PROTOCOLO

GERENCIAMENTO DE CRISES CIBERNÉTICAS

SUMÁRIO

1. HISTÓRICO DE ELABORAÇÃO/REVISÃO

Versão	Data	Descrição da Ação / Alteração	Responsável
1	24/07/2023	Versão Inicial	Gestor de Segurança da Informação
2	30/07/2025	Atualização ações	Gestor de Segurança da Informação
3	22/01/2025	Atualização ações	Gestor de Segurança da Informação
4	13/08/2025	Atualização de Informações	Gestos de Segurança da Informação

2. SIGLAS

SIGLA	DESCRIÇÃO
CNJ	Conselho Nacional de Justiça
ENSEC	Estratégia Nacional de Segurança Cibernética do Poder Judiciário
ETIR	Equipe de Tratamento e Resposta a Incidentes de Redes Computacionais
PMI	*Project Management Institute*
PSI	Política de Segurança da Informação
RACI	Responsável (*Responsible*), Aprovador (*Accountable*), Consultado (*Consulted*) e Informado (*Informed*)
SI	Segurança da Informação
STI	Secretaria de Tecnologia da Informação e Comunicação
TIC	Tecnologia da Informação e Comunicação

3. INTRODUÇÃO

3.1. Visando minimizar e mitigar riscos e conseqüentes explorações e incidentes de Segurança da Informação, cenário crescente na realidade atual de todos os Órgãos da Administração Pública Federal e do Judiciário Nacional e, considerando a transformação digital da Justiça que atua e oferece cada vez mais serviços digitais, o Conselho Nacional de Justiça (CNJ) criou a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), instituída pela Resolução nº 396/2021.

3.2. Em atenção à referida Resolução e à Portaria nº 162 CNJ de 10/06/2021, que aprovou Protocolos e Manuais criados pela ENSEC-PJ, a Secretaria de Tecnologia da Informação e Comunicação (STIC), com apoio do Gestor de Segurança da Informação, elaborou este Protocolo de Gerenciamento de Crises Cibernéticas (PGCRC).

3.3. O PGCRC é complementar ao *Protocolo de Prevenção de Incidentes Cibernéticos* e prevê as ações responsivas a serem colocadas em prática quando ficar evidente que um incidente de segurança cibernética não será mitigado rapidamente, podendo perdurar por dias, semanas ou meses.

4. IDENTIFICAÇÃO DE CRISES CIBERNÉTICAS

4.1. Ao avaliar um problema ou incidente, levando-se em consideração o definido na Portaria PR nº 50/2023 que institui a Política de Gerenciamento de Crises Cibernéticas no Âmbito do TRE-DF, é fundamental identificar quando se trata de uma crise, pois esse diagnóstico irá determinar a forma de proceder.

O gerenciamento de crise se inicia quando:

1. Ficar caracterizado grave dano material ou de imagem
2. Ficar evidenciado que serão necessárias ações em resposta ao incidente cibernético por longo período.
3. O incidente impactar a continuídade de serviços críticos prestados pelo TRE-DF
4. A gravidade e o impacto do incidente impactar a população em geral e envolver a grande mídia

5. MATRIZ RACI / Matriz de Responsabilidade

5.1. A Matriz RACI é uma ferramenta de gestão de projetos e processos que ajuda a definir e esclarecer os papéis e responsabilidades dos membros de uma equipe em relação às atividades específicas do projeto ou tarefa. O acrônimo "RACI" representa quatro possíveis atribuições de responsabilidades:

5.1.1. Responsável (Responsible - R): A pessoa ou grupo que executa a atividade. É quem é diretamente responsável pela conclusão da demanda ou tarefa.

5.1.2. Aprovador (Accountable - A): O responsável final pela atividade ou decisão de aprovação da entrega. Essa pessoa ou grupo tem a responsabilidade de garantir que a tarefa seja concluída de forma adequada e dentro do prazo.

5.1.3. Consultado (Consulted - C): As pessoas ou grupos que fornecem informações ou orientações técnicas para a realização da atividade que irá atender a uma demanda ou entrega solicitada. Embora não executem diretamente a tarefa, sua contribuição é importante para que a conclusão da demanda, da entrega solicitada, seja bem-sucedida, atenda à necessidade para qual foi solicitada. O Consultado poderá ser demandado pelo Responsável ou pelo Aprovador sempre que for necessário para esclarecer alguma dúvida para realizar a atividade ou demanda.

5.1.4. Informado (Informed - I): As pessoas ou grupos que precisam ser informados sobre o progresso da atividade, mas não precisam ser consultados ou envolvidos na execução dela.

5.2. Abaixo segue a matriz de responsabilidades (RACI) construída abordando as etapas que envolvem a Gestão de Crises Cibernéticas.

Atividade	Comitê de Crises Cibernéticas	Comissão de SI	Gestor de SI	Secretário de TIC	ETIR	Responsável pelo ativo de TIC	Gestores dos processos
Pré-crise	CI	ACI	R	CI	CI	CI	CI
Identificação	CI	CAI	CI	CI	R	CI	CI

de crises cibernéticas (Processo de Gerenciamento de Incidentes de Segurança da Informação)							
Acionar Comitê de Crises Cibernéticas	CI	AR	AR	CI	R	CI	CI
Durante a crise	AR	CI	CI	CI	CI	CI	CI
Pós-crise	AR	CI	CI	CI	CI	CI	CI
Revisão de processos	CI	CI	ACI	CI	CI	CI	R

6. GERENCIAMENTO DE CRISES CIBERNÉTICAS

6.1. O gerenciamento de crises cibernéticas é o conjunto de práticas e procedimentos que devem ser adotados pelo Tribunal e suas equipes responsáveis (ETIR, Comitê de Gestão de Crises Cibernéticas, Comissão e Gestor de SI, STIC, e demais envolvidos direta ou indiretamente), para identificar, responder e mitigar os impactos de incidentes de segurança cibernética. Essas crises podem envolver ataques cibernéticos, vazamento de dados sensíveis, infecções por malware, entre outros eventos que possam comprometer a integridade, confidencialidade e disponibilidade dos sistemas e informações de uma organização, e pode ser dividido em 3 (três) fases, quais sejam:

6.1.1. Pré-Crise - Planejamento

6.1.1.1. O Tribunal deve ter um plano de gerenciamento de crises cibernéticas, que deve ser revisado e atualizado regularmente. Esse plano deve incluir procedimentos para identificar, responder e mitigar incidentes cibernéticos. Todos os servidores do TRE-DF devem estar familiarizados com o plano e saber como aplicá-lo.

6.1.1.2. Um plano de gerenciamento de crises cibernéticas pode ajudar a proteger o Tribunal de ataques cibernéticos e minimizar o impacto de qualquer incidente que ocorra.

6.1.1.3. Dentre os benefícios de se ter um plano de gerenciamento de crises cibernéticas, destacam-se:

6.1.1.3.1. Auxiliar na proteção dos dados e sistemas do TRE-DF, e a minimizar o impacto financeiro em caso de ataque.

6.1.1.3.2. Mitigar os impactos à reputação e melhorar a confiança nos serviços prestados

6.1.1.4. O plano de gerenciamento de crise do Tribunal tem que estar alinhado com a Portaria PR nº 50/2023, e deve ter a capacidade de prevenir e minimizar efeitos negativos gerados pela crise.

6.1.1.5. Fundamental para o Tribunal e equipes envolvidas saberem lidar com as crises cibernéticas que se apresentem, e que seja estabelecido um programa de gestão de continuidade de serviços que contemple minimamente:

6.1.1.5.1. A criação do Protocolo de Prevenção a Incidentes Cibernéticos;

6.1.1.5.2. Que as atividades críticas e fundamentais para o funcionamento das atividades finalisticas do Tribunal, sejam utilizadas como referencia para tomada de qualquer ação ou procedimento;

6.1.1.5.3. Que os ativos de informação críticos, sejam mapeados, incluindo pessoas, processos, infraestrutura e recursos de TIC;

6.1.1.5.4. Que os riscos sejam mapeados e avaliados constantemente, e que as ações e procedimentos realizados sejam pautados primeiramente pelos riscos mais críticos;

6.1.1.5.5. Que sejam realizadas simulações e testes para validação dos planos e procedimentos estabelecidos para recuperação do ambiente.

6.1.1.6. A compreensão de como agir e o papel de cada área no manejo de uma crise são elementos fundamentais. Por esse motivo, é imperativo que o Plano de Gestão de Incidentes Cibernéticos contenha, no mínimo, as categorias de incidentes às quais os ativos críticos estão expostos, bem como a definição dos procedimentos de resposta específicos a serem aplicados em caso de ocorrência do incidente e sua respectiva severidade.

6.1.1.7. É importante destacar a importância de estabelecer uma sala de situação ou sala de guerra para gestão da crise em caso de necessidade. Essa sala tem que estar alinhada minimamente ao que está previsto na

Portaria nº 50/2023 da Presidência do Tribunal, e tem como objetivo reunir o Comitê de Gestão de Crises Cibernéticas, para tratar, coordenar e monitorar as atividades, ações ou procedimentos que precisarão ser executados para reestabelecer os serviços prestados à situação normal.

6.1.2. Execução – Crise em andamento

6.1.2.1. Identificada que a crise cibernética está evidenciada, o Comitê de Gestão de Crises Cibernéticas, convoca seus integrantes para formalizarem, estabelecerem a sala de crise.

6.1.2.2. Importante salientar que o protocolo de Gerenciamento de Incidente de Segurança da Informação, é quem tem em suas definições competência para identificar que o incidente realmente é grave e que o Comitê de Gestão de Crises Cibernéticas precisa ser convocado.

6.1.2.3. Estabelecida a Sala de Crise, caberá ao Presidente do Comitê, auxiliado pelo Gestor de Segurança da Informação e demais integrantes do Comitê, tomar todas as ações e procedimentos definidos nos Art. 6º e 7º da Portaria nº 50/2023 da Presidência que trata sobre o assunto, bem como demais ações previstas na mesma.

6.1.3. Pós-Crise – Lições aprendidas e melhoria contínua

6.1.3.1. Após a crise cibernética, e após a retomada à normalidade, o Comitê de Gestão de Crises Cibernéticas deve avaliar de forma criteriosa as ações tomadas, destacando as que atingiram seu objetivo e as que foram inadequadas. Essa avaliação deve ser feita com base nos seguintes critérios:

6.1.3.1.1. Efetividade: as ações tomadas foram eficazes em atingir seu objetivo? Quais foram eficazes e os procedimentos realizados?

6.1.3.1.2. Custo-benefício: o custo das ações tomadas foi justificado pelos benefícios alcançados? Elencar quais ações se justificaram e as estimativas dos custos envolvidos?

6.1.3.1.3. Segurança: as ações tomadas aumentaram a segurança do Tribunal contra ataques cibernéticos? Elencar quais contribuíram para essa melhoria.

6.1.3.2. A avaliação deve ser feita por uma equipe multidisciplinar, composta por especialistas em segurança cibernética, gerenciamento de crises e gestão de riscos. A equipe deve elaborar um relatório com as conclusões da avaliação, que deve ser encaminhado ao Presidente do TRE-DF e aos demais membros do Comitê de Gestão de Crises Cibernéticas.

6.1.3.3. A avaliação é uma ferramenta importante para melhorar a capacidade do Tribunal de responder a ataques cibernéticos. Ao identificar as ações

que foram eficazes e as que foram inadequadas, o Tribunal pode aprender com seus erros e melhorar sua preparação para futuras crises.

7. PLANO DE AÇÃO PARA IMPLEMENTAÇÃO INTREGAL DO PGCRC-PJ

7.1. Visando atender ao PGCRC-PJ definido no Anexo II da Portaria nº 162/2021 do CNJ, foram definidas algumas ações e procedimentos, conforme tabela abaixo.

Item	Ação / Procedimento
1	Existe programa de gestão de continuidade de serviços críticos estabelecido e formalizado na organização?
2	O Protocolo de Prevenção a Acidentes Cibernéticos do Poder Judiciário - PPINC-PJ, está implementado e em uso na organização?
3	As atividades e serviços críticos necessárias para realização da atividade finalistica da organização estão definidas e mapeadas?
4	Os ativos de informação críticos necessários para realização das atividades finalisticas da organização foram identificados?
5	Os riscos derivados das atividades críticas que podem impactar a continuídade dos negócios da organização são avaliados continuamente?
6	Os incidentes identificados são categorizados?
7	Procedimentos de resposta específicos (playbooks), são criados para apoiar a ETIR e demais equipes envolvidas em caso de incidente cibernético?
8	Os ativos de informação críticos são monitorados?
9	O plano de contingência e de mitigação de incidentes cibernéticos foi criado pela organização?
10	O plano de contingência e de mitigação de incidentes cibernéticos está formalizado na organização?
11	Os planos que tratam da gestão de continuídade de serviços críticos são validados e testados continuamente?
12	Existe normativo que estabele o Comitê de Crises Cibernéticas formalizado na organização?
13	A formação do Comitê de Crises e composta por representantes da alta administração e as atividades são apoiadas pela ETIR e outras equipes quando necessário?
14	Os integrantes do Comitê de Crise estão cientes de que precisarão se reunir caso incidente relevante e de impacto seja confirmado pela ETIR?
15	Exite Plano de Gestão de Incidentes Cibernéticos definido e formalizado na organização?
16	O Plano de Gestão de Incidentes Cibernéticos define os

	incidentes por categoria, por severidade e estabelece os procedimentos de resposta em caso de incidente?
17	Existe processo mapeado e em uso para elaboração de procedimentos de resposta em situações de crise cibernética estabelecido na organização?
18	Existe modelo de relatório de comunicação de incidentes de segurança cibernética estabelecido na organização?
19	Existe modelo de relatório de pós-crise de incidentes cibernéticos que aborda ações de melhoria que poderão ser aplicadas em caso de nova crise cibernética?

7.2. Para consecução, implementação e execução das ações e procedimentos definidos, foi estabelecido o seguinte cronograma:

Status	Nível de Conformidade	Prazo para atendimento	Medições	Observações
Atual	**31,58%**		**31,58%**	**Medição inicial – Mai/2023**
1ª Evolução	**54,39%**	Set/2024	**42,11%**	**Julho/2024**
2ª Evolução	**77,19%**	Jun/2025	**47,37%**	**Jan/2025**
3ª Evolução	**100%**	Dez/2025		

8. REFERÊNCIAS

- DECRETO Nº 10.222, DE 5 DE FEVEREIRO DE 2020: Aprovou a Estratégia Nacional de Segurança Cibernética, E-Ciber.
- Decreto nº 9.637, de 26 de dezembro de 2018, que instituiu a Política Nacional de Segurança da Informação.
- Dicionário virtual da Michaelis.
- Lei nº 12.527, de 18 de novembro de 2011.
- Lei nº 12.965, de 23 de abril de 2014.
- Lei nº 13.709, de 14 de agosto de 2018.
- Portaria CNJ n.º 172/2022, de 25 de maio de 2022, que institui o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ).
- Portaria CNJ nº 162, de 10 de junho de 2021.
- Portaria CNJ nº 46, de 10 de fevereiro de 2022.
- Portaria nº 93, de 26 de setembro de 2019, do Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República, a qual aprova o Glossário de Segurança da Informação.

- Portaria TRE-DF nº 50/2023, que instituiu a Política de Gerenciamento de Crises e o Comitê de Gestão de Crises Cibernéticas.

- Relatório TCU: TC 001.873/2020-2 - levantamento objetivando conhecer a macroestrutura de governança e gestão de segurança da informação e de segurança cibernética na Administração Pública Federal (APF).
- Resolução CNJ nº 361, de 17 de dezembro de 2020.
- Resolução CNJ nº 370/2021, de 28 de janeiro de 2021.