PLANO DE GESTÃO DE INCIDENTES CIBERNÉTICOS PARA A ADMINISTRAÇÃO PÚBLICA FEDERAL – PLANGIC

(PORTARIA DSI/GSI/PR Nº 120 DE 21 DE DEZEMBRO DE 2022)

Brasília - 2022

Sumário

1. INTRODUÇÃO 3
1.1. Considerações gerais 3
1.2. Atividades preparatórias 4
2. PREVENÇÃO 4
2.1. Definição e implementação de controles de segurança preventivos 4
2.2. Gerenciamento de vulnerabilidades 5
2.3. Educação: conscientização e capacitação em cibernética 6
3. DETECÇÃO 6
3.1. Estabelecimento de linhas de base 6
3.2. Monitoramento contínuo 6
3.3. Comunicação 7
4. TRATAMENTO DE INCIDENTES CIBERNÉTICOS 8
4.1. Triagem 8
4.2. Análise 8
5. RESPOSTA 9
5.1. Contenção 10
5.2. Erradicação 10
5.3. Recuperação 11
6. PÓS-INCIDENTE 12
6.1. Melhoria contínua dos processos 12

1. INTRODUÇÃO

1.1. Considerações gerais

O universo cibernético permeia e influencia todas as atividades da sociedade humana.

> Os rápidos avanços na área de tecnologia da informação e comunicação resultaram no uso intenso do espaço cibernético para as mais variadas atividades, inclusive a oferta de serviços por parte do Governo federal, em coerência com as tendências globais. Entretanto, novas e crescentes ameaças cibernéticas surgem na mesma proporção, e colocam em risco a administração pública e a sociedade.[1]

Os incidentes cibernéticos precisam ser continuamente enfrentados para garantir que a disponibilidade, a integridade, a confidencialidade e a autenticidade dos serviços e das informações sejam preservadas.

Especialmente, um incidente cibernético em ativo de informação governamental pode causar grave impacto negativo para a sociedade. Essa realidade obriga o estabelecimento de adequadas medidas de segurança da informação e de segurança cibernética. Assim, ao estabelecer as prioridades para emprego dos recursos da organização, a alta administração deve procurar viabilizar a aprovação e a execução dos planos para proteção dos ativos de informação, incluindo os investimentos necessários para instituir e implementar a Equipe de Prevenção, Tratamento e Resposta a Incidente Cibernético (ETIR).

Nesse sentido, o presente Plano tem por objetivo estabelecer procedimentos de gestão de incidentes cibernéticos para os participantes da Rede Federal de Gestão de Incidentes Cibernéticos (Regic). Ele complementa as políticas, estratégias e instruções normativas sobre o tema e deve ser observado pelos gestores e profissionais de segurança da informação dos órgãos e entidades participantes da Regic. Os procedimentos estabelecidos neste Plano incluem ações a serem desenvolvidas pelos diversos níveis da administração de cada participante da Regic, sendo fundamental a atuação das ETIRs.

Cabe lembrar que as equipes de coordenação setorial deverão observar, também, o plano setorial de gestão de incidentes cibernéticos de sua unidade, o qual deve estar alinhado com o Plano Nacional de Segurança das Infraestruturas Críticas (Plansic). Ressalta-se, ainda que o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) do GSI/PR é, no âmbito da administração pública federal (APF), o único **Computer Security Incident Response Team (CSIRT)** nacional, responsável pela coordenação da Regic.

Registre-se que, para fins deste Plano, serão considerados os conceitos constantes da Portaria GSI/PR nº 93, de 18 de outubro de 2021, que aprova o glossário de segurança da informação.

---

[1] Conforme Anexo do Decreto nº 10.222, de 5 de fevereiro de 2020 (Aprova a Estratégia Nacional de Segurança Cibernética).

1.2. Atividades preparatórias

As atividades preparatórias consistem na execução das seguintes ações pelos participantes da Regic:

- designar gestor de segurança da informação;
- instituir e implementar 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, no mínimo, os processos de mapeamento de ativos de informação, de gestão de riscos de segurança da informação, de gestão de continuidade de negócios em segurança da informação e de 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.

2. PREVENÇÃO

A prevenção é um processo constante de ações proativas com o objetivo de reduzir a probabilidade de ataques cibernéticos bem-sucedidos. Entre essas ações, enfatizam-se as de definição e de implementação de controles de segurança, de gerenciamento de vulnerabilidades, de conscientização e de capacitação.

As ações preventivas de segurança cibernética deverão contemplar aquelas previstas na política de segurança da informação do integrante da Regic.

2.1. Definição e implementação de controles de segurança preventivos

Os controles de segurança preventivos constituem-se em tecnológicos, organizacionais e físicos.

Os controles tecnológicos são aqueles utilizados para reduzir vulnerabilidades no **hardware** e no **software**. Entre os principais de controles tecnológicos estão:

- dispositivos **endpoint** do usuário;
- restrição de acesso à informação;
- autenticação segura;
- proteção contra **malware**;
- **backup** das informações;
- atividades de monitoramento (log);
- segurança de redes;
- uso de criptografia; e
- gestão de mudanças.

Por sua vez, os controles organizacionais são utilizados para assegurar a adequação contínua e efetiva da gestão de segurança da informação. Entre os principais controles organizacionais estão:

- política de segurança da informação;
- definição de papéis e responsabilidades pela segurança da informação;
- segregação de funções;
- mapeamento de ativos de informação;
- controle de acesso;
- classificação e rotulagem de informações; e
- norma de segurança da informação para uso de serviços em nuvem.

Por fim, os controles físicos têm por finalidade prevenir ou evitar o acesso não autorizado à área ou material sensível, bem como danos e interferências às áreas que contenham informações críticas ou sensíveis. Entre os principais controles físicos estão:

- definição dos perímetros de segurança física;
- monitoramento de segurança física;
- proteção contra ameaças físicas e ambientais;
- localização e proteção de equipamentos;
- segurança de ativos fora das instalações da organização; e
- manutenção de ativos.

2.2. Gerenciamento de vulnerabilidades

Trata-se de um processo contínuo e proativo que visa controlar riscos, realizar monitoramento, corrigir falhas e adotar ações de proteção contra ataques cibernéticos e violação de dados. O objetivo desse processo é reduzir a exposição geral da organização a riscos, mitigando o maior número possível de vulnerabilidades.

Esse processo é desafiador em virtude do número crescente de possíveis vulnerabilidades e da limitação de recursos disponíveis tempestivamente para correção. Em função disso, as ações de prevenção devem ser sempre complementadas pelas ações de detecção e de tomada de decisão sobre o ativo da informação vulnerável.

Para tanto, o participante da Regic deverá, no mínimo, por meio do mapeamento de ativos de informação:

- 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.

A fim de operacionalizar as atividades supracitadas, o participante da Regic deverá:

- acompanhar as notificações, os alertas e as recomendações emitidas por parceiros, dentre eles, o CTIR Gov e os fornecedores de ativos constantes de seu mapeamento 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 orientações sobre correção ou mitigação, bem como o procedimento para aplicação de medidas corretivas, deverão ser estabelecidas em documentação interna.

2.3. Educação: conscientização e capacitação em cibernética

Visando aprimorar a educação em segurança cibernética, devem ser desenvolvidas ações de conscientização e de capacitação em todos os níveis de administração do participante da Regic.

O participante deverá estabelecer, para todos os seus colaboradores, um processo de divulgação de boas práticas sobre o tema segurança cibernética. As informações relativas à prevenção devem utilizar efetivos canais de comunicação, além de possuírem linguagem adequada ao público-alvo. Podem ser realizadas iniciativas no âmbito da própria organização, tais como seminários, colóquios, estágios, treinamentos, palestras, boletins informativos e memorandos.

É necessário que a conscientização sobre a segurança da informação contemple 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.

3. DETECÇÃO

É um processo de melhoria contínua que analisa todo o ambiente de informação, a fim de identificar atividades maliciosas que possam comprometer os ativos de informação. Tem por objetivo reduzir o impacto do incidente cibernético, antecipando o início do processo de tratamento e de resposta. Logo, a detecção pressupõe o estabelecimento de linhas de base, de monitoramento contínuo e de comunicação dos incidentes cibernéticos.

3.1. Estabelecimento de linhas de base

A organização necessita estabelecer linhas de base que caracterizem o uso normal da rede. As anormalidades são consideradas indícios de incidente e, se identificadas, devem ser investigadas. Os critérios para analisar e caracterizar uma anormalidade como suposto incidente são essenciais para a eficácia do processo.

3.2. Monitoramento contínuo

O participante da Regic 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;

- 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.

Este processo pode ser complementado com ações de detecção proativa, que incluem:

- exploração controlada de vulnerabilidades;
- atividades proativas de equipes de análise;
- correlação de log e eventos;
- teste de penetração; e
- monitoramento proativo de rede.

Uma vez identificada uma anomalia, as informações referentes ao evento adverso deverão ser encaminhadas para triagem.

O CTIR Gov disponibiliza, em seu sítio eletrônico, as orientações de como emitir notificações de prováveis incidentes detectados.

3.3. Comunicação

Os participantes da Regic deverão informar um endereço de correio eletrônico institucional de sua ETIR para troca de informações relacionadas a incidentes cibernéticos com o CTIR Gov, por intermédio do termo de adesão disponibilizado no sítio eletrônico do CTIR Gov. Esse canal será empregado futuramente na operacionalização de uma plataforma computacional dedicada.[2]

Havendo indisponibilidade da comunicação por meio do correio eletrônico, excepcionalmente, poderão ser utilizados outros canais para comunicação, como:

- voz;
- **Inter-Network Operation Center Dial By Autonomous System Number (INOC-DBA)**[3];
- mensagem instantânea;
- reunião por videoconferência;
- sítios eletrônicos e mídias sociais institucionais; e
- reunião presencial de representantes.

As principais mensagens que serão transmitidas por meio desses canais de comunicação dizem respeito à notificação de incidentes cibernéticos, as quais devem seguir a padronização definida e disponibilizada pelo CTIR Gov em seu sítio eletrônico.

---

[2] Conforme previsto no art. 11, inciso II, do Decreto nº 10.748, de 16 de julho de 2021.

[3] Trata-se de uma rede **Voice over Internet Protocol (VoIP)**, de âmbito global, exclusiva para os sistemas autônomos que são as redes que compõem a Internet. **INOC-DBA** fornece uma **hotline**, forma rápida e simples de comunicação entre seus **Network Operations Centers (NOCs)** e os **Computer Security Incident Response Teams (CSIRTs)**, conforme descrito em <https://inoc.nic.br/>.

É importante ressaltar que a comunicação de tais incidentes deve ocorrer com a maior brevidade possível.

4. TRATAMENTO DE INCIDENTES CIBERNÉTICOS

O tratamento de incidentes cibernéticos inicia-se imediatamente após a detecção ou a notificação de provável ocorrência destes, pelo processo de triagem, seguido pelo processo de análise.

4.1. Triagem

O processo de triagem consiste em (Figura 1):

- confirmar se se trata de um incidente cibernético e, caso este não pertença à **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.

Cada ETIR deve estabelecer suas próprias prioridades, em função do tipo do incidente cibernético, considerando os planos e as peculiaridades do setor em que atua, a estratégia de negócio da sua organização, sua área de atuação, cadeia de suprimentos, geolocalização e outros fatores considerados relevantes.

Após estabelecer essa priorização, a ETIR deverá classificar o incidente cibernético de acordo com o impacto na disponibilidade, integridade, confidencialidade e autenticidade no ativo de informação em um dos seguintes níveis: crítico, alto, médio ou baixo.

Figura 1 - Questões de triagem

4.2. Análise

O processo de análise consiste nas atividades listadas abaixo e detalhadas na Figura 2:

- 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.

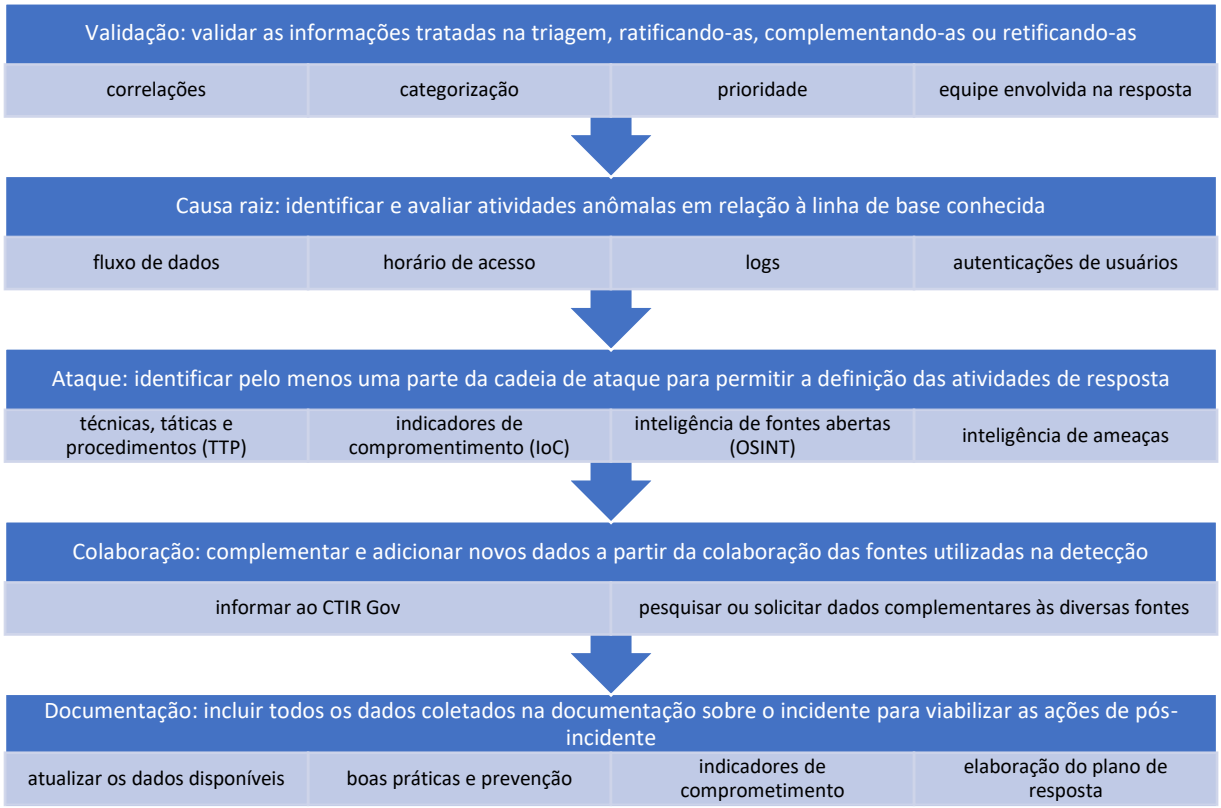

Figura 2 - Atividades da análise

Na atividade da Colaboração (Figura 2), 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
- possuam potencial de exploração danosa em larga escala.

5. RESPOSTA

O processo de resposta a um incidente cibernético consiste em ações de:

- contenção;
- erradicação; e

- recuperação.

As ações de contenção, erradicação e recuperação devem constar do plano de continuidade de negócios em segurança da informação[4] e devem ser baseadas neste Plano e nos seguintes critérios:

- criticidade dos ativos afetados;
- tipo e gravidade do incidente;
- necessidade de preservar a evidência;
- importância de quaisquer sistemas afetados para processos de negócio críticos; e
- recursos necessários para implementar a estratégia.

A ETIR deverá encaminhar, tempestivamente, em função do tipo e do impacto, os dados relativos ao incidente cibernético para o gestor de segurança da informação, os quais deverão ser analisados em conjunto com a área jurídica do órgão ou da entidade, de forma que sejam adotadas as medidas legais, administrativas e cíveis cabíveis, incluindo a comunicação com as autoridades policiais competentes.

Havendo exfiltração de dados pessoais, o encarregado de dados pessoais do órgão ou da entidade deverá informar à Autoridade Nacional de Proteção de Dados (ANPD) de acordo com os procedimentos previstos em legislação, normativos e orientações.

5.1. Contenção

O objetivo da contenção é limitar os danos causados pelo atual incidente de segurança e evitar outros.

Devem ser aplicadas medidas para mitigar o incidente, evitando-se a destruição de provas que possam servir de subsídios para possível processo cível, penal ou administrativo.

A ação de contenção poderá envolver 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.

5.2. Erradicação

A erradicação consiste em remover ou inutilizar artefatos utilizados pelos atacantes e em restaurar o ambiente afetado.

[4] Conforme art. 23 da Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021.

A ação de erradicação poderá envolver as seguintes atividades:

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

5.3. Recuperação

O objetivo da recuperação é restabelecer o pleno funcionamento do ambiente afetado após garantir que as ameaças foram neutralizadas ou removidas.

A ação de recuperação poderá envolver as seguintes atividades:

- 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 o término do processo de recuperação, os participantes da Regic deverão encaminhar ao CTIR Gov um relatório do 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.

Por fim, a Figura 3 ilustra os papéis dos atores que participam do processo de resposta.

Tipos de ETIR	*Contenção*	*Erradicação*	*Recuperação*
ETIR	Executar	Executar	Executar
ETIR SETORIAL[5]	Coordenar	Coordenar	Coordenar
ETIR PRINCIPAL[6]	Executar	Executar	Executar
CTIR Gov	Determinar escopo do incidente. Identificar órgãos envolvidos no incidente.	-	Receber relatório do incidente

Figura 3 - Responsabilidade dos atores no processo de resposta

6. PÓS-INCIDENTE

O objetivo desta fase é realizar a análise da documentação dos incidentes, do processo de comunicação e das regras de proteção do ambiente para evitar incidentes semelhantes e aperfeiçoar os processos existentes.

6.1. Melhoria contínua dos processos

No intuito de evoluir em maturidade e nas ações perante incidentes cibernéticos, o participante da Regic deverá realizar a análise dos processos de prevenção, detecção, tratamento e resposta do incidente.

[5] ETIR Setorial refere-se à equipe de coordenação setorial, conforme definida no art. 4º, inciso II, do Decreto nº 10.748, de 16 de julho de 2021.

[6] ETIR Principal refere-se à equipe principal, conforme definida no art. 4º, inciso III, do Decreto nº 10.748, de 16 de julho de 2021.

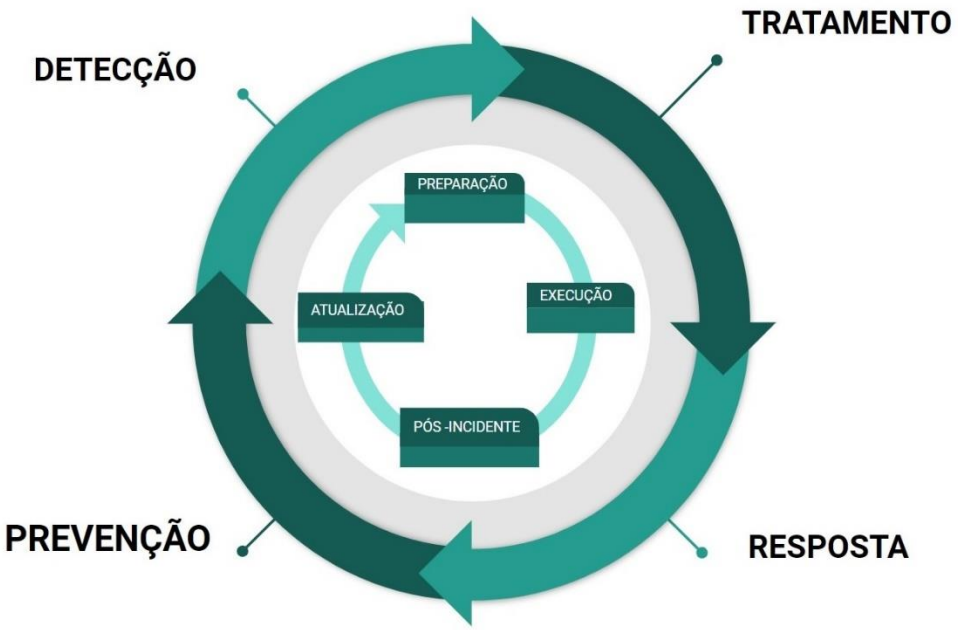

Figura 4 - Ciclo de melhoria na gestão de incidentes cibernéticos

A Figura 4 representa o ciclo de melhoria contínua, representado no anel interno, que ocorre simultaneamente com os processos de gestão de incidentes cibernéticos, representado no anel externo.

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.

O participante da Regic deverá atualizar as atividades preparatórias e os processos de prevenção, detecção, tratamento e resposta a partir das análises do pós-incidente, devendo:

- 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.