ANEXO I

Exemplo de Plano de Gestão de Incidentes Cibernéticos

Indicação do incidente cibernético	Descrição	Procedimento	Severidade
Campanha de *phishing*	O órgão é alvo de uma campanha de *phishing*	Identificação do documento de procedimento de resposta específico	Média
Degradação de serviços	Degradação ou interrupção de serviços ou sistemas por ataque de negação de serviço (DoS)	Identificação do documento de procedimento de resposta específico	Alta
Comprometimento de credenciais	Comprometimento de credenciais com acesso a informações sensíveis	Identificação do documento de procedimento de resposta específico	Alta
Impossibilidade de acesso a informação	Importantes informações organizacionais inacessíveis por encriptação (Ransomware)	Identificação do documento de procedimento de resposta específico	Crítica
Vazamento de informação e dados pessoais	Informações críticas encontradas fora da organização	Identificação do documento de procedimento de resposta específico	Crítica

PORTARIA Nº 291, DE 17 DE DEZEMBRO DE 2020.

Institui o Protocolo de Investigação para Ilícitos Cibernéticos no âmbito do Poder Judiciário.

O **PRESIDENTE DO CONSELHO NACIONAL DE JUSTIÇA (CNJ)**, no uso de suas atribuições legais e regimentais,e nos termos da Resolução CNJ nº 362/2020,

CONSIDERANDO o disposto nos incisos X e XII do art. 5º da Constituição da República, que instituem os direitos à privacidade;

CONSIDERANDO a Lei nº13.709/2018 – Lei Geral de Proteção de Dados;a Lei nº12.965/2014 – Marco Civil da Internet; o Decreto nº8.771/2016, e a Lei nº12.527/2011 – Lei de Acesso à Informação; bem como as Resoluções CNJ nº 121/2010 e nº 215/2015 e a Recomendação do CNJ nº 73/2020;

CONSIDERANDO a Portaria CNJ nº 242/2020, que institui o Comitê de Segurança Cibernética do Poder Judiciário e dispõe sobre a normatização para criação do Centro de Tratamento de Incidentes de Segurança Cibernética (CTISC) do CNJ, que funcionará como canal oficial para orquestração e divulgação de ações preventivas e corretivas, em caso de ameaças ou de ataques cibernéticos;

CONSIDERANDO a Instrução Normativa GSI nº 1/2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal;

CONSIDERANDO a Instrução Normativa GSI nº 2/2020, que altera a Instrução Normativa GSI nº 1/2020, a qual dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal;

CONSIDERANDO a Norma Complementar nº 04/IN01/DSIC/GSIPR, que estabelece Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) nos órgãos e entidades da Administração Pública Federal;

CONSIDERANDO a Norma Complementar nº 06/IN01/DSIC/GSIPR, que estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF);

CONSIDERANDO a Norma Complementar nº 08/IN01/DSIC/GSIPR, que estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal;

CONSIDERANDO a Norma Complementar nº 21/IN01/DSIC/GSIPR, que estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta;

RESOLVE:

Art. 1º Instituir, no âmbito dos órgãos do Poder Judiciário, à exceção do Supremo Tribunal Federal, o Protocolo de Investigação para Ilícitos Cibernéticos.

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 2º É interesse do Estado e da sociedade a investigação das condutas ilícitas que danifiquem ou exponham a segurança das redes e sistemas computacionais ou que possam comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações no âmbito do Poder Judiciário.

CAPÍTULO II

DO OBJETIVO

Art. 3º.O Protocolo de Investigação para Ilícitos Cibernéticos tem por finalidade estabelecer os procedimentos básicos para coleta e preservação de evidências, bem como para comunicação dos fatos penalmente relevantes ao órgão de polícia judiciária com atribuição para o início da persecução penal.

CAPÍTULO III

DAS DEFINIÇÕES

Art. 4º Para efeito desta Portaria, são estabelecidos os seguintes conceitos e definições:

I – 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;

II – Agente responsável pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais(ETIR): servidor público do Poder Judiciário incumbido de chefiar e gerenciar a ETIR;

III – Aquisição de evidência: processo de coleta e cópia das evidências de incidente de segurança em redes computacionais;

IV – 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;

V – Auditoria: processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se 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;

VI – Autenticação: processo de identificação das partes envolvidas em um processo;

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

VIII – Autorização: processo que visa garantir que as informações são acessíveis exclusivamente àqueles com permissão de acesso;

IX – 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. Esse processo inclui a aquisição, ou seja, a geração das cópias das mídias, ou coleção de dados que contenham evidências do incidente;

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

XI – 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;

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

XIII – 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;

XIV – 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;

XV – Log ou registro de auditoria:registro de eventos relevantes em um dispositivo ou sistema computacional.

XVI – Metadados:conjunto de dados estruturados que descrevem informação primária;

XVII – 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;

XIII – Resumo criptográfico: é um método criptográfico que, quando aplicado sobre uma informação, independentemente do tamanho desta, gera resultado único e de tamanho fixo, também chamado de "*hash*"; e

XIX – 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.

CAPÍTULO IV

DOS REQUISITOS PARA ADEQUAÇÃO DOS ATIVOS DE INFORMAÇÃO

Art. 5º O horário dos ativos de informação deve ser ajustado por meio de mecanismos de sincronização de tempo, de forma a garantir que as configurações de data, hora e fuso horário do relógio interno estejam sincronizados com a "Hora Legal Brasileira (HLB)", de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON).

Art. 6º Os ativos de informação devem ser configurados de forma a registrar todos os eventos relevantes de Segurança da Informação e Comunicações (SIC), tais como:

I –autenticação, tanto as bem-sucedidas quanto as malsucedidas;

II –acesso a recursos e dados privilegiados; e

III –acesso e alteração nos registros de auditoria.

Art. 7º Os registros dos eventos previstos no artigo anterior devem incluir as seguintes informações:

I –identificação inequívoca do usuário que acessou o recurso;

II –natureza do evento, como por exemplo, sucesso ou falha de autenticação, tentativa de troca de senha, etc;

III –data, hora e fuso horário, observando o previsto no art. 5º; e

IV –endereço IP (*Internet Protocol*), porta de origem da conexão, identificador do ativo de informação, coordenadas geográficas, se disponíveis, e outras informações que possam identificar a possível origem do evento.

Art. 8º Os ativos de informação que não permitem os registros dos eventos acima listados devem ser mapeados e documentados quanto ao tipo e formato de registros de auditoria permitidos e armazenados.

Art. 9º Os sistemas e redes de comunicação de dados devem ser monitorados, registrando-se, minimamente, os seguintes eventos de segurança, sem prejuízo de outros considerados relevantes:

I –utilização de usuários, perfis e grupos privilegiados;

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 por meio de quaisquer mecanismos de segurança existentes.

Art. 10. Os servidores de hospedagem de página eletrônica, bem como todo e qualquer outro ativo de informação que assim o permita, devem ser configurados para armazenar registros históricos de eventos (*logs*) em formato que permita a completa identificação dos fluxos de dados.

Parágrafo único. Os registros devem ser armazenados pelo período mínimo de seis meses, sem prejuízo de outros prazos previstos em normativos específicos.

Art. 11. Recomenda-se que os ativos de informação sejam configurados de forma a armazenar seus registros de auditoria não apenas localmente, como também remotamente, por meio do uso de tecnologia aplicável.

CAPÍTULO V

DOS PROCEDIMENTOS PARA COLETA E PRESERVAÇÃO DAS EVIDÊNCIAS

Art. 12. A ETIR, sob a supervisão de seu responsável, durante o processo de tratamento do incidente penalmente relevante, deverá, sem prejuízo de outras ações, coletar e preservar:

I –as mídias de armazenamento dos dispositivos afetados ou as suas respectivas imagens forenses;

II–os dados voláteis armazenados nos dispositivos computacionais, como a memória principal (memória RAM); e

III –todos os registros de eventos citados no Capítulo IV.

Art. 13. Nos casos de inviabilidade de preservação das mídias de armazenamento mencionadas no inciso I, do art. 12, em razão da necessidade de pronto restabelecimento do serviço afetado, a ETIR, sob a supervisão do seu responsável, deverá coletar e armazenar cópia dos arquivos afetados pelo incidente, tais como: *logs*, configurações do sistema operacional, arquivos do sistema de informação, e outros julgados necessários, mantendo-se a estrutura de diretórios original e os “metadados” desses arquivos, como data, hora de criação e permissões.

Parágrafo único. O agente responsável pela ETIR deverá fazer constar em relatório a eventual impossibilidade de preservação das mídias afetadas e listar todos os procedimentos adotados.

Art. 14. As ações de restabelecimento do serviço não devem comprometer a coleta e a preservação da integridade das evidências.

Art. 15. Para a preservação dos arquivos coletados, deve-se:

I –gerar arquivo contendo a lista dos resumos criptográficos de todos os arquivos coletados;

II –gravar os arquivos coletados, acompanhado do arquivo com a lista dos resumos criptográficos descritos no inciso anterior; e

III –gerar resumo criptográfico do arquivo a que se refere o inciso I.

Art. 16. Todo material coletado deverá ser lacrado e custodiado pelo agente responsável pela ETIR, o qual deverá preencher Termo de Custódia dos Ativos de Informação relacionados ao Incidente de Segurança penalmente relevante.

Parágrafo único. O material coletado ficará à disposição da autoridade responsável pelo órgão do Poder Judiciário competente.

CAPÍTULO VI

DA COMUNICAÇÃO DO INCIDENTE DE SEGURANÇA

Art. 17. Assim que tomar conhecimento de Incidente de Segurança em Redes Computacionais penalmente relevante, deverá o responsável pelo órgão do Poder Judiciário afetado comunicá-lo de imediato ao órgão de polícia judiciária com atribuição para apurar os fatos.

Parágrafo Único. Considerado o incidente uma Crise Cibernética, o Comitê de Crise deverá ser acionado, nos termos do Protocolo de Gerenciamento de Crises Cibernéticas.

Art. 18. Após a conclusão do processo de coleta e preservação das evidências do incidente penalmente relevante, o responsável pela ETIR deverá elaborar Relatório de Comunicação de Incidente de Segurança em Redes Computacionais, descrevendo detalhadamente os eventos verificados.

§1º O Relatório de Comunicação de Incidente de Segurança em Redes Computacionaisdeverá ser instruído com as seguintes informações, sem prejuízo de outras julgadas relevantes:

I –o nome do responsável pela preservação dos dados do incidente, com informações de contato;

II –o nome do agente responsável pela ETIR e informações de contato;

III –órgão comunicante com sua localização e informações de contato;

IV –número de controle da ocorrência;

V –relato sobre o incidente, descrevendo como ocorreu, como foi detectado e quais dados foram coletados e preservados;

VI –descrição das atividades de tratamento e resposta ao incidente e todas as providências tomadas pela ETIR, incluindo as ações de preservação e coleta, a metodologia e as ferramentas utilizadas e o local de armazenamento das informações preservadas;

VII –o resumo criptográfico citado no art. 16;

VIII – Termo de Custódia dos Ativos de Informação Relacionados ao Incidente de Segurança;

IX –número de lacre de material físico preservado, se houver; e

X –justificativa sobre a eventual inviabilidade de preservação das mídias de armazenamento dos dispositivos afetados, nos termos do parágrafo único, do art. 14.

§2º O Relatório de Comunicação de Incidente de Segurança em Redes Computacionaisdeverá ser acondicionado em envelope lacrado e rubricado pelo agente responsável pela ETIR, protocolado e encaminhado formalmente à autoridade responsável pelo órgão do Poder Judiciário afetado.

§3º Deverá constar no documento formal de encaminhamento a que se refere o parágrafo anterior, apenas a informação de que se trata de comunicação de evento relacionado à segurança da informação, sem a descrição dos fatos.

Art. 19. Recebida a Comunicação de Incidente de Segurança em Redes Computacionais, a autoridade responsável pelo órgão do Poder Judiciário deverá encaminhá-la formalmente ao órgão de polícia judiciária com atribuição para apurar os fatos, juntamente com o material a que se refere o art. 16, para fins de instrução da notícia crime.

CAPÍTULO VII

DAS DISPOSIÇÕES FINAIS

Art. 20.Os órgãos do Poder Judiciário deverão elaborar e formalizar plano de ação, com vistas à construção de seu Protocolo de Investigação para Ilícitos Cibernéticos, no prazo máximo de sessenta dias e comunicar ao CNJ.

Art. 21.Nos termos da Portaria CNJ nº 242/2020, que instituiu o Comitê de Segurança Cibernética do Poder Judiciário, e da Resolução CNJ nº XXX/2020, que determinou a adoção do Protocolo de Investigação para Ilícitos Cibernéticos, o protocolo definido neste ato normativo será objeto de reavaliação por ocasião da edição da Estratégia da Segurança Cibernética e da Informação do Poder Judiciário, bem como remanescerá passível de atualização a qualquer tempo.

Art. 22.EstaPortaria entra em vigor na data de sua publicação, revogando-se as disposições contrárias.

Ministro LUIZ FUX

ANEXO I DA PORTARIA Nº291, DE 16 DE DEZEMBRO DE 2020.

A – EXEMPLO DE MODELO DE RELATÓRIO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA EM REDES COMPUTACIONAIS

B – EXEMPLO DE MODELO DE TERMO DE CUSTÓDIA DOS ATIVOS DE INFORMAÇÃO RELACIONADOS AO INCIDENTE DE SEGURANÇA

ANEXO I – EXEMPLO DE MODELO DE RELATÓRIO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA EM REDES COMPUTACIONAIS

DADOS GERAIS:

Nº da ocorrência/ano: _____/_____.

1. Nome do agente responsável pela preservação dos dados do incidente:
_____

Matrícula: _____

Endereço eletrônico: _____ Telefone: (___) _____

2. Nome do responsável pela ETIR: _____
_____ Matrícula: _____

Endereço eletrônico: _____ Telefone: (___) _____

Nome do órgão/instituição: _____

Endereço: _____

RELATO SOBRE O INCIDENTE:

DESCREVA O INCIDENTE:

_____
_____
_____
_____
_____
_____
_____
_____

SE POSSÍVEL, DESCREVA AORIGEM 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

ANEXO II DA PORTARIA Nº 291, DE 16 DE DEZEMBRO DE 2020.

ANEXO II – EXEMPLO DE MODELO DE TERMO DE CUSTÓDIA DOS ATIVOS DE INFORMAÇÃO RELACIONADOS AO INCIDENTE DE SEGURANÇA

DADOS GERAIS:

Nome do custodiante:
Matrícula:
Nome do órgão/entidade da APF:
Cargo/Função:
Endereço:
Telefone:
Endereço eletrônico:

MATERIAIS SOB CUSTÓDIA:

ITEM	TIPO	QTDE	DESCRIÇÃO	IDENTIF./LACRE

_____

Local e data

_____

Assinatura do Custodiante

PORTARIA Nº 292, DE 17 DE DEZEMBRO DE 2020.

Determina a adoção de Protocolo de Prevenção a Incidentes Cibernéticos no âmbito do Poder Judiciário (PPICiber/PJ).

O **PRESIDENTE DO CONSELHO NACIONAL DE JUSTIÇA (CNJ)**, uso de suas atribuições legais e regimentais, e nos termos da Resolução CNJ nº361/2020,

CONSIDERANDO competir ao CNJ a atribuição de coordenar o planejamento e a gestão estratégica de Tecnologia da Informação e Comunicação (TIC) do Poder Judiciário;

CONSIDERANDO que é imprescindível garantir a segurança cibernética do ecossistema digital do Poder Judiciário brasileiro;

CONSIDERANDO o número crescente de incidentes cibernéticos no ambiente da rede mundial de computadores e a necessidade de processos de trabalho orientados para a boa gestão da segurança da informação;

CONSIDERANDO os termos da Resolução CNJ nº 211/2015, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), e estabeleceu as diretrizes para sua governança, gestão e infraestrutura;