PROTOCOLO

INVESTIGAÇÃO DE ILÍCITOS CIBERNÉTICOS

SUMÁRIO

1. HISTÓRICO DE ELABORAÇÃO/REVISÃO

Versão	Data	Descrição da ação / alteração	Responsável
1	28/07/2023	Versão inicial	Gestor de Segurança da Informação
2	30/07/2024	Atualização de ações	Gestor de Segurança da Informação
3	22/01/2024	Atualizações de ações	Gestor de Segurança da Informação
4	13/08/2025	Atualização do documento	Gestor 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
ETIR	Equipe de Tratamento e Resposta a Incidentes de Redes Computacionais
PSI	Política de Segurança da Informação do TRE-BA, Portaria n.º 405/2021
RACI	Responsável (*Responsible*), Aprovador (*Accountable*), Consultado (*Consulted*) e Informado (*Informed*)
SI	Segurança da Informação
SIC	Segurança da Informação e Comunicações
STI	Secretaria de Tecnologia da Informação e Comunicação
TIC	Tecnologia da Informação e Comunicação

3. GLOSSÁRIO DE TERMOS

3.1 Para efeito deste Protocolo, aplicam-se os seguintes conceitos e definições:

Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade.

Agente responsável pela ETIR: Servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

Aquisição de evidência: processo de coleta e cópia das evidências de incidente de segurança em redes computacionais.

Ativos de Informação: os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.

Auditoria: processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas (em conformidade) à consecução dos objetivos.

Autenticação: processo de identificação das partes envolvidas em um processo.

Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

Autorização: processo que visa a garantir que as informações são acessíveis exclusivamente àqueles com permissão de acesso.

Coleta de evidências de segurança em redes computacionais: processo de obtenção de itens físicos que contém uma potencial evidência, mediante a utilização de metodologia e ferramentas adequadas. Este processo inclui a aquisição, ou seja, a geração das cópias das mídias, ou coleção de dados que contenham evidências do incidente.

Endereço IP (*Internet Protocol)*: refere-se ao conjunto de elementos numéricos ou alfanuméricos que identifica um dispositivo eletrônico em uma rede de computadores.

Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR): grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em redes de

computadores.

Evidência digital: informação ou dado, armazenado ou transmitido eletronicamente, em modo binário, que pode ser reconhecida como parte de um evento.

Incidente de segurança em redes computacionais: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

Informação sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo.

Log ou Registro de Auditoria: registro de eventos relevantes em um dispositivo ou sistema computacional.

Metadados: conjunto de dados estruturados que descrevem informação primária.

Preservação de evidência de incidentes em redes computacionais: é o processo que compreende a salvaguarda das evidências e dos dispositivos, de modo a garantir que os dados ou metadados não sofram alteração, preservando-se a integridade e a confidencialidade das informações.

Resumo Criptográfico: é um método criptográfico que, quando aplicado sobre uma informação, independente do tamanho desta, gera um resultado único e de tamanho fixo, também chamado de "*hash*".

Tratamento da Informação Classificada: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle de informação classificada em qualquer grau de sigilo.

4. INTRODUÇÃO

4.1 A Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), instituída pela Resolução nº 396/2021, derivou a Portaria nº 162 CNJ de 10/06/2021, que aprova Protocolos e Manuais criados pela ENSEC-PJ.

4.2 Para atender ao previsto no Anexo III da mencionada Portaria do CNJ, que trata do Protocolo de Investigação de Ilícitos Cibernéticos (PIILC), e considerando que é interesse do Estado e da sociedade a investigação e a responsabilização por condutas ilícitas que danifiquem ou exponham a segurança das redes e sistemas computacionais ou que possam comprometer a disponibilidade, integridade, confidencialidade e autenticidade da informação na Administração Pública Federal, foi criado este documento que tem por finalidade estabelecer os procedimentos básicos para coleta e preservação de evidências.

4.3 Este documento tem a finalidade também de orientar os procedimentos referentes à comunicação obrigatória dos fatos penalmente relevantes às autoridades responsáveis, como o Ministério Público e demais Órgãos de Polícia Judiciária e outras especializadas no assunto para o início da persecução penal.

5. ADEQUAÇÃO DOS ATIVOS DE INFORMAÇÃO

5.1 Preliminarmente deve-se considerar que os normativos internos estabelecidos pelo Tribunal relacionados ao correto uso e gestão dos serviços e ativos de informação estejam em uso e sendo executados conforme as diretrizes estabelecidas nestes, bem como devidamente monitorados pela equipe da Secretaria de Tecnologia e Comunicações – STIC.

5.2 Importante destacar os normativos criados e vigentes que tem relação direta e indireta sobre este tema:

5.2.1 Resolução TSE nº 23.644/2021 - Institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

5.2.2 Portaria Diretoria-Geral Nº 83/2023 – Institui a Comissão de Segurança da Informação – CSI, no âmbito do TRE-DF ;

5.2.3 Portaria da Presidência do TRE-DF Nº 69/2023 – Institui a Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR);

5.2.4 Portaria-GP Nº 189/2010 – Dispõe sobre o acesso aos sistemas de informação do TRE-DF;

5.2.5 Portaria da Presidência Nº 183/2024 – Institui a Política de Acesso aos Recursos de TIC (PARTIC);

5.3. Todos os equipamentos, serviços e sistemas de TIC devem estar sincronizados com a Hora Legal Brasileira (HLB), de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON).

5.4. Todos os ativos de Tecnologia da Informação, sistemas e redes de comunicação de dados, devem estar configurados para registrar os eventos de segurança elencados abaixo, sem prejuízo de outros considerados relevantes em caso de necessidade observada pela equipe da STIC e do Gestor de Segurança da Informação:

i. Registros de autenticação de usuários, perfis, grupos privilegiados e serviços;
ii. Inicialização, suspensão e reinicialização de serviços;
iii. Acoplamento e desacoplamento de dispositivos de hardware, com especial atenção para mídias removíveis;
iv. Modificações da lista de membros de grupos privilegiados;
v. Modificações de política de senhas, como por exemplo, tamanho, expiração, bloqueio automático após exceder determinado número de tentativas de autenticação, histórico; etc.
vi. Acesso ou modificação de arquivos ou sistemas considerados críticos; e
vii. Eventos obtidos de quaisquer mecanismos de segurança existentes.

5.5. Os registros dos eventos relevantes de Segurança da Informação e Comunicações (SIC) devem incluir a identificação inequívoca do usuário que acessou o recurso, data, hora e fuso horário, endereço IP, porta de origem da conexão, coordenadas geográficas, quando for possível e se houver a possibilidade de coleta.

5.6. Todo ativo de informação, que assim o permita, deve ser configurado para armazenar registros históricos de eventos (logs) em formato que possibilite a completa identificação dos fluxos de dados.

5.7. Todos os registros devem ser armazenados localmente e também remotamente sempre que possível pelo período mínimo de 6 (seis) meses, sem prejuízo de outros prazos previstos em normativos específicos.

6. MATRIZ RACI ou MATRIZ DE RESPONSABILIDADES

6.1 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:

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

6.1.2 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.

6.1.3 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.

6.1.4 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.

6.2 Abaixo segue a matriz de responsabilidades (RACI) construída abordando as etapas que envolvem a Investigação de Ilícitos Cibernéticos.

Atividade	Comissão de SI	Gestor de SI	Secretário de TIC	ETIR	Responsável pelo ativo de	Gestores dos processos	Equipe técnica designada
Adequar ativos de informação	-	-	I	I	RA	CI	-
Informar ocorrência de incidente cibernético	I	CI	I	ACI	R	I	-

Identificar evento penalmente relevante e acionar protocolo	**CI**	**CAI**	**CI**	**R**	**C**	**C**	**C**
Realizar medidas de manuseio da evidência digital	**I**	**CI**	**CI**	**AC**	**CI**	**I**	**R**

7. ORIENTAÇÕES QUANTO A COLETA E PRESERVAÇÃO DAS EVIDÊNCIAS

7.1 Inicialmente todos os integrantes de ETIR, precisam estar bem capacitados em matérias relacionadas com forense digital, sendo os conhecimentos mínimos desejáveis:

7.1.1 Conhecimento de Sistemas Operacionais, Redes, Bancos de Dados e Soluções básicas de segurança e de administração de infraestrutura (Firewalls, Firewalls de aplicação, Proxy, Controladores de Domínio,...);

7.1.2 Conhecimento no uso de ferramentas forenses;

7.1.3 Possuir conhecimentos básicos sobre programação e lógica de programação.

7.1.4 Ter experiência prática e saber trabalhar em equipe.

7.2 A preservação de evidências digitais é uma parte crítica na resposta a incidentes de segurança cibernética e investigações de crimes cibernéticos. É fundamental garantir que a integridade das evidências seja mantida para que elas possam ser utilizadas de forma válida em processos judiciais ou para análise forense. Abaixo estão algumas das melhores práticas e procedimentos para a preservação de evidências digitais, bem como as competências e conhecimentos mínimos necessários para as equipes de tratamento e resposta a incidentes:

7.3 A ETIR, sob a supervisão de seu responsável, durante o processo de tratamento do incidente penalmente relevante, deverá, sem prejuízo de outras ações, IDENTIFICAR, COLETAR, ADQUIRIR e PRESERVAR as mídias de armazenamento dos dispositivos afetados, bem como todos os registros mencionados neste Protocolo.

7.4 Caso seja inviável preservar as mídias de armazenamento dos dispositivos afetados ou das suas respectivas imagens forenses, o agente responsável pela ETIR deverá coletar e armazenar cópia dos arquivos afetados pelo incidente, e dados como: logs, configurações do sistema operacional, arquivos do sistema de informação, e outros julgados necessários, mantendo-se a estrutura de diretórios original, bem como os "metadados" desses arquivos, como data, hora de criação e permissões.

7.5 Importante salientar que o responsável pela ETIR deverá fazer constar em relatório a impossibilidade de preservar as mídias afetadas e listar todos os procedimentos adotados. Ressalta-se, também, que as ações de restabelecimento do serviço afetado não devem comprometer a coleta e preservação da integridade das evidências.

7.6 O processo de preservação de evidências digitais em uma investigação de ilícitos cibernéticos envolve várias fases ou etapas essenciais. A preservação adequada das evidências é crucial para garantir sua admissibilidade em um tribunal e para manter a integridade das informações coletadas. As principais etapas e ações envolvidas no processo são as seguintes:

7.6.1 **Identificação:** Nesta fase, os investigadores devem identificar as evidências digitais relevantes que precisam ser preservadas. Isso pode incluir dispositivos eletrônicos, sistemas de armazenamento, logs de servidores, mídias removíveis, arquivos em nuvem, entre outros.

7.6.2 **Coleta:** Após a identificação, é necessário coletar as evidências digitais de forma adequada utilizando técnicas de forense digital. A coleta pode envolver o uso de ferramentas específicas para garantir que os dados sejam copiados sem alterações ou danos. O uso de métodos forenses apropriados é essencial para garantir a aceitabilidade das evidências em caso de necessidade.

7.6.3 **Documentação:** Durante todo o processo, é essencial manter uma documentação detalhada de todas as ações realizadas. Isso inclui registros de quem coletou as evidências, quando e onde foram coletadas, quais técnicas e ferramentas foram usadas, etc. Essa documentação é importante para criar uma cadeia de custódia e garantir a integridade das evidências.

7.6.4 **Preservação:** A preservação adequada é a etapa crítica para evitar a adulteração ou destruição das evidências digitais. As cópias forenses das evidências devem ser armazenadas em um local seguro, e medidas devem ser tomadas para garantir que elas não sejam modificadas acidentalmente ou intencionalmente.

7.6.5 **Autenticação:** Para que as evidências sejam admissíveis em um tribunal, elas precisam ser autenticadas. Isso envolve comprovar a integridade e a origem das evidências, garantindo que elas não foram falsificadas ou alteradas desde a coleta.

7.6.6 **Análise:** Após a preservação e autenticação das evidências, a análise forense é realizada para extrair informações relevantes das evidências digitais coletadas. Isso pode envolver a busca por arquivos, dados de logs, rastreamento de atividades, entre outras técnicas forenses.

7.6.7 Relatório: Finalmente, os resultados da análise são compilados em um relatório forense detalhado, que descreve as descobertas, metodologia utilizada e conclusões alcançadas. O relatório deve ser claro e compreensível, tanto para especialistas em TI quanto para leigos.

7.7 É importante destacar que, em uma investigação de ilícitos cibernéticos, a preservação das evidências digitais deve ser realizada por profissionais devidamente treinados em forense digital, para garantir que todas as etapas sejam conduzidas de maneira adequada e que a integridade das evidências seja mantida. A negligência ou a má preservação das evidências podem comprometer todo o processo, análises e conclusões sobre o incidente, o caso em específico.

7.8 Todo material coletado deve estar sob custodia do agente responsável pela ETIR, o qual deve preencher um Termo de Custódia dos Ativos de Informação relacionado ao Incidente de Segurança. O material coletado deverá ficar à disposição da autoridade responsável pelo órgão do Poder Judiciário competente.

7.9 Para orientar a documentação e efetivação de todas as etapas previstas no processo, é fundamental a criação de documentos, ou procedimento em solução de gestão de serviços, que permita a criação de toda a documentação para subsidiar os procedimentos necessários à preservação das evidências em processo de investigação de ilícitos cibernéticos.

7.10 Os documentos e documentações mencionados, preferencialmente, deverão também ser inseridos em processos administrativos no SEI durante todo o transcorrer da análise e do processo de investigação, para acompanhamento da autoridade competente.

8. CADEIA DE CUSTÓDIA

8.1 A cadeia de custódia, conforme estabelecida na ISO nº 23.037, tem como principal objetivo assegurar o controle e a rastreabilidade do manuseio das evidências, garantindo que o material coletado e adquirido não sofra negligência ou ações intencionais para prejudicar a legítima investigação de possíveis ilícitos cibernéticos.

8.2 Essencialmente, a cadeia de custódia consiste em um registro que documenta a cronologia de movimentação e manuseio das potenciais evidências digitais. Todas as aquisições de dados e dispositivos sob custódia são descritas, traçando-se o histórico do item desde o momento em que foi identificado, coletado ou adquirido pela equipe de investigação. Esse registro possibilita a identificação do acesso e movimento das evidências a qualquer momento, além de garantir a adequada guarda, e dentro do tempo estipulado legalmente.

8.3 A documentação da cadeia de custódia também é fundamental para subsidiar eventuais apurações de responsabilidade funcional por ações inadequadas dos envolvidos na investigação. É de suma importância registrar minuciosamente o acondicionamento e todas as tramitações dos ativos de TIC e possíveis evidências coletadas e adquiridas na cadeia de custódia.

8.4 A observância rigorosa dos cuidados necessários durante a execução dos procedimentos afetos à cadeia de custódia, são de extrema relevância para garantir a utilidade e validade jurídica de todo o trabalho realizado pela equipe designada. É fundamental enfatizar a importância de documentar todas as particularidades e ocorrências ao longo do processo.

9. DA COMUNICAÇÃO ÀS AUTORIDADES COMPETENTES

9.1 Seguindo as recomendações da Portaria CNJ nº 162/2021 e da Resolução TSE nº 23.644/2021, que institui a Política de Segurança da Informação do Poder Judiciário (PSI), assim que o incidente de segurança cibernética for identificado como penalmente relevante, o responsável pela equipe de Tratamento e Resposta a Incidentes do TRE-DF, deverá comunicar o fato de imediato ao órgão de polícia judiciária com atribuição para apurar os fatos e ao Ministério Público.

9.2 Caso seja identificado que o incidente cibernético desencadeou crise cibernética, deverá ser acionado o Comitê de Crise Cibernética, em consonância com o Protocolo de Gerenciamento de Crises Cibernéticas.

9.3 Se o incidente cibernético for considerado penalmente relevante, e findos os trabalhos relacionados ao processo de coleta e preservação das evidências, o responsável pela ETIR deverá elaborar Relatório de Comunicação de Incidente de Segurança Cibernética, descrevendo detalhadamente os eventos verificados.

9.4 O Relatório de Comunicação de Incidente de Segurança Cibernética deverá conter as seguintes informações, sem prejuízo de outras julgadas relevantes:

Nome do responsável pela preservação dos dados do incidente e do agente responsável pela ETIR, com informações de contato.
Órgão comunicante com sua localização e informações de contato.
Número de controle da ocorrência.
Relato sobre o incidente que descreva o que ocorreu, como foi detectado e quais dados foram coletados e preservados.
Descrição das atividades de tratamento e resposta ao incidente e todas as providências tomadas, incluindo ações de preservação e coleta, a metodologia e as ferramentas utilizadas e o local de armazenamento das informações preservadas.

9.5 Além das informações acima mencionadas, no relatório deve constar:

I. Resumo criptográfico dos arquivos coletados;
II. Termo de Custódia dos Ativos de Informação Relacionados ao Incidente de Segurança;
III. Justificativa sobre a eventual inviabilidade de preservação das mídias de armazenamento dos dispositivos afetados, diante da impossibilidade de mantê-las.

9.6 A preservação da privacidade e sigilo dos dados custodiados deverá ser observada durante todo o processo de coleta das evidências do incidente de segurança em redes computacionais, na elaboração do relatório, bem como quando do seu envio às autoridades competentes, conforme legislação vigente.

9.7 Deverá constar no documento formal de encaminhamento ao Ministério Público e ao órgão de polícia judiciária com atribuição para apurar os fatos apenas a informação de que se trata de comunicação de evento relacionado à segurança da informação, sem a descrição dos fatos.

10. PLANO DE AÇÃO PARA IMPLEMENTAÇÃO INTEGRAL DO PCIIC-PJ

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

Item	Ação/Procedimento
1	Todos os ativos, serviços e sistemas estão sincronizando tempo com base na hora legal brasileira (HLB) e com o observatório nacional (ON)?
2	Os registros de eventos (logs) de todos os ativos críticos de TI estão sendo armazenados por pelo menos 180 dias?
3	Os registros de eventos (logs) de autenticação (sucesso e insucesso) no AD estão sendo armazenados por pelo menos 180dias?
4	Os registros de eventos (logs) dos acessos a recursos críticos de TIC e dados privilegiados estão sendo armazenados por pelo menos 180 dias?
5	Os registros de eventos (logs) dos acessos e alteração de auditoria, estão sendo armazenados por pelo menos 180 dias?
6	Os registros de eventos (logs), estão configurados para identificar o usuário, a natureza do evento, a data, hora, endereço IP e portas de conexão utilizadas?
7	Os serviços críticos disponibilizados são monitorados e as informações como usuários perfis e grupos com privilégio de acesso são armazenadas?
8	A solução de Administração do Domínio utilizada, está com a auditoria ativa e monitora todos os eventos realizados pelos usuários, grupos de usuários e contas de sistema?
9	A solução de Administração do Domínio utilizada, está com a auditoria ativa e monitora todos os eventos realizados referentes à política de senhas?
10	A solução de Administração de Banco de Dados utilizada pelos serviços e sistemas críticos, está auditando e monitorando todas as ações e eventos realizados?
11	Os dados dos eventos registrados pelas soluções que estão auditando o ambiente, são armazenados por pelo menos 180 dias?
12	Todos os dados dos eventos registrados pelas soluções que estão auditando e armazenando eventos do ambiente, estão em formato que possibilita a identificação do fluxo dos dados?
13	Os dados dos eventos registrados pelas soluções que estão auditando e sendo armazenados, são replicados para solução de consolidação, tratamento e análise de logs (SIEM)?
14	A equipe da ETIR foi capacitada para realizar procedimento de forense digital visando a coleta e preservação de evidências?
15	A equipe da ETIR possui ferramental e soluções específicas para realizar procedimento de forense digital visando a coleta e preservação de evidências?

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

Status	Nível de Conformidade	Prazo para atendimento	Medições	Observações
Inicial	**20,00%**		**20%**	**Medição inicial – Mai/2023**
1ª Evolução	**46,66%**	Set/2024	**46,67%**	**Julho/2024**
2ª Evolução	**73,34%**	Jun/2025	**66,67%**	**Jan/2025**
3ª Evolução	**100%**	Dez/2025		

11. 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.
- 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
- Norma Complementar nº 21/IN21/DSIC/GSIPR, do Departamento de Segurança da Informação e Comunicações da Presidência da República.
- 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.
- 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 396, de 07 de junho de 2021
- Resolução CNJ nº 370/2021, de 28 de janeiro de 2021

ANEXO A– Termo de Custódia dos Ativos de Informação Relacionados ao Incidente de Segurança

DADOS GERAIS:

Nome do custodiante:

Matrícula:

Nome do Órgão:

Cargo/Função:

Endereço:

Telefone:

Endereço eletrônico:

MATERIAIS SOB CUSTÓDIA:

ITEM	TIPO	QTDE	DESCRIÇÃO	IDENTIF./LACRE

_____

Local e data

_____

Assinatura do Custodiante

ANEXO B – RELATÓRIO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA EM REDES COMPUTACIONAIS

DADOS GERAIS:

Número da ocorrência/Ano: _____/_____.

Nome do agente responsável pela preservação dos dados do incidente:

_____ Matrícula: _____

Endereço eletrônico:_____Telefone: (___) _____

Nome do responsável pela ETIR:
_____Matrícula: _____

Endereço eletrônico:_____Telefone: (___) _____

Nome do Órgão:
_____

Endereço:
_____

RELATO SOBRE O INCIDENTE:

DESCREVA O INCIDENTE:
SE POSSÍVEL, DESCREVA A ORIGEM DO INCIDENTE, OU A RAZÃO DE NÃO SER POSSÍVEL IDENTIFICÁ-LA:

COMO FOI DETECTADO O INCIDENTE?
QUAIS FORAM OS DADOS COLETADOS E PRESERVADOS?
OUTROS DADOS JULGADOS RELEVANTES**:**
QUAIS FORAM AS AÇÕES DE TRATAMENTO E RESPOSTA AO INCIDENTE?
COMO FORAM PRESERVADOS OS REGISTROS DO INCIDENTE? QUAIS AS FERRAMENTAS UTILIZADAS?
QUAL FOI O LOCAL DE ARMAZENAMENTO DAS INFORMAÇÕES PRESERVADAS?

Local e data: _____, _____/____/_____.

_____

Assinatura do agente responsável pela preservação dos dados do incidente