Modelo para o Gerenciamento de Incidentes Cibernéticos na Administração Pública Federal

Gracieth Valenzuela
Faculdade de Tecnologia
Universidade de Brasília
Brasília, Brasil
valenzuela@presidencia.gov.br

Daniel Café
Faculdade de Tecnologia
Universidade de Brasília
Brasília, Brasil
dcafe@unb.br

Éder Gualberto
Faculdade de Tecnologia
Universidade de Brasília
Brasília, Brasil
eder.gualberto@redes.unb.br

***Resumo* — Este artigo propõe um modelo prático e adaptado de gerenciamento de incidentes cibernéticos para instituições da Administração Pública Federal (APF), alinhado à norma ISO/IEC 27035, à Lei Geral de Proteção de Dados (Lei nº 13.709/2018 – LGPD) e ao Plano Nacional de Gestão de Incidentes Cibernéticos (PLANGIC), instituído pela Portaria GSI/PR nº 120/2022. A proposta apresenta um modelo de gerenciamento de incidentes que possibilita padronizar processos e elevar o grau de maturidade organizacional em segurança cibernética. A metodologia adotada inclui a elaboração de um instrumento de diagnóstico com escala de maturidade, aplicável ao contexto da Rede Federal de Gestão de Incidentes Cibernéticos (REGIC). Ao alinhar práticas técnicas e normativas, o modelo contribui de forma significativa para o aumento da resiliência cibernética, o atendimento às exigências legais e o aprimoramento contínuo das políticas e processos institucionais de segurança da informação.**

***Palavras-chave* — Gestão de Incidentes Cibernéticos, PLANGIC, ISO/IEC 27035, LGPD, Administração Pública Federal, REGIC, Segurança da Informação.**

***Abstract*—This article proposes a practical and adapted cyber incident management model for Federal Public Administration (APF) institutions, aligned with the ISO/IEC 27035 standard, the General Data Protection Law (Law No. 13,709/2018 – LGPD) and the National Cyber Incident Management Plan (PLANGIC), established by Ordinance GSI/PR No. 120/2022. The proposal presents an incident management model, which makes it possible to standardize processes and increase the degree of organizational maturity in cybersecurity. The methodology adopted includes the development of a diagnosis instrument with a maturity scale, applicable to the context of the Federal Cyber Incident Management Network (REGIC). By aligning technical and regulatory practices, the model contributes significantly to increasing cyber resilience, meeting legal requirements, and continuously improving institutional information security policies and processes.**

***Keywords*—Cyber Incident Management, PLANGIC, ISO/IEC 27035, LGPD, Federal Public Administration, REGIC, Information Security.**

I. Introdução

A transformação digital remodelou a atuação estatal, ampliando a oferta de serviços públicos eletrônicos, integração de bases governamentais e uso intensivo de tecnologias em nuvem, inteligência analítica e automação. Em contrapartida, elevou-se a superfície de ataque das instituições públicas.

Eventos recentes demonstram a criticidade do tema, como o ataque sofrido pelo Superior Tribunal de Justiça em 2020 [14], a indisponibilidade de sistemas do Ministério da Saúde em 2021[15].

Esses episódios evidenciam que incidentes cibernéticos impactam não apenas ativos tecnológicos, mas a continuidade de políticas públicas, a confiança social e a proteção de dados pessoais.

O gráfico **"Notificações Reportadas pelo CTIR Gov – 2021 a 2025"** apresenta a evolução das notificações registradas no período, contemplando incidentes e vulnerabilidades.

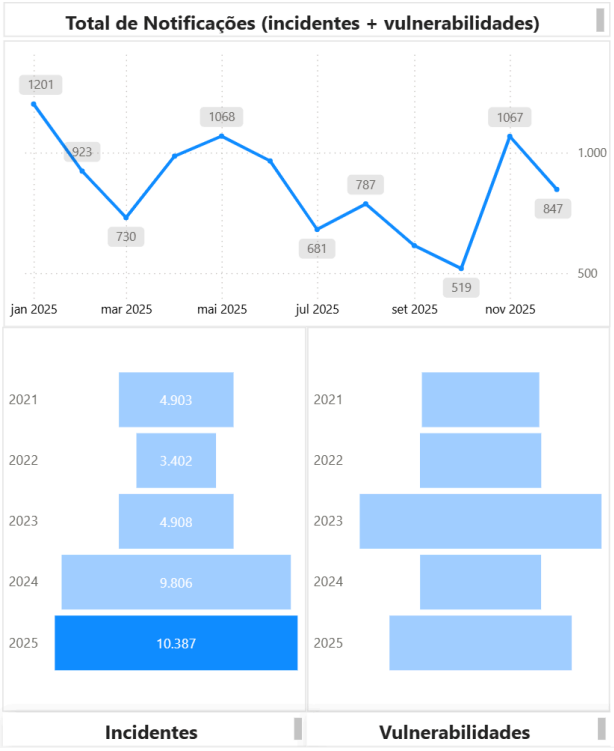
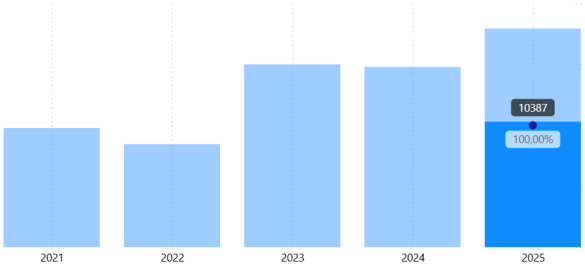


Fig.1 Notificações Reportadas pelo CTIR Gov (2021 a 2025)
Fonte: CTIR Gov [16]

Na Figura 1, Observa-se crescimento expressivo do volume total de notificações reportadas ao CTIR nos anos (2021-2025), com destaque para 2024, que registrou 9.806 notificações, e 2025, que alcançou 10.387 notificações, o maior valor da série apresentada. Em comparação aos anos anteriores, como 2021, com 4.903 registros, 2022, com 3.402, e 2023, com 4.908, os dados evidenciam aumento

relevante da demanda relacionada à gestão, comunicação e tratamento de eventos de segurança cibernética.

A Figura 2 ilustra as notificações trimestrais de incidentes e vulnerabilidade no recorte de 2025, o gráfico indica que o total de notificações foi composto majoritariamente por incidentes, com 10.387 registros, além de 684 vulnerabilidades reportadas. A distribuição mensal demonstra variações ao longo do ano, com maiores volumes em janeiro, maio e novembro, respectivamente com 1.201, 1.068 e 1.067 notificações. Por trimestre, observa-se maior concentração no 2º trimestre, com 3.018 registros, seguido do 1º trimestre, com 2.854, do 4º trimestre, com 2.433, e do 3º trimestre, com 2.082 notificações.



Ano	Vulnerabilidades	Incidentes	Total
2025	684	10387	10387
Total	**684**	**10387**	**10387**

Mês	Vulnerabilidades	Incidentes	Total
janeiro		1201	1201
fevereiro	4	923	923
março	9	730	730
abril	6	985	985
maio	9	1068	1068
junho	2	965	965
julho	3	681	681
agosto	2	787	787
setembro	2	614	614
outubro	4	519	519
novembro	3	1067	1067
dezembro	640	847	847
Total	**684**	**10387**	**10387**

Trimestre	Vulnerabilidades	Incidentes	Total
Trim 4	647	2433	2433
Trim 3	7	2082	2082
Trim 2	17	3018	3018
Trim 1	13	2854	2854
Total	**684**	**10387**	**10387**

Fig. 2 Gráfico de Vulnerabilidade e Incidentes (Trimestre)
Fonte: CTIR Gov [16]

Esses dados reforçam a relevância da temática investigada neste estudo, uma vez que o crescimento e a persistência das notificações reportadas ao CTIR Gov indicam a necessidade de fortalecimento das capacidades institucionais de prevenção, detecção, tratamento, resposta e melhoria contínua em incidentes cibernéticos. Nesse contexto, avaliar a maturidade das instituições em gestão de incidentes torna-se essencial para identificar lacunas, orientar ações de aprimoramento e apoiar a consolidação de processos mais estruturados, padronizados e efetivos no âmbito da segurança cibernética governamental.

Segundo o CTIR Gov [16], a descrição dos tipos de incidentes, são:

- Abuso de Sítio Web: Notificações de incidentes relacionados a comprometimentos confirmados de servidores ou desfigurações de páginas Web na Internet.
- Abuso no Serviço de E-mail (SMTP): Notificações de incidentes ligados à utilização indevida de credenciais de acesso a e-mail.
- Página Falsa: Notificações de incidentes sobre páginas fraudulentas, normalmente usadas para capturar dados de usuários.
- Phishing: Notificações de incidentes relacionados a e-mails com conteúdo malicioso ou não-solicitado.
- Scan: Notificações de incidentes sobre tráfego não-usual, como varreduras em redes de computadores.
- Vazamento de Dados: Notificações de incidentes relacionados à dados indevidamente expostos na Internet.
- Software Vulnerável: Notificações preventivas alertando sobre necessidade de atualização de determinado sistema, visando evitar explorações ou outras atividades maliciosas.
- Vulnerabilidade de Criptografia: Notificações preventivas alertando sobre necessidade de atualização de sistemas criptográficos vulneráveis a ataques contra a confidencialidade de dados.
- Vulnerabilidade DRDoS: Notificações preventivas sobre serviços que permitem amplificação, normalmente abusados por agentes maliciosos para compor ataques de negação de serviços distribuídos por reflexão (DRDoS).

O gráfico de atividades por tipo de incidente em 2025 apresenta um total de 18.093 registros, com maior concentração em Vazamento de Dados, que representa 6.864 ocorrências, seguido por Vulnerabilidade DRDoS, com 3.582 registros, e Software Vulnerável, com 2.755 registros. Também se destacam Abuso de Sítio Web, com 2.026 ocorrências, Página Falsa, com 1.119, Vulnerabilidade de Criptografia, com 816, e Phishing, com 737 registros.

Em menor volume, aparecem Abuso no Serviço de E-mail (SMTP), com 150 ocorrências, Scan, com 37, e Ransomware, com 7 registros. A distribuição evidencia que os principais eventos reportados em 2025 estão associados à exposição indevida de dados, vulnerabilidades técnicas e fragilidades em serviços digitais, reforçando a necessidade de fortalecer controles de prevenção, detecção, correção de vulnerabilidades, proteção de dados e resposta a incidentes cibernéticos.

Por Tipo	Contagem
Vazamento de Dados	6864
Vulnerabilidade DRDoS	3582
Software Vulnerável	2755
Abuso de Sítio Web	2026
Página Falsa	1119
Vulnerabilidade de Criptografia	816
Phishing	737
Abuso no Serviço de E-mail (SMTP)	150
Scan	37
Ransomware	7
Total	**18093**

Fig.3 Tipos Notificações Reportadas (2021 a 2025)
Fonte: CTIR Gov [16]

Esses dados da Figura 3, reforçam a relevância da gestão de incidentes cibernéticos no contexto governamental, especialmente diante da predominância de notificações associadas à exposição indevida de dados, vulnerabilidades exploráveis e fragilidades em serviços digitais.

A concentração de registros em categorias relacionadas a vazamento de dados e vulnerabilidades técnicas indica a necessidade de fortalecer práticas institucionais de prevenção, detecção, tratamento e resposta, incluindo gestão de vulnerabilidades, proteção de dados, monitoramento contínuo, correção tempestiva de falhas e melhoria dos processos de governança em segurança cibernética.

Assim, o gráfico da figura 3, sustenta a justificativa deste estudo ao demonstrar que a maturidade institucional em gestão de incidentes é um fator crítico para reduzir riscos operacionais, proteger informações sensíveis e aumentar a resiliência das organizações públicas frente a ameaças cibernéticas.

Este artigo propõe um modelo prático para o gerenciamento de incidentes cibernéticos em instituições da Administração Pública Federal (APF). A proposta pretende combinar a norma ISO/IEC 27035 [8] e as exigências da Lei Geral de Proteção de Dados (LGPD) [10] com o intuito de atender ao Plano Nacional de Gerenciamento de Incidentes Cibernéticos (PLANGIC), conforme Portaria DSI/GSI/PR nº 120/2022 [9].

Como parte da proposta, será elaborado um instrumento de diagnóstico baseado em questionário com escala de desenvolvimento, visando avaliar o nível de maturidade institucional para lidar com **incidentes cibernéticos.** A abordagem visa apoiar a implementação padronizada de processos de resposta, aumentar a conformidade legal e promover a melhoria contínua da segurança da informação na APF.

A. Definição do Problema

Apesar da existência de normativos relevantes no Brasil, muitos órgãos públicos ainda apresentam dificuldades para operacionalizar processos padronizados de prevenção, detecção, tratamento e resposta a incidentes cibernéticos.

Há, portanto, uma lacuna entre o cumprimento formal das normas e a capacidade prática institucional.

Apesar da existência de normativos claros como o PLANGIC [9], muitas instituições da APF carecem de modelos operacionais práticos que integrem diretrizes técnicas, legais e organizacionais. A norma ISO/IEC 27035 [8] oferece estruturas robustas de conhecimentos que, combinadas ao arcabouço normativo brasileiro, pode orientar a criação e organização de processos, fluxos e procedimentos para a implantação do Plano de Gerenciamento de Incidentes Cibernéticos institucional.

B. *Objetivos*

1) *Objetivo Geral*

Propor um modelo de gerenciamento de incidentes cibernéticos para instituições da APF, integrando da norma ISO/IEC 27035 [8] e a LGPD [10], de acordo com as diretrizes estabelecidas pelo PLANGIC, conforme Portaria GSI/PR nº 120/2022 [9].

2) Objetivos Específicos

- Desenvolver um instrumento de diagnóstico sob a forma de questionário com escala de maturidade, baseado na Portaria GSI/PR nº 120/2022 [9], para avaliar o nível de maturidade das instituições da APF quanto à gestão de incidentes cibernéticos;
- Estruturar um framework de gestão e resposta a incidentes cibernéticos, baseado no PLANGIC e subdividido em 6 etapas: Preparação, Prevenção, Detecção, Tratamento, Resposta e aprendizado pós-incidente
- Integrar os domínios de conhecimento da norma ISO/IEC 27035 [8] aos requisitos do PLANGIC [9] e da LGPD [10], promovendo uma abordagem alinhada às necessidades técnicas, legais e organizacionais da esfera pública federal.

O artigo está dividido em cinco seções: Introdução, Trabalhos Relacionados,Plano de Gestão de Incidentes Cibernéticos (PLANGIC), Metodologia, Instrumento de Avaliação de Maturidade, Modelo Proposto e Conclusão.

II. Trabalhos Relacionados

O gerenciamento de incidentes cibernéticos tem se consolidado como uma área estratégica da segurança da informação, sobretudo no setor público. Diversos estudos propõem frameworks e modelos que estruturam respostas mais eficazes, combinando aspectos técnicos, organizacionais e de governança. O modelo aqui proposto se inspira em abordagens complementares amplamente reconhecidas na literatura nacional e internacional.

O trabalho de Giorgini et al. [1] propõe uma abordagem baseada em *Socio-Technical Systems* (STS) para modelagem de requisitos de segurança em ambientes complexos para restringir interações entre os atores do sistema, com foco na mitigação de riscos desde a fase de concepção.

Em [2], os autores apresentam um modelo estruturado de resposta a incidentes, enfatizando a integração entre a gestão da segurança da informação e a resposta a incidentes. A abordagem adota fundamentos da teoria do aprendizado organizacional, organizando o ciclo de vida da resposta em fases críticas.

O estudo de *Gkioulos* et al. [3] desenvolve um framework de treinamento baseado em cenários, visando superar barreiras sociotécnicas dentro das organizações. A contribuição reside na elaboração de cenários realistas para desenvolver competências institucionais de resposta a incidentes.

No contexto de ecossistemas de softwares proprietários, Silva et al. [4] propõem um framework de gerenciamento de incidentes desenvolvido em colaboração com especialistas do setor, demonstrando adaptabilidade e viabilidade operacional.

No cenário brasileiro, o guia da ABRATE [5] fornece orientações específicas ao setor elétrico para a implementação de frameworks de segurança cibernética, com foco na autoavaliação e melhoria contínua. Em complemento, o guia da Secretaria de Governo Digital [6] apresenta um framework voltado à APF, fundamentado no Programa de Privacidade e Segurança da Informação (PPSI) — regulamentado na Portaria SGD/MGI nº 852/2023 [6] —, abordando aspectos normativos e operacionais; - PPSI versão 2.0 [17].

Por fim, destaca-se o guia do NIST [7], amplamente utilizado como referência global. A publicação sistematiza o tratamento de incidentes em cinco fases e é base para o

NIST *Cybersecurity Framework* (CSF) 2.0 [15], sendo adotado como padrão por diversos setores e países.

Essas referências formam a base comparativa que fundamenta a proposta apresentada neste artigo, a qual visa adaptar essas boas práticas ao contexto e às diretrizes estabelecidas pelo PLANGIC [9] para a APF.

III. Plano de Gestão de Incidentes Cibernéticos (PLANGIC)

O Plano de Gestão de Incidentes Cibernéticos - PLANGIC, instituído pela Portaria DSI/GSI/PR nº 120/2022 [9], com a finalidade de estabelecer diretrizes e procedimentos que padronizam e orientem a atuação dos órgãos e entidades da APF nas atividades de prevenção, detecção, tratamento, resposta e recuperação de incidentes cibernéticos.

Diante da intensificação das ameaças no ambiente digital e da crescente dependência dos ativos de informação para a governança pública, a implementação do PLANGIC [9] torna-se um instrumento essencial para garantir a continuidade dos serviços públicos, assegurar a proteção dos dados institucionais e dos dados pessoais sob responsabilidade do Estado, além de fortalecer a resiliência cibernética no âmbito da APF.

Sua adoção é de caráter obrigatório para todas as instituições que compõem a Rede Federal de Gestão de Incidentes Cibernéticos (Regic) [12], estando diretamente condicionada ao comprometimento da alta administração, à alocação adequada de recursos humanos, tecnológicos e financeiros, bem como à formalização das Equipes de Tratamento e Resposta a Incidentes Cibernéticos (ETIR).

A coordenação nacional da Regic está sob responsabilidade do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov), que exerce papel central na articulação institucional, na emissão de orientações técnicas e na supervisão das ações relativas à gestão de incidentes cibernéticos no âmbito da APF.

IV. METODOLOGIA

Esta seção descreve as medidas a serem adotadas por órgãos da APF, o modelo proposto está baseado no PLANGIC. O modelo proposto é subdividido em 6 etapas: Preparação, Prevenção, Detecção, Tratamento, Resposta e aprendizado pós-incidente.

A. Preparação

A fase de atividades preparatórias é a base para a estruturação da gestão de incidentes cibernéticos em conformidade com o PLANGIC [9]. Essa etapa contempla a adoção de medidas organizacionais, técnicas e operacionais que visam estabelecer as condições mínimas necessárias para que o órgão público esteja apto a prevenir, detectar, tratar e responder a incidentes.

A seguir, são descritas as principais ações que devem ser executadas por cada participante da Regic para garantir sua integração efetiva à rede nacional de gestão de incidentes, conforme a Portaria DSI/GSI/PR nº 120/2022 [9]:

- Designar gestor de segurança da informação;
- Instituir e formalizar a ETIR ou estrutura equivalente;
- Elaborar o documento de constituição da ETIR ou de estrutura equivalente, o qual designará as atribuições e o escopo de atuação;
- Informar ao Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (DSI/GSI/PR) o contato direto do ponto focal responsável pelo compartilhamento de informações relacionadas às atividades da ETIR ou da estrutura equivalente;
- Implementar processos mínimos de:
  - Mapeamento de ativos de informação;
  - Gestão de riscos de segurança da informação;
  - Gestão de Continuidade de negócios em segurança da informação;
  - Gestão de mudanças nos aspectos de segurança da informação; e
- Disponibilizar infraestrutura mínima para realização das atividades de segurança da informação com capacidade de executar os processos de prevenção, detecção, tratamento e resposta a incidentes cibernéticos.

B. Prevenção

A fase de prevenção contempla o conjunto de ações proativas voltadas à redução da probabilidade de ocorrência de incidentes cibernéticos. Essas ações devem ser contínuas e integradas à política institucional de segurança da informação, com foco na definição e implementação de controles de segurança, de gerenciamento de vulnerabilidades, de conscientização e de capacitação.

Os controles de segurança preventivos estão organizados em três eixos principais: controles preventivos, gerenciamento de vulnerabilidades e programas de conscientização e capacitação, conforme itens a seguir:

1) *Controles Preventivos:*

- Tecnológicos: autenticação, *malware*, backup, criptografia, *logs*, *firewall*, redes seguras;
- Organizacionais: políticas, papéis e responsabilidades, controle de acesso, rotulagem;
- Físicos: segurança perimetral, monitoramento, localização e proteção de equipamentos.

Controles de Segurança - Preventivos

Principais Controles		
Tecnológicos	***Organizacionais***	***Físicos***
dispositivos *endpoint* do usuário;	política de segurança da informação;	definição dos perímetros de segurança física;
restrição de acesso à informação;	definição de papéis e responsabilidades pela segurança da informação;	monitoramento de segurança física;

AUTENTICAÇÃO SEGURA;	SEGREGAÇÃO DE FUNÇÕES;	PROTEÇÃO CONTRA AMEAÇAS FÍSICAS E AMBIENTAIS;
PROTEÇÃO CONTRA *MALWARE*;	MAPEAMENTO DE ATIVOS DE INFORMAÇÃO;	LOCALIZAÇÃO E PROTEÇÃO DE EQUIPAMENTOS;
BACKUP DAS INFORMAÇÕES;	CONTROLE DE ACESSO;	SEGURANÇA DE ATIVOS FORA DAS INSTALAÇÕES DA ORGANIZAÇÃO; E
ATIVIDADES DE MONITORAMENTO (*LOG*);	CLASSIFICAÇÃO E ROTULAGEM DE INFORMAÇÕES; E	MANUTENÇÃO DE ATIVOS.
SEGURANÇA DE REDES;	NORMA DE SEGURANÇA DA INFORMAÇÃO PARA USO DE SERVIÇOS EM NUVEM.	
USO DE CRIPTOGRAFIA;		
GESTÃO DE MUDANÇAS.		

a. Fonte: Portaria DSI/GSI/PR nº 120/2022 [9].

2) Gerenciamento de Vulnerabilidades

O gerenciamento de vulnerabilidades é um processo contínuo, estruturado e proativo, que abrange a identificação, análise, tratamento e monitoramento de falhas passíveis de exploração por agentes mal-intencionados. Tem como finalidade reduzir a superfície de exposição da organização, mitigando riscos cibernéticos e prevenindo incidentes como acessos não autorizados, vazamentos de dados e interrupções de serviços.

Diante do aumento constante de vulnerabilidades e da limitação de recursos para sua pronta mitigação, torna-se essencial adotar uma abordagem que combine ações preventivas com práticas robustas de detecção, priorização e resposta. A efetividade desse processo depende da capacidade institucional de avaliar o risco associado a cada vulnerabilidade, considerando o impacto nos ativos de informação.

No contexto da Regic, é requisito mínimo que os órgãos e entidades realizam o mapeamento dos ativos de informação, devendo:

- classificar os ativos de informação de acordo com sua criticidade;
- identificar continuamente as vulnerabilidades neles existentes; e
- priorizar as ações de correção e de mitigação por meio da avaliação do nível de ameaça e de criticidade da vulnerabilidade.

O mapeamento dos ativos de informação é fundamental para viabilizar a gestão adequada de vulnerabilidades, assegurando a proteção dos ativos críticos e o cumprimento das diretrizes estabelecidas pela PLANGIC. Para executar o gerenciamento de vulnerabilidades, o participante da Regic deve:

- acompanhar as notificações, os alertas e as recomendações emitidas por parceiros, entre eles o CTIR Gov e os fornecedores de ativos, adotando as ações necessárias;
- estabelecer um processo para gerenciamento de patches; e
- estabelecer um processo para gerenciamento de configuração e de correção de vulnerabilidades.

As diretrizes referentes à correção, mitigação e aos procedimentos para aplicação de medidas corretivas devem ser formalmente definidas e registradas em documentos institucionais.

3) Conscientização e Capacitação

Com o objetivo de fortalecer a cultura organizacional em segurança cibernética, o participante da Regic deve promover ações contínuas de conscientização e capacitação em todos os níveis da administração.

Deve ser instituído um processo sistemático de divulgação de boas práticas de segurança cibernética a todos os colaboradores, utilizando canais de comunicação eficazes e linguagem compatível com os diferentes públicos-alvo. As ações educativas podem incluir seminários, colóquios, treinamentos, palestras, estágios internos, boletins informativos e memorandos, promovidos no âmbito institucional.

A conscientização em segurança da informação deve abranger, no mínimo, os seguintes aspectos:

- Compromisso da alta administração com a segurança da informação;
- Responsabilização dos colaboradores por ações e omissões; e
- Familiarização e compliance em relação às regras e obrigações aplicáveis de segurança da informação.

Com relação à capacitação, é necessário:

- Preparação de um plano de treinamento adequado para equipes técnicas cujos papéis requerem habilidades e conhecimentos específicos; e
- Constante atualização e aprimoramento do conhecimento técnico e profissional.

A implementação eficaz dessas medidas contribui diretamente para a redução da possibilidade de ataque, a minimização de riscos operacionais e o fortalecimento da política de segurança institucional.

C. Detecção

Trata-se de um processo de melhoria contínua, voltado à análise permanente do ambiente de informação, com o objetivo de identificar atividades maliciosas que possam comprometer os ativos de informação. Sua finalidade é reduzir o impacto de incidentes cibernéticos, permitindo antecipar o início dos processos de tratamento e resposta.

Nesse contexto, a detecção exige a definição de linhas de base, a implementação de monitoramento contínuo e a comunicação tempestiva dos incidentes identificados.

A seguir, detalham-se os principais componentes desta etapa:

1. Estabelecimento de linhas de base

A organização deve estabelecer linhas de base operacionais que representem o padrão de funcionamento e o uso regular da rede e dos ativos de informação. Desvios em relação a esses parâmetros devem ser considerados potenciais indícios de incidente cibernético, sendo obrigatória sua análise e investigação.

A eficácia do processo de detecção depende da definição de critérios técnicos, mensuráveis e objetivos, que orientem a identificação, a classificação e a caracterização de anomalias como possíveis incidentes de segurança da informação. A instituição deve:

- Estabelecer padrões de normalidade para identificar anomalias.

2. Monitoramento Contínuo:

O monitoramento contínuo dos ativos de informação é uma prática essencial no contexto da gestão de segurança cibernética, especialmente para os participantes da Regic.

Este processo tem como objetivo identificar, em tempo hábil, comportamentos anômalos e potenciais indícios de incidentes, garantindo maior capacidade de resposta e mitigação de riscos. Para isso, é fundamental que a organização defina linhas de base que representem o funcionamento esperado dos sistemas, permitindo que desvios sejam prontamente detectados e analisados.

A instituição deve estabelecer o monitoramento contínuo de seus ativos de informação, cabendo a verificação contínua de:

- Alteração de comportamento pela comparação com as linhas de base;
- Testes de penetração e correlação de eventos;
- Acesso de usuários, particularmente quanto a horários e ativos acessados;
- Volumetria do tráfego de saída;
- *Logs*;
- Funcionamento e atualização das ferramentas de segurança cibernética, em especial as de *antimalware*; e
- Execução não autorizada de serviço, software ou código.

O aprimoramento desse processo pode ser alcançado mediante técnicas de detecção proativa, tais como:

- Exploração controlada de vulnerabilidades;
- Atividades proativas de equipes de análise;
- Correlação de log e eventos;
- Teste de penetração; e
- Monitoramento proativo de rede.

Após a detecção de uma anomalia, as informações sobre o evento adverso devem ser encaminhadas à triagem. As orientações para notificar incidentes potenciais estão disponíveis no sítio eletrônico do CTIR Gov.

3. Comunicação

Conforme o Decreto nº 10.748, de 16 de julho de 2021 [12], os participantes da Regic devem informar um endereço de correio eletrônico institucional vinculado à sua ETIR, destinado à troca de informações sobre incidentes cibernéticos com o CTIR Gov. Esse cadastro deve ser realizado por meio do termo de adesão disponibilizado no sítio eletrônico do CTIR Gov.

Este canal será utilizado, futuramente, para a operacionalização de uma plataforma computacional dedicada.

Na indisponibilidade do canal de correio eletrônico, poderão ser utilizados, excepcionalmente, outros meios de comunicação, tais como:

- Voz;
- *Inter-Network Operation Center Dial By Autonomous System Number* (INOC-DBA);
- Mensagem instantânea;
- Reunião por videoconferência;
- Sítios eletrônicos e mídias sociais institucionais;
- Reunião presencial de representantes.

As comunicações que trafegam por esses canais terão, principalmente, a finalidade de notificar incidentes cibernéticos, observando o formato padronizado disponibilizado pelo CTIR Gov em seu sítio eletrônico. Tais notificações devem ser encaminhadas com a máxima brevidade possível.

D. Tratamento

A fase de tratamento é acionada imediatamente após a detecção ou notificação de um incidente cibernético. Seu objetivo principal é confirmar a ocorrência, classificar a gravidade, entender a natureza e o impacto do incidente, e iniciar as ações técnicas necessárias para sua contenção, erradicação e recuperação.

1) Etapa 1: Triagem

A triagem é uma etapa fundamental no processo de gerenciamento de incidentes cibernéticos. Ela tem como objetivo garantir que os eventos reportados sejam devidamente analisados, classificados e encaminhados de forma correta para o devido tratamento.

Esse processo envolve as seguintes atividades, conforme PLANGIC [9]:

- Confirmar se se trata de um incidente cibernético e, caso este não pertença à verificação de escopo (*constituency)*, redirecionar a informação para o responsável pelo tratamento;
- Verificar se há correlação com outros incidentes;
- Estabelecer a prioridade para o tratamento do incidente;
- Registrar o incidente na base de incidentes cibernéticos; e
- Atribuir o tratamento do incidente ao analista ou à equipe responsável.

A seguir, este artigo descreve processos e procedimentos que devem ser implementados pela instituição na etapa de triagem de incidentes cibernéticos, em conformidade com a ISO/IEC 27035 [8], PLANGIC [9], PPSI-SGD/MGI [6] e

demais normativos aplicáveis, como a LGPD (Lei nº 13.709/2018) [10].

a) Processos e Procedimentos para a Etapa de Triagem de Incidentes Cibernéticos

A etapa de triagem é essencial para garantir que os incidentes sejam devidamente identificados, classificados e encaminhados para tratamento adequado. Para isso, a instituição deve implementar os seguintes processos e procedimentos:

Validação e Verificação de Escopo do Incidente

Processo: Avaliar tecnicamente se o evento reportado de fato caracteriza um incidente cibernético, ou seja, se há impacto real ou potencial sobre a confidencialidade, integridade ou disponibilidade dos ativos de informação, sistemas, redes ou dados pessoais.

Procedimentos:

- Estabelecer critérios claros, com base na ISO/IEC 27035, na PSI institucional e na LGPD, para distinguir entre:
  - Evento de segurança;
  - Incidente de segurança da informação;
  - Incidente cibernético relevante.
- Implementar um roteiro de verificação técnica (*checklist*) para apoiar a análise preliminar.
- Verificar se o incidente está relacionado aos ativos, serviços ou sistemas sob responsabilidade da instituição (verificação de *constituency*).
- Caso o incidente não pertença ao escopo da instituição, redirecionar imediatamente as informações para:
  - A ETIR do órgão responsável;
  - CTIR Gov (quando aplicável, no âmbito da APF);
  - Ou a entidade responsável pelo ambiente afetado.

Verificação de Correlação com Outros Incidentes

Processo: Analisar se o incidente apresenta relação com outros incidentes ou eventos formalmente registrados, permitindo identificar tendências, ataques em cadeia, campanhas persistentes ou vulnerabilidades recorrentes.

Procedimentos:

- Implementar ferramentas de gestão de incidentes que permitam a busca, análise e correlação de registros.
- Utilizar indicadores compartilhados por fontes confiáveis (CTIR Gov, ETIRs, CERTs e comunidade especializada).
- Documentar as relações encontradas no próprio registro do incidente.

Estabelecimento de Prioridade para Tratamento

Processo: Avaliar o nível de criticidade do incidente para definir a prioridade de atendimento, assegurando que recursos sejam alocados de forma proporcional à gravidade e urgência do evento.

Procedimentos:

Aplicar critérios baseados em:

- Impacto sobre operações institucionais;
  - Severidade do comprometimento (dados pessoais sensíveis, sistemas críticos etc.);
  - Escalabilidade e potencial de propagação;
  - Obrigações legais e regulatórias (ex.: LGPD, se envolver dados pessoais).

Classificar o incidente em níveis de prioridade, como:

- Alta;
- Média;
- Baixa.

Registro Formal do Incidente

Processo: Documentar o incidente de forma estruturada na base de gestão de incidentes cibernéticos da instituição, garantindo rastreabilidade, controle e histórico.

Procedimentos:

Definir um modelo padronizado de registro contendo:

- Dados de identificação (ID, data, hora);
- Descrição detalhada do incidente;
- Sistemas, serviços ou ativos afetados;
- Avaliação preliminar do impacto;
- Classificação de prioridade;
- Ações iniciais realizadas;
- Histórico da triagem e dos encaminhamentos.

Assegurar que o registro atenda também às exigências de:

- Auditoria;
- Relatórios gerenciais;
- Comunicação à alta gestão;
- Comunicação à Autoridade Nacional de Proteção de Dados (ANPD) — quando aplicável, no caso de incidentes que envolvam dados pessoais, conforme Art. 48 da LGPD.

Atribuição para Tratamento

Processo: Designar formalmente o responsável pelo tratamento do incidente, seja um analista específico, uma equipe técnica ou um grupo multidisciplinar, conforme a natureza e gravidade do incidente.

Procedimentos:

- Consultar a matriz de responsabilidades da ETIR e das equipes técnicas da instituição;
- Atribuir o incidente a:
  - Um analista;
  - Uma equipe, unidade especializada ou equivalente;
  - Ou um grupo composto por segurança da informação, jurídico, comunicação e áreas de negócio (quando o incidente exigir abordagem multidisciplinar, como em vazamento de dados pessoais).
- Formalizar a atribuição no sistema de gestão de incidentes e comunicar aos responsáveis.
- Definir prazos e SLAs para acompanhamento do tratamento, alinhados às políticas internas.

2) ***Fluxo Operacional Proposto*** – *Triagem de Incidentes Cibernéticos*

A Tabela II, apresenta as etapas do fluxo proposto por este artigo:

Tabela II - Etapas do processo

1. **Recebimento do Evento ou Notificação**
Receber alertas, notificações, comunicações internas ou externas sobre possíveis eventos de segurança.
2. **Validação – Classificação do Evento**
Analisar tecnicamente o evento para determinar se se trata de um incidente cibernético.
1. Se não for incidente: Encerrar o registro como evento, arquivando para histórico e aprendizado. 2. Se for incidente: Prosseguir para a verificação de escopo.
3. **Verificação de Escopo (*Constituency*)**
Avaliar se o incidente está relacionado aos ativos, sistemas, redes ou dados sob responsabilidade da instituição.
1. Se não pertence à constituency: Redirecionar imediatamente ao órgão, entidade ou equipe competente (como outro ETIR ou CTIR Gov) e registrar internamente o ocorrido. 2. Se pertence: Seguir para as etapas seguintes.
4. **Verificação de Correlação**
Analisar se há relação do incidente com outros incidentes ou eventos anteriores, identificando possíveis ataques coordenados, campanhas ou recorrências.
5. **Classificação de Prioridade**
Avaliar o impacto e a urgência do incidente para definir a prioridade de tratamento, considerando critérios como: 1. ***Impacto sobre operações;*** 2. ***Gravidade do comprometimento;*** 3. ***Dados pessoais afetados (LGPD);*** 4. ***Potencial de propagação.***
6. **Registro Formal na Base de Incidentes**
Documentar o incidente na base de dados, com: 1. ***Dados de identificação;*** 2. ***Descrição detalhada;*** 3. ***Avaliação preliminar;*** 4. ***Prioridade;*** 5. ***Histórico da triagem;*** 6. ***Ações tomadas até o momento.***
7. **Atribuição para Tratamento**
Designar formalmente o incidente para um analista ou equipe técnica especializada, que assumirá a responsabilidade pelo tratamento, contenção e resolução.

Fonte: Elaboração própria

A **Figura 4** ilustra o Fluxo de Triagem de Incidentes Cibernéticos:

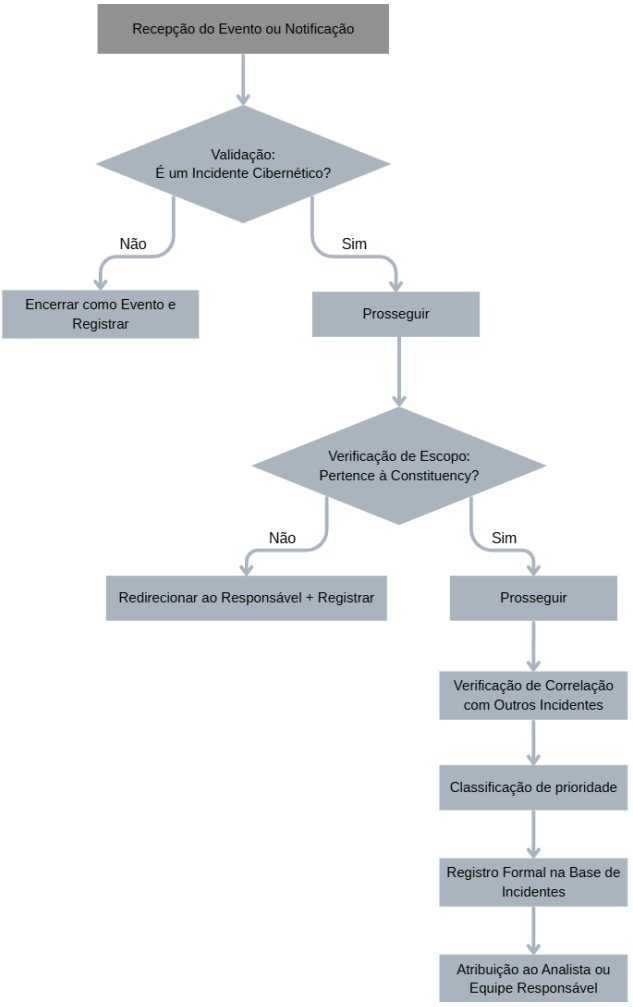


Fig. 4 Fluxo de Triagem de Incidentes Cibernéticos. Fonte: elaboração própria

3) *Etapa 2: Análise*

Conforme o PLANCIG [9], a etapa de análise consiste nas atividades listadas a seguir:

- validar as informações tratadas na triagem, ratificando-as, complementando-as ou retificando-as;
- identificar e avaliar atividades anômalas em relação à linha de base conhecida;
- identificar pelo menos uma parte da cadeia de ataque para permitir a definição das atividades de resposta;

- complementar e adicionar novos dados a partir da colaboração das fontes utilizadas na detecção; e
- Incluir todos os dados coletados na documentação sobre o incidente para viabilizar as ações de pós-incidente.

Na atividade da Colaboração, é obrigatória a comunicação ao CTIR Gov apenas dos incidentes que:

- possam implicar em perda de vidas;
- afetem a disponibilidade, integridade, confiabilidade e autenticidade de ativos de informação de:
  - infraestruturas críticas – energia, água, transporte, finanças, comunicações, defesa e biossegurança; e
  - serviços governamentais digitais;
- implique em vazamento de:
  - dados pessoais; e
  - informação classificada ou sensível; e
- possuem potencial de exploração danosa em larga escala.

4) Proposta - Fluxo de Processos para a Etapa de Análise

Este trabalho elaborou o Fluxo de Processos para a Etapa de Análise no Tratamento de Incidentes Cibernéticos do PLANGIC [9]

A etapa de análise tem como objetivo compreender a natureza do incidente, seu impacto, sua origem, vetor de ataque, abrangência e, a partir disso, subsidiar as atividades de contenção, erradicação, recuperação e ações corretivas.

Etapas do Processo de Análise:

1. Validação das Informações da Triagem

Revisar os dados coletados na triagem, realizando:

- Ratificação das informações;
- Correção de dados inconsistentes (retificação);
- Complementação de dados faltantes.

2. Análise de Atividades Anômalas

Identificar e avaliar comportamentos anômalos, comparando-os com a linha de base conhecida dos sistemas, redes e operações normais da instituição.

- Examinar logs, tráfego de rede, acessos e padrões operacionais.

3. Identificação da Cadeia de Ataque

Analisar o incidente para identificar, pelo menos, uma ou mais etapas da cadeia de ataque, tais como:

- Reconhecimento;
- Exploração de vulnerabilidades;
- Execução;
- Persistência;
- Movimento lateral;
- Exfiltração de dados.

Esta identificação é essencial para direcionar as ações de resposta.

4. Coleta e Consolidação de Novas Informações

Agregar dados provenientes de múltiplas fontes, como:

- Ferramentas de detecção (EDR, SIEM, IDS, IPS);
- Relatórios de inteligência (CTIR Gov, ETIRs, CERTs);
- Feedbacks de áreas internas (TI, segurança, unidades de negócio).

5. Documentação Completa do Incidente

Atualizar a base de registro do incidente com todas as informações analisadas, incluindo:

- Novos dados coletados;
- Cronologia detalhada dos eventos;
- Descrição das atividades maliciosas e vetores explorados;
- Evidências técnicas para subsidiar as fases seguintes (contenção, erradicação, recuperação e pós-incidente).

A seguir, a **Figura 5** ilustra o *Fluxo de Processos para a Etapa de Análise.*

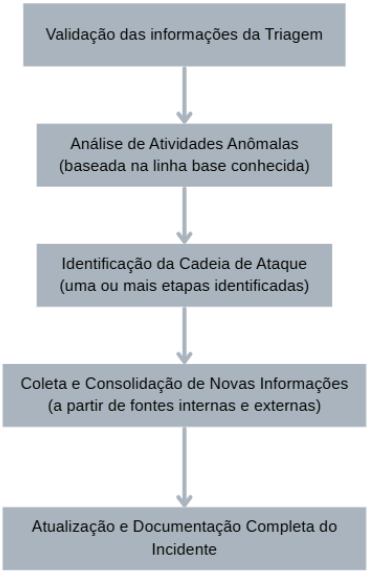


Fig. 5 Fluxo de Análise no Tratamento de Incidentes Cibernéticos. Fonte: elaboração própria

E. Resposta

A **etapa de resposta** a um incidente cibernético compreende um conjunto de ações coordenadas e estruturadas com o objetivo de conter, erradicar e recuperar os sistemas e ativos de informação afetados. Essas ações devem ser conduzidas com base em critérios definidos no Plano de Continuidade de Negócios em Segurança da Informação e devem levar em consideração a criticidade dos ativos impactados, o tipo e a gravidade do incidente, a necessidade de preservação de evidências, a importância dos sistemas para a continuidade dos serviços institucionais e os recursos disponíveis para implementar as estratégias de resposta.

A contenção visa interromper a propagação do incidente e limitar seus impactos imediatos.

Na sequência, realiza-se a erradicação, com o objetivo de remover completamente os vetores de ataque e eliminar a

presença de agentes maliciosos nos ativos afetados. Essa etapa requer a investigação aprofundada da causa raiz do incidente, com a identificação de atividades anômalas em relação à linha de base comportamental conhecida. Para isso, são analisados elementos como fluxo de dados, registros de acesso (logs), autenticações de usuários e padrões de horário.

Simultaneamente, é necessário garantir a validação contínua das informações tratadas nas fases anteriores, revisando, complementando ou retificando os dados coletados durante a triagem. A categorização adequada do incidente, a priorização das ações e a confirmação das equipes envolvidas são fundamentais para a eficácia da resposta. A análise de correlações entre eventos e a consulta a diferentes fontes, tanto internas quanto externas, também contribuem para ampliar a compreensão do incidente.

Durante toda a resposta, é imprescindível manter a documentação atualizada, registrando todos os dados coletados, decisões tomadas, fontes consultadas e ações executadas. Essa documentação será fundamental para viabilizar as atividades de pós-incidente, como análise de impacto, melhoria de controles e atualização de procedimentos internos. Além disso, o compartilhamento de informações relevantes com o CTIR Gov ou com outros órgãos competentes, quando aplicável, fortalece a capacidade de resposta coordenada no âmbito da APF.

Por fim, a fase de recuperação consiste na restauração dos serviços, sistemas e dados ao seu estado normal de funcionamento, de forma segura e controlada. Essa etapa deve ser alinhada ao plano de continuidade de negócios e pode incluir ações de correção de vulnerabilidades, restauração de backups, reforço de controles de segurança e comunicação às partes interessadas.

Conforme o PLANGIC [9], a ETIR deverá encaminhar todas as informações relevantes ao gestor de segurança da informação. Esses dados deverão ser avaliados em conjunto com a assessoria jurídica do órgão ou entidade, com o objetivo de viabilizar a adoção das medidas legais, administrativas e cíveis aplicáveis, inclusive, quando necessário, a comunicação às autoridades policiais competentes.

Na ocorrência de incidentes que envolvam o vazamento de dados pessoais, caberá ao encarregado pelo tratamento de dados pessoais do órgão ou entidade realizar a comunicação à Autoridade Nacional de Proteção de Dados (ANPD), observando os procedimentos estabelecidos na legislação vigente, nos normativos aplicáveis e nas orientações específicas da referida autoridade.

1) Etapa: Contenção

O objetivo da **fase de contenção** é limitar os impactos e os danos decorrentes do incidente de segurança, bem como prevenir sua propagação e a ocorrência de novos comprometimentos. As medidas adotadas nesta etapa devem mitigar os efeitos do incidente, preservando, sempre que possível, as evidências necessárias para subsidiar eventuais processos administrativos, civis ou penais.

As ações de contenção podem compreender, entre outras, as seguintes atividades:

- contenção a curto prazo, que consiste em:
  - limitar os danos antes que o incidente piore;
  - isolar segmentos de rede; e
- executar um *failover routing* (desvio de tráfego de rede para os recursos que estejam saudáveis e disponíveis);
- realização de imagem forense do ambiente afetado; e
- contenção a longo prazo, que consiste em:
  - identificar vulnerabilidades exploradas pelos atacantes e os mecanismos que permitiram o ataque; e
  - aplicar correções temporárias que permitam a volta ao funcionamento dos sistemas afetados.

Este trabalho elaborou uma proposta de ***Fluxo de Processos da Etapa de Contenção de Incidentes Cibernéticos***, elaborado com base nas boas práticas da ISO/IEC 27035 [8], nas diretrizes do PLANGIC [9] e alinhado às políticas de segurança da informação e proteção de dados da APF. A seguir a sua descrição:

Proposta - Fluxo de Processos – Etapa de Contenção de Incidentes Cibernéticos

Objetivo: Conter o incidente para evitar sua propagação, mitigar impactos, preservar evidências e garantir a continuidade segura das operações.

A fase de contenção tem como finalidade adotar ações rápidas e sustentáveis que restrinjam os impactos do incidente, impeçam sua propagação e preservem a integridade dos sistemas afetados. Além disso, essa etapa visa garantir a adequada coleta de evidências para análises forenses, investigações internas e eventuais processos legais. De acordo com as diretrizes estabelecidas na ISO/IEC 27035 [8] e no PLANGIC [9], o processo de contenção é estruturado em três fases principais: contenção de curto prazo, preservação de evidências e contenção de longo prazo, apresentados na **Figura 6.**

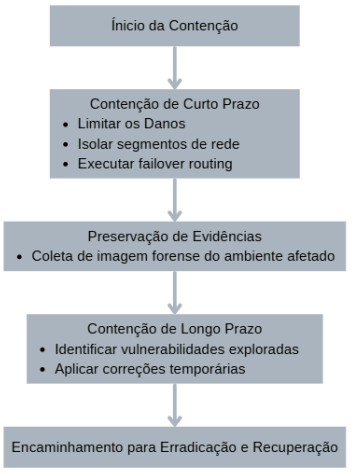


Fig. 6 Fluxo de Análise no Tratamento de Incidentes Cibernéticos. Fonte: elaboração própria

A contenção de curto prazo corresponde à implementação de medidas emergenciais que buscam mitigar os efeitos imediatos do incidente e impedir sua escalada. Inicialmente, são aplicadas ações para limitar os danos, como o bloqueio de acessos, a restrição de tráfego malicioso ou a desconexão de ativos comprometidos. Posteriormente, realiza-se o isolamento dos sistemas

afetados, utilizando métodos como a segregação lógica — via VLANs, regras de firewall ou ACLs —, ou o isolamento físico, quando necessário. Complementarmente, aplica-se o *failover routing*, que consiste no redirecionamento de tráfego ou serviços para infra-estruturas não impactadas, garantindo, assim, a continuidade dos processos críticos da organização.

A etapa subsequente envolve a preservação de evidências, essencial para assegurar a integridade dos dados relacionados ao incidente. Esta atividade permite sustentar análises técnicas detalhadas, bem como eventuais investigações administrativas, cíveis ou penais.

A coleta forense deve incluir a criação de imagens dos discos rígidos dos sistemas afetados, captura da memória volátil, extração de registros de logs e de fluxos de rede. Essa coleta deve ser realizada antes de qualquer intervenção corretiva que possa modificar o ambiente comprometido, garantindo a rastreabilidade e a manutenção da cadeia de custódia das evidências digitais.

Por sua vez, a contenção de longo prazo visa estabilizar o ambiente operacional de forma controlada até que seja possível realizar a erradicação completa do incidente. Nesse estágio, são identificadas as vulnerabilidades exploradas e os mecanismos utilizados pelos atacantes, como falhas de configuração, exploração de vulnerabilidades conhecidas, uso de credenciais comprometidas, entre outros vetores.

A partir dessa análise, são aplicadas medidas de mitigação temporária, incluindo atualizações emergenciais, reconfiguração de parâmetros de segurança, fortalecimento dos controles de acesso, aplicação de regras específicas em dispositivos de segurança, como firewalls e sistemas de prevenção de intrusão (IPS), além da intensificação das atividades de monitoramento dos ativos impactados.

Encerradas as ações de contenção, o processo é direcionado para as fases de erradicação e recuperação, nas quais serão executadas ações corretivas definitivas, como a remoção dos vetores de ataque, a correção das vulnerabilidades exploradas e a restauração segura dos serviços e sistemas afetados.

Essas etapas devem ser conduzidas em consonância com os princípios e diretrizes estabelecidos no PLANGIC [9] e no Plano de Continuidade de Negócios (PCN) da organização, garantindo uma resposta coordenada, eficiente e que assegure a retomada plena das operações institucionais.

2) *Etapa: Erradicação*

Segundo o PLANGIC [9] a ação de erradicação poderá envolver as seguintes atividades ilustrada na figura 7:

1. **restauração** completa das imagens de unidades de armazenamento, implicando na exclusão de todos os dados atuais;
2. **recuperação dos dados** a partir dos backups existentes;
3. **identificação das causas** principais que originaram o ataque;
4. realização dos procedimentos necessários para **limpar a unidade** de armazenamento, removendo ou isolando os artefatos utilizados pelos atacantes; e
5. **correção das vulnerabilidades** encontradas.

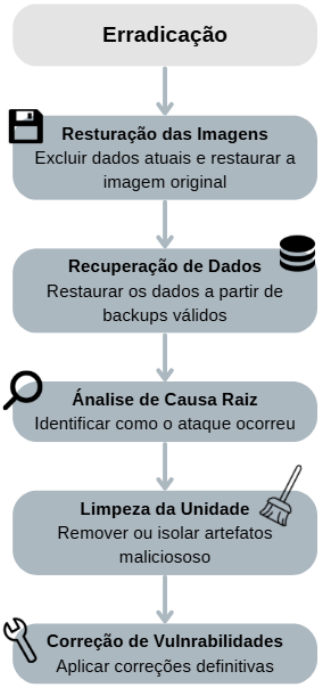


Fig. 7 Etapas de Erradicação

3) *Etapa: Recuperação*

O objetivo da fase de recuperação é restabelecer, de forma segura, o pleno funcionamento dos sistemas, serviços e ativos impactados, assegurando que todas as ameaças foram devidamente neutralizadas, removidas ou mitigadas.

A Figura 8 descreve as etapas de recuperação PLANGIC [9]:

Etapa	Recuperação
1.Definição de cronograma	Estabelecer plano de restauração das operações pelos responsáveis, com base nos subsídios fornecidos pela ETIR
2. Varredura do ambiente	Realizar inspeção completa do ambiente restaurado para garantir que esteja apto ao uso seguro
3.Testes de funcionamento	Validar o ambiente com base nas linhas de base definidas, à medida em que os serviços forem sendo restabelecidos
4.Monitoramento Pós Restabelecimento	Observar o ambiente por período determinado, buscando identificar comportamentos atípicos

Fig. 8 Etapas de Recuperação

As atividades relacionadas à recuperação podem incluir, entre outras PLANGIC [9]:

- definição de cronograma para a restauração das operações pelos responsáveis pelos ativos de informação afetados, com base em subsídios apresentados pela ETIR;

- realização de varredura completa do ambiente recuperado, de forma a garantir que este esteja apto para uso seguro;
- realização de testes de funcionamento do ambiente recuperado, validando os resultados com as linhas de base definidas, à medida em que estarão novamente disponibilizados para uso; e
- monitoramento do ambiente recuperado, a ser executado num período após o incidente cibernético, de forma a verificar comportamentos atípicos ou anormalidade nas operações.

Após a conclusão do processo de recuperação, os integrantes da REGIC deverão encaminhar ao CTIR Gov um relatório detalhado sobre o incidente, contendo as seguintes informações:

- atores atacantes e atacados;
- atores envolvidos no tratamento e resposta do incidente;
- evidências coletadas;
- indicadores de comprometimento (IoCs), bem como táticas, técnicas e procedimentos (TTPs);
- ativos de infraestrutura, serviços e total de usuários afetados;
- volume de dados exfiltrados;
- cronologia dos fatos;
- medidas de contenção, erradicação e recuperação adotadas; e
- medidas preventivas propostas para ocorrências similares.

A **Tabela III** descreve os papéis dos atores que participam do processo de resposta.

Tabela III. Atores no Processo de Resposta

Tipos de ETIR	Contenção	Erradicação	Recuperação
ETIR	Executar	Executar	Executar
ETIR SETORIAL	Coordenar	Coordenar	Coordenar
ETIR PRINCIPAL	Executar	Executar	Executar
CTIR Gov	Determinar escopo do incidente Identificar órgãos envolvidos no incidente	----	Receber relatório do incidente

Fonte: Responsabilidade dos atores no processo de resposta [9]

F. Pós Incidente

A fase de pós-incidente tem como objetivo realizar uma análise da documentação do incidente, dos procedimentos de comunicação executados e dos controles de segurança implementados no ambiente afetado. Essa etapa visa identificar oportunidades de melhoria, corrigir falhas, mitigar a possibilidade de recorrência de incidentes semelhantes e fortalecer a cultura de melhoria contínua nos processos de gestão de segurança cibernética da organização.

1) Melhoria Contínua dos Processos

Com foco na elevação da maturidade organizacional em segurança da informação e no fortalecimento da capacidade de prevenção, detecção, tratamento e resposta a incidentes cibernéticos, os integrantes da REGIC devem realizar uma análise detalhada dos processos envolvidos no incidente. Essa avaliação deve contemplar desde os mecanismos de prevenção até as ações executadas durante a resposta, permitindo identificar falhas, lacunas e pontos de aprimoramento nos procedimentos institucionais.

2) Análise Pós-incidente

Conforme o PLANGIC [9], os principais objetivos da análise pós-incidente incluem:

- confirmar que a causa raiz foi eliminada ou mitigada;
- estabelecer medidas preventivas para incidentes similares;
- identificar os erros ou ausências de infraestrutura a serem resolvidos;
- identificar as oportunidades de melhoria na política organizacional, normativos ou nos processos;
- revisar e atualizar as funções, as responsabilidades, o processo de comunicação e a autoridade da ETIR para garantir a resposta oportuna e adequada;
- identificar necessidades de treinamento técnico ou operacional; e
- melhorar as ferramentas, ações e capacidades necessárias para realizar a prevenção, a detecção, o tratamento e a resposta.

Com base nas análises realizadas na fase de pós-incidente, o participante da REGIC deverá atualizar as atividades preparatórias e os processos de prevenção, detecção, tratamento e resposta a incidentes cibernéticos. Para isso, deverá:

- identificar IoCs ou TTPs da ameaça, encaminhando esses dados obrigatoriamente ao CTIR Gov, a fim de realizar ações colaborativas no âmbito da Regic;
- adicionar outros critérios para detecção e triagem da ameaça; e
- identificar e propor soluções para situações omissas verificadas no incidente.

Diante do exposto, a fase de pós-incidente se consolida como uma etapa essencial no ciclo de gestão de incidentes cibernéticos, uma vez que permite não apenas confirmar a efetiva mitigação da causa raiz, mas também fortalecer os processos organizacionais por meio da identificação de fragilidades, lacunas operacionais e oportunidades de aprimoramento.

Ao promover a revisão dos processos, das responsabilidades e dos procedimentos de resposta, além de fomentar a atualização de controles, ferramentas e capacidades técnicas, essa etapa contribui diretamente para o aumento da resiliência cibernética institucional.

V. Instrumento de Avaliação de Maturidade

Este instrumento foi desenvolvido pelo presente artigo com o objetivo de mensurar o nível de maturidade das

instituições públicas federais na gestão de incidentes cibernéticos, em conformidade com as diretrizes estabelecidas na Portaria GSI/PR nº 120/2022, que institui o PLANGIC [9]. Estruturado em seis blocos temáticos, o formulário abrange todas as fases do ciclo de vida da gestão de incidentes cibernéticos, estando alinhado às recomendações da norma ISO/IEC 27035 [8] e aos princípios operacionais da REGIC.

A. A Escala Linear de Avaliação

O instrumento de avaliação foi construído com base em uma escala linear de cinco níveis, que permite mensurar o grau de implementação dos controles previstos no PLANGIC [9] relacionados à gestão de incidentes cibernéticos. Cada questão do formulário deverá ser respondida considerando o estágio atual de implementação na instituição, utilizando os seguintes critérios:

0 – Não implementado: A prática ou controle não existe na organização, nem está em fase de planejamento.

1 – Menor parte implementado: A prática está em fase inicial, restrita a ações isoladas, pilotos ou iniciativas informais, sem cobertura significativa.

2 – Parcialmente implementado: Existem processos ou controles formalizados, porém aplicados de forma limitada, com cobertura parcial, inconsistências ou falhas relevantes.

3 – Maior parte implementado: A maior parte dos requisitos está implantada e operacionalizada, abrangendo boa parte da organização, embora ainda existam pontos de melhoria ou lacunas pontuais.

4 – Totalmente implementado: A prática ou controle está completamente implementado, institucionalizado e aplicado de forma consistente em toda a organização, com monitoramento contínuo, revisão periódica e melhoria contínua.

O cálculo da maturidade geral é obtido por meio da média aritmética das pontuações atribuídas às questões, resultando na classificação do nível de maturidade, conforme apresentado na Tabela**,** Classificação dos Níveis de Maturidade.

Tabela IV – Classificação dos Níveis de Maturidade.

Média	Nível de Maturidade	Descrição
0,00 – 0,99	**Não implementado**	**Práticas não implementadas. Alto risco institucional.**
1,00 – 1,99	**Parcialmente implementado**	**Implementação muito limitada, sem processos padronizados.**
2,00 – 2,99	**Implementado**	**Controles aplicados de forma ilimitada, com falhas ou lacunas significativas.**
3,00 – 3,49	**Gerenciado**	**A maioria dos controles está implementada, com pontos pontuais de melhoria**
3,50 – 4,00	**Otimizado**	**Práticas consolidadas, monitoradas e sujeitas a melhoria contínua**

B. Questionário

Este questionário visa avaliar o nível de maturidade da sua instituição pública federal na gestão de incidentes cibernéticos, conforme as diretrizes definidas no PLANGIC [9].

1) Atividades Preparatórias

Avalia a existência de governança, infraestrutura e processos básicos necessários para suportar a gestão de incidentes.

1.1 A instituição possui um gestor formalmente designado para segurança da informação?

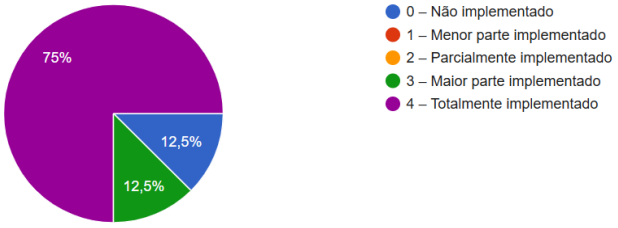


Fig. 9. Gestor de Segurança Designado

O gráfico da Figura 6 refere-se ao item 1.1 – **"A instituição possui um gestor formalmente designado para Segurança da Informação?"** Apresenta 8 respostas válidas e evidencia um elevado grau de implementação desse controle entre as instituições analisadas.

Os resultados indicam que:

- **75%** das instituições classificaram o controle como **totalmente implementado**, o que demonstra que a designação formal do gestor de Segurança da Informação encontra-se institucionalizada e operacionalizada na maior parte da amostra.
- Além disso, **12,5%** informaram que a **maior parte do controle está implementada**, indicando estágio avançado de adoção, ainda que com possíveis lacunas residuais.
- Por outro lado, **12,5%** declararam que o **controle não está implementado**, evidenciando ausência de formalização dessa função em parte das instituições respondentes.

A **média ponderada** obtida para o item foi de **3,37**, enquadrando o controle no nível de **maturidade Gerenciado**, conforme a escala adotada.

1.2 A instituição possui ETIR ou estrutura equivalente formalmente instituída e implementada?

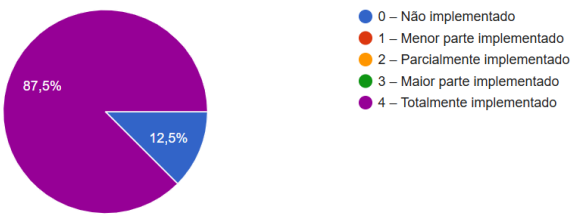


Fig. 10. Estrutura da ETIR

O gráfico da Figura 10 refere-se ao item 1.2 – "A instituição possui ETIR ou estrutura equivalente formalmente instituída e implementada?" ilustra e evidencia elevado grau de implementação desse controle entre as instituições analisadas.

Os resultados indicam que **87,5%** das instituições classificaram o **controle como totalmente implementado**, o que demonstra que a **Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR**, ou estrutura equivalente, encontra-se formalmente instituída e operacionalizada na maior parte da amostra. Por outro lado, **12,5%** declararam que o **controle não está implementado**, evidenciando ausência de estrutura formal de tratamento e resposta a incidentes em parte das instituições respondentes. Com base na escala de classificação adotada, a **média 3,50** enquadra o **controle no nível de maturidade Otimizado.**

1.3 Existe documento formal instituindo a ETIR, contendo atribuições e escopo de atuação?

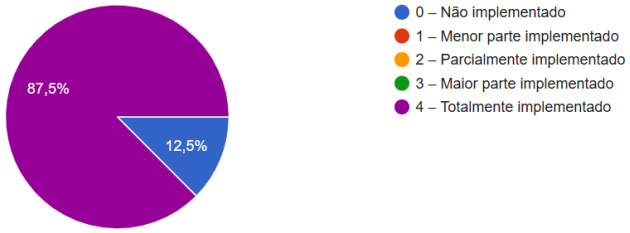


Fig.11. Formalização da ETIR

O gráfico referente ao item **1.3 – "Existe documento formal instituindo a ETIR, contendo atribuições e escopo de atuação?"** Apresenta **8 respostas válidas** e demonstra elevado grau de formalização desse controle entre as instituições analisadas. Os dados indicam que **87,5%** das instituições classificaram a prática como **totalmente implementada**, enquanto **12,5%** informaram que o controle ainda **não foi implementado**.

A média ponderada obtida foi de **3,50**, enquadrando o item no nível de maturidade **Otimizado**, conforme a escala adotada. Esse resultado evidencia que a maior parte das instituições possui instrumento formal de instituição da ETIR ou estrutura equivalente, com definição de atribuições e escopo de atuação. Entretanto, a presença de respostas no nível **"não implementado"** revela lacunas pontuais de governança, que podem comprometer a clareza das responsabilidades institucionais e a efetividade dos processos de tratamento e resposta a incidentes cibernéticos

1.4 O ponto focal institucional foi informado formalmente ao CTIR Gov / órgão competente?

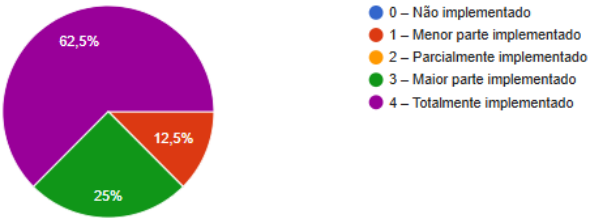


Fig.11 Ponto focal institucional

O gráfico referente ao item 1.4 – "O ponto focal institucional foi informado formalmente ao CTIR Gov / órgão competente?" Apresenta 8 respostas válidas e indica um grau relevante de implementação do controle. Os dados mostram que 62,5% das instituições classificaram a prática como totalmente implementada, 25% informaram que a maior parte está implementada e 12,5% indicaram que a prática está em menor parte implementada. A média ponderada obtida foi de **3,38**, enquadrando o item no nível de maturidade **Gerenciado**, conforme a escala adotada. Esse resultado demonstra que a formalização do ponto focal institucional junto ao CTIR Gov ou órgão competente está implementada na maior parte das instituições analisadas, embora ainda existam lacunas pontuais relacionadas à consolidação e padronização desse processo de comunicação institucional.

1.5 Existe processo de mapeamento de ativos de segurança da informação?

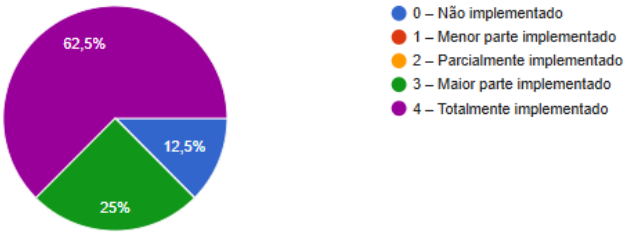


Fig.13. Mapeamento de ativos de SI

O gráfico referente ao item 1.5 – **"Existe processo de mapeamento de ativos de segurança da informação?"** Apresenta 8 respostas válidas e os dados indicam que **62,5%** das instituições classificaram a prática como **totalmente implementada**, **25%** informaram que a **maior parte do controle está implementada** e **12,5%** declararam que o **controle não está implementado.** A média ponderada obtida foi de 3,25, enquadrando o item no nível de maturidade Gerenciado.

1.6 Existe processo de gestão de riscos de segurança da informação?

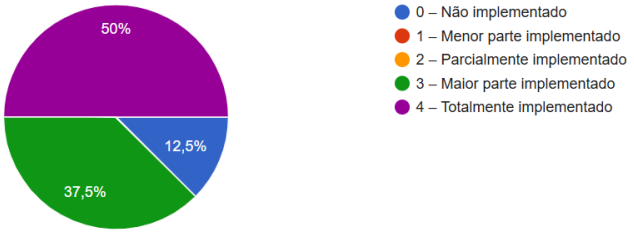


Fig.14. Gestão de riscos de SI

O gráfico referente ao item 1.6 - **"Existe processo de gestão de riscos de segurança da informação?"** Apresenta 8 respostas válidas e indica um **grau elevado de implementação** desse controle entre as instituições analisadas. Os dados demonstram que **50%** das instituições classificaram a prática como **totalmente implementada**, **37,5%** informaram que a **maior parte do controle está implementada** e **12,5%** declararam que o **controle não está implementado.**

A média ponderada do item foi de 3,25, classificando-o no nível de maturidade Gerenciado, conforme a escala definida na pesquisa. Esse resultado indica que o processo de gestão de riscos de segurança da informação está majoritariamente implementado nas instituições analisadas, com evidências de adoção operacional do controle; contudo, ainda não alcança o nível Otimizado.

1.7 Existe processo de continuidade de negócios relacionado à segurança da informação?

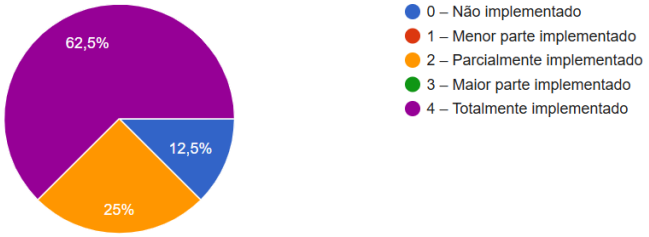


Fig.15. Processo de continuidade de negócios

O gráfico referente ao item 1.7 – "Existe processo de continuidade de negócios relacionado à segurança da informação?" Apresenta 8 respostas válidas e indica predominância de implementação avançada do controle.

Os dados mostram que 62,5% das instituições classificaram a prática como totalmente implementada, 25% como parcialmente implementada e 12,5% como não implementada.

A média ponderada do item foi de 3,00, classificando-o no nível de maturidade Gerenciado. O resultado indica implementação predominante do processo de continuidade de negócios associado à segurança da informação, embora ainda existam lacunas de formalização, abrangência e integração com as práticas institucionais de resiliência e resposta a incidentes.

1.8 Existe processo de gestão de mudanças com análise de impactos de segurança?

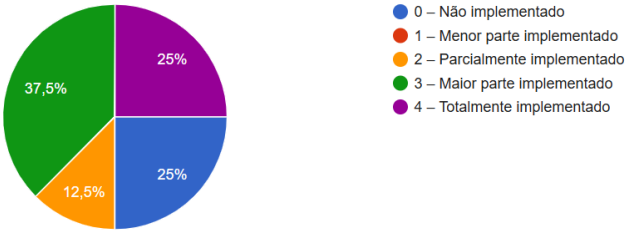


Fig.16. Processo de gestão de mudanças

O gráfico referente ao item 1.8 - **"Existe processo de gestão de mudanças com análise de impactos de segurança?"** Apresenta 8 respostas válidas e demonstra distribuição mais heterogênea em relação aos itens anteriores. Os dados indicam que 25% das instituições classificaram a prática como totalmente implementada, 12,5% como maior parte implementada, 37,5% como parcialmente implementada e 25% como não implementada.

A média ponderada do item foi de 2,13, classificando-o no **nível de maturidade implementado**. O resultado indica que o processo de gestão de mudanças com análise de impactos de segurança existe em parte das instituições analisadas, porém ainda apresenta limitações relevantes de formalização, abrangência e consistência operacional, especialmente pela concentração de respostas nos níveis "parcialmente implementado" e "não implementado".

1.9 A instituição possui infraestrutura mínima (equipe, ferramentas e recursos) para prevenção, detecção, tratamento e resposta?

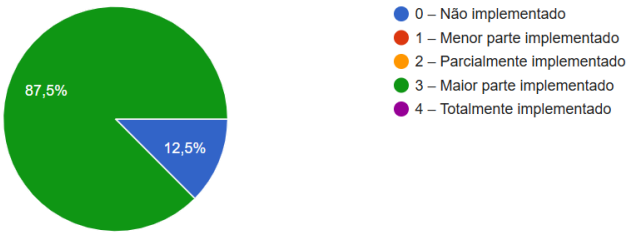


Fig.17. Infraestrutura mínima

O gráfico referente ao item 1.9 – "A instituição possui infraestrutura mínima, equipe, ferramentas e recursos para prevenção, detecção, tratamento e resposta?" Apresenta 8 respostas válidas e indica elevado grau de implementação desse controle. Os dados mostram que 87,5% das instituições classificaram a prática como totalmente implementada, enquanto 12,5% declararam que o controle não está implementado.

A média ponderada do item foi de 3,50, classificando-o no nível de maturidade Otimizado. O resultado evidencia que a maior parte das instituições analisadas dispõe de infraestrutura mínima para apoiar as capacidades de prevenção, detecção, tratamento e resposta a incidentes cibernéticos; contudo, a existência de resposta no nível "não implementado" indica lacuna pontual que pode comprometer a capacidade operacional de resposta em parte da amostra.

2) Prevenção

Avalia a adoção de medidas preventivas que visam reduzir a probabilidade de ocorrência de incidentes. PLANGIC [9]

2.1 A instituição definiu e implementou controles preventivos tecnológicos, organizacionais e físicos?

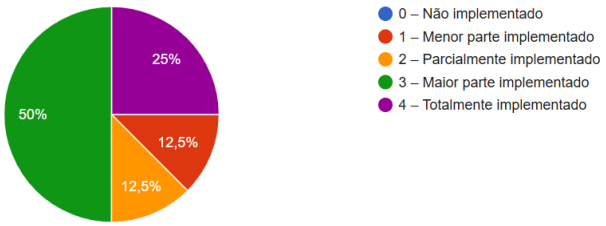


Fig.18. Controles preventivos

O gráfico referente ao item 2.1 – "A instituição definiu e implementou controles preventivos tecnológicos, organizacionais e físicos?" Apresenta 8 respostas válidas e indica predominância de implementação avançada do controle. Os dados mostram que 25% das instituições classificaram a prática como totalmente implementada, 50% como maior parte implementada, 12,5% como parcialmente implementada e 12,5% como menor parte implementada.

A média ponderada do item foi de 2,88, classificando-o no nível de maturidade implementado. O resultado indica que os controles preventivos tecnológicos, organizacionais e físicos estão presentes na maior parte das instituições analisadas, embora ainda existam lacunas de padronização, abrangência e consolidação operacional para que esse controle alcance níveis superiores de maturidade.

2.2 Existe processo estruturado de gerenciamento de vulnerabilidades?

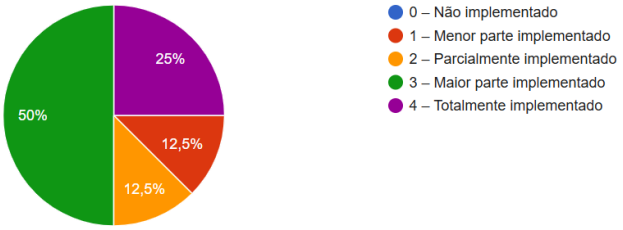


Fig.19. Gerenciamento de vulnerabilidades

O gráfico referente ao item 2.2 – "Existe processo estruturado de gerenciamento de vulnerabilidades?" Apresenta 8 respostas válidas e indica implementação intermediária a avançada do controle. Os dados mostram que 12,5% das instituições classificaram a prática como totalmente implementada, 50% como maior parte implementada, 25% como parcialmente implementada e 12,5% como menor parte implementada.

A média ponderada do item foi de 2,63, classificando-o no nível de maturidade implementado. O resultado indica que o gerenciamento de vulnerabilidades está presente na maioria das instituições analisadas, porém ainda apresenta limitações quanto à estruturação, padronização e cobertura do processo, o que impede sua classificação em níveis mais elevados de maturidade.

2.3 Existe rotina de aplicação de patches e correções críticas?

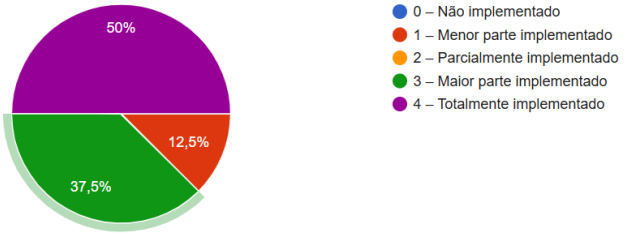


Fig.20. Patches e correções críticas

O gráfico referente ao item 2.3 – "Existe rotina de aplicação de patches e correções críticas?" Apresenta 8 respostas válidas e indica predominância de implementação avançada do controle. Os dados mostram que 37,5% das instituições classificaram a prática como totalmente implementada, 50% como maior parte implementada e 12,5% como parcialmente implementada.

A média ponderada foi de 3,25, classificando o item no nível Gerenciado. O resultado indica que a aplicação de patches e correções críticas está majoritariamente implementada, mas ainda requer aprimoramentos em padronização, tempestividade e monitoramento contínuo.

2.4 Os backups são executados regularmente e protegidos?

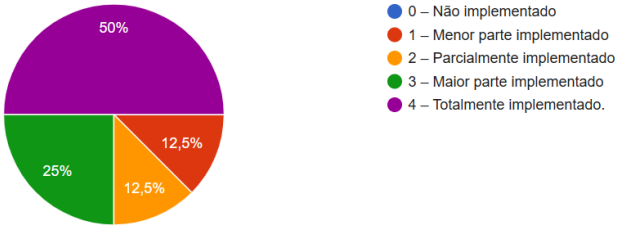


Fig.21. execução regular de backups

O gráfico referente ao item 2.4 – "Os backups são executados regularmente e protegidos?" Apresenta 8 respostas válidas e revela que a maior concentração de respostas está no nível parcialmente implementado, representando 50% da amostra, seguida por 25% das instituições que indicaram a maior parte implementada. Apenas 12,5% classificaram a prática como totalmente implementada, enquanto outros 12,5% informaram que o controle está em menor parte implementado.

A média ponderada do item foi de 2,38, classificando-o no nível de maturidade implementado. O resultado indica que os backups estão presentes nas instituições analisadas, mas ainda carecem de consolidação, especialmente quanto à regularidade, proteção, padronização e validação das rotinas.

2.5 O controle de acesso utiliza mecanismos seguros (*MFA*, privilégio mínimo e revisão periódica)?

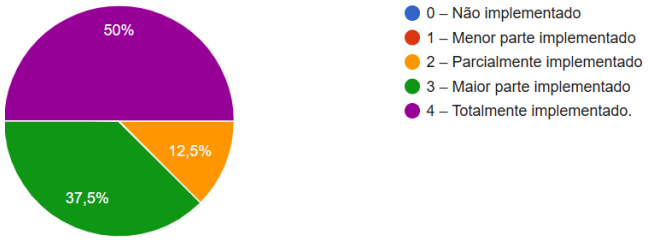


Fig.22. controle de acesso

O gráfico referente ao item 2.5 – "O controle de acesso utiliza mecanismos seguros (MFA, privilégio mínimo e revisão periódica)?" Apresenta 8 respostas válidas e indica predominância de implementação avançada do controle. Os dados mostram que 37,5% das instituições classificaram a prática como totalmente implementada, 50% como maior parte implementada e 12,5% como parcialmente implementada.

A média ponderada foi de **3,25**, classificando o item no nível **Gerenciado**. O resultado indica que o controle de acesso está majoritariamente implementado, mas ainda requer aprimoramentos na adoção de MFA, no princípio do menor privilégio e na revisão periódica dos acessos.

2.6 A instituição realiza ações contínuas de conscientização em segurança cibernética?

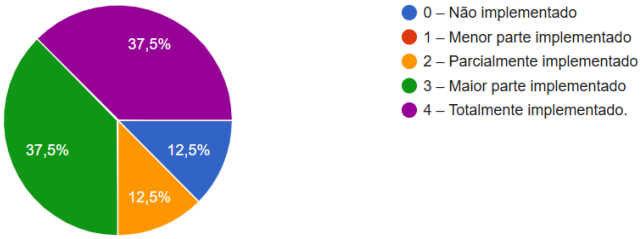


Fig.23. Conscientização em segurança cibernética

O gráfico referente ao item 2.6 – "A instituição realiza ações contínuas de conscientização em segurança cibernética?" Apresenta 8 respostas válidas e indica distribuição concentrada em níveis intermediários de implementação. Os dados mostram que 37,5% das instituições classificaram a prática como maior parte implementada, 37,5% como parcialmente implementada, 12,5% como totalmente implementada e 12,5% como não implementada.

A média ponderada do item foi de 2,50, classificando-o no nível de maturidade implementado. O resultado indica que ações de conscientização em segurança cibernética estão presentes na maioria das instituições analisadas, mas ainda carecem de maior continuidade, padronização e institucionalização para alcançar níveis superiores de maturidade.

2.7 Equipes técnicas recebem capacitação periódica em segurança cibernética?

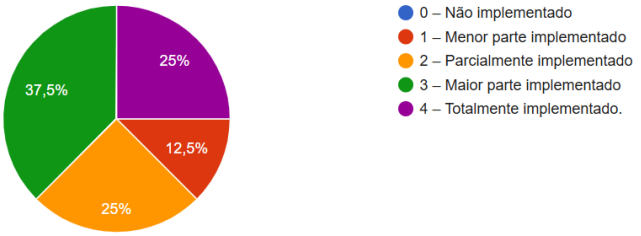


Fig.24. Capacitação da equipe técnica

O gráfico referente ao item 2.7 – "Equipes técnicas recebem capacitação periódica em segurança cibernética?" Apresenta 8 respostas válidas e indica concentração em níveis intermediários e avançados de implementação. Os dados mostram que 25% das instituições classificaram a prática como totalmente implementada, 37,5% como maior parte implementada, 25% como parcialmente implementada e 12,5% como não implementada.

A média ponderada do item foi de 2,63, classificando-o no nível de maturidade implementado. O resultado indica que a capacitação periódica das equipes técnicas em segurança cibernética ocorre na maior parte das instituições analisadas, mas ainda demanda maior regularidade, padronização e institucionalização para fortalecer a capacidade técnica de prevenção, detecção e resposta a incidentes.

3) Detecção

Analisa a capacidade da instituição em monitorar ambientes e detectar eventos de segurança. PLANGIC [9]

3.1 A instituição realiza monitoramento contínuo dos ativos críticos?

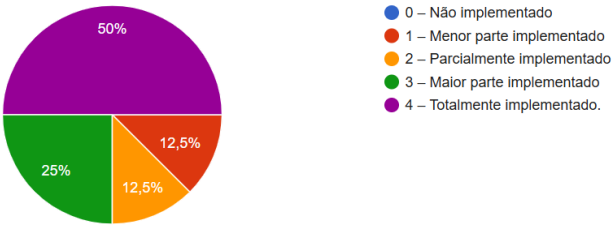


Fig.25. Monitoramento contínuo dos ativos críticos

O item 3.1 apresenta 8 respostas válidas e indica implementação majoritariamente avançada do monitoramento contínuo dos ativos críticos, com 50% das instituições no nível totalmente implementado e 25% com a maior parte implementada. Apesar desse resultado positivo, as respostas nos níveis parcialmente implementado e menor parte implementado, ambas com 12,5%, demonstram variações de maturidade e lacunas na execução do controle.

A média ponderada foi de 3,13, classificando o item no nível de maturidade Gerenciado. O resultado indica que o monitoramento contínuo dos ativos críticos está majoritariamente implementado, embora ainda haja lacunas

de abrangência, padronização e continuidade no processo de detecção e acompanhamento de eventos de segurança.

3.2 Existem linhas de base definidas para identificar desvios de comportamento?

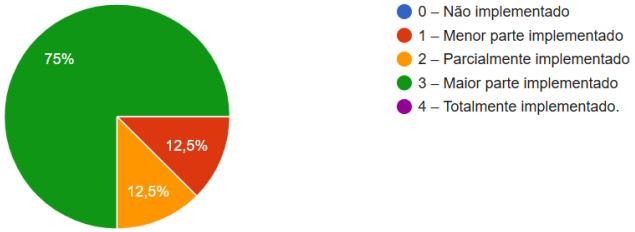


Fig.26. Linhas de base definidas

O item 3.2 apresentou 8 respostas válidas, com predominância do nível maior parte implementada (75%), seguido por 12,5% em parcialmente implementada e 12,5% em menor parte implementada. A média ponderada foi de 2,63, classificando o item no nível Implementado, o que indica que as linhas de base para identificação de desvios de comportamento existem na maioria das instituições, mas ainda demandam maior padronização e integração aos processos de monitoramento e detecção.

3.3 Logs de segurança são coletados, armazenados e analisados?

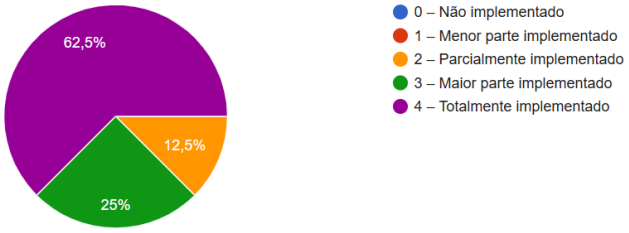


Fig.27. Logs de segurança

O gráfico referente ao item 3.3 – "Logs de segurança são coletados, armazenados e analisados?" Apresenta 8 respostas válidas e indica predominância de implementação avançada do controle. Os dados mostram que 62,5% das instituições classificaram a prática como totalmente implementada, 25% como maior parte implementada e 12,5% como não implementada.

A média ponderada foi de 3,25, classificando o item no nível Gerenciado. O resultado indica que a gestão de logs está majoritariamente implementada, embora lacunas pontuais ainda possam afetar a rastreabilidade, a detecção e a investigação de incidentes cibernéticos.

3.4 Ferramentas de segurança geram alertas acompanhados pela equipe responsável?

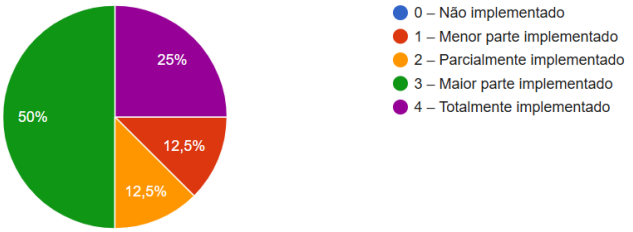


Fig.28. Ferramentas de segurança

3.5 Existe processo formalizado para comunicação de incidentes ao CTIR Gov e demais instâncias competentes?

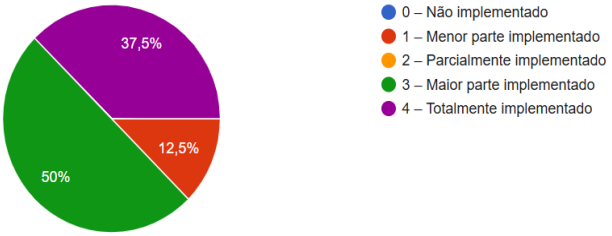


Fig.29. Comunicação de incidentes ao CTIR Gov

O gráfico referente ao item 3.5 – "Existe processo formalizado para comunicação de incidentes ao CTIR Gov e demais instâncias competentes?" Apresenta 8 respostas válidas e indica predominância de implementação avançada do controle. Os dados mostram que 50% das instituições classificaram a prática como totalmente implementada, 37,5% como maior parte implementada e 12,5% como não implementada.

A média ponderada foi de 3,13, classificando o item no nível Gerenciado. O resultado indica que a comunicação formal de incidentes ao CTIR Gov e demais instâncias competentes está majoritariamente implementada, embora ainda existam lacunas que podem afetar a tempestividade, a rastreabilidade e a conformidade do processo.

4) Tratamento de Incidentes

Verifica a existência e eficácia dos processos de triagem, análise e resposta aos incidentes. PLANGIC [9]

4.1 A instituição possui procedimento formal para registro e triagem inicial de incidentes?

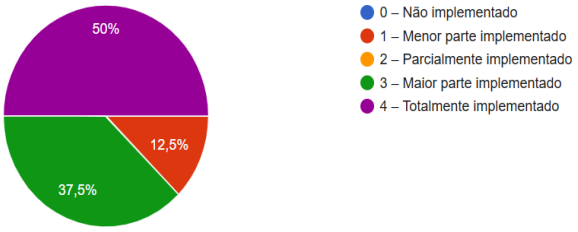


Fig.30. Registro e triagem inicial de incidentes

O item 4.1 apresentou 8 respostas válidas, com predominância de implementação avançada: 37,5% das instituições indicaram o controle como totalmente

implementado, 50% como maior parte implementado e 12,5% como não implementado.

A média ponderada foi de 3,00, classificando o item no nível Gerenciado, o que indica que o procedimento formal de registro e triagem inicial de incidentes está majoritariamente implementado, embora ainda existam lacunas pontuais que podem afetar a padronização, a rastreabilidade e a eficiência no tratamento inicial dos incidentes cibernéticos.

4.2 Os incidentes são classificados por impacto, urgência e criticidade?

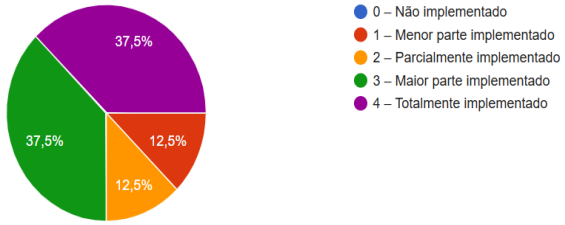


Fig.31. Classificação de incidentes

O item 4.2 – "Os incidentes são classificados por impacto, urgência e criticidade?" apresentou 8 respostas válidas, com distribuição concentrada em níveis intermediários: 37,5% das instituições classificaram o controle como parcialmente implementado, 37,5% como maior parte implementado, 12,5% como totalmente implementado e 12,5% como não implementado.

A média ponderada foi de 2,38, classificando o item no nível Implementado, o que indica que a classificação de incidentes existe na maior parte das instituições, mas ainda demanda maior padronização, formalização e consistência na aplicação dos critérios de impacto, urgência e criticidade.

4.3 Existem planos documentados para diferentes tipos de incidentes?

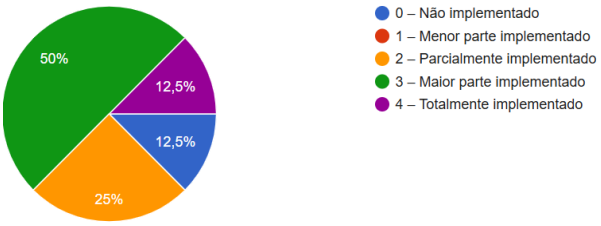


Fig.32. Planos de Incidentes documentados

O item 4.3 – "Existem planos documentados para diferentes tipos de incidentes?" apresentou 8 respostas válidas, com predominância de implementação avançada: 25% das instituições classificaram o controle como totalmente implementado, 50% como maior parte implementado, 12,5% como parcialmente implementado e 12,5% como não implementado.

A média ponderada foi de 2,75, classificando o item no nível Implementado, indicando que os planos documentados para diferentes tipos de incidentes estão presentes na maioria das instituições, mas ainda demandam maior padronização, cobertura e formalização para alcançar níveis mais elevados de maturidade.

4.4 As evidências técnicas são preservadas adequadamente durante a investigação?

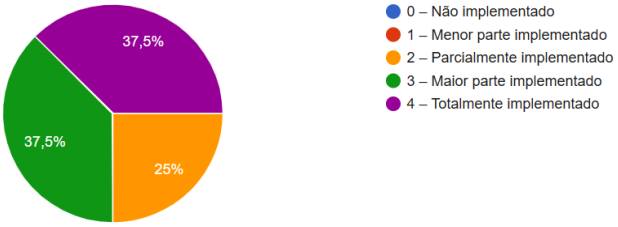


Fig.33. Preservação de Evidências Técnicas

O item 4.4 – "As evidências técnicas são preservadas adequadamente durante a investigação?" apresentou 8 respostas válidas, com concentração em níveis intermediários e avançados: 25% das instituições classificaram o controle como totalmente implementado, 37,5% como maior parte implementado e 37,5% como parcialmente implementado.

A média ponderada foi de 2,88, classificando o item no nível Implementado, indicando que a preservação de evidências técnicas durante a investigação de incidentes está presente nas instituições analisadas, mas ainda demanda maior padronização, formalização e consistência operacional para fortalecer a rastreabilidade, a integridade e a confiabilidade das evidências no processo de resposta a incidentes cibernéticos.

4.5 Há integração entre áreas técnicas, jurídica, comunicação e gestão quando necessário?

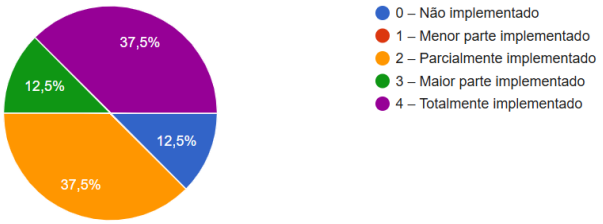


Fig.34. Integração entre as áreas

O item 4.5 – "Há integração entre áreas técnicas, jurídica, comunicação e gestão quando necessário?" apresentou 8 respostas válidas, com distribuição entre diferentes níveis de implementação: 37,5% das instituições classificaram o controle como totalmente implementado, 12,5% como maior parte implementado, 37,5% como parcialmente implementado e 12,5% como não implementado.

A média ponderada foi de 2,63, classificando o item no nível Implementado, o que indica que a integração entre áreas existe em parte relevante das instituições, mas ainda requer maior formalização, coordenação e padronização para fortalecer a atuação conjunta no tratamento de incidentes cibernéticos.

5) Resposta

Avalia a capacidade da instituição de coordenar ações reativas para minimizar impactos PLANGIC [9].

5.1 Existem procedimentos formais de contenção para limitar danos de incidentes em andamento?

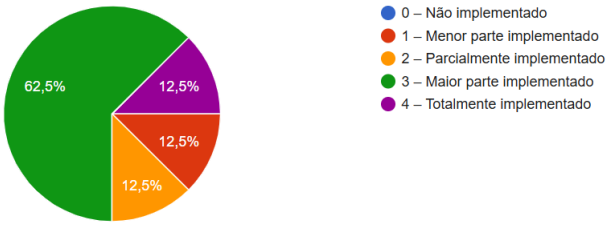


Fig.35. Procedimentos formais de contenção

O item 5.1 – "Existem procedimentos formais de contenção para limitar danos de incidentes em andamento?" apresentou 8 respostas válidas. A maior parte das instituições, equivalente a 62,5%, informou que o controle está com a maior parte implementada. Além disso, 12,5% classificaram a prática como totalmente implementada, 12,5% como parcialmente implementada e 12,5% como menor parte implementada.

A média ponderada foi de 2,75, classificando o item no nível Implementado. O resultado indica que os procedimentos de contenção existem na maioria das instituições, mas ainda requerem maior formalização, padronização e consolidação operacional para reduzir danos de forma consistente durante incidentes cibernéticos.

5.2 Existem procedimentos formais de erradicação para remoção de ameaças e artefatos maliciosos?

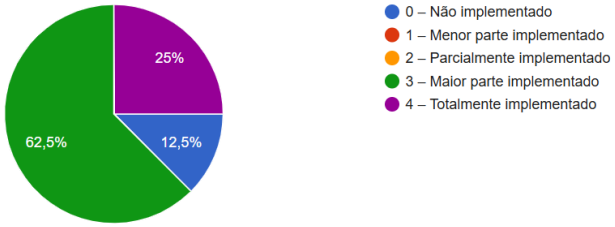


Fig.36. Procedimentos formais de erradicação

O item 5.2 – "Existem procedimentos formais de erradicação para remoção de ameaças e artefatos maliciosos?" Apresentou 8 respostas válidas, com predominância do nível maior parte implementado (62,5%), seguido por 25% em parcialmente implementado e 12,5% em menor parte implementado.

A média ponderada foi de 2,50, classificando o item no nível de maturidade Implementado, o que indica que os procedimentos de erradicação estão presentes na maioria das instituições, embora ainda demandem maior formalização, padronização e consolidação operacional para garantir a remoção consistente de ameaças e artefatos maliciosos após a contenção de incidentes cibernéticos.

5.3 Existem procedimentos formais de recuperação para restabelecimento seguro do ambiente?

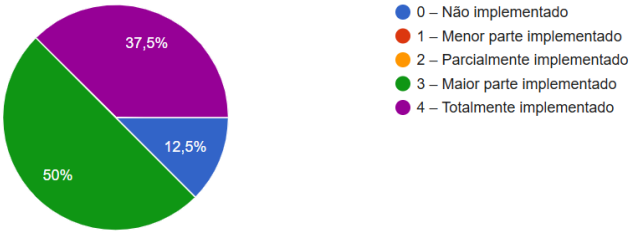


Fig.37. Procedimentos formais de recuperação

O item 5.3 – "Existem procedimentos formais de recuperação para restabelecimento seguro do ambiente?" Apresentou 8 respostas válidas, com predominância do nível maior parte implementado (50%), seguido por 37,5% em totalmente implementado e 12,5% em não implementado.

A média ponderada foi de 3,13, classificando o item no nível de maturidade Gerenciado, o que indica que os procedimentos de recuperação estão majoritariamente implementados, embora ainda existam lacunas pontuais que podem comprometer o restabelecimento seguro e consistente do ambiente após incidentes cibernéticos.

5.4 Serviços críticos possuem prioridade definida para restauração?

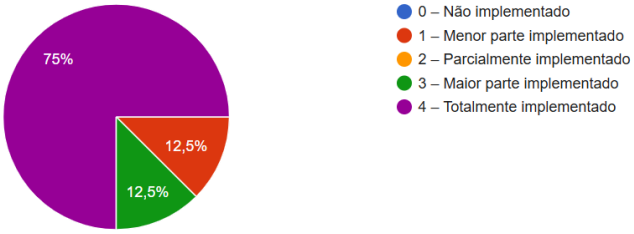


Fig.38. Procedimentos em Serviços críticos

O item 5.4 – "Serviços críticos possuem prioridade definida para restauração?" Apresentou 8 respostas válidas, com predominância do nível totalmente implementado (75%), seguido por 12,5% em maior parte implementado e 12,5% em menor parte implementado.

A média ponderada foi de 3,50, classificando o item no nível de maturidade Otimizado, o que indica que a priorização de serviços críticos para restauração está amplamente consolidada na maioria das instituições, embora ainda exista lacuna pontual de formalização ou aplicação integral do controle em parte da amostra.

5.5 A alta administração é comunicada tempestivamente em incidentes críticos?

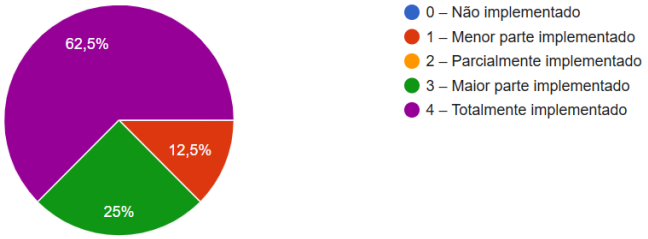


Fig.39. Procedimentos em Incidentes críticos

O item 5.5 – "A alta administração é comunicada tempestivamente em incidentes críticos?" Apresentou 8 respostas válidas, com predominância do nível maior parte implementado (62,5%), seguido por 25% em totalmente implementado e 12,5% em não implementado.

A média ponderada foi de 2,88, classificando o item no nível de maturidade Implementado, o que indica que a comunicação tempestiva à alta administração em incidentes críticos ocorre na maioria das instituições, embora ainda demande maior formalização, padronização e garantia de acionamento oportuno nos processos de resposta a incidentes cibernéticos.

5.6 São realizados testes periódicos dos planos de resposta?

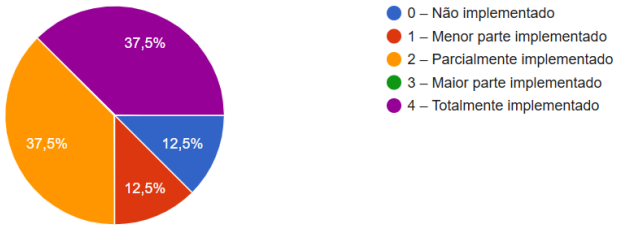


Fig.40. Procedimentos em Planos de Resposta

O item 5.6 – "São realizados testes periódicos dos planos de resposta?" Apresentou 8 respostas válidas, com 37,5% das instituições indicaram o controle como parcialmente implementado e 37,5% como maior parte implementado. Além disso, 12,5% declararam o controle totalmente implementado e 12,5% não implementado.

A média ponderada foi de 2,38, classificando o item no nível Implementado, o que indica que os testes dos planos de resposta existem em parte relevante das instituições, mas ainda precisam de maior regularidade, formalização e padronização para validar a efetividade da resposta a incidentes cibernéticos.

6) Pós-Incidente

Analisa as práticas voltadas ao aprendizado e à melhoria contínua após a resolução de incidentes. PLANGIC [9]

6.1 São realizadas análises pós-incidente para identificar causa raiz, impactos e oportunidades de melhoria?

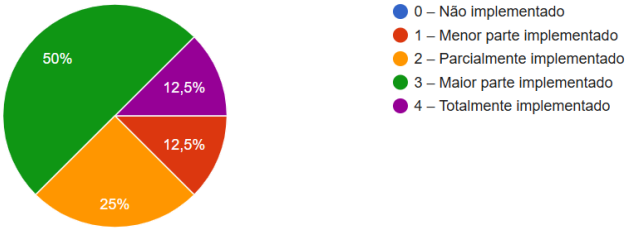


Fig.41. Procedimentos em Análises pós-incidente

O item 6.1 – "São realizadas análises pós-incidente para identificar causa raiz, impactos e oportunidades de melhoria?" Apresentou 8 respostas válidas, com predominância do nível maior parte implementado (50%), seguido por 25% em totalmente implementado, 12,5% em parcialmente implementado e 12,5% em não implementado.

A média ponderada foi de 2,75, classificando o item no nível Implementado. O resultado indica que as análises pós-incidente ocorrem na maioria das instituições, mas ainda requerem maior formalização, padronização e aplicação sistemática para fortalecer a identificação de causa raiz e a melhoria contínua da resposta a incidentes cibernéticos.

6.2 A instituição atualiza políticas, controles e procedimentos com base nas lições aprendidas?

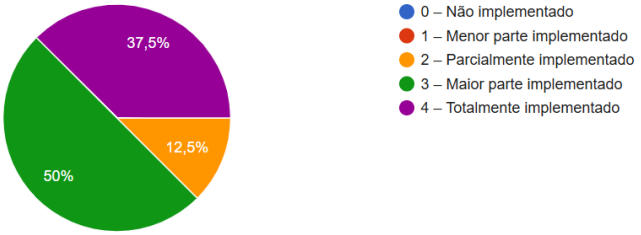


Fig.42. Políticas, controles e procedimentos com base nas lições aprendidas

O item 6.2 – "A instituição atualiza políticas, controles e procedimentos com base nas lições aprendidas?" Apresentou 8 respostas válidas, com predominância de totalmente implementado (50%), seguido por maior parte implementado (37,5%) e não implementado (12,5%).

A média ponderada foi de 3,13, classificando o item no nível Gerenciado, indicando que a atualização de políticas, controles e procedimentos a partir das lições aprendidas está majoritariamente implementada, embora ainda existam lacunas pontuais para consolidar a melhoria contínua no ciclo pós-incidente.

6.3 Existe processo formal para elaboração e envio de relatório pós-incidente ao CTIR Gov, quando aplicável?

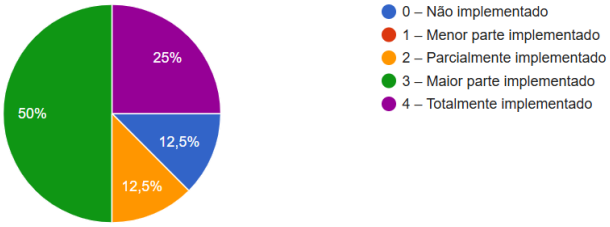


Fig.43. Elaboração e envio de relatório pós-incidente ao CTIR Gov

O item 6.3 – "Existe processo formal para elaboração e envio de relatório pós-incidente ao CTIR Gov, quando aplicável?" Apresentou 8 respostas válidas, com predominância de maior parte implementado (50%), seguido por parcialmente implementado (25%), totalmente implementado (12,5%) e não implementado (12,5%).

A média ponderada foi de 2,50, classificando o item no nível Implementado, indicando que o processo de relatório pós-incidente ao CTIR Gov existe na maioria das instituições, mas ainda requer maior formalização, padronização e consistência para assegurar conformidade, rastreabilidade e melhoria contínua no ciclo pós-incidente

6.4 Indicadores e métricas de incidentes são acompanhados pela gestão?

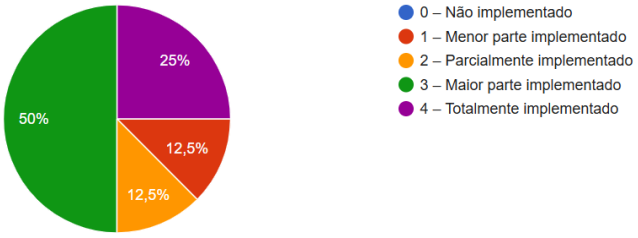


Fig.44. Indicadores e métricas de incidentes

O item 6.4 – "Indicadores e métricas de incidentes são acompanhados pela gestão?" Apresentou 8 respostas válidas, com predominância de maior parte implementado (50%), seguido por parcialmente implementado (25%), totalmente implementado (12,5%) e não implementado (12,5%).

A média ponderada foi de 2,50, classificando o item no nível Implementado, indicando que o acompanhamento de indicadores e métricas de incidentes ocorre na maioria das instituições, mas ainda requer maior padronização, regularidade e uso gerencial para apoiar a melhoria contínua da gestão de incidentes cibernéticos.

6.5 Incidentes anteriores são utilizados para aperfeiçoar treinamentos e controles?

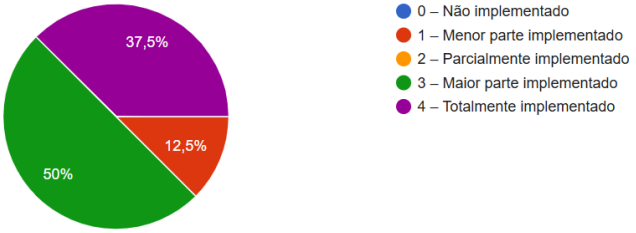


Fig.45. Incidentes anteriores são utilizados para aperfeiçoar treinamentos e controles

O item 6.5 – "Incidentes anteriores são utilizados para aperfeiçoar treinamentos e controles?" Apresentou 8 respostas válidas, com predominância de totalmente implementado (50%), seguido por maior parte implementado (37,5%) e não implementado (12,5%).

A média ponderada foi de 3,13, classificando o item no nível Gerenciado, indicando que o uso de incidentes anteriores para aprimorar treinamentos e controles está majoritariamente implementado, embora ainda existam lacunas pontuais para consolidar a retroalimentação sistemática do processo de melhoria contínua em segurança cibernética.

C. Aplicação e Relevância do Instrumento

O instrumento de avaliação foi desenvolvido para diagnóstico do nível de maturidade das instituições públicas federais na gestão de incidentes cibernéticos, atendendo às exigências do PLANGIC e da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD). A sua aplicação periódica permite às organizações:

- Mapear lacunas e fragilidades no seu processo de gestão de incidentes.
- Priorizar investimentos e alocar recursos de forma mais eficiente.
- Promover a evolução contínua dos processos de segurança da informação.
- Fortalecer sua resiliência cibernética e seu alinhamento às diretrizes da REGIC.

VI. MODELO PROPOSTO

Este artigo realizou a adaptação do Ciclo de Vida de um Incidente da norma ISO/IEC 27035 [8] às diretrizes do PLANGIC, considerando o que estabelece a Portaria DSI/GSI/PR nº 120/2022 [9], bem como os princípios e práticas operacionais exigidos na REGIC.

A. Modelo Operacional de Gestão de Incidentes Cibernéticos (Adaptado ao PLANGIC + ISO/IEC 27035)

O Ciclo de Vida de um Incidente, no contexto da Administração Pública Federal, é estruturado para estar em total alinhamento com o PLANGIC [9], mantendo coerência com as boas práticas internacionais descritas na ISO/IEC 27035 [8].

Fig. 46 - Ciclo de Vida – Modelo Proposto

O modelo proposto, relembrado na Figura 41, garante a adoção de processos coordenados, colaborativos e orientados à resposta eficaz, conforme a atuação exigida no âmbito da REGIC e das diretrizes nacionais de segurança cibernética.

1) Planejamento e Preparação

Esta fase estabelece a base para uma gestão eficiente de incidentes cibernéticos. As atividades incluem:

I. Formalização da ETIR, por meio de ato administrativo.
II. Elaboração e manutenção do **Plano de Gerenciamento de Incidentes Cibernéticos (PGIC)**, alinhado às diretrizes da REGIC e do PLANGIC.
III. Definição dos processos operacionais, fluxos de trabalho e responsabilidades da ETIR.
IV. Mapeamento de ativos críticos, dados sensíveis e serviços essenciais.
V. Seleção, aquisição e configuração de ferramentas de monitoramento, detecção e resposta.
VI. Estabelecimento de canais de comunicação internos e externos, incluindo integração formal com o CTIR Gov e a REGIC.
VII. Realização de treinamentos e capacitações periódicas.

2) Detecção e Notificação

Esta etapa visa identificar e registrar rapidamente os incidentes, incluindo:

I. Monitoramento contínuo de ativos, redes e serviços.
II. Identificação de eventos suspeitos que possam representar ameaças.
III. Validação dos eventos para confirmação como incidente.
IV. Registro formal no sistema de gestão de incidentes.
V. Classificação preliminar do incidente (ex.: *ransomware*, vazamento de dados, DDoS).
VI. Notificação obrigatória e tempestiva aos órgãos competentes, como CTIR Gov, conforme diretrizes da REGIC e do PGIC.
VII. Comunicação interna às áreas impactadas e, quando aplicável, à ANPD.

3) *Avaliação e Classificação*

A avaliação permite entender a gravidade e orientar a resposta. As atividades incluem:

I. Análise da natureza do incidente (técnico, operacional, intencional, acidental).
II. Avaliação do impacto sobre ativos, serviços e a missão institucional.
III. Definição dos níveis de severidade e criticidade.
IV. Priorizar as ações de contenção e resposta.
V. Decidir sobre escalonamento para outras autoridades ou parceiros da REGIC.

4) *Resposta e Mitigação*

A fase de resposta concentra-se em restaurar a normalidade e mitigar danos. Inclui:

I. Ações imediatas de contenção para limitar a propagação do incidente.
II. Erradicação da ameaça, como remoção de malware ou isolamento de sistemas comprometidos.
III. Recuperação dos sistemas e serviços afetados.
IV. Preservação de evidências para suporte a auditorias, investigações e ações legais.
V. Manutenção de comunicação contínua com o CTIR Gov, parceiros e autoridades.
VI. Documentação das ações realizadas durante o tratamento do incidente.

5) Lições Aprendidas e Melhoria Contínua

Após a resolução, realiza-se uma análise para aprimorar continuamente a segurança. Inclui:

I. Condução de reunião de post-mortem para análise das causas e respostas aplicadas.
II. Identificação de falhas e oportunidades de melhoria nos processos e controles.
III. Atualização do PGIC, dos procedimentos operacionais e dos treinamentos.
IV. Implementação de novos controles preventivos e corretivos.
V. Elaboração de relatório final do incidente, com recomendações e plano de ação para mitigação futura.
VI. Comunicação das lições aprendidas ao CTIR Gov e às partes interessadas.

6) Disposições Finais

Este processo operacional deve ser revisado periodicamente, especialmente após a ocorrência de

incidentes significativos ou mudanças nas diretrizes da REGIC, do PLANGIC ou nos ativos críticos da organização. A sua correta aplicação é fundamental para assegurar a resiliência cibernética institucional e a proteção dos ativos e dados sob a guarda da organização.

B. *Fluxo de Processos e Procedimentos – Gestão de Incidentes Cibernéticos*

1) *Planejamento e Preparação:*

- **Ações:**

I. Formalizar a ETIR (publicação de portaria interna).
II. Elaborar e manter o Plano de Gerenciamento de Incidentes Cibernéticos - PGIC atualizado.
III. Mapear ativos críticos e dados sensíveis.
IV. Definir papéis, responsabilidades e matriz RACI.
V. Configurar ferramentas de monitoramento, detecção e comunicação.
VI. Estabelecer e testar canais com o CTIR Gov, ANPD e demais partes.
VII. Realizar treinamentos e simulações periódicas.

- **Saída:** Ambiente preparado, processos definidos e equipe capacitada.

Figura 47, ilustra o fluxo dos processos e procedimentos descritos na fase Planejamento e Preparação.

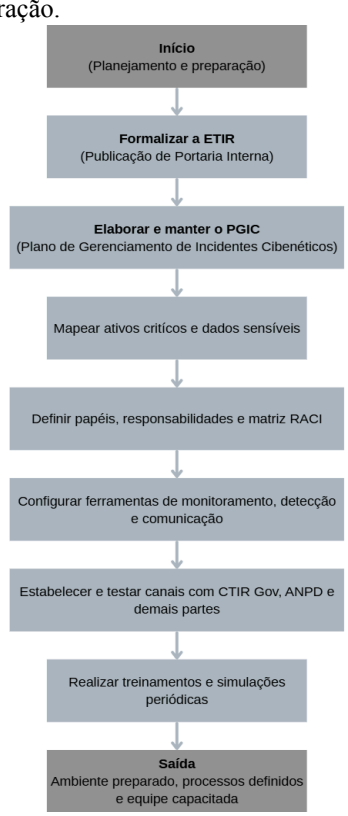


Fig. 47. Planejamento e Preparação (PLANGIC + ISO 27035)

2) *Detecção e Notificação*

- **Ações:**

- Monitoramento contínuo de ativos e redes.
- Detecção de evento suspeito.
- Validação técnica: é um incidente?
  - Não: Arquivar como evento.
  - Sim: Registrar como incidente.
- Classificação preliminar: tipo, severidade, impacto potencial.
- Notificação:
  - ✔ Interna: Áreas impactadas, alta gestão, responsáveis.
  - ✔ Externa: CTIR Gov (obrigatório), ANPD (quando envolver dados pessoais) e parceiros da REGIC, conforme necessidade.

- **Decisão:** Ativação dos procedimentos de resposta.

Figura 48, apresenta o fluxo dos processos e procedimentos descritos na fase 2. Detecção e Notificação.

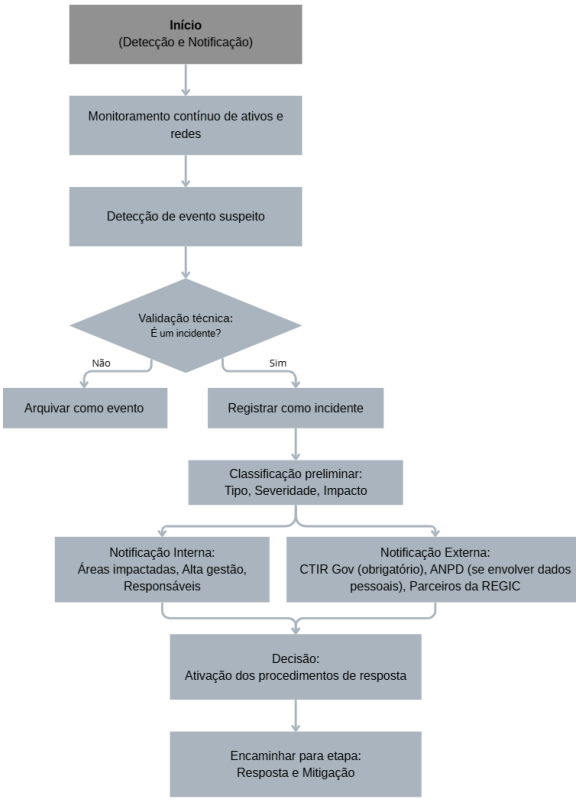


Fig. 48. Detecção e Notificação (PLANGIC + ISO 27035)

3) *Avaliação e Classificação*

 Ações:

- Avaliar a natureza do incidente (técnico, operacional, acidental ou intencional).
- Determinar impacto (dados, sistemas, serviços, operação institucional).
- Avaliar severidade (baixo, médio, alto, crítico).
- Definir prioridade da resposta.
- Verificar necessidade de escalonamento:
  - ✔ Autoridades superiores.
  - ✔ CTIR Gov e órgãos parceiros da REGIC.
  - ✔ Fornecedores e suporte externo especializado.

 Saída: Incidente avaliado, priorizado e pronto para resposta técnica.

Figura 49, apresenta o fluxo dos processos e procedimentos descritos na fase 3. Avaliação e Classificação.

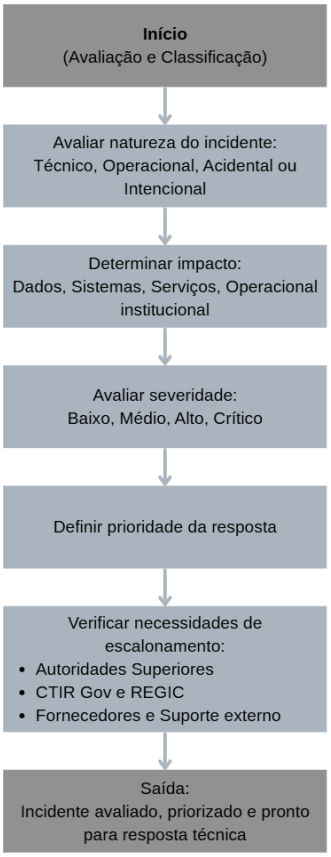


Fig. 49. Avaliação e Classificação (PLANGIC + ISO 27035)

4) Resposta e *Mitigação*

 Ações:

- Contenção:
  - ✔ Isolar sistemas afetados.
  - ✔ Desabilitar acessos comprometidos.

- Erradicação:
  - ✔ Remover malware, encerrar sessões suspeitas, corrigir vulnerabilidades.

- Recuperação:
  - ✔ Restaurar sistemas a partir de backups confiáveis.
  - ✔ Verificar integridade dos dados e dos sistemas.

- Preservação de Evidências:
  - ✔ Capturar logs, imagens forenses, relatórios técnicos.

- Comunicação contínua:
  - ✔ CTIR Gov, stakeholders internos, fornecedores e outras ETIRs da REGIC.

- Documentação de todas as ações realizadas.

 Saída: Incidente controlado e ambiente recuperado.

Figura 50, apresenta o fluxo dos processos e procedimentos descritos na fase 4. Resposta e Mitigação (PLANGIC + ISO 27035).

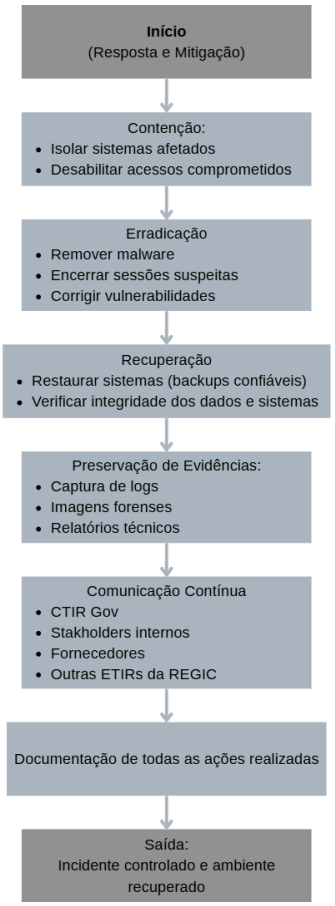


Fig. 50. Resposta e Mitigação (PLANGIC + ISO 27035)

5) Lições Aprendidas e Melhoria Contínua

 Ações:

- Realizar reunião de análise pós-incidente (post-mortem).

- Analisar causas raiz, falhas nos processos, controles ou respostas.
- Elaborar relatório técnico conclusivo.

- Atualizar:

  ✔ Plano de Gerenciamento de Incidentes Cibernéticos - PGIC.
  ✔ Procedimentos operacionais.
  ✔ Matriz de riscos.
  ✔ Plano de continuidade e resposta.

- Promover capacitação e treinamentos baseados no incidente.
- Compartilhar lições aprendidas com o CTIR Gov e, quando pertinente, com a REGIC.

 Saída: Organização mais preparada, processos aprimorados e risco de recorrência mitigado.

Figura 51, ilustra o fluxo dos processos e procedimentos descritos na fase 5. Lições Aprendidas e Melhoria Contínua

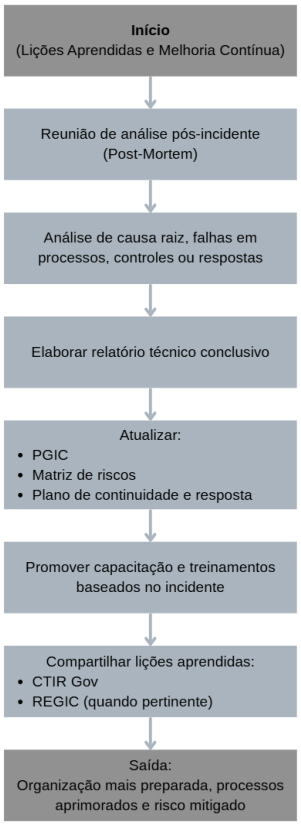


Fig. 51. Lições Aprendidas e Melhoria Contínua

Figura 52, ilustra o fluxo integrado dos processos e procedimentos do Modelo Proposto (PLANGIC + ISO 27035).

A Figura 52 ilustra o fluxo integrado do Modelo Proposto de gerenciamento de incidentes cibernéticos, estruturado de forma sequencial e cíclica.

O processo tem início na etapa de **planejamento e preparação**, que contempla a formalização da Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR), a atualização do Plano de Gerenciamento de Incidentes Cibernéticos, o mapeamento dos ativos institucionais, a definição das responsabilidades, a configuração das ferramentas de apoio, o estabelecimento dos canais de comunicação e a realização de treinamentos e simulações.

Essa etapa constitui a base organizacional, técnica e operacional necessária para que a instituição esteja preparada para detectar, analisar e responder adequadamente a eventos de segurança.

Na sequência, a fase de **detecção e notificação** é iniciada pelo monitoramento contínuo dos ambientes e ativos institucionais, permitindo a identificação de eventos suspeitos. Após a detecção, o evento é submetido a uma decisão inicial para verificar se apresenta características de incidente. Caso não seja confirmado, o evento é arquivado.

Quando confirmado, deve ser registrado como incidente e receber uma classificação preliminar, seguida da comunicação à ETIR e, quando aplicável, às autoridades e entidades competentes, como a Autoridade Nacional de Proteção de Dados, o CTIR Gov e os órgãos reguladores. Essa etapa assegura a rastreabilidade do incidente e o acionamento das estruturas responsáveis por sua gestão.

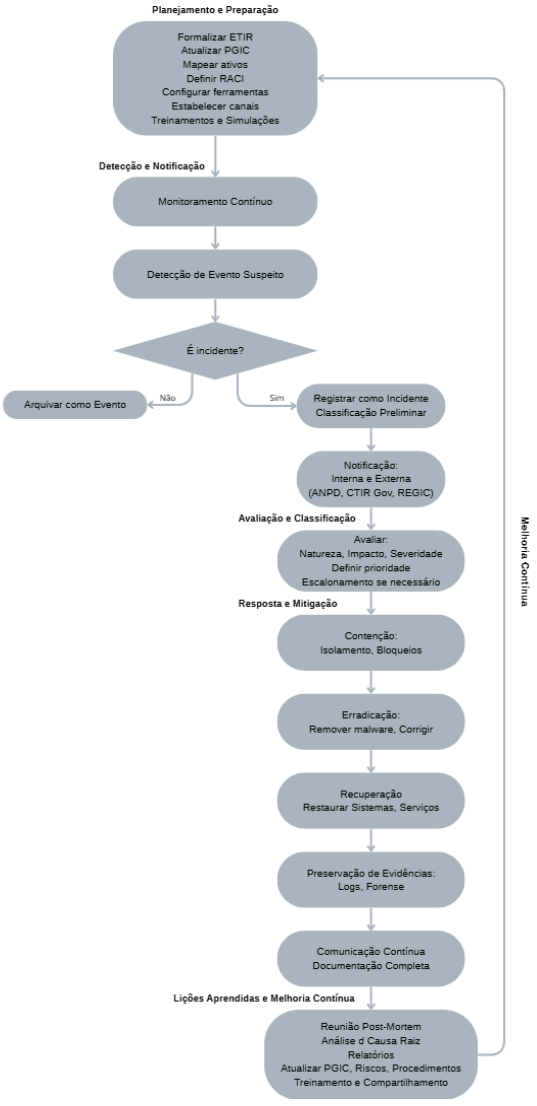


Fig. 52 Fluxo integrado do **Modelo Proposto** de gerenciamento de incidentes cibernéticos

A fase de **avaliação e classificação** compreende a análise da natureza, do impacto e da severidade do incidente, bem como a definição das prioridades de tratamento e a avaliação da necessidade de escalonamento.

Com base nessa avaliação, inicia-se a etapa de **resposta e mitigação**, composta por ações de contenção, como isolamento de ativos e bloqueio de acessos; erradicação, mediante a remoção de códigos maliciosos, vulnerabilidades ou outros elementos causadores; e recuperação dos sistemas e serviços afetados. Durante todo o processo, deve ser realizada a preservação de evidências digitais, incluindo registros de logs e informações forenses, de modo a subsidiar investigações, responsabilizações e análises posteriores.

O fluxo também prevê a manutenção de comunicação contínua e documentação completa, garantindo que as decisões, ações executadas, impactos e resultados sejam devidamente registrados e compartilhados com as partes interessadas.

Ao final do tratamento, a etapa de **lições aprendidas e melhoria contínua** inclui a realização de reunião pós-incidente, análise da causa raiz, registro das conclusões e atualização das políticas, procedimentos, riscos, controles e ações de capacitação. A retroalimentação do fluxo evidencia que o gerenciamento de incidentes não se encerra com a recuperação dos serviços, mas deve produzir aprendizado organizacional e aperfeiçoamento contínuo da capacidade institucional de prevenção e resposta.

VII. CONCLUSÃO

A proposta apresentada neste artigo responde à necessidade premente de modelos operacionais aplicáveis à realidade da APF no que diz respeito à gestão de incidentes cibernéticos.

A integração entre os princípios da norma ISO/IEC 27035 [8], as diretrizes do PLANGIC [9] e os requisitos legais da LGPD [10] resulta em um Modelo/framework, que contempla todas as fases do ciclo de vida de um incidente.

Ao alinhar práticas técnicas e normativas, o modelo contribui para o atendimento às exigências legais e o aprimoramento contínuo das políticas e processos institucionais de segurança da informação.

Este artigo também apresentou uma abordagem direcionada à avaliação do nível de maturidade das instituições públicas no gerenciamento de incidentes cibernéticos. Para esse fim, foi estruturado um instrumento prático de autoavaliação, cuja aplicação está prevista para etapas futuras da pesquisa.

Referências

[1] Zamfiroiu;Sharma."Cybersecurity Management for Incident Response" Romanian Cyber Security Journal, Spring 2022, No. 1 Vol. 4. Disponível em: https://rocys.ici.ro/documents/9/2022_spring_article_8.pdf.

[2] Courage Ojo et al., "Incident Response: A Structured Model from Detection to Containment and Recovery," World Journal of Advanced Research and Reviews 24(1):1401-1407, 2024. Disponível em: https://www.researchgate.net/publication/385382098.

[3] Ashley O'Neil et al., "Cybersecurity Incident Response in Organisations: A Meta-level Framework for Scenario-based Training," arXiv, Aug. 2021. Disponível em: https://arxiv.org/abs/2108.04996.

[4] L. S. Silva et al., "Towards an Incident Management Framework in Proprietary Software Ecosystems," arXiv preprint, Oct. 2024. Disponível em: https://arxiv.org/abs/2410.09320.

[5] ABRATE, Guia de Implementação do Framework de Segurança Cibernética, 2020. Disponível em: https://abrate.org.br/wp-content/uploads/2020/03/Guia-de-Implementacao-do-Framework-de-Seguranca-Cibernetica-ABRATE.pdf.

[6] PPSI, Secretaria de Governo Digital – MGI, Guia do Framework de Privacidade e Segurança da Informação, 2023. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf.

[7] NIST, National Institute of Standards and Technology, Computer Security Incident Handling Guide, NIST SP 800-61r3, 2025. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf

[8] ISO, ISO/IEC 27035-1:2023 — Tecnologia da informação — Técnicas de segurança — Gestão de incidentes de segurança da informação — Parte 1: Princípios e processo, Associação Brasileira de Normas Técnicas, Rio de Janeiro, 2023. ISO/IEC 27035-2:2023 — Tecnologia da informação — Técnicas de segurança — Gestão de incidentes de segurança da informação — Parte 2: Diretrizes para planejar e preparar a resposta a incidentes, Associação Brasileira de Normas Técnicas, Rio de Janeiro, 2023.

[9] PLANGIC. Gabinete de Segurança Institucional da Presidência da República. Portaria GSI/PR nº 120, de 15 de dezembro de 2022. Institui o Plano Nacional de Gestão de Incidentes Cibernéticos - PLANGIC no âmbito da Administração Pública Federal direta, autárquica e fundacional. Diário Oficial da União: seção 1, Brasília, DF, p. 14, 16 dez. 2022. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-120-de-15-de-dezembro-de-2022-451222092. Acesso em: maio 2025.

[10] LGPD, Lei Geral de Proteção de Dados. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais. Diário Oficial da União: seção 1, Brasília, DF, p. 1, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: maio 2025

[11] R. S. Wazlawick, "*Metodologia de Pesquisa para Ciência da Computação"*, 3ª ed., Rio de Janeiro: GEN LTC, 2021.

[12] REGIC. Decreto nº 10.748, de 16 de julho de 2021. Institui a Rede Federal de Gestão de Incidentes Cibernéticos – REGIC, dispõe sobre a atuação coordenada das equipes de tratamento e resposta a incidentes cibernéticos e altera o Decreto nº 9.637, de 26 de dezembro de 2018. Diário Oficial da União: seção 1, Brasília, DF, p. 4, 19 jul. 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Decreto/D10748.htm. Acesso em: maio 2025.

[13] Pascoe, C., Quinn, S., & Scarfone, K., "The NIST Cybersecurity Framework (CSF) 2.0," NIST Cybersecurity White Papers (CSWP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.CSWP.29, Acesso em: 31 maio 2025

[14] STJ, 2020. "Comunicado da Presidência do STJ", Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/19112020-Comunicado-da-Presidencia-do-STJ.aspx. Acesso em: 07/julho/2026

[15] Ministerio da Saude, 2021

[16] CTIR Gov - link: https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros

[17] PPSI2.0 . Secretaria de Governo Digital – MGI, Guia do Framework de Privacidade e Segurança da Informação, 2023. Conforme o disposto no art. 14 da Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025, Disponivel em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-2.0