AD, Proxy, Gateway de VPN).

2. Implementação Técnica

A configuração deve ser feita via **GPO (Group Policy Object)** no Windows ou ferramentas de **MDM** (como Intune ou Jamf).

Configurações de Entrada (Inbound)

- **Regra de Negação Geral:** Action: Block para todas as conexões que não correspondam a uma regra específica.
- **Permissões Essenciais:**
    - **ICMP (Ping):** Permitir apenas de subnets de gerenciamento de TI.
    - **Gestão Remota (RDP/WinRM):** Permitir apenas a partir de IPs de “Jump Servers” ou VLAN de administração.
    - **DHCP/DNS:** Permitir resposta dos servidores autorizados.

Configurações de Saída (Outbound)

- **Restrição Lateral:** Criar regra bloqueando o destino para o range de IPs das próprias estações.

Exemplo: Block Outbound -> Remote IP: 192.168.1.0/24 (Workstation Range).

- **Destinos Permitidos:** Permitir tráfego apenas para portas específicas (80, 443, 853) destinadas ao Gateway/Proxy e portas de autenticação para o Domain Controller.

3. Gerenciamento e Monitoramento

Exemplo:

Atividade	Descrição Técnica
Log de Auditoria	Habilitar Audit Disposable Connections para identificar tentativas de violação de regra.
Centralização	Encaminhar logs (SIEM) para detectar padrões de varredura de rede (Port Scanning).
Modo de Teste	Antes do "Deny" total, utilize o modo **Audit Only** por XX dias para identificar fluxos legítimos esquecidos.
Exceptions	Crie grupos de segurança no serviço de diretório (ex.: AD, LDAP ou FreeIPA) para aplicar exceções temporárias via políticas de grupo (GPO) ou ferramentas de gerenciamento de configuração apenas a usuários ou servidores específicos.

4. Melhores Práticas de Hardening

- **Proteção de Interface:** Impedir que o usuário final desative o serviço de firewall (Remover privilégios de Admin local).
- **Perfil de Rede:** Diferenciar regras para perfis **Domínio, Privado e Público** (reforçando a segurança quando o dispositivo estiver fora da organização).
- **IPsec:** Se possível, utilize autenticação IPsec para garantir que apenas dispositivos autenticados no domínio possam sequer tentar uma conexão.

Fonte: NIST Special Publication 800-53 (Rev. 5), Arquitetura Zero Trust (NIST SP 800-207), CIS Controls (v8), ISO/IEC 27001:2022 (Anexo A), Microsoft Security Best Practices, MITRE ATT&CK Framework e o PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 41

Isolar ativos institucionais e infraestruturas de rede

Isolar ativos institucionais e infraestruturas de rede legadas que não possam ser plenamente atualizados, alocando-os em segmentos de rede altamente restritos para conter a exploração de vulnerabilidades

A segregação de sistemas legados em zonas desmilitarizadas (DMZ) ou VLANs restritas mitiga o risco de **movimentação lateral** ao reduzir drasticamente a superfície de ataque explorável. Essa arquitetura de **microsegmentação** aplica controles rígidos de filtragem de tráfego (L4-L7), garantindo que ativos vulneráveis permaneçam operacionais sem expor o núcleo da infraestrutura a ameaças externas. Através do princípio do **privilégio mínimo**, o isolamento estabelece um perímetro de contenção que preserva a integridade institucional diante da impossibilidade de atualizações de segurança. Abaixo, **são apresentadas** as orientações técnicas para a implementação de Zonas de Rede Restritas (Enclaves Legados) baseadas em princípios de Zero Trust e Defense in Depth.

1. Identificação e Inventário

Antes de isolar, é preciso entender as dependências do ativo para não interromper serviços críticos.

- **Mapeamento de Fluxos:** Identifique todas as portas, protocolos e endereços IP com os quais o sistema legado se comunica.
- **Classificação de Risco:** Documente as vulnerabilidades conhecidas que justificam o isolamento (ex: SMBv1, TLS 1.0, SO sem suporte).

2. Arquitetura de Segmentação Restrita

A técnica principal consiste em mover o ativo para uma **VLAN de Quarentena** ou **Enclave Seguro**.

- **Gateways de Segmentação:** Utilize Firewalls de Próxima Geração (NGFW) como gateway padrão para esses segmentos.
- **Princípio do Privilégio Mínimo:** Aplique uma política de **Deny-All (Negar Tudo)** por padrão. Libere apenas os fluxos estritamente necessários mapeados na fase 1 (Identificação e Inventário).
- **Isolamento Lateral:** Impeça que ativos dentro do mesmo segmento legado se comuniquem entre si (Private VLANs ou isolamento de portas).

3. Controles de Segurança Compensatórios

Como o ativo está vulnerável, a rede deve atuar como uma “bolha de proteção”:

- **Inspeção de IPS/IDS:** Ative assinaturas de Virtual Patching no firewall para bloquear tentativas de exploração direcionadas às vulnerabilidades do legado.
- **Proxies de Aplicação:** Para sistemas web legados, utilize um **WAF (Web Application Firewall)** para filtrar o tráfego antes que ele atinja o servidor.
- **Terminação de VPN:** Se o acesso remoto for necessário, exija autenticação multifator (MFA) e uma VPN que termine em um gateway seguro antes de acessar o segmento restrito.

4. Monitoramento e Gestão de Acesso

- **Logging Extensivo:** Monitore 100% das tentativas de conexão (aceitas e negadas) vindas ou destinadas ao segmento legado.
- **Jump Servers (Bastion Hosts):** Proíba o acesso administrativo direto. Administradores devem passar por um servidor de salto que audita sessões (RDP/SSH) e limita ferramentas de transferência de arquivos.
- **Alerta de Anomalias:** Configure alertas para qualquer tráfego que fuja do padrão comportamental estabelecido.

Nota: O isolamento é uma medida paliativa. Estas orientações visam reduzir a superfície de ataque e o raio de explosão (blast radius) de um eventual comprometimento, mas o plano de descontinuidade ou substituição do ativo deve permanecer como meta.

Fonte: NIST SP 800-215 (Guide to a Secure Enterprise Network Landscape), NIST SP 800-123 (Guide to General Server Security), CIS Controls (v8), SANS Institute (Critical Security Controls para ICS/OT), Zero Trust Architecture (ZTA), OWASP (Virtual Patching Best Practices), MITRE ATT&CK Framework e o PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 42

Estabelecer e manter o inventário contínuo de contas de usuários

Estabelecer e manter o inventário contínuo de contas de usuários e contas de serviço , realizando auditorias regulares para remover acessos administrativos desnecessários ou esquecidos

O inventário contínuo e a auditoria rigorosa de contas mitigam o risco de **movimentação lateral** e exploração de privilégios ao reduzir drasticamente a superfície de ataque explorável. Essa prática assegura a aplicação do **Princípio do Menor Privilégio (PoLP)**, eliminando vetores críticos como contas "órfãs" ou administrativas inativas que servem de porta de entrada para invasores. Estruturalmente, o controle sistemático permite uma resposta a incidentes mais ágil, garantindo que apenas identidades autorizadas e monitoradas possuam acesso a ativos sensíveis da organização. Aqui estão as orientações técnicas para estruturar esse processo de forma eficaz:

1. Inventário Contínuo e Automatizado

O inventário deve ser dinâmico.

- **Centralização de Identidades:** Utilize um provedor de identidade central para consolidar contas de usuários e de serviço.
- **Descoberta Ativa:** Implemente ferramentas de varredura de rede para identificar "contas fantasmas" ou locais criadas fora do diretório central.
- **Classificação de Contas:** Diferencie claramente as contas em pelo menos três categorias:
    - **Contas de Usuário:** Atreladas a uma pessoa física.
    - **Contas de Serviço (Managed Service Accounts):** Usadas por aplicações/scripts.
    - **Contas Administrativas:** Com altos privilégios (Domain Admins, Root).

2. Gestão de Contas de Serviço

Contas de serviço são frequentemente esquecidas e possuem senhas que nunca expiram, tornando-se alvos críticos.

- **Vinculação de Responsável:** Toda conta de serviço deve ter um "dono" (owner) técnico no inventário.
- **Restrição de Logon:** Configure essas contas para que não permitam logon interativo (terminal) e restrinja seu uso a servidores específicos via políticas de grupo (GPO).
- **Rotação de Credenciais:** Utilize soluções de PAM (Privileged Access Management) para rotacionar senhas automaticamente sem quebrar a aplicação.

3. Auditoria e Higiene de Acessos

A auditoria não deve ser apenas uma revisão de nomes, mas uma validação de necessidade.

- **Revisão de Acesso (Access Certification):** Periodicamente (ex.: Mensalmente, Bimestralmente, Trimestralmente etc.), gestores devem confirmar se seus subordinados ainda necessitam dos acessos atuais.
- **Remoção de Contas Inativas:** Desativar automaticamente contas sem logon por mais de **XX dias** (ex.: **30 a 45 dias**).
    - Excluir contas desativadas após **XX dias** (ex.: **90 dias**).
- **Expurgo de Privilégios Administrativos:**
    - Remova usuários de grupos de administração permanente.
    - Implemente o modelo **Just-In-Time (JIT)**: o acesso administrativo é concedido apenas pelo tempo necessário para a tarefa e revogado automaticamente depois.

4. Monitoramento e Alertas

- **Logs de Auditoria:** Monitore eventos de criação de novas contas, alterações em grupos de segurança e falhas de logon.
- **Alertas de Comportamento:** Configure alertas para uso de contas de serviço fora do horário comercial ou em estações de trabalho comuns.

5. Tabela de Verificação Rápida

Sugerimos produzir uma tabela de verificação rápida. Exemplo:

Ação	Frequência	Objetivo
Varredura de Contas Locais	ex.: Semanal	Detectar contas criadas fora do padrão.
Revisão de Privilégios	ex.: Trimestral	Aplicar o privilégio mínimo.
Rotação de Senhas de Serviço	ex.: Automática	Prevenir ataques de Pass-the-Hash(PtH), técnicas de roubo de credenciais.
Desativação de Inativos	ex.: Mensal	Reduzir a superfície de ataque.

Fonte: NIST Special Publication 800-53, CIS Controls (Center for Internet Security), ISO/IEC 27001:2022 e o PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 43

Limitar os privilégios de administrador

Limitar os privilégios de administrador estritamente a contas de administrador dedicadas. Atividades gerais (como navegação na internet e leitura de e-mails corporativos) devem ser realizadas exclusivamente pela conta primária não privilegiada do usuário

A separação de funções mitiga o vetor de ataque conhecido como **escalada de privilégios**, garantindo que processos rotineiros, como a execução de navegadores e clientes de e-mail, operem sob um **token de segurança restrito**. Essa prática limita o raio de explosão (blast radius) de malwares e exploits de dia zero, impedindo modificações não autorizadas no kernel do sistema ou no registro. Ao isolar credenciais administrativas em contas dedicadas, a organização fortalece a conformidade com o **Princípio do Menor Privilégio** (PoLP) e reduz drasticamente a superfície de ataque para ameaças persistentes. Abaixo, são apresentadas as orientações técnicas para implementar a **Separação de Funções** (SoD) e o **Princípio do Menor Privilégio** (PoLP).

1. Separação de Identidades

- **Contas Dedicadas:** Crie contas exclusivas para tarefas administrativas (ex: admin.nome.usuario). Estas contas **não** devem possuir caixas de e-mail ativas.
- **Contas de Uso Geral:** Mantenha as contas nominais (ex: nome.usuario) como **Usuários Padrão**. Elas devem ser as únicas utilizadas para produtividade (ex: E-mail, Teams, Navegação Web).

2. Restrições de Acesso e Navegação

- **Bloqueio de Internet:** Contas com privilégios administrativos devem ser tecnicamente impedidas de acessar a internet externa e serviços de e-mail, via GPO ou Proxy.
- **Acesso a Dados:** Contas administrativas não devem ter permissão de leitura em pastas de documentos de usuários ou volumes de dados compartilhados, exceto para fins de backup/manutenção.

3. Implementação Técnica (Workstations e Servidores)

- **Controle de privilégios no nível de segurança máximo:** no Windows, mantenha o Controle de Conta de Usuário (UAC) em 'Sempre notificar'; no Linux, configure o sudo para exigir a senha do usuário a cada execução (evitando o NOPASSWD) e utilize ferramentas como PolKit para gerenciar autorizações de interface gráfica.
- **Administração Remota:** Utilize ferramentas de gerenciamento (como RSAT ou Windows Admin Center) a partir de uma estação de trabalho comum, em vez de realizar login interativo diretamente em servidores.
- **Privileged Access Workstations (PAW):** Para administradores de infraestrutura crítica (ex: AD, Cloud, Servidores Linux/Unix), recomenda-se o uso de máquinas físicas ou virtuais isoladas e endurecidas.

4. Gerenciamento de Credenciais

- **Soluções de PIM/PAM:** Implemente ferramentas de Privileged Identity Management (PIM) para fornecer acesso administrativo “Just-In-Time” (apenas quando necessário e por tempo limitado).
- **Gerenciamento de Senhas Locais:** Utilize o LAPS (Local Administrator Password Solution) para Windows ou ferramentas de PAM (Privileged Access Management) e Cofres de Senhas para Linux, para gerenciar e rotacionar automaticamente as credenciais de contas administrativas locais (como Administrator e root/sudo), garantindo que cada estação tenha uma senha única e temporária.

Nota: O uso de contas administrativas para tarefas rotineiras é um dos principais vetores de movimentação lateral e incidentes de ransomware. A separação rigorosa é a defesa mais eficaz contra essas ameaças.

Fonte: NIST SP 800-53, CIS Controls (Center for Internet Security), PPSI (Programa de Privacidade e Segurança da Informação) e ISO/IEC 27001.

Anexo 44

Remover direitos de administrador

Remover direitos de administrador local nos dispositivos de usuário final, restringindo modificações indevidas no sistema operacional

A remoção de direitos de administrador local é um pilar fundamental do modelo de **Privilégio Mínimo**, reduzindo drasticamente a superfície de ataque ao impedir a execução de malwares auto instaláveis e movimentações laterais. Ao restringir modificações no sistema operacional, a organização assegura a integridade da configuração padrão, mitigando riscos decorrentes de softwares não autorizados e alterações acidentais em arquivos críticos de sistema.

Essa prática não apenas fortalece a postura de segurança cibernética, como também otimiza a estabilidade operacional, resultando em uma mitigação substancial de incidentes de suporte derivados de degradação de integridade de dados e explorações de vulnerabilidades 0-day (dia zero). Aqui estão as orientações técnicas para implementar essa restrição de forma estruturada e segura.

1. Mapeamento e Inventário

Antes de remover os acessos, é fundamental entender quem realmente precisa deles.

- **Identificação:** Liste todos os usuários que fazem parte do grupo “Administradores” local nos endpoints.
- **Análise de Dependência:** Identifique softwares legados ou fluxos de trabalho que exigem privilégios elevados para funcionar.

2. Estratégia de Implementação

Para ambientes Windows

Em ambientes Windows Server (Active Directory), a forma mais eficiente é utilizar **Diretivas de Grupo (GPOs)**.

Configuração via Grupos Restritos:

- Acesse o Editor de Gerenciamento de Grupo de Diretivas.
- Navegue
  até: Configuração do Computador > Configurações do Windows > Configurações de Segurança > Gru pos Restritos.
- Adicione o grupo **Administradores**.
- Na seção **Membros deste grupo**, adicione apenas as contas que devem ter acesso (ex: Administrator local e o grupo de Suporte de TI do domínio).
- **Atenção:** Qualquer usuário que não esteja nessa lista será removido automaticamente do grupo de administradores locais na próxima atualização da diretiva.

Para ambientes Linux

No Linux, a administração local é controlada principalmente pela inclusão de usuários no grupo sudo (Debian/Ubuntu) ou wheel (RHEL/CentOS/Fedora) e pelas configurações no arquivo /etc/sudoers.

Configuração via Grupos Restritos:

- Identificar usuários Admin: Liste todos os usuários e grupos que possuem privilégios de sudo.
- Mapear Necessidades: Identifique quais ferramentas (ex: instalar impressora, atualizações) exigem privilégios.
- Criar Grupos de Exceção: Defina um grupo restrito (ex: sysadmin_local) para usuários que realmente precisam de privilégios elevados, se houver.
- Implementar Automação: Utilize ferramentas de gerenciamento de configuração (Ansible, Puppet, Chef) para aplicar as mudanças em massa, evitando ações manuais.
- Criar Política de Sudoers: Prepare um arquivo em /etc/sudoers.d/ para remover privilégios padrão e definir comandos específicos permitidos, se necessário.
- Remover Usuários do Grupo: Remova os usuários comuns dos grupos sudo ou wheel.
- Restringir o Arquivo Sudoers: Certifique-se de que o usuário não está listado diretamente no arquivo /etc/sudoers com privilégios ALL.
- Configurar Sudoers Restritivo: Utilize visudo para editar com segurança e remover regras genéricas de acesso root.

3. Gestão de Exceções: O Princípio do Privilégio Mínimo

Para não impactar a produtividade, adote uma solução de **Privileged Access Management (PAM)** ou **Endpoint Privilege Management (EPM)**.

- **Self-Service Elevation:** Permita que o usuário solicite elevação temporária para tarefas específicas (instalação de drivers homologados, etc.) mediante justificativa.
- **Whitelist de Aplicações:** Configure o sistema para que aplicações conhecidas rodem com privilégios elevados sem que o usuário precise ser administrador.

4. Medidas Complementares

- **Gerenciamento de Senhas Locais:** Implemente soluções de LAPS (como o Microsoft LAPS para Windows e alternativas compatíveis ou gerenciadores de segredos para Linux) para rotacionar automaticamente as senhas de contas administrativas locais, garantindo credenciais únicas e complexas para cada máquina.
- **Controle de Privilégios (UAC e Sudo):** Configure o UAC no nível máximo (Windows) e o sudo/polkit (Linux) para exigir reautenticação sempre que uma alteração administrativa for solicitada, garantindo que usuários comuns não executem comandos de alto impacto sem autorização explícita.

Fonte: NIST Cybersecurity Framework (NIST CSF), CIS Controls (Center for Internet Security), Microsoft Learn (Best Practices for Windows) e o PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 45

Estabelecer processos ágeis

Estabelecer processos ágeis de concessão e revogação de acesso lógico aos ativos, preferencialmente automatizando o modelo de acesso Just-In-Time (JIT) para limitar a janela temporal em tarefas administrativas

A implementação de processos ágeis e automatizados de acesso **Just-In-Time (JIT)** reduz drasticamente a superfície de ataque ao eliminar privilégios permanentes (standing privileges) e a persistência de contas administrativas. Através da orquestração via APIs e ferramentas de IAM, a organização garante que permissões elevadas existam apenas durante a execução da tarefa, mitigando riscos de movimentação lateral e abuso de credenciais. Essa abordagem fortalece o modelo **Zero Trust**, convertendo o controle de acesso de um gargalo operacional em uma barreira de segurança dinâmica e auditável em tempo real. Aqui estão as orientações técnicas para estruturar esse processo:

1. Arquitetura do Modelo JIT

O objetivo é eliminar contas com "privilégios permanentes" (*Standing Privileges*). O fluxo sugerido deve seguir este ciclo:

- **Solicitação:** O usuário solicita acesso via portal de autoatendimento ou integração com ITSM (ex: ServiceNow, Citsmart).
- **Validação:** Verificação automática de políticas (quem, onde, por que e por quanto tempo).
- **Provisionamento Temporário:** Criação de uma conta efêmera ou adição do usuário a um grupo de privilégios.
- **Desprovisionamento:** Revogação automática imediata após o término do TTL (*Time-to-Live*) definido.

2. Pilares para Automação

Gestão de Identidade Privilegiada (PIM/PAM)

Utilize ferramentas de **Privileged Access Management (PAM)** que suportem conectores de API.

- **Contas Efêmeras:** Em vez de usar senhas de contas admin existentes, o sistema gera credenciais únicas que expiram em minutos/horas.
- **Elevação de Grupo:** O usuário é inserido em um grupo de identidade e acesso (ex: Active Directory/Entra ID) apenas durante a janela de manutenção.

Infraestrutura como Código (IaC) e APIs

- **Integração CI/CD:** Automatize a revogação de acessos em ambientes de Cloud (ex: AWS, Azure, GCP) utilizando políticas de IAM dinâmicas via Terraform ou scripts Python/Go.
- **Webhooks (comunicação automatizado entre aplicações):** Configure gatilhos para que, ao fechar um chamado técnico, o acesso seja revogado instantaneamente, sem intervenção humana.

3. Diretrizes de Governança e Segurança

Definição de Políticas

- **RBAC vs ABAC:** Combine o Controle de Acesso Baseado em Funções (RBAC) com Atributos (ABAC) — como localização IP, horário e dispositivo — para decidir sobre a concessão do JIT.
- **Aprovação Multi-Nível:** Para tarefas críticas, exija aprovação manual (Workflow de Aprovação) antes da liberação automática do acesso.

Monitoramento e Auditoria

- **Logging Full-Session (Registro Completo de Sessão):** Toda sessão iniciada via JIT deve ser gravada (vídeo ou logs de comandos).
- **Revisão de Acesso:** Implemente Access Reviews (Revisão de Acess) automatizados para auditar se os gatilhos de revogação estão funcionando conforme o esperado.

4. Checklist de Implementação Técnica

Etapa	Ação Técnica Principal
Mapeamento	Identificar contas com alto privilégio (ex: Domain Admins, Cloud Owners).
Integração	Conectar a ferramenta de PAM ao diretório central (ex: LDAP/Azure AD).
Configuração	Definir janelas de tempo padrão (ex: 2h para suporte, 4h para deploy).
Automação	Criar scripts de limpeza (Cleanup) para remover permissões residuais.
Zero Trust	Exigir MFA (Múltiplo Fator de Autenticação) obrigatoriamente no pedido de JIT.

Nota Técnica: A eficácia do JIT reside na revogação. O sistema deve ser configurado para priorizar a "falha segura": se o cronômetro expirar ou houver erro de comunicação, o acesso deve ser bloqueado por padrão.

Fonte: NIST SP 800-207 (Zero Trust Architecture), ISO/IEC 27001, Princípio do Menor Privilégio (PoLP) e o PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 46

Gerenciar adequadamente contas padrão nos ativos institucionais

Gerenciar adequadamente contas padrão nos ativos institucionais (como administrador local), desabilitando-as ou utilizando soluções de randomização de credenciais/strong>

A gestão rigorosa de contas administrativas locais é vital para mitigar o movimento lateral e ataques de *Pass-the-Hash (Roubo de hash de senha/credenciais)*, pois credenciais estáticas e idênticas em múltiplos ativos facilitam a escalada de privilégios. A desativação de contas padrão ou o uso de soluções de **Privileged Access Management (PAM)**, como o **LAPS**, garante a unicidade e a randomização de senhas, reduzindo drasticamente a superfície de ataque. Essa prática isola comprometimentos individuais, impedindo que a quebra de um único endpoint resulte no controle total da infraestrutura institucional. Abaixo, são apresentadas as orientações técnicas para mitigar esses riscos de forma estruturada.

1. Tratamento de Contas Padrão e Built-in

O primeiro passo é reduzir a superfície de exposição desativando o que não é estritamente necessário.

- **Desabilitação da Conta 'Administrator' (Built-in):** Utilize ferramentas de gerenciamento centralizado (GPO/MDM para Windows e Gerenciadores de Configuração como Ansible, Puppet ou Chef para Linux) para desabilitar a conta de administrador nativa ou o acesso direto ao root em todos os endpoints.
- **Renomeação:** Se a desabilitação não for possível por questões de legado, renomeie a conta para algo não óbvio, dificultando ataques de força bruta.
- **Remoção de Usuários Comuns:** Garanta que contas de usuários comuns não pertençam ao grupo local de "Administradores".

2. Implementação de Randomização de Credenciais

Para as contas que precisam de privilégios locais (ex: suporte técnico), a solução ideal é a randomização automatizada.

Soluções Recomendadas:

- **Windows LAPS (Local Administrator Password Solution):** Solução gratuita da Microsoft que rotaciona automaticamente a senha do administrador local e a armazena de forma criptografada no Active Directory ou Azure AD/Entra ID.
- **PAM (Privileged Access Management):** Para ambientes heterogêneos (Linux/Windows/Unix), utilize cofres de senhas que realizam o check-out da credencial, alterando-a automaticamente após cada uso.

3. Fluxo de Operação com Credenciais Randomizadas

A aplicação deste ciclo de vida à automação é fundamental para preservar a integridade do ativo:

- **Solicitação:** O técnico solicita a senha local via console (LAPS ou PAM).
- **Uso Limitado:** A senha é revelada apenas para o técnico autorizado e permanece válida por um período curto (ex: 2 a 8 horas).

- **Expiração e Troca:** Após o tempo definido ou após o uso, o agente no host detecta a expiração e gera uma nova senha complexa e aleatória.
- **Sincronização:** A nova senha é enviada ao repositório central seguro.

4. Gerenciamento de Privilégios e Segurança de Endpoint

Para fortalecer o controle de acesso, aplique as seguintes restrições técnicas via ferramentas de gerenciamento centralizado (GPO/MDM para Windows e Gerenciadores de Configuração para Linux):

Bloqueio de Acesso Remoto Privilegiado

Impeça que contas administrativas locais ou nativas realizem login através da rede. Isso confina o uso de privilégios elevados ao acesso físico ou via console de gerenciamento seguro.

- **No Windows:** Configure a política **"Deny access to this computer from the network"** para a conta de **Administrador Local**.
- **No Linux:** Desabilite o login remoto do root no arquivo de configuração do SSH (PermitRootLogin no).

Controle Estrito de Grupos Administrativos

Utilize mecanismos de conformidade para garantir que apenas usuários e grupos autorizados possuam privilégios de superusuário ou administrador local.

- **No Windows:** Utilize a política de **"Grupos Restritos"** para limpar membros indesejados do grupo de Administradores.
- **No Linux:** Gerencie centralizadamente o arquivo /etc/sudoers ou o grupo wheel/sudo, garantindo a remoção de usuários não autorizados.

Fonte: NIST Special Publication 800-53, CIS Controls (Center for Internet Security), MITRE ATT&CK (Técnica T1078.003 - Local Accounts), Microsoft Windows LAPS Documentation e o PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 47

Estabelecer e manter recursos computacionais dedicados

Estabelecer e manter recursos computacionais dedicados (física ou logicamente isolados da rede primária) para tarefas administrativas, garantindo que contas altamente privilegiadas nunca se autentiquem em estações de trabalho de uso comum

A implementação de **Administrative Workstations (PAWs)** mitiga o risco de movimentação lateral e roubo de credenciais ao criar um perímetro de confiança isolado para funções críticas. Esse desacoplamento lógico ou físico impede que vetores de ataque comuns em redes de produtividade, como phishing e navegação web, comprometam hashes de contas privilegiadas. Ao restringir o uso de identidades de alto impacto a hardware endurecido, garante-se a integridade do plano de controle e a sobrevivência da infraestrutura ante uma invasão na rede corporativa. Abaixo, são apresentadas as orientações técnicas estruturadas para a implementação de **Privileged Access Workstations (PAWs)** e o conceito de Administração em Camadas (Tiered Administration).

1. Estratégia de Isolamento de Rede

Independentemente do SO, a estação administrativa deve residir em uma **VLAN de Gerenciamento** restrita.

- **Regra de Ouro:** O tráfego deve ser unidirecional (da PAW para os servidores/recursos), nunca o contrário.
- **Acesso à Internet:** Bloqueado ou limitado estritamente a repositórios de atualização oficiais via Proxy/Gateway específico.

2. Implementação em Ambientes Windows

O foco aqui é o modelo de **Administração em Camadas (Tiered Administration Model)**.

- **Contas Separadas:** Administradores devem ter uma conta para uso diário (e-mail/Teams) e outra distinta para tarefas administrativas ($adm\_username$).

Restrições via GPO:

  - Configurar **“Allow log on locally”** e **“Allow log on through Remote Desktop Services”** apenas para o grupo de admins nas PAWs.
  - Configurar **“Deny log on locally”** e **“Deny log on through Remote Desktop Services”** para contas privilegiadas em todas as estações de trabalho de uso comum.

- **Hardware/Virtualização:** Utilizar o Windows Defender Device Guard e Credential Guard para proteger segredos de autenticação no hardware.

3. Implementação em Ambientes Linux

O foco reside no endurecimento do kernel e no controle estrito de SSH/PAM.

- **Jump Servers (Bastion Hosts):** Estabelecer um host intermediário endurecido. O acesso aos servidores finais só deve ser permitido a partir do IP estático desta máquina.

- **Configuração do SSH:** No servidor de destino, editar /etc/ssh/sshd_config:

```
Bash
_____________________________________________________________________
AllowUsers admin_user@10.0.5.50    # Permite apenas o IP da PAW/Bastion
PasswordAuthentication no          # Força o uso de chaves SSH/MFA
```

- **Isolamento de Sessão:** Utilizar o módulo **PAM (Pluggable Authentication Modules)** para restringir onde contas de superusuário podem logar:
    - Editar /etc/security/access.conf para negar root em terminais não autorizados.
- **Integridade:** Utilizar distribuições com foco em segurança (como Alpine ou Fedora Silverblue) ou instâncias stateless que resetam o sistema de arquivos a cada reboot.

4. Diretrizes Comuns (Checklist de Segurança)

Recurso	Windows (PowerShell/GPO)	Linux (Bash/Config)
MFA	Mandatório via Hello for Business ou Token.	Mandatório via SSH Keys + TOTP/Yubikey.
Navegação Web	Proibida (AppLocker/Windows Defender).	Proibida (remover browsers ou via iptables).
Produtividade	Sem Office, e-mail ou redes sociais.	Sem clientes de e-mail ou suítes de escritório.
Atualizações	WSUS / Intune forçado.	Unattended-upgrades / Cron jobs.

5. Monitoramento e Auditoria

- **Logs Centrais:** Enviar logs de eventos (Windows Event Logs) e Syslog (Linux) para um SIEM centralizado imediatamente.
- **Alertas:** Configurar alertas em tempo real para qualquer tentativa de login de uma conta privilegiada em uma estação de “Tier 2” (uso comum).

Fonte: NIST SP 800-207 (Zero Trust Architecture), CIS Critical Security Controls (v8), Microsoft Enterprise Access Model (EAM), Documentação Técnica Microsoft PAW (Privileged Access Workstations), Guias de Hardening Linux (Comunidade e Vendor) e o PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 48

Estabelecer um processo de remediação fundamentado em risco

Estabelecer um processo de remediação fundamentado em risco, priorizando a correção de vulnerabilidades em ativos institucionais e soluções de software expostos externamente (como portais web, appliances de VPN e firewalls)

Uma abordagem de remediação baseada em risco otimiza a resiliência cibernética ao concentrar recursos computacionais e humanos na mitigação de vulnerabilidades com maior probabilidade de exploração ativa. Priorizar ativos expostos, como portais web e gateways de VPN, reduz drasticamente a superfície de ataque externa, neutralizando vetores críticos de entrada antes que falhas teóricas em ambientes internos sejam exploradas. Essa estratégia utiliza inteligência de ameaças para alinhar a correção técnica à criticidade do negócio, garantindo que o tempo médio de remediação (MTTR) proteja as funções institucionais mais vitais. O objetivo é transitar de um modelo de correção massiva para uma resposta cirúrgica, priorizando ativos que compõem a "vitrine" da instituição e que apresentam maior probabilidade de exploração real.

1. Mapeamento e Visibilidade da Superfície de Ataque

Antes de remediar, a organização deve ter clareza total sobre quais ativos estão expostos ao tráfego externo e quais serviços estão ativos.

- **Identificação de Exposição:** Utilize ferramentas de varredura externa (ex: Nmap, Shodan) para listar IPs, portas abertas e serviços que um atacante veria a partir da internet.
- **Inventário Dinâmico de Portas:** Realize auditorias internas constantes para identificar serviços escutando em interfaces externas (Linux: ss -tulpn | Windows: netstat -ano).
- **Classificação de Ativos Críticos:** Catalogue especificamente soluções de borda, como Portais Web, gateways de VPN e Firewalls, tratando-os como zonas de alto risco imediato.

2. Estratégias de Priorização e Hardening Técnico

A priorização deve ser baseada em dados de ameaças em tempo real e na redução da superfície de ataque por meio de configurações restritivas.

- **Hierarquia de Inteligência (KEV/EPSS):** Vulnerabilidades no catálogo CISA KEV ou com alto score EPSS devem furar a fila de patches tradicionais, independentemente da nota CVSS.
- **Higiene de Protocolos:** Em ativos expostos, desabilite protocolos legados e inseguros (como SMBv1 e TLS 1.0/1.1) que servem como vetores comuns de exploração inicial.
- **Uso de Edições Enxutas:** Para servidores Windows expostos, utilize a instalação Server Core para remover a interface gráfica e componentes desnecessários, reduzindo drasticamente a superfície de ataque.

3. Passos Práticos para Implementação

Passo 1: Triagem de Ativos "Na Vitrine"

- Identifique todos os pontos de entrada externos e cruze esses ativos com o inventário institucional.

- Verifique se softwares de terceiros ou bibliotecas específicas nos portais web possuem vulnerabilidades conhecidas.

Passo 2: Análise de Risco e Inteligência

- Consulte o catálogo CISA KEV e o score EPSS para definir a urgência. Se o exploit for público (Metasploit/GitHub), a correção é emergencial.
- Determine o impacto de uma possível indisponibilidade durante a correção versus o risco da exploração.

Passo 3: Ciclo de Patching e Validação

- Aplique os patches em ambiente de homologação (Staging) para garantir que a correção não "quebre" o serviço crítico.
- Implemente a atualização em produção utilizando automação (unattended-upgrades no Linux ou políticas agressivas de WSUS/SCCM no Windows).

Passo 4: Implementação de Mitigações Compensatórias

- Caso o patch imediato seja impossível, ative o Virtual Patching via WAF (Web Application Firewall) para bloquear assinaturas de ataque.
- Isole o ativo em uma DMZ (Zona Desmilitarizada) restrita e torne o MFA (Segundo Fator de Autenticação) obrigatório para qualquer acesso administrativo.

4. Considerações de Sustentação e Monitoramento

Se uma correção imediata quebrar o serviço:

- **Verificação de Fechamento:** Execute um rescan imediato após o deploy para confirmar tecnicamente que a vulnerabilidade foi eliminada.
- **Proteção de Identidade Privilegiada:** Aplique o Princípio do Mínimo Privilégio e utilize PAW (Privileged Access Workstations) para qualquer tarefa administrativa em ativos de perímetro.
- **Higiene de Sessão:** Force o encerramento de sessões inativas em consoles de gerência de firewalls e VPNs para impedir o sequestro de sessões autenticadas.

Fonte: NIST SP 800-40 Rev. 4, CIS Controls (Center for Internet Security), CISA (Cybersecurity & Infrastructure Security Agency), Framework [FIRST.org](http://first.org/), Microsoft Security Update Guide, Red Hat / Debian Security Advisories e o PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 49

Priorizar a correção de falhas

Priorizar a correção de falhas listadas em catálogos de vulnerabilidades ativamente exploradas (ex.: KEV - Known Exploited Vulnerabilities)

A priorização baseada em catálogos como o **KEV** é crítica pois substitui a triagem teórica por evidências reais de ataque, reduzindo drasticamente a janela de exposição contra ameaças iminentes. Focar em vulnerabilidades comprovadamente exploradas otimiza a alocação de recursos de segurança, mitigando riscos de maior probabilidade de impacto em vez de apenas seguir pontuações estáticas de severidade. O objetivo é direcionar o esforço técnico da equipe para as falhas que representam perigo real e imediato, utilizando inteligência de ameaças para furar a fila do gerenciamento de patches tradicional e mitigar riscos de ataques iminentes. Abaixo, será apresentado as orientações técnicas para estruturar esse processo de priorização.

1. Identificação e Inteligência de Ameaças

Antes da remediação, a organização deve transformar o inventário passivo em um mapa de riscos alimentado por fontes externas de inteligência cibernética.

Mapeamento de CVEs: Identifique softwares e versões na rede que possuam vulnerabilidades listadas no catálogo CISA KEV (Known Exploited Vulnerabilities).

Integração via API: Utilize ferramentas de gestão de vulnerabilidades que suportem conexão automática com bases de dados de inteligência para gerar alertas em tempo real.

Uso do Score EPSS: Utilize o Exploit Prediction Scoring System para prever a probabilidade de uma falha ser explorada nos próximos 30 dias, refinando a urgência da correção técnica.

2. Estratégias Técnicas por Plataforma (Hardening)

A remediação rápida exige abordagens específicas para cada ecossistema, garantindo a aplicação sem comprometer a disponibilidade.

Conformidade Acelerada (Windows): Utilize o Windows Update for Business via Intune ou GPO para forçar a instalação de KBs vinculados ao KEV em um ciclo emergencial de 24-48 horas.

Live Patching (Linux): ara vulnerabilidades de Kernel listadas no KEV, utilize tecnologias como Canonical Livepatch, kpatch ou Oracle Ksplice para corrigir o sistema sem necessidade de reboot.

Segregação de Processos: Em casos onde a atualização imediata é impossível, utilize AppArmor, SELinux ou Microsoft Defender Exploit Protection para restringir permissões e bloquear comportamentos típicos de exploração.

3. Passos Práticos para Implementação

A fragmentação exige uma abordagem baseada em repositórios e gestão de dependências.

Passo 1: Triagem e Inventário Ativo

- Cruze o inventário de ativos institucionais com o catálogo CISA KEV e identifique quais serviços estão expostos à internet.
- Priorize ativos de perímetro (VPNs, Firewalls e Portais) e sistemas que processam dados sensíveis.

Passo 2: Configuração de Ciclos Emergenciais

- Configure janelas de manutenção imediatas para ativos de alto risco, ignorando o ciclo mensal de patches padrão para vulnerabilidades comprovadamente exploradas.
- Utilize o PowerShell (Get-HotFix) ou scripts Ansible para validar rapidamente a presença de correções em larga escala.

Passo 3: Aplicação de Mitigações de "Dia 0"

- Se o patch oficial ainda não foi testado, implemente mitigações temporárias como o isolamento do host da rede externa ou a desativação de serviços desnecessários.
- Ative proteções de integridade de código e isolamento de processos para dificultar o sucesso de exploits públicos disponíveis (Metasploit/GitHub).

Passo 4: Validação e Verificação Técnica

- Execute uma varredura de vulnerabilidades autenticada imediatamente após a aplicação do patch para confirmar a remediação definitiva.
- Realize o monitoramento retrospectivo de logs (Event Viewer/journalctl) em busca de Indicadores de Comprometimento (IoCs) que possam ter ocorrido antes da correção.

4. Considerações de Segurança e Monitoramento

Após a aplicação, a validação é mandatória para garantir que o "curativo" funcionou:

Mentalidade "Assume Breach": Se uma falha estava no KEV, assuma que ela pode ter sido explorada antes da sua intervenção. Monitore o comportamento do sistema após o patch para detectar persistências.

Matriz de Priorização: Utilize a exposição como critério de desempate. Ativos voltados para a internet devem ser corrigidos primeiro, independentemente do score CVSS original.

Manutenção da Higiene Geral: A priorização pelo KEV é uma "via expressa" para crises. Ela não substitui o ciclo de vida tradicional de patches, que deve continuar tratando as vulnerabilidades não exploradas ativamente.

Referência: (https://www.cisa.gov/known-exploited-vulnerabilities-catalog)

Fonte: NIST SP 800-40 Rev. 4, CTIR Gov (Brasil), CIS Controls (Center for Internet Security), CISA (Cybersecurity & Infrastructure Security Agency), Framework [FIRST.org](http://first.org/), Microsoft Learn, Microsoft Security Response Center (MSRC), Projetos SELinux e AppArmor, Red Hat / Debian Security Advisories e o PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 50

Focar na aplicação ágil

Focar na aplicação ágil de atualizações em servidores de correio eletrônico e sistemas que possuam serviços de acesso remoto habilitados (ex.: RDP)

A rápida aplicação de patches em servidores de e-mail e serviços de RDP é crítica para mitigar vulnerabilidades de execução remota de código (RCE), frequentemente exploradas como vetores primários de intrusão. Essa agilidade interrompe a cadeia de ataque inicial, impedindo o movimento lateral e o comprometimento da integridade de dados em ativos expostos diretamente à rede externa.

O objetivo é garantir a integridade do perímetro e a continuidade da comunicação institucional através de um ciclo de atualização acelerado em ativos de alta exposição, minimizando a janela de oportunidade para ataques de ransomware e exfiltração de dados.

1. Estratégia de Patching Ágil e Automação

Para garantir rapidez sem comprometer a estabilidade, a organização deve adotar métodos que permitam a aplicação de correções de segurança sem a necessidade de interrupções prolongadas.

- **Hotpatching e Livepatching:** Utilize tecnologias que permitem aplicar atualizações críticas diretamente na memória (RAM) sem reiniciar o sistema (Windows: Azure Edition
- **Hotpatching | Linux:** Canonical Livepatch ou kpatch).
- **Atualizações Automáticas de Segurança:** Configure os servidores para instalar automaticamente apenas os pacotes de segurança, mantendo as atualizações de funcionalidades para ciclos manuais (Debian: unattended-upgrades | RHEL: dnf-automatic).
- **Gerenciamento via Rings (Anéis):** Implemente um “Ring 0” composto por servidores de teste ou instâncias de correio não críticas para validar os patches em até 24 horas antes do deploy massivo.

2. Endurecimento de Serviços Críticos (Mail & Remote)

A agilidade na atualização deve ser acompanhada por configurações de hardening que protejam o serviço caso uma vulnerabilidade de “Dia Zero” seja explorada.

- **Isolamento de Servidores de Correio:** Utilize módulos de segurança (como SELinux ou AppArmor) para restringir o que os binários do serviço de e-mail (Postfix, Exim, Exchange) podem acessar no sistema de arquivos.
- **Proteção de Acesso Remoto (RDP/SSH):** Force o uso de NLA (Network Level Authentication) no Windows e desabilite autenticação por senha no Linux em favor de chaves criptográficas (Ed25519).
- **Ocultação de Perímetro:** Nunca exponha portas padrão (3389, 22) diretamente à internet. Utilize Gateways de acesso, VPNs ou soluções de ZTNA (Zero Trust Network Access) como intermediários obrigatórios.

3. Passos Práticos para Implementação

A agilidade na atualização deve ser acompanhada do “endurecimento” da configuração para evitar acessos via força bruta.

Passo 1: Mapeamento de Pontos de Entrada

- Identifique todos os servidores que escutam nas portas de correio (25, 465, 587, 993) e acesso remoto (3389, 22).
- Garanta que esses ativos possuam snapshots ou backups de estado consistentes antes de iniciar o ciclo de patching ágil.

Passo 2: Validação em Ambiente de Homologação

- Aplique as atualizações críticas no “Ring 0” e realize testes de fluxo de mensagens (SMTP/IMAP) e estabilidade de conexão remota.
- Verifique se o patch não alterou permissões de pastas críticas ou configurações de firewall locais.

Passo 3: Deploy Automatizado e em Massa

- Utilize ferramentas de orquestração (como Ansible, Terraform ou Azure Update Manager) para disparar as atualizações simultaneamente em todo o parque.
- No Windows, utilize o PowerShell Remoting ou o módulo PSWindowsUpdate para auditar a conformidade em tempo real.

Passo 4: Verificação e Ativação de MFA

- Após o patching, valide a aplicação com um rescan de vulnerabilidades para garantir que nenhum binário antigo permaneceu em execução.
- Torne o MFA (Autenticação de Múltiplos Fatores) mandatório para todos os serviços de acesso remoto; o MFA é a última linha de defesa se a credencial for roubada via vulnerabilidade.

4. Considerações de Segurança e Monitoramento

- **Monitoramento de Força Bruta:** Implemente ferramentas como o Fail2Ban ou proteções nativas de IPS para banir automaticamente IPs que tentem conexões repetitivas em serviços de acesso remoto.
- **Análise de Relay e Spam:** Monitore logs de servidores de correio imediatamente após atualizações para garantir que configurações de segurança (como SPF, DKIM e DMARC) permaneçam íntegras.
- **Higiene de Sessão Remota:** Configure o encerramento automático de sessões RDP/SSH inativas para evitar que sessões “esquecidas” na memória sejam alvos de ataques de sequestro de tokens.

Fonte: NIST CSF 2.0 (National Institute of Standards and Technology), CIS Benchmarks (Center for Internet Security) 2026, Microsoft Security Best Practices (2026), Canonical & Red Hat Security Guides, SSH Audit & Hardening Standards, Patch Management Lifecycle (SANS Institute) e o PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 51

Elaborar uma lista de scripts autorizados

Elaborar uma lista de scripts autorizados e implementar controles técnicos para bloquear a execução de macros em arquivos oriundos da internet e de scripts não assinados digitalmente

A implementação de whitelisting de scripts e o bloqueio de macros externas mitigam vetores críticos de **RCE (Remote Code Execution)** e ataques onde os invasores não instalam malwares externos, mas utilizam ferramentas legítimas, confiáveis e já existentes no sistema operacional alvo, **LotL (Living-off-the-Land)**. Esses controles estabelecem uma camada rigorosa de **integridade** e **procedência**, garantindo que apenas processos autenticados operem no ambiente, reduzindo drasticamente a superfície de exposição a malwares e *ransomwares*. O objetivo é mitigar o risco de execução de código malicioso através da imposição de assinaturas digitais em scripts e da neutralização de vetores de entrada clássicos, como macros do Office oriundas de fontes externas (Internet). Abaixo, será apresentada orientações para a elaboração da lista de scripts autorizados e o bloqueio de execuções não confiáveis.

1. Scripts Autorizados e Assinatura Digital

A segurança baseada em nomes de arquivos é frágil; a confiança deve ser estabelecida através da identidade do autor via certificados digitais.

- **Imposição de Assinatura (Windows):** Utilize a *Execution Policy* do PowerShell configurada como **AllSigned**. Isso garante que apenas scripts assinados por um certificado presente no repositório de "Editores Confiáveis" sejam executados.
- **Integridade no Linux:** Implemente o **fapolicyd** (File Access Policy Daemon) para criar listas de permissão (Allowlisting) baseadas em integridade de arquivos, impedindo que scripts em diretórios temporários ou não autorizados ganhem permissão de execução.
- **Assinatura GnuPG:** Para automações críticas em Linux, utilize o **GnuPG** para assinar os scripts. Implemente verificações de assinatura nos hooks do gerenciador de pacotes ou antes da execução de jobs de manutenção.

2. Bloqueio de Macros e Mark of the Web (MotW)

Arquivos provenientes da internet recebem uma "marca" (MotW) que deve ser utilizada pelo sistema operacional para aplicar políticas restritivas automáticas.

Bloqueio via GPO (Microsoft Office): Ative a política "Bloquear a execução de macros em arquivos do Office provenientes da Internet". Esta configuração ignora a decisão do usuário e impede a ativação do conteúdo mesmo em arquivos com o botão "Habilitar Edição" visível.

Hardening no LibreOffice: Defina o nível de segurança de macros para "Muito Alto". Isso restringe a execução apenas a documentos localizados em "Caminhos Confiáveis" ou assinados por certificados pré-aprovados pela administração.

Desativação de Protocolos de Script: Bloqueie a execução de motores de script legados (como VBScript e JScript) em navegadores e documentos através de políticas de restrição de software.

3. Passos Práticos para Implementação

Passo 1: Centralização e Inventário de Scripts

- Mova todos os scripts autorizados para um repositório Git centralizado com controle de acesso rigoroso. Identifique quais scripts são essenciais para a operação e devem ser assinados.

Passo 2: Implementação da Infraestrutura de Assinatura

- Utilize uma Autoridade Certificadora (CA) interna para emitir certificados de "Assinatura de Código" para os desenvolvedores e administradores de sistema. Distribua a chave pública desta CA para todas as máquinas da rede.

Passo 3: Ativação do Bloqueio de Macros via GPO

- Configure os Modelos Administrativos do Office no AD e aplique o bloqueio de macros MotW. Teste primeiro em uma Unidade Organizacional (OU) piloto para garantir que fluxos de trabalho legítimos (que usem caminhos de rede confiáveis) não sejam afetados.

Passo 4: Transição para a Política AllSigned

- Assine digitalmente todos os scripts do repositório central. Altere a Execution Policy gradualmente, começando por servidores críticos e expandindo para as estações de trabalho, monitorando logs de bloqueio para ajustar scripts esquecidos.

4. Considerações de Segurança e Monitoramento

- **Monitoramento de Logs de Script:** Habilite o log detalhado do PowerShell (Event ID 4104) para capturar o conteúdo de scripts executados, permitindo a análise forense mesmo em scripts que foram assinados, mas que podem ter sido utilizados de forma abusiva.
- **Proteção da Chave Privada:** O certificado de assinatura de código é o "selo de confiança" da organização. Proteja a chave privada em módulos de segurança de hardware (HSM) ou dispositivos criptográficos protegidos por senha forte.
- **Higiene de Repositórios:** Realize auditorias periódicas no repositório de scripts autorizados. A remoção de scripts obsoletos e a revogação de certificados de colaboradores que mudaram de função são fundamentais para manter a eficácia do controle.

Fonte: NIST SP 800-53, CIS Benchmarks (Center for Internet Security) 2026, Essential Eight (Australian Cyber Security Centre), Microsoft Learn (PowerShell), Windows Defender Application Control (WDAC) e AppLocker, Red Hat / Fedora Security Guide, Man pages do GNU Privacy Guard (GnuPG), MITRE ATT&CK e o PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 52

Implementar controles técnicos rigorosos

Implementar controles técnicos rigorosos (como AppLocker ou listas de soluções de software permitidas) para impedir a execução de softwares e scripts não autorizados, inclusive a partir de pastas temporárias

A implementação de lista de permissões (Allowlisting) via AppLocker mitiga vetores de ataque ao restringir a execução de binários e scripts apenas a diretórios e assinaturas confiáveis. Essa postura de Zero Trust (Dia zero) no endpoint (Dispositivo/Equipamento final) impede que malwares e ferramentas de movimentação lateral operem a partir de pastas temporárias, neutralizando ameaças que burlam defesas perimetrais. O objetivo é transitar de um modelo de confiança implícita para um modelo de "Negação por Padrão" (Default Deny), garantindo que apenas softwares e scripts previamente validados e assinados possam ser executados no ambiente institucional.

1. Estratégias de Controle de Aplicações (Whitelisting)

Antes da implementação técnica, a organização deve definir as regras de confiança que regem o que é permitido rodar nos endpoints e servidores.

- **Regras baseadas em Assinatura (Editor):** A forma mais segura de controle. Permite a execução de binários assinados por certificados digitais confiáveis (ex: Microsoft, Adobe, ou a própria CA da instituição), ignorando o caminho onde o arquivo está salvo.
- **Bloqueio de Pastas Temporárias:** A execução de qualquer arquivo a partir de diretórios graváveis pelo usuário (como %Temp%, %AppData% ou /tmp) deve ser bloqueada por padrão, neutralizando o local preferido para o payload inicial de malwares.
- **Lockdown de Interpretadores:** Além de binários, é necessário restringir scripts. No Windows, isso é feito via *Constrained Language Mode* (PowerShell); no Linux, via perfis de segurança para os interpretadores (Python, Perl, Bash).

2. Endurecimento do Sistema de Arquivos (Linux)

Diferente do Windows, o Linux permite um controle nativo e performático através do gerenciamento de montagem de partições.

- **Flags de Montagem (noexec):** A aplicação da flag noexec no arquivo /etc/fstab para partições como /tmp e /var/tmp impede a execução de qualquer binário ou script nessas áreas, independentemente das permissões de arquivo (chmod +x).
- **Fapolicyd (File Access Policy Daemon):** Essencial para distribuições modernas, este serviço verifica cada tentativa de execução contra um banco de dados de arquivos confiáveis, impedindo softwares não autorizados mesmo em diretórios permitidos.
- **Módulos de Segurança (LSM):** O uso de **AppArmor** ou **SELinux** fornece uma camada adicional, criando "jaulas" em torno de aplicações específicas para que não consigam executar comandos fora de seu escopo operacional.

3. Passos Práticos para Implementação

Passo 1: Inventário e Modo de Auditoria

- Não ative o bloqueio total imediatamente. Inicie o AppLocker (Windows) ou fapolicyd (Linux) em Modo de Auditoria. Analise os logs para identificar softwares legítimos que seriam bloqueados e crie as exceções necessárias.

Passo 2: Configuração de Restrições de Partição (Linux)

- Edite o /etc/fstab e configure as partições temporárias com as flags defaults,nosuid,nodev,noexec. Reinicie as montagens e teste a tentativa de execução de um script simples em /tmp para validar o bloqueio.

Passo 3: Implementação de Regras de Editor e Caminho (Windows)

- Via GPO, configure o AppLocker para permitir a execução de tudo em C:\Windows e C:\Program Files. Adicione regras de negação explícita para caminhos de perfil de usuário e regras de permissão baseadas em certificados de editores confiáveis.

Passo 4: Restrição de Scripts e PowerShell

- Configure o PowerShell para operar em Constrained Language Mode para usuários comuns. Garanta que scripts administrativos legítimos estejam assinados digitalmente para que não sejam afetados pela política de restrição.

4. Considerações de Segurança e Monitoramento

- **Gerenciamento de Exceções:** Estabeleça um processo formal para que desenvolvedores ou usuários avançados solicitem a homologação de novos softwares. A exceção deve ser feita, preferencialmente, pela assinatura do binário e não pelo hash (que muda a cada atualização).

- **Remoção de Privilégios Administrativos:** O controle de execução perde eficácia se o usuário possuir privilégios de administrador local, pois ele poderá desativar os serviços de proteção ou alterar as políticas de GPO localmente.

- **Análise de Logs de Bloqueio:** Monitore constantemente os eventos de bloqueio nos logs do sistema (Event ID 8004 no Windows). Picos de bloqueios em pastas temporárias são indicadores claros de uma tentativa de infecção por malware ou ataque de phishing em curso.

Fonte: Framework de Segurança "Essential Eight" (ACSC), CIS Benchmarks (Center for Internet Security) 2026, Guia de Segurança do PowerShell, Microsoft Learn (Documentação Oficial), Windows Defender Application Control (WDAC) e AppLocker, Red Hat Enterprise Linux (RHEL) Hardening Guide, Kernel Documentation (fanotify/AppArmor) e o PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 53

Estabelecer um processo de configuração segura

Estabelecer um processo de configuração segura e desativar serviços e protocolos de rede desnecessários, legados ou inerentemente inseguros (ex.: SMBv1, LLMNR e NetBIOS)

A implementação de configurações endurecidas (hardening) mitiga vetores de ataque ao reduzir a superfície de exposição sistêmica e eliminar vulnerabilidades exploráveis em serviços redundantes. Esse controle rigoroso garante o princípio do privilégio mínimo na rede, prevenindo a exploração de protocolos obsoletos e o movimento lateral de ameaças. O objetivo é reduzir a superfície de ataque através da eliminação de serviços desnecessários e protocolos legados, garantindo que apenas comunicações essenciais, autenticadas e criptografadas transitem pela infraestrutura institucional. Abaixo, será apresentado as orientações técnicas estruturadas para implementar esse processo de forma eficaz.

1. Desativação de Protocolos Legados e Inseguros

Protocolos antigos carecem de criptografia moderna e são alvos primários para ataques de interposição (Man-in-the-Middle) e envenenamento de rede.

- **Neutralização do SMBv1:** Este protocolo é inerentemente vulnerável a ataques de Ransomware e interceptação. Deve ser desativado via PowerShell (Disable-WindowsOptionalFeature) ou GPO em todo o parque.
- **Bloqueio de Resolução Multicast (LLMNR/NetBIOS):** Desative o LLMNR e o NetBIOS sobre TCP/IP para impedir que atacantes capturem hashes de credenciais através de respostas falsas na rede local.
- **Remoção de Serviços de Texto Claro (Linux):** Elimine ferramentas como Telnet, RSH e FTP. Utilize apenas protocolos que suportem criptografia de ponta a ponta (SSH, SFTP, HTTPS).

2. Gestão de Serviços e Minimização de Funções

Mantenha apenas o estritamente necessário para a função específica do ativo (Princípio da Função Única).

- **Desativação de Serviços de Impressão:** Em servidores de infraestrutura (Web, BD), o serviço de Spooler de Impressão deve ser parado e desativado para mitigar vulnerabilidades críticas de escalonamento de privilégios.
- **Restrição de Registro Remoto:** Desative o *Remote Registry* no Windows para impedir que atacantes ou malwares realizem alterações remotas nas configurações de segurança do sistema.
- **Limpeza de Unidades Ativas (Linux):** Utilize o systemctl para desativar daemons de descoberta de rede (Avahi), impressão (CUPS) ou compartilhamento de arquivos (NFS) que não sejam essenciais para a operação do servidor.

3. Passos Práticos para Implementação

Passo 1: Inventário e Baseline de Portas

- Realize uma varredura completa (ss -tunlp ou netstat) para identificar todos os serviços que estão ouvindo em portas de rede. Documente a finalidade de cada serviço ativo antes de proceder com a desativação.

Passo 2: Hardening de Protocolos de Rede

- No Windows, aplique via GPO a desativação do SMBv1 e LLMNR. No Linux, adicione net.ipv6.conf.all.disable_ipv6 = 1 ao sysctl.conf caso o IPv6 não seja utilizado, reduzindo vetores de comunicação não monitorados.

Passo 3: Restrição de Serviços e Acesso Remoto

- Configure o SSH para aceitar apenas chaves públicas e desativar o login de root. No RDP, force o nível de criptografia "Alto" e exija Autenticação em Nível de Rede (NLA). Desative serviços de sistema irrelevantes para o papel do servidor.

Passo 4: Implementação de Firewall "Default Deny"

- Configure o firewall (Windows Firewall ou nftables/UFW) para bloquear todas as conexões de entrada por padrão. Crie regras explícitas apenas para as portas e IPs de origem estritamente necessários (ex: permitir apenas porta 443 de origens confiáveis).

4. Considerações de Segurança e Monitoramento

- **Gestão de Dependências:** Antes de desativar um serviço em larga escala, realize testes em ambiente de homologação. Serviços como o NetBIOS podem ser necessários para aplicações legadas específicas que ainda não suportam DNS moderno.
- **Controle de "Config Drift" (Desvio):** Utilize ferramentas de automação (Ansible para Linux, Intune/GPO para Windows) para garantir que as configurações de hardening sejam persistentes e não sejam revertidas manualmente por usuários ou outros administradores.
- **Auditoria de Conexões Bloqueadas:** Monitore os logs do firewall e do sistema em busca de tentativas de conexão em portas desativadas. Um aumento de atividade em portas como 445 (SMB) ou 137 (NetBIOS) pode indicar a presença de um invasor tentando se movimentar lateralmente na rede.

Fonte: NIST (National Institute of Standards and Technology) NIST SP 800-123, CIS Benchmarks (Center for Internet Security) 2026, NSA (Cybersecurity Technical Reports 2025/2026), CISA (Cross-Sector Cybersecurity Performance Goals), Guia de Hardening da ANSSI/SUSE (2026), OpenSSH Security Guidance e o PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 54

Atualizar as ferramentas de linha de comando

Atualizar as ferramentas de linha de comando (ex.: PowerShell) e habilitar compulsoriamente a coleta de logs de auditoria sobre a sua utilização, a fim de identificar comportamentos anômalos

A atualização de CLI reduz a superfície de ataque via correção de vulnerabilidades, enquanto o log de auditoria compulsório viabiliza a observabilidade forense necessária para detectar desvios comportamentais em tempo real. Essa combinação assegura a integridade do ambiente operacional, transformando ações de terminal em trilhas auditáveis que expõem tentativas de escalada de privilégio ou exfiltração de dados. O objetivo é erradicar "zonas cegas" na administração do sistema, garantindo que os interpretadores de comandos (Shells) sejam modernos, estejam corrigidos e operem sob monitoramento estrito, transformando cada comando executado em uma evidência auditável.

Abaixo, será apresentado o roteiro técnico para garantir que suas ferramentas estejam atualizadas e que cada comando digitado seja devidamente registrado.

1. Modernização e Gestão de Patching

Manter os interpretadores atualizados reduz a superfície de ataque e garante o suporte aos recursos de segurança mais recentes, como o log detalhado de blocos de código.

- **Padronização no Windows:** Utilize o **Winget** (winget upgrade –all) ou o Microsoft Store para manter o PowerShell (pwsh) na versão mais recente. Versões legadas (PowerShell 5.1) devem ser mantidas apenas por compatibilidade, enquanto a administração principal ocorre em versões 7.x.
- **Manutenção no Linux (Bash/Zsh):** Garanta que os binários em /bin/bash ou /usr/bin/zsh sejam atualizados via gerenciadores de pacotes (apt upgrade ou dnf update). Versões desatualizadas de Shells podem conter vulnerabilidades de estouro de buffer ou falhas na gestão de variáveis de ambiente.
- **Eliminação de Interpretadores Obsoletos:** Remova ou restrinja o acesso a Shells menos seguros ou desnecessários (como o sh puro ou versões muito antigas do Python) que possam ser usados para contornar políticas de auditoria.

2. Configuração de Telemetria Avançada

A auditoria deve ser configurada de forma compulsória e centralizada para impedir que um invasor apague seus rastros localmente.

- **Registro de Bloco de Script (PowerShell):** Habilite o log de cada trecho de código processado. Isso é vital para capturar comandos ofuscados ou scripts que são baixados diretamente na memória (sem tocar o disco).
- **Transcrição de Sessão:** Configure a transcrição automática para um diretório de rede protegido e de escrita única (Write-Once). Isso cria um "gravador de caixa preta" de toda a interação do usuário com o terminal.

- **Auditoria de Syscalls (Linux):** Utilize o framework **auditd** para monitorar a chamada de sistema execve. Isso permite saber exatamente qual binário foi executado, por qual usuário e com quais argumentos, mesmo que o histórico do Bash seja limpo.

3. Passos Práticos para Implementação

Passo 1: Padronização e Update Global

- Identifique as versões de interpretadores em uso no parque. Force a atualização para as versões mais recentes estáveis para garantir que os recursos de auditoria (como o Event ID 4104 no Windows) estejam disponíveis.

Passo 2: Ativação de Políticas via GPO (Windows)

- Navegue até Componentes do Windows > Windows PowerShell e habilite: **Ativar Transcrição, Ativar Registro de Bloco de Script e Ativar Execução de Scripts** (configurada como Allow only trusted scripts).

Passo 3: Implementação do Auditd (Linux)

- Instale o serviço e configure as regras em /etc/audit/rules.d/audit.rules. Adicione regras para monitorar execuções (-a exit,always -F arch=b64 -S execve) e proteja o log contra modificações de usuários não root.

Passo 4: Centralização em SIEM

- Configure o encaminhamento de logs (WinRM/Event Forwarding no Windows ou rsyslog no Linux) para um servidor central. Logs de auditoria de linha de comando só têm valor se estiverem protegidos fora da máquina de origem.

4. Considerações de Segurança e Monitoramento

- **Detecção de Ofuscação:** Monitore o uso frequente de comandos codificados (como -EncodedCommand ou -e em Base64). Atacantes utilizam essa técnica para esconder strings suspeitas de ferramentas de segurança básicas.

- **Monitoramento de Comandos de Download:** Crie alertas imediatos para o uso de ferramentas de transferência de arquivos (curl, wget, iwr, certutil -urlcache) por usuários que não fazem parte da equipe de infraestrutura.

- **Uso de IEX (Invoke-Expression):** O comando IEX é um dos principais indicadores de comprometimento, pois permite executar código diretamente da memória. Sua utilização deve ser tratada como um evento de alta severidade em contas não administrativas.

- **Higiene de Histórico:** No Linux, torne o arquivo de histórico (.bash_history) imutável ou configure o envio em tempo real para o syslog, impedindo que comandos como history -c apaguem as evidências de uma intrusão.

Fonte: MITRE ATT&CK, CIS Benchmarks (Center for Internet Security) 2026, Windows Security Auditing, Microsoft Learn (PowerShell Documentation), Linux Audit Documentation (Manual do auditd), Padrões de Log da Linux Foundation e o PPSI (Programa de Privacidade e Segurança da Informação).

Anexo 55

Estabelecer e manter o inventário preciso e detalhado de ativos

Estabelecer e manter o inventário preciso e detalhado de ativos institucionais e soluções de software, identificando claramente os proprietários, as unidades organizacionais e aprovando os sistemas críticos de negócio.

O inventário detalhado de ativos e softwares é o alicerce da governança de TI, permitindo a mitigação de riscos operacionais e a rápida resposta a incidentes de segurança. Ao vincular sistemas críticos a proprietários e unidades específicas, a instituição garante a rastreabilidade necessária para a conformidade regulatória e a otimização estratégica de recursos. Abaixo, será apresentado as orientações técnicas para implementar e manter esse inventário de forma eficaz.

1. Classificação de Ativos e Escopo

O inventário deve ser dividido em categorias lógicas para facilitar a gestão e a atribuição de controles de segurança:

- **Ativos de Hardware:** Servidores (físicos e virtuais), estações de trabalho, dispositivos móveis, ativos de rede e periféricos críticos.
- **Ativos de Software e Cloud:** Sistemas operacionais, aplicações de prateleira, softwares desenvolvidos internamente e serviços SaaS/PaaS (Cloud).
- **Sistemas Críticos de Negócio:** Soluções cuja interrupção impacta diretamente a operação core, a conformidade legal ou o faturamento da instituição.

2. Estrutura de Propriedade e Governança

A eficácia do inventário depende da definição clara de responsabilidades para evitar sistemas “órfãos”:

- **Proprietário do Ativo (Asset Owner):** Gestor da unidade de negócio que utiliza a solução. É o responsável por aprovar acessos e definir a criticidade dos dados tratados.
- **Custodiante Técnico:** Equipe de TI ou Segurança responsável pela manutenção, backup, atualização (patching) e proteção do ativo.
- **Vínculo Organizacional:** Cada ativo deve estar associado a uma Unidade Organizacional (OU) ou Centro de Custo para fins de auditoria e ciclo de vida.

3. Passos Práticos para Implementação

Passo 1: Descoberta e Identificação Automática

- **Varredura Ativa e Passiva:** Utilize ferramentas de Network Scanning para identificar ativos na rede e ferramentas de escuta passiva para detectar dispositivos que se conectam esporadicamente.
- **Mapeamento de Software:** Implemente agentes de gestão ou ferramentas agentless para extrair a lista de softwares instalados, versões de kernel e bibliotecas em uso.

Passo 2: Catalogação, Registro e Identificação Única

- **Enriquecimento de Dados:** Registre o fabricante, versão, data de aquisição, ciclo de vida (End-of-Life) e localização lógica (VLAN/Cloud Region).
- **Tagging e Etiquetagem:** Atribua um identificador único institucional (ID de Ativo). Para ativos físicos, utilize etiquetas.

Passo 3: Atribuição de Proprietários e Unidades Organizacionais

- **Vinculação de Responsabilidade:** Todo ativo deve ter um "Dono de Negócio" (quem paga/usa) e um "Custodiante Técnico" (quem mantém).
- **Estrutura Hierárquica:** Agrupe os ativos por Unidade Organizacional para facilitar a aplicação de políticas de grupo e o rateio de custos.

Passo 4: Avaliação de Criticidade e Impacto no Negócio

- **Classificação de Importância:** Submeta os ativos a uma análise de impacto. Determine se o sistema é crítico (paralisa a organização), Importante (gera atrasos) ou Suporte (baixa relevância imediata).
- **Aprovação Formal:** Garanta que sistemas críticos de negócio sejam formalmente aprovados pelo comitê de segurança ou diretoria antes da entrada em produção.

Passo 5: Verificação de Conformidade e Vulnerabilidades

- **Baseline de Segurança:** Verifique se o software instalado condiz com a "Lista de Softwares Permitidos".
- **Correlação de Vulnerabilidades:** Integre o inventário com feeds de CVE (Common Vulnerabilities and Exposures) para identificar automaticamente quais ativos possuem versões de software vulneráveis.

Passo 6: Gestão de Mudanças e Fluxo de Saída

- **Controle de Alterações:** Estabeleça que qualquer nova instalação ou alteração de hardware deve atualizar automaticamente o inventário via processos de Change Management.
- **Descomissionamento Seguro:** Ao remover um ativo, assegure a limpeza de dados e a baixa formal no inventário para evitar o surgimento de "ativos fantasmas" que ainda possuem acesso à rede.

Passo 7: Ciclo de Auditoria e Higiene (Shadow IT)

- **Revisão Trimestral:** Execute varreduras de comparação para identificar dispositivos e softwares não catalogados (Shadow IT).
- **Remoção de Inativos:** Identifique contas de máquinas e servidores que não se comunicam com a rede há mais de 30 dias e mova-os para quarentena antes da exclusão definitiva.

4. Considerações de Contingência e Manutenção

- **Indisponibilidade de Ferramentas:** Mantenha uma cópia offline (ou em cofre seguro) do inventário de sistemas críticos para consulta durante incidentes de indisponibilidade total de rede.

- **Auditoria de Conformidade:** Realize verificações periódicas para garantir que os softwares instalados correspondem às licenças e aprovações registradas, evitando riscos jurídicos.
- **Gestão de Vulnerabilidades:** Utilize o inventário como entrada para o scanner de vulnerabilidades, garantindo que 100% dos ativos conhecidos sejam analisados.

Fonte: ISO/IEC 27001 (Controle A.8: Gestão de Ativos), CIS Controls (Controles 1 e 2: Inventário e Controle de Hardware/Software) e NIST Cybersecurity Framework (Função ID.AM: Gerenciamento de Ativos).

Anexo 56

Estabelecer e manter um esquema geral de classificação de dados

Estabelecer e manter um esquema geral de classificação de dados fundamentado na criticidade para a organização, avaliando o impacto imediato da indisponibilidade sistêmica na operação.

A classificação de dados baseada em criticidade permite a priorização estratégica de recursos de segurança e resiliência, garantindo a continuidade dos processos vitais ao alinhar a proteção à tolerância a riscos. Ao avaliar o impacto da indisponibilidade sistêmica, a organização estabelece métricas objetivas para tempos de recuperação, mitigando perdas operacionais e financeiras severas. Abaixo, será apresentado as **Orientações Técnicas** estruturadas para operacionalizar esse conceito.

1. Níveis de Classificação de Dados

Os dados devem ser rotulados de acordo com o dano potencial que sua perda ou exposição causaria à instituição:

- **Público:** Informações que podem ser divulgadas sem prejuízo (ex.: material de marketing, editais públicos).
- **Uso Interno:** Dados que, se expostos fora da organização, causam baixo impacto, mas não devem ser públicos (ex.: comunicados internos).
- **Confidencial:** Informações sensíveis que exigem proteção (ex.: dados pessoais de clientes/LGPD, contratos com fornecedores).
- **Restrito/Crítico:** Dados vitais cuja exposição ou perda inviabiliza a operação ou causa danos irreparáveis (ex.: segredos industriais, chaves mestras de criptografia).

2. Avaliação de Impacto de Indisponibilidade

Além da sensibilidade, o esquema deve considerar o quão dependente a operação é do acesso imediato ao dado:

- **Impacto Imediato:** Sistemas onde a indisponibilidade de segundos ou minutos paralisa a operação (ex.: sistemas de vendas em tempo real, linhas de produção automatizadas).
- **Impacto Diferido:** Sistemas que podem ficar indisponíveis por algumas horas sem comprometer a continuidade do negócio (ex.: sistemas de treinamento, portais de RH).
- **Dependência Sistêmica:** Mapeamento de quais bases de dados "alimentam" outros sistemas, evitando o efeito cascata de indisponibilidade.

3. Passos Práticos para Implementação

Passo 1: Definição do Esquema de Rotulagem e Taxonomia

- **Padronização de Termos:** Estabeleça níveis claros (ex.: Público, Interno, Confidencial, Restrito). Cada nível deve ter uma definição curta e inequívoca.

- **Guia de Exemplos:** Documente exemplos práticos para cada categoria (ex.: “Lista de ramais é Interno; Folha de pagamento é Confidencial”) para que os colaboradores classifiquem ativos de forma objetiva e sem hesitação.

Passo 2: Inventário e Atribuição de Proprietários (Data Owners)

- **Mapeamento de Custódia:** Identifique quem é o gestor responsável por cada conjunto de dados (ex.: Diretor Financeiro para dados bancários).
- **Análise de Impacto Temporal:** Solicite que cada proprietário avalie formalmente o impacto financeiro, legal e reputacional caso o dado fique indisponível por 1 hora, 1 dia ou 1 semana. Isso define a criticidade real.

Passo 3: Implementação de Controles Técnicos e Criptografia

- **Proteção Proporcional:** Aplique controles baseados na classificação. Dados “Restritos” devem obrigatoriamente utilizar criptografia em repouso e trânsito, além de MFA para acesso.
- **Marcação de Metadados:** Utilize ferramentas para inserir “etiquetas” digitais nos arquivos, permitindo que outros sistemas de segurança reconheçam a sensibilidade do dado automaticamente.

Passo 4: Configuração de Ferramentas de DLP e Automação

- **Prevenção de Fuga (DLP):** Configure ferramentas de Data Loss Prevention para bloquear o envio de arquivos “Confidenciais” para e-mails externos ou dispositivos USB não autorizados.
- **Descoberta Automatizada:** Utilize motores de busca que identifiquem padrões (como CPF ou números de cartão) para sugerir a classificação correta de documentos esquecidos em servidores de arquivos.

Passo 5: Definição de Níveis de Serviço (SLAs) e Recuperação

- **Vínculo com DR/Backup:** Dados de “Impacto Imediato” devem ser incluídos em rotinas de backup com os menores objetivos de tempo de recuperação (RTO).
- **Priorização de Restauração:** Em caso de desastre, a fila de recuperação deve seguir a ordem decrescente de criticidade definida neste passo.

4. Considerações de Sustentabilidade

- **Reclassificação Periódica:** Dados perdem ou ganham valor com o tempo. Estabeleça uma revisão anual da classificação.
- **Treinamento de Cultura:** Garanta que todos os colaboradores entendam que a responsabilidade pela classificação inicial é de quem gera a informação.
- **Segregação de Armazenamento:** Sempre que possível, mantenha dados de diferentes criticidades em ambientes ou repositórios lógicos separados para evitar o vazamento colateral.

Fonte: ISO/IEC 27001 (Controle A.8.2: Classificação da Informação), NIST SP 800-60 (Guide for Mapping Types of Information to Security Categories) e LGPD (Lei Geral de Proteção de Dados).

Anexo 57

Elaborar e manter diagramas da arquitetura de rede e documentar o fluxo de dados

Elaborar e manter diagramas da arquitetura de rede e documentar o fluxo de dados, garantindo a rastreabilidade estrutural para identificar pontos únicos de falha e dependências vitais (ex.: vínculo entre sistemas de gestão, bancos de dados e serviços de resolução de nomes DNS).

A documentação arquitetural e o mapeamento de fluxos são críticos para a **resiliência operacional**, pois permitem a visualização analítica de gargalos e dependências lógicas que impactam a continuidade do negócio. Essa rastreabilidade transforma infraestruturas complexas em topologias auditáveis, facilitando a mitigação proativa de Single Points of Failure (SPOF) e a rápida resolução de incidentes. Abaixo, será apresentado as orientações técnicas estruturadas para elevar o nível da sua documentação de infraestrutura.

1. Escopo da Documentação de Arquitetura

A documentação não deve ser apenas um desenho estático, mas uma representação fiel das interconexões que sustentam o negócio:

- **Topologia de Rede (Camada Física e Lógica):** Identificação de ativos de rede (switches, roteadores, firewalls), segmentação de VLANs e zonas de confiança (DMZ, Interna, Gerenciamento).
- **Mapa de Fluxo de Dados:** Representação de como a informação transita entre as camadas (ex.: do App Server para o Banco de Dados) e quais protocolos são utilizados (ex.: HTTPS/443, SQL/1433).
- **Inventário de Dependências de Infraestrutura:** Mapeamento de serviços “invisíveis” que, se falharem, paralisam os demais (ex.: DNS, NTP, Servidores de Autenticação/IAM).

2. Identificação de Pontos Únicos de Falha (SPOF)

O objetivo principal da rastreabilidade é localizar e mitigar os Single Points of Failure:

- **SPOF de Hardware:** Um único switch ou firewall que, se desligado, isola um data center inteiro.
- **SPOF de Serviço:** Um serviço de resolução de nomes (DNS) sem redundância que impede o acesso a todos os sistemas de gestão (ERP).
- **SPOF de Caminho:** Circuitos de internet ou links de dados que utilizam a mesma infraestrutura física (mesmo duto ou poste), apesar de serem de operadoras diferentes.

3. Passos Práticos para Implementação

Passo 1: Descoberta e Mapeamento de Ativos

- Utilize ferramentas de varredura (Network Discovery) para identificar todos os nós da rede.
- Documente endereçamentos IP, máscaras de sub-rede e gateways de cada segmento.

Passo 2: Desenho da Topologia Lógica

- Crie diagramas que mostrem a hierarquia da rede.
- Destaque os perímetros de segurança e os pontos onde o tráfego é inspecionado (Firewalls/IPS).

Passo 3: Rastreabilidade do Fluxo de Dados (Data Flow)

- Escolha um sistema crítico (ex.: ERP) e trace o caminho do dado desde o dispositivo do usuário até o armazenamento final.
- Identifique todas as dependências no caminho: autenticação, balanceadores de carga, proxies e bancos de dados.

Passo 4: Matriz de Dependências Vitais

- Crie uma tabela de "Serviços de Apoio". Para cada sistema crítico, liste o que ele precisa para funcionar:
    - Exemplo: O Sistema X depende do Banco de Dados Y, que depende da autenticação no Serviço de Diretório Z, que depende da resolução de nomes DNS.

Passo 5: Análise de Resiliência

- Para cada conexão mapeada, questione: "E se este link/serviço cair agora?".
- Documente as redundâncias existentes (ex.: HA Cluster, Teaming de placas de rede, Multi-homing de links).

Passo 6: Ciclo de Atualização e Manutenção

- Estabeleça que qualquer mudança na rede (Change Management) deve obrigatoriamente resultar na atualização dos diagramas.
- Realize uma revisão técnica semestral para validar se o diagrama "no papel" condiz com a configuração real dos equipamentos.

4. Considerações de Utilização e Segurança

- **Acesso Restrito:** Diagramas de arquitetura são "mapas do tesouro" para atacantes. Devem ser armazenados de forma segura, com acesso restrito apenas às equipes técnicas autorizadas.
- **Nomenclatura Padronizada:** Utilize padrões de ícones e nomenclatura consistentes para facilitar a leitura por diferentes equipes (Redes, Sistemas e Segurança).
- **Simulações de Falha:** Utilize os diagramas para planejar testes de DR (Disaster Recovery). Simule a queda de um componente mapeado para validar se a redundância funciona conforme documentado.

Fonte: ISO/IEC 27001 (Controle A.12.1.1: Procedimentos operacionais documentados), NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment) e ITIL 4 (Service Configuration Management).

Anexo 58

Integrar o processo de gestão de continuidade de negócios em segurança da informação

Integrar o processo de gestão de continuidade de negócios em segurança da informação, definindo junto às áreas de negócio as métricas de Tempo de Recuperação (RTO) e Ponto de Recuperação (RPO), a fim de estabelecer os critérios de priorização no processo de recuperação de cópias de segurança (backups).

A integração da Gestão de Continuidade de Negócios à Segurança da Informação garante que a resiliência operacional seja pautada pela criticidade dos processos, utilizando **RTO** e **RPO** como parâmetros técnicos fundamentais. Essas métricas permitem alinhar a infraestrutura de backup às necessidades de disponibilidade e integridade das áreas de negócio, assegurando uma recuperação priorizada e eficiente em cenários de desastre. Abaixo, será apresentado um guia técnico estruturado para alinhar essas áreas e definir os critérios críticos de recuperação.

1. Definição de Métricas de Recuperação (RTO e RPO)

O sucesso de um plano de recuperação depende da clareza sobre dois conceitos fundamentais definidos em conjunto com os donos de processos:

- **RPO (Recovery Point Objective - Objetivo de Ponto de Recuperação):** Define a quantidade tolerável de perda de dados em termos de tempo.
    - *Exemplo:* Se o RPO é de 1 hora, os backups devem ser feitos a cada hora; se houver um incidente, a organização aceita perder, no máximo, os dados gerados na última hora.
- **RTO (Recovery Time Objective - Objetivo de Tempo de Recuperação):** Define o tempo máximo para restabelecer o serviço após uma falha.
    - *Exemplo:* Se o RTO é de 4 horas, o sistema deve estar funcional para o usuário final em até 4 horas após a interrupção.

2. Critérios de Priorização no Processo de Restauração

Em um cenário de desastre total, é impossível restaurar tudo simultaneamente. A priorização deve seguir a criticidade do negócio:

1. **Serviços de Infraestrutura Core:** Autenticação (Diretórios), Resolução de Nomes (DNS) e Conectividade. Sem eles, nenhum outro sistema funciona.
2. **Sistemas Críticos de Missão:** Aplicações que geram receita imediata ou atendem obrigações legais/vida.
3. **Sistemas de Apoio Operacional:** Ferramentas de colaboração interna e sistemas administrativos.
4. **Sistemas Periféricos:** Arquivos históricos e aplicações de baixo uso.

3. Passos Práticos para Implementação

Passo 1: Análise de Impacto no Negócio (BIA)

- Realize entrevistas com os gestores de cada área para entender o impacto financeiro e operacional de uma parada.
- Questione: “Quanto tempo sua área sobrevive sem o Sistema X?” e “Qual o prejuízo de perder os dados registrados desde ontem?”.

Passo 2: Alinhamento de Expectativas (Métricas vs. Tecnologia)

- Compare o RTO/RPO desejado pelo negócio com a capacidade técnica atual.
    - *Nota:* Se o negócio exige RPO de 5 minutos, mas o backup é diário, existe um “Gap de Continuidade” que deve ser reportado e mitigado.

Passo 3: Configuração da Estratégia de Backup

- Ajuste a frequência de backup para atender ao RPO definido.
- Selecione a tecnologia de restauração (ex.: snapshots, replicação em nuvem, fitas) para atender ao RTO.

Passo 4: Formalização da Matriz de Priorização

- Documente a “Ordem de Restauração”. Em caso de crise, a equipe técnica não deve decidir o que volta primeiro; ela deve seguir o plano aprovado pela diretoria.

Passo 5: Testes de Recuperação e Validação (DR Drill)

- Não teste apenas se o backup “foi feito”. Teste o tempo total de restauração.
- Cronometre o processo desde o alerta de falha até o sistema estar disponível para o usuário final. Se o tempo exceder o RTO, o plano precisa de ajustes.

4. Governança e Resiliência

- **Regra 3-2-1:** Mantenha ao menos 3 cópias dos dados, em 2 tipos de mídia diferentes, com 1 cópia fora do site (offsite) ou imutável (protegida contra deleção por Ransomware).
- **Atualização de Contatos:** Mantenha uma lista de acionamento de emergência (Stakeholders e Fornecedores) atualizada e disponível em formato físico.
- **Revisão do Plano:** O negócio muda. Novos produtos ou sistemas exigem a revisão imediata do RTO e RPO associados.

Fonte: ISO/IEC 27031 (Diretrizes para prontidão da tecnologia da informação e comunicação para a continuidade de negócios), ISO 22301 (Gestão de Continuidade de Negócios) e NIST SP 800-34 (Contingency Planning Guide for Federal Information Systems).

Anexo 59

Assegurar que as documentações estratégicas sejam mantidas

Assegurar que as documentações estratégicas (planos de continuidade, inventários e diagramas) sejam mantidas em uma instância isolada e de acesso restrito (como um sistema off-line ou ambiente segregado em nuvem), garantindo disponibilidade total da informação para a equipe de crise mesmo em caso de comprometimento da rede corporativa principal.

A manutenção de ativos estratégicos em ambientes segregados ou *air-gapped* neutraliza o risco de **movimentação lateral** e indisponibilidade de dados críticos durante incidentes de larga escala. Essa arquitetura garante que a equipe de resposta opere com base em informações íntegras, assegurando a **continuidade operacional** mesmo sob comprometimento total da infraestrutura principal. Abaixo, será apresentado as orientações técnicas para estruturar esse ambiente isolado.

1. O Conceito de Instância Isolada (Out-of-Band)

A documentação estratégica deve residir em um ambiente que não compartilhe as mesmas credenciais, rede ou infraestrutura do ambiente de produção. Se o domínio principal for comprometido, a instância isolada deve permanecer íntegra e acessível.

- **Segregação Lógica:** Ambiente em nuvem com provedor ou inquilino (*tenant*) diferente, utilizando autenticação totalmente distinta.
- **Segregação Física:** Dispositivos de armazenamento criptografados e mantidos em cofres físicos ou sistemas *off-line* (Air-gapped).
- **Disponibilidade "Break-Glass":** O acesso a este ambiente é restrito e monitorado, ativado apenas durante crises ou janelas de manutenção autorizadas.

2. Conteúdo Vital para Custódia

Somente documentos necessários para a sobrevivência e reconstrução do negócio devem ser mantidos nesta instância para minimizar a superfície de exposição:

- **Planos de Continuidade e DR:** Passo a passo técnico para restauração de serviços.
- **Inventários de Ativos e Softwares:** Lista de servidores, IPs e versões críticas.
- **Diagramas de Arquitetura:** Mapas de rede e fluxos de dados essenciais.
- **Contatos de Emergência:** Lista de acionamento de provedores, órgãos reguladores e equipe de crise.
- **Cofre de Senhas de Emergência:** Credenciais de contas Break-glass e chaves mestras de criptografia.
- **Playboks e Runbooks de Segurança:** Passo a passo técnico para resposta a incidentes de segurança.

3. Passos Práticos para Implementação

Passo 1: Seleção do Ambiente de Hospedagem

- Escolha uma solução que garanta acesso externo à rede da organização.

- **Opção A (Cloud Segregada):** Um repositório em nuvem protegido por MFA forte (não vinculado ao SSO da organização) e acesso restrito por IP.
- **Opção B (Hardware Isolado):** Unidades de armazenamento seguras (Tokens/HDs criptografados) distribuídas geograficamente entre membros da equipe de crise.

Passo 2: Estabelecimento do Controle de Acesso

- Utilize o princípio do **Privilégio Mínimo**: Apenas a Célula de Gestão de Crise deve ter acesso.
- Implemente autenticação multifator (MFA) baseada em hardware (como YubiKeys) para evitar interceptação digital.

Passo 3: Processo de Sincronização e Atualização

- A documentação isolada não pode ser estática. Defina uma rotina mensal ou trimestral para atualizar os arquivos.
- **Sincronização Unidirecional:** Se automatizado, garanta que o fluxo de dados ocorra apenas da produção para o isolamento, nunca o contrário, para evitar que um ransomware se propague para o ambiente de backup.

Passo 4: Teste de Acesso em Cenário de Falha

- Simule a queda total da rede interna e do acesso à internet corporativa.
- Valide se a equipe de crise consegue acessar os documentos a partir de redes externas (4G/5G ou conexões domésticas seguras).

4. Governança e Resiliência

- **Criptografia em Repouso:** Todos os dados na instância isolada devem ser criptografados com chaves que não residam na rede principal.
- **Versão Física (Papel):** Para os procedimentos de nível 0 (como o reset de senhas do provedor de nuvem), mantenha uma versão impressa em cofre físico, prevendo a indisponibilidade total de meios eletrônicos.
- **Trilha de Auditoria:** Todo acesso a esta instância deve gerar um alerta imediato para a diretoria, garantindo que o “cofre” não seja aberto sem uma justificativa legítima.

Fonte: ISO/IEC 27031 (Prontidão de TIC para Continuidade de Negócios), NIST SP 800-34 (Contingency Planning Guide) e CERT.br (Práticas de Gestão de Incidentes).

Anexo 60

Parece que fomos atacados

Imagine que a segurança da rede da sua organização é como a segurança de um prédio comercial. Um ataque de ransomware não acontece num passe de mágica; o "ladrão" precisa entrar, circular, trancar as portas e levar o que é valioso.

Aqui está o porquê de cada um desses sinais ser um "alerta vermelho" para quem está cuidando do prédio:

1. Mudança de Extensões e Renomeação em Massa

- **O que significa:** Se seus arquivos mudam de nome (ex: relatorio.pdf vira relatorio.pdf.locked) ou se milhares de arquivos mudam de nome ao mesmo tempo.
- **Por que importa:** É o sinal mais óbvio de que o "sequestro" está em curso. O ransomware está passando por cada pasta e colocando um cadeado digital nos seus dados. Quando o nome muda, o computador já não consegue mais abrir o arquivo.

2. Notas de Resgate (ReadMe.txt)

- **O que significa:** Surgimento de arquivos de texto ou imagens na área de trabalho explicando como pagar o resgate.
- **Por que importa:** É o cartão de visitas do criminoso. Se isso apareceu, a invasão já está em um estágio avançado. É a confirmação de que não é um erro técnico, mas um crime.

3. Shadow Copies Deletadas

- **O que significa:** O Windows cria "fotos" automáticas dos seus arquivos para recuperação (as Shadow Copies). O comando vssadmin list shadows mostra se elas ainda existem.
- **Por que importa:** Os atacantes apagam essas cópias propositalmente. Eles querem garantir que você não tenha como recuperar os arquivos sem pagar. Se elas sumiram, o bandido "queimou as pontes" de volta para a segurança.

4. Uso de PowerShell, PsExec ou Compressores

- **O que significa:** Ferramentas que administradores usam para manutenção sendo usadas de forma estranha ou arquivos sendo compactados (ZIP/RAR) em massa.
- **Por que importa:** O PowerShell é como o "painel de controle mestre" do Windows. Criminosos o usam para espalhar o vírus rapidamente. Já os compressores servem para empacotar seus dados e roubá-los com mais facilidade.

5. Tráfego de Saída Incomum

- **O que significa:** Muita informação saindo da sua rede para endereços de internet estranhos.

- **Por que importa:** Hoje, o ransomware não só tranca seus dados, ele rouba cópias antes. Esse tráfego é o caminhão de mudança do bandido levando seus segredos para fora da organização para te chantagear depois.

6. Alertas de Antivírus Ignorados ou Desabilitados

- **O que significa:** O sistema de segurança avisou algo ou, pior, parou de funcionar sozinho.
- **Por que importa:** Hackers tentam "cegar" a segurança antes de agir. Se o antivírus foi desativado, é sinal de que alguém com intenções ruins já tem as chaves da casa.

7. Logins em Horários ou Locais Atípicos

- **O que significa:** O usuário "João", que trabalha em São Paulo das 9h às 18h, fez login às 3h da manhã direto da Rússia.
- **Por que importa:** Indica que a conta do João foi roubada. Os criminosos usam contas legítimas para circularem pela rede sem levantar suspeitas imediatas.

Resumo: Olhar para esses indicadores é como monitorar câmeras de segurança. Sozinhos, alguns podem parecer erros técnicos, mas juntos, eles formam o desenho de uma invasão iminente ou em curso.

Anexo 61

Contenção

Se as etapas anteriores eram a perícia, estas agora são o “Protocolo de Emergência”. Imagine que o prédio está pegando fogo em alguns andares: estas são as medidas para impedir que o incêndio destrua a estrutura inteira.

Aqui está a explicação simplificada:

1. Desconectar Sistemas Infectados (O “Corte de Contágio”)

O que significa: Tirar o cabo de rede ou desligar o Wi-Fi dos computadores que já mostram sinais de ataque.

Por que importa: O ransomware é como um vírus biológico: ele pula de um computador para o outro através da rede. Ao tirar o cabo, você cria uma “barreira física”. O computador infectado fica isolado em uma ilha, sem conseguir “sujar” o restante da organização.

2. Matar Túneis VPN e Conexões Remotas

O que significa: Derrubar imediatamente todos os acessos de quem está trabalhando de casa ou de fora da organização.

Por que importa: Frequentemente, o hacker está controlando o ataque de longe, usando uma conexão legítima (VPN). Ao cortar esses acessos, você “tranca as portas” para o invasor, impedindo que ele continue enviando comandos ou roubando dados.

3. Isolar no Nível do Switch (Fechar as Alas)

O que significa: Se o vírus já se espalhou por vários departamentos, o técnico desliga a comunicação entre setores inteiros (ex: bloqueia a conversa entre o Financeiro e o RH).

Por que importa: É como fechar as portas corta-fogo de um prédio. Mesmo que o setor de Vendas esteja comprometido, você impede que o ataque chegue ao Servidor Central ou à Contabilidade.

4. Desabilitar Contas Suspeitas e Resetar Senhas

O que significa: Bloquear contas de usuários que estão agindo estranho e trocar a senha de todos os “chefes” (administradores) do sistema.

Por que importa: O invasor geralmente rouba a identidade de alguém para agir. Resetar as senhas é como trocar todas as fechaduras do prédio de uma vez só: quem estava lá dentro com uma chave roubada perde o acesso na hora.

5. Isolar Sistemas Críticos Preventivamente

O que significa: Desligar da rede os computadores mais importantes (como o que emite notas fiscais ou o banco de dados) antes que o vírus chegue neles.

Por que importa: É melhor parar a organização por algumas horas por precaução do que ficar semanas parado porque o coração do negócio foi criptografado. É o “seguro morrer de velho”.

6. Bloquear IPs e Domínios no Firewall

O que significa: Dizer para o seu "porteiro digital" (Firewall) que ninguém pode conversar com certos endereços da internet que são conhecidos por serem de hackers.

Por que importa: O vírus muitas vezes precisa "ligar para casa" para receber instruções ou enviar a chave de criptografia. Se você corta essa ligação, o vírus pode ficar paralisado, sem saber o que fazer.

7. Correção de Emergência (Patching)

O que significa: Instalar rapidamente atualizações de segurança em programas que têm falhas conhecidas.

Por que importa: Muitas vezes o hacker entra por um "buraco" no software que a fabricante já avisou como consertar. Corrigir isso durante o ataque impede que o invasor use o mesmo truque para entrar em outras máquinas que ainda estão limpas.

Decisão de "desligar tudo" (Kill Switch)

Essas medidas formam o que chamamos de Contenção. O objetivo não é mais salvar o arquivo que já foi trancado, mas salvar tudo o que ainda resta.

Essas ações de isolamento podem ser drásticas e parar a operação da organização temporariamente. Você sente que teria autonomia ou suporte para tomar uma decisão de "desligar tudo" caso percebesse esses sinais? Discuta isso com a Alta Administração e seus pares.

Anexo 62

Preservação de evidências

Entramos agora na fase de Forense Computacional. Se as etapas anteriores eram para “apagar o fogo”, estas são para “investigar a cena do crime” sem contaminar as provas.

Aqui o detalhamento é vital, pois erros nesta fase podem impossibilitar a identificação dos criminosos ou a recuperação dos dados no futuro.

1. Captura de Memória RAM (Onde o “crime” está vivo)

- **Por que é profundo:** A memória RAM é volátil; se você desligar o computador da tomada, tudo o que está nela desaparece. Muitos malwares modernos rodam apenas na memória (sem arquivos no disco) ou armazenam as chaves de criptografia nela temporariamente.
- **Ferramentas:** O **FTK Imager** cria um “dump” (uma foto completa) da RAM. O **Volatility** é o laboratório que analisa essa foto para encontrar senhas, processos escondidos e conexões de rede que estavam ativas no momento do ataque.

2. Imagens Forenses de Disco (Cópia bit-a-bit)

- **Por que é profundo:** Não é um simples “copiar e colar”. Uma imagem bit-a-bit cópia inclusive os espaços vazios do HD, onde podem existir rastros de arquivos deletados pelo hacker.
- **A regra de ouro:** Você nunca analisa o disco original. Você faz a imagem e trabalha na cópia. Isso garante que, se você cometer um erro na investigação, a prova original continua intacta.

3. Exportação e Armazenamento de Logs

- **Por que é profundo:** Logs são o “rastro de migalhas”.
    - PowerShell: Mostra quais comandos o hacker executou.
        - O PowerShell é poderoso porque permite que o hacker execute comandos diretamente na memória, sem precisar baixar um arquivo .exe que o antivírus detectaria facilmente.
        - Onde entro:
            - Pressione <Win + R>, digite **eventvwr.msc** e dê . Isso abre o Visualizador de Eventos do Windows.
            - Vá em: Logs de Aplicativos e Serviços > Microsoft > Windows > PowerShell > Operational.
            - O que fazer (O que procurar):
                - ID de Evento 4104: Este é o registro mais importante. Ele registra o conteúdo do script. Se o hacker rodou um comando para baixar o vírus, o texto completo estará aqui.

- Busque por termos suspeitos: Use o filtro de busca para palavras como Invoke-WebRequest (usado para baixar arquivos), EncodedCommand (usado para esconder o que o comando faz em códigos ilegíveis) ou IEX (execução imediata).

- VPN/Firewall: Mostra de onde ele veio e para onde enviou seus dados.
  - Se for o Firewall do Windows: Vá em C:\Windows\System32\LogFiles\Firewall\pfirewall.log. (Nota: Isso precisa estar habilitado previamente).
  - Se for um Firewall de borda (Fortigate, Cisco, pfSense): Você deve acessar a interface web do aparelho e ir na seção de Traffic Logs ou FortiView.
  - O que fazer (O que procurar):
    - Conexões para IPs Estrangeiros: Filtre por tráfego de saída (Egress) em portas comuns como 443 (HTTPS) ou 80 (HTTP).
    - Volumes de dados: Procure por registros onde um único computador interno enviou GBs de dados para um IP desconhecido. Isso indica o roubo (exfiltração) de documentos.
    - Portas de comando: Veja se há tentativas de conexão na porta 445 (SMB), que é como o ransomware se espalha de um PC para outro dentro da organização.
- DNS: Mostra quais sites maliciosos o vírus tentou acessar.
  - O DNS é o que transforma nomes (https://www.google.com/) em IPs. Antes de o ransomware agir, ele geralmente consulta o endereço do servidor do criminoso (o Servidor de Comando e Controle - C2).
  - Onde entro:
    - No Servidor Windows (Domain Controller): Abra o console de Gerenciamento de DNS > Clique com o botão direito no servidor > Propriedades > Log de Depuração (Logging).
    - Logs Locais: No Visualizador de Eventos, vá em Logs de Aplicativos e Serviços > Microsoft > Windows > DNS-Client > Operational.
  - O que fazer (O que procurar):
    - Domínios Aleatórios: Procure por consultas a sites com nomes sem sentido, como xhz123-malware.top ou asdfghjkl.ru.
    - Consultas repetitivas: Um computador tentando “ligar” para o mesmo endereço estranho a cada 5 minutos é um sinal clássico de uma máquina infectada tentando receber ordens.

- **Ação imediata:** Logs podem ser sobrescritos rapidamente. Você deve exportá-los para um ambiente seguro (fora da rede afetada) imediatamente.

4. Preservação de Notas e Documentação Técnica

Por que é profundo: A nota de resgate contém o ID único da vítima e, às vezes, o endereço da "dark web" do grupo. Documentar o timestamp (hora exata) ajuda a correlacionar eventos: se o arquivo foi criptografado às 14:05, o log de rede das 14:04 dirá quem deu a ordem.

5. Amostras de Arquivos e o Fator "Esperança" (Operação Cronos)

Por que é profundo: Ransomwares têm falhas. Às vezes, a polícia internacional (como no caso da Operação Cronos contra o grupo LockBit) invade os servidores dos hackers e recupera as chaves mestras.

Estratégia: Guardar uma amostra de arquivos criptografados e a nota de resgate permite que, daqui a 6 meses ou 1 ano, você tente descriptografar tudo de graça se uma chave for publicada.

- **Cadeia de Custódia e Hashes (SHA-256)**
    - **Por que é profundo:** Para que uma evidência tenha valor legal (em um processo ou seguro), você precisa provar que ela não foi alterada.
    - **O que é o Hash:** Imagine que o Hash é a "impressão digital" digital de um arquivo. Ao gerar um código SHA-256 de uma evidência, você sela o arquivo. Se um único bit mudar, o código muda completamente. Isso prova para a justiça que a prova é íntegra.
        - Gerar um hash SHA-256 é como criar uma "assinatura digital" única para um arquivo. Se o arquivo for alterado em um único bit (uma vírgula que seja), o hash mudará completamente. Isso é fundamental na perícia para provar que a evidência coletada não foi manipulada.
            - **No Windows (PowerShell)**
                - O Windows possui um comando nativo chamado Get-FileHash. Ele é o padrão ouro para quem precisa de rapidez e precisão.
                - **Como fazer:**
                    - Abra o PowerShell (pressione Win + X e selecione Windows PowerShell ou Terminal).
                    - Digite o seguinte comando (substituindo pelo caminho do seu arquivo):
                        - Get-FileHash "C:\Caminho\Para\O\Arquivo.txt" -Algorithm SHA256
                    - O que você verá:
                        - O Windows retornará uma tabela com o algoritmo usado e uma longa sequência de letras e números (o Hash).

- Para salvar o resultado direto em um arquivo de texto para sua documentação, use: Get-FileHash “arquivo.exe” -Algorithm SHA256 | Out-File “hash_evidencia.txt”

- **No Linux (Terminal)**
  - No Linux, o utilitário sha256sum já vem instalado em praticamente todas as distribuições (Ubuntu, Debian, CentOS, etc.).
  - **Como fazer:**
    - Abra o Terminal.
    - Digite o comando seguido do nome do arquivo:
    - sha256sum arquivo_suspeito.bin
    - O que você verá:

O terminal imprimirá o hash seguido do nome do arquivo.

- Se você quiser gerar o hash de todos os arquivos de uma pasta para documentar a cena do crime:
- sha256sum * > lista_de_hashes.sha256

- Por que usar SHA-256 e não MD5?
  - Antigamente, usava-se muito o MD5. No entanto, o MD5 é considerado “quebrado” para segurança forense porque é possível sofrer um ataque de colisão (quando dois arquivos diferentes geram o mesmo hash). O SHA-256 é muito mais robusto e é o padrão exigido em auditorias e processos judiciais hoje em dia.

Anexo 63

Erradicação

Após a coleta de evidências e o isolamento inicial, entramos na fase de **Erradicação**. Se a fase anterior era a perícia do crime, esta é a fase de **"Limpeza Profunda"**. O objetivo aqui é garantir que não sobrou nenhum "espião" ou "porta aberta" dentro da sua rede antes de tentar voltar ao trabalho normal.

Aqui está o detalhamento técnico e estratégico de cada etapa:

1. Revalidação Total do Inventário

- **O que significa:** Conferir cada servidor, notebook, tablet e até impressora ou câmeras IP da organização.
- **Por que importa:** O ransomware adora se esconder em dispositivos "esquecidos" (aquele servidor antigo de testes que ninguém usa). Se você limpar 99 máquinas e deixar uma infectada, essa única máquina vai reinfetar toda a rede assim que você ligar os sistemas novamente.

2. Mitigação de Vulnerabilidades e Erros de Configuração

- **O que significa:** Não basta remover o vírus; você tem que fechar o buraco por onde ele entrou. Isso inclui aplicar "patches" (atualizações), desativar protocolos antigos (como SMBv1) e corrigir configurações fracas.
- **Por que importa:** Se o hacker entrou por uma falha no sistema de e-mail e você não corrigiu essa falha, ele (ou outro grupo) entrará novamente em questão de minutos usando a mesma técnica.

3. Remoção de Malware e Scripts

- **O que significa:** Limpar os arquivos executáveis maliciosos e scripts que o atacante deixou para trás.
- **Por que importa:** Muitas vezes, o atacante deixa "bombas lógicas" programadas para explodir (criptografar) dias depois da limpeza inicial.

4. Gestão de Contas Violadas ou Criadas

- **O que significa:** Bloquear contas que o hacker roubou e deletar contas que ele mesmo criou (com nomes como admin_backup ou support_temp) para tentar passar despercebido.
- **Por que importa:** O acesso por "credenciais legítimas" é o método favorito dos invasores. Se você não limpar a lista de usuários, o hacker continua tendo "a chave da porta da frente".

5. Remoção de Persistência (Onde o hacker "mora")

- **O que significa:** Procurar por Backdoors (portas dos fundos).
    - **Tarefas Agendadas:** O Windows pode estar programado para rodar o vírus todo dia às 3 da manhã.
    - **Chaves de Registro:** O vírus pode estar configurado para iniciar junto com o Windows.

- **Por que importa:** Sem remover a persistência, você reinicia o computador e o malware volta à vida automaticamente.

6. Erradicação Automatizada (EDR/XDR)

- **O que significa:** Usar ferramentas de segurança modernas para que elas procurem e matem o vírus em todos os computadores da organização ao mesmo tempo.
- **Por que importa:** Em uma rede com 500 computadores, é impossível limpar um por um manualmente. A automação garante velocidade e escala para que o vírus não se espalhe mais rápido do que você consegue limpar.

7. Autoridade para Ações Manuais

- **O que significa:** Garantir que o técnico que está resolvendo o problema tenha "carta branca" para tomar decisões drásticas sem precisar de aprovação burocrática demorada.
- **Por que importa:** No meio de um ataque, cada minuto conta. Se o técnico precisa esperar uma reunião de diretoria para desligar um servidor crítico infectado, o prejuízo pode dobrar de tamanho nesse intervalo.

8. Acionamento de Fornecedores/Terceiros (Cloud e ISPs)

- **O que significa:** Ligar para o suporte da Microsoft (Azure), Amazon (AWS), e seu provedor de internet.
- **Por que importa:** Se o hacker está atacando através de um servidor na nuvem, você pode não ter controle total sobre o hardware. O provedor pode ajudar a bloquear o tráfego malicioso antes mesmo dele chegar na sua organização, ou ajudar a restaurar máquinas virtuais "limpas".

PROTOCOLO DE ERRADICAÇÃO (CHECKLIST)

1. Varredura e Limpeza de Ameaças

- **Ação:** Executar scan completo (Full Scan) em todos os dispositivos da rede usando ferramentas de EDR ou Antivírus atualizados.
- **Ferramenta:** EDR (CrowdStrike, SentinelOne, Microsoft Defender for Endpoint).
- **Critério de Sucesso:** 100% dos dispositivos validados com status "Limpo" e zero ameaças ativas detectadas.

2. Correção de Vulnerabilidades (Patching)

- **Ação:** Identificar a falha que permitiu a entrada (ex: um servidor sem atualização) e aplicar a correção de segurança imediatamente.
- **Ferramenta:** Windows Update, WSUS ou instalação manual de patches (arquivos .msu).
- **Critério de Sucesso:** A vulnerabilidade específica (CVE) está fechada e os sistemas críticos estão na versão mais segura.

3. Higiene de Contas e Identidades

- **Ação:** Desabilitar contas criadas pelo invasor, bloquear usuários comprometidos e forçar a troca de senha (reset) de todos os administradores e contas de serviço.
- **Ferramenta:** Active Directory (AD) ou Azure AD (Entra ID).
- **Critério de Sucesso:** Nenhuma conta desconhecida ativa e todas as senhas administrativas alteradas para padrões complexos.

4. Remoção de Mecanismos de Persistência

- **Ação:** Localizar e deletar Tarefas Agendadas (Scheduled Tasks) suspeitas e entradas no Registro do Windows (Run/RunOnce) que iniciam scripts maliciosos.
- **Ferramenta:** Autoruns (suíte Sysinternals) ou comandos PowerShell (Get-ScheduledTask).
- **Critério de Sucesso:** O sistema reinicia sem que nenhum processo estranho ou conexão externa seja reativada automaticamente.

5. Bloqueio de Backdoors de Rede

- **Ação:** Bloquear no Firewall todos os endereços IP e domínios identificados durante a investigação como sendo do atacante (C2 - Comando e Controle).
- **Ferramenta:** Firewall de borda (Fortigate, Palo Alto, pfSense) e Proxy.
- **Critério de Sucesso:** Tentativas de comunicação do malware com a internet são barradas e logadas pelo Firewall.

6. Auditoria de Acessos Remotos

- **Ação:** Revisar todas as configurações de VPN e RDP. Desativar acessos que não possuam Autenticação de Dois Fatores (MFA).
- **Ferramenta:** Configurações de VPN e logs de acesso remoto.
- **Critério de Sucesso:** Somente conexões autenticadas via MFA são permitidas para acessar a rede interna.

7. Saneamento de Ambiente em Nuvem

- **Ação:** Verificar se o hacker criou aplicativos (App Registrations) ou alterou permissões em ambientes Cloud para manter acesso persistente.
- **Ferramenta:** Console de Administração do Azure, AWS ou Google Cloud.
- **Critério de Sucesso:** Nenhuma regra de acesso ou “aplicativo espião” detectado no painel da nuvem.

Anexo 64

Recuperar - Passo 1 - Infraestrutura de identidade

1. Restaurar Active Directory (AD) e Servidores DNS

O AD é o "controlador" da rede; ele sabe quem é cada usuário e o que cada um pode acessar. O DNS é a "lista telefônica" que faz tudo se encontrar.

- **Por que é o pré-requisito?** Nada funciona sem eles. Se você restaurar um servidor de arquivos sem o AD estar online, ninguém conseguirá logar.
- **O cuidado técnico:** Você deve restaurar o AD a partir de um backup "limpo" (de antes da invasão). Se o backup estiver infectado, o hacker já terá um "pé dentro" assim que o sistema subir.
- **Isolamento:** Idealmente, essa restauração acontece em uma rede isolada (VLAN de quarentena) para garantir que o AD não tente se comunicar com máquinas ainda infectadas.

2. Resetar TODAS as Senhas (incluindo o KRBTGT)

Não basta trocar a senha do "João" ou da "Maria". Você precisa trocar a senha que o próprio sistema usa para validar quem é quem.

- **O que é o KRBTGT?** É a conta mais importante do domínio. Ela gera os "tickets" (passes de entrada) que permitem que os usuários acessem pastas e sistemas sem digitar a senha o tempo todo. Se o hacker roubou o hash desta conta, ele tem um "Golden Ticket" (um passe livre eterno), mesmo que você troque todas as outras senhas.
- **O reset duplo (Intervalo de 10-12h):** * 1º Reset: Invalida tickets antigos, mas o sistema mantém o histórico para não derrubar todo mundo imediatamente.
    - **2º Reset:** Após a propagação (10-12h), o histórico antigo é apagado. Isso garante que qualquer "Golden Ticket" que o hacker tenha criado se torne lixo eletrônico.

3. Rotacionar Senhas de Contas de Serviço (MSAs/gMSAs)

Contas de serviço são usadas por softwares (ex: o sistema de backup que fala com o banco de dados).

- **O perigo:** Hackers amam essas contas porque elas geralmente têm senhas que nunca expiram e privilégios altos.
- **Privilégios Delegados:** Você deve verificar se o hacker não deu permissão para uma conta comum (como a de um estagiário) "controlar o domínio". Isso é uma técnica de Escalação de Privilégio.

4. Revogar Tickets Kerberos e Sessões Ativas (Cloud/Híbrido)

Se sua organização usa Office 365 ou Azure (Ambiente Híbrido), o problema vai além do servidor físico.

- **Tokens de Sessão:** Quando você loga no e-mail, o navegador guarda um "token" para você não precisar logar de novo por dias. O hacker pode roubar esse token (Cookie Hijacking).

- **Revogação:** Você deve forçar o comando de “Revogar Sessões” no painel do Azure/M365. Isso desloga o hacker de qualquer celular ou computador onde ele esteja espiando seus e-mails ou arquivos na nuvem.

5. Auditoria de Persistência (A Caça aos “Presentes” do Hacker)

O invasor quer voltar. Para isso, ele deixa “portas dos fundos” escondidas na configuração da organização.

- **GPOs Alteradas:** O hacker pode mudar uma Política de Grupo para que, toda vez que qualquer computador da organização ligar, ele baixe o vírus novamente.
- **Certificados Instalados:** Eles podem instalar um certificado digital falso para interceptar comunicações criptografadas (Man-in-the-Middle).
- **Tarefas Agendadas Suspeitas:** Verifique se há scripts programados para rodar em horários estranhos. O invasor pode programar uma tarefa para criar um novo usuário administrador daqui a 30 dias, caso ele perca o acesso atual.

Anexo 65

Recuperar - Passo 2 - Serviços de núcleo de rede

1. Restaurar DHCP, Firewalls e Switches Core

- **DHCP (Distribuição de IPs):** Se o seu servidor DHCP foi afetado, as máquinas não conseguirão obter endereços para se comunicar. Ao restaurar, certifique-se de que o escopo de IPs não foi alterado para incluir gateways falsos que desviariam o seu tráfego para o servidor do hacker.
- **Switches Núcleo (Core):** São o coração da rede. Verifique se não há portas espelhadas (Port Mirroring) configuradas. Hackers usam isso para "snifar" (farejar) todo o tráfego da organização e roubar senhas em texto claro.
- **Firewalls:** Devem ser restaurados de backups de configuração (arquivos .conf ou .xml) que você sabe que são seguros.

2. Validar Regras de Firewall e Bloqueio SMB

Aqui aplicamos a Segmentação Horizontal, uma das defesas mais eficazes contra o espalhamento de vírus.

- **O problema do SMB (Porta 445):** O protocolo SMB é usado para compartilhar pastas e impressoras. É por ele que o ransomware "pula" de um computador para o outro dentro do escritório.
- **Ação:** Bloqueie o tráfego SMB entre estações de trabalho. Um computador de um vendedor não tem motivo para falar diretamente com o computador do RH. Eles devem falar apenas com o Servidor de Arquivos.
- **Exceções Temporárias:** Durante crises, é comum técnicos abrirem "portas" para facilitar o suporte. Verifique se não ficou nenhuma regra do tipo Permitir Qualquer -> Qualquer ativa.

3. Revisar Acessos Administrativos (VLAN de Gerenciamento)

Muitos ataques escalam porque a interface de gerenciamento do Firewall ou do Switch estava acessível para qualquer usuário da rede.

- **VLAN de Gerenciamento:** É uma rede isolada, exclusiva para o pessoal de TI.
- **Ação:** Configure o Firewall e os Switches para que a "página de login" deles só responda se o pedido vier de uma lista restrita de IPs (da TI).
- **Por que importa:** Se um hacker infectar o computador da recepção, ele não conseguirá nem sequer "enxergar" a tela de login do seu Firewall para tentar um ataque de força bruta.

Anexo 66

Recuperar - Passo 3 - Sistemas críticos de negócio

1. Restaurar por Ordem de RTO (Recovery Time Objective)

O RTO é o tempo máximo que um serviço pode ficar parado antes que o prejuízo seja catastrófico. Nem todos os sistemas são iguais.

- **Ação:** Siga a prioridade definida no seu Plano de Continuidade de Negócios (PCN). Geralmente, a ordem é:
    1. *Serviços de Infraestrutura:** (AD, DNS, DHCP) — Sem eles, nada loga.
    2. *Sistemas Críticos de Operação:** (ERP, Banco de Dados, Emissão de Nota Fiscal).
    3. *Sistemas de Comunicação:** (E-mail, VoIP).
    4. *Sistemas Administrativos:** (RH, Intranet).
- **Por que importa:** Tentar restaurar tudo ao mesmo tempo sobrecarrega a rede e os discos, fazendo com que o sistema mais importante demore mais para subir.

2. Sanitização de Backups (O "Banho de Desinfetante")

Este é o erro mais comum em recuperações de ransomware: restaurar um backup que já continha o vírus adormecido (o chamado "período de incubação").

- **O que é a Sandbox:** É um ambiente virtual totalmente isolado, como uma bolha, que não tem conexão com a sua rede principal nem com a internet.
- **Ação** (O Processo de Sanitização):
    - **Montagem:** Você restaura o backup dentro dessa bolha.
    - **Escaneamento Profundo:** Roda o EDR/Antivírus atualizado com as vacinas mais recentes (que não existiam quando o backup foi feito).
    - **Busca por IoCs:** Procura por indicadores de comprometimento (arquivos .exe estranhos, scripts de persistência).
    - **Promoção:** Só depois de "limpo" é que o servidor sai da bolha e vai para a rede de produção.

3. Validar Integridade e Consistência dos Dados

Restaurar o arquivo não significa que o dado lá dentro está bom. O ransomware pode ter corrompido o banco de dados antes mesmo de criptografá-lo.

- **Integridade de Arquivo:** Verificar se os arquivos abrem corretamente (se um PDF não está corrompido, por exemplo).

- **Consistência de Banco de Dados:** Rodar comandos de verificação (como o DBCC CHECKDB no SQL Server) para garantir que as tabelas não estão quebradas logicamente.

- **Ação:** Antes de liberar para os usuários, peça para um "usuário chave" (Key User) de cada departamento validar se as últimas transações antes do ataque estão lá e se o sistema se comporta normalmente.

Anexo 67

Recuperar - Passo 4 - Sistemas de Comunicação

Esta etapa é extremamente perigosa porque o e-mail é o canal preferido para a espionagem contínua e para o roubo de dados silencioso. Mesmo que você limpe o servidor, o atacante pode ter deixado uma "escuta" configurada.

Aqui está o detalhamento técnico de como garantir que sua comunicação seja restaurada de forma segura:

1. Restaurar E-mail e Sistemas de Comunicação

Seja o seu ambiente local (Exchange) ou em nuvem (Microsoft 365 / Google Workspace), a restauração deve ser acompanhada de uma auditoria de acesso.

- **Ação:** Restabelecer a conectividade, mas garantir que todos os serviços de MFA (Autenticação de Múltiplos Fatores) estejam ativos e operacionais antes de permitir que o primeiro usuário faça login.
- **Sistemas de Chat (Teams/Slack):** Verifique se não foram adicionados "usuários convidados" (Guests) externos durante o período da invasão. O atacante pode estar lendo as conversas da equipe de resposta a incidentes.

2. Validar Regras de Encaminhamento (A "Escuta" Oculta)

Esta é uma técnica clássica de Exfiltração de Dados. O hacker não precisa mais invadir sua rede se cada e-mail que o seu CEO recebe for enviado automaticamente para um Gmail controlado pelo criminoso.

- **Regras de Caixa de Entrada:** Verifique as regras individuais dos usuários. Procure por regras que contenham termos como "encaminhar", "mover para itens excluídos" ou "marcar como lido" para esconder o rastro do encaminhamento.
- **Regras de Transporte (Nível de Servidor):** No Exchange/O365, existem regras que afetam a organização inteira. O hacker pode ter criado uma regra silenciosa que diz: "Toda mensagem enviada para o setor Financeiro deve ter uma cópia oculta (BCC) enviada para o endereço X".

Procedimentos Técnicos de Verificação

Para Microsoft 365 / Exchange: Você deve rodar scripts para varrer todas as caixas em busca de encaminhamentos externos. O comando PowerShell abaixo é um exemplo do que procurar:

```
Get-Mailbox | Get-InboxRule | Where-Object { $_.ForwardTo -ne $null }
```

Para Auditoria de Regras de Fluxo (Transport Rules):

1. Acesse o **Centro de Administração do Exchange**.
2. Vá em **Fluxo de Mensagens > Regras**.
3. Verifique cada regra existente, especialmente as que possuem ações como "Cópia oculta para..." (Bcc) ou "Redirecionar a mensagem para...".

Anexo 68

Recuperar - Passo 5 - Servidores de arquivo e aplicações secundárias

Por que isso é importante?

Se você restaurar o servidor de arquivos, mas um usuário abrir um “Relatório de Vendas.xlsm” que contém uma macro maliciosa, o hacker ganha acesso novamente à rede em questão de segundos. A limpeza de arquivos é o que impede o ciclo de reinfecção.

1. Restaurar e Validar Aplicações

Uma aplicação não é apenas um ícone na tela; ela é composta por binários, arquivos de configuração e conexões com bancos de dados.

- **Ação:** Em vez de apenas restaurar a máquina virtual inteira, o ideal é reinstalar os binários da aplicação do zero (usando o instalador original) e apenas restaurar os dados (o banco de dados e arquivos de mídia) sanitizados.
- **Validação de “Check-Sum”:** Compare o hash dos arquivos executáveis da aplicação com os arquivos originais do fabricante. Se o tamanho ou o hash do sistema.exe mudou, o atacante pode ter injetado um código malicioso (trojanizado) no seu software.
- **Testes de Integração:** Antes de abrir para todos, teste se a aplicação consegue se comunicar com o banco de dados e se as permissões de acesso (quem pode ver o quê) não foram alteradas.

2. Limpeza de Arquivos (Macros e Triggers)

Este é um ponto onde muitos falham. O ransomware pode ter deixado documentos Office (.docm, .xlsm) que contêm Macros maliciosas. Quando um usuário abre o arquivo restaurado e clica em “Habilitar Conteúdo”, a macro baixa o ransomware novamente.

- **O Perigo das Macros:** Uma macro é um script que roda dentro do Word/Excel. Hackers as usam como “triggers” (gatilhos) para reinfecção silenciosa.
- **Pastas Públicas e Compartilhadas:** Verifique arquivos ocultos (como desktop.ini, .vbs ou .js) em pastas onde todos têm permissão de escrita. O atacante pode ter deixado um script que, ao ser clicado por engano, reinicia o ataque.

Procedimentos Técnicos de Higienização

Segurança de Documentos:

- **GPO de Macros:** Configure uma Política de Grupo (GPO) para desabilitar macros de arquivos que venham da internet ou de fontes não confiáveis.

- **Conversão Temporária:** Se o risco for alto, considere converter documentos críticos de formatos que aceitam macros (ex: .xlsm) para formatos sem macros (.xlsx) durante a transição.

Varredura de Conteúdo: Use ferramentas de linha de comando ou o seu EDR para buscar por extensões de scripts dentro de pastas de documentos: `dir /s /b *.vbs, *.js, *.ps1, *.bat` (Busca por scripts comuns que não deveriam estar em pastas de usuários).

Anexo 69

Recuperar - Passo 6 – Endpoints

Por que essa abordagem é "altamente preferível"?

Restaurar um backup de uma máquina que foi infectada é como tentar lavar uma esponja que caiu em tinta: por mais que você limpe, sempre pode sobrar um resquício no centro. A Golden Image descarta a esponja velha e entrega uma nova, garantindo que o ambiente de produção seja verdadeiramente "confiável" (Trusted).

Aqui está o detalhamento técnico de por que e como fazer isso:

1. Reinstalar a partir de Golden Images

Uma **Golden Image** é uma cópia mestre de um sistema operacional perfeitamente configurado, atualizado e endurecido (hardened) pela equipe de TI.

- **Por que é preferível à restauração de backup?**
    1. **Eliminação total de persistência:** Backups de máquinas infectadas podem conter cavalos de Troia ou modificações no registro que o antivírus ainda não conhece. Ao usar uma imagem limpa, você garante que 100% dos binários do sistema são legítimos.
    2. **Padronização:** Você tem a certeza de que todas as máquinas estão saindo com as mesmas configurações de segurança e sem softwares desnecessários que aumentam a superfície de ataque.
- **O Processo:**
    1. Provisione uma nova Máquina Virtual (VM) usando a Golden Image.
    2. Conecte os **discos de dados** (após serem sanitizados na Sandbox) a essa nova VM.
    3. Reinstale as aplicações a partir dos instaladores originais.

2. Instalação Imediata de Patches (Zero-Day Readiness)

O momento em que um sistema operacional acaba de ser instalado e "sobe" pela primeira vez é o seu ponto de maior vulnerabilidade. Se ele for conectado à rede sem estar atualizado, ele pode ser infectado em segundos por worms que se espalham sozinhos.

- **O Conceito de "VLAN de Patching":** Antes de colocar a máquina na rede de produção, ela deve passar por uma rede isolada onde o único acesso permitido é aos servidores de atualização (Windows Update, WSUS ou repositórios Linux).
- **Ação:** Garanta que o sistema operacional suba já com o **Patch de Segurança Crítico** que corrigiu a vulnerabilidade usada pelo hacker.

Não espere o ciclo automático de 24h do Windows; force a busca por atualizações manualmente antes de instalar qualquer outro software.

gov.br

Quer saber mais?

Acompanhe as publicações

na página do PPSI 2.0

https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-2.0

MINISTÉRIO DA
GESTÃO E DA INOVAÇÃO
EM SERVIÇOS PÚBLICOS