ANEXO 8

NSI008 – Gestão de Incidentes de Segurança da Informação

(Incluído pela Portaria GP.TRT4 nº 7.791/2015 e alterado pelas Portarias GP.TRT4 nº 7.137/2017, 6.493/2019, 4.786/2020, 299/2022, 4.920/2022, 4.095/2023 e 4.742/2024)

1. Objetivos

1.1. Estabelecer as diretrizes e definir o processo de Gestão de Incidentes de Segurança da Informação no âmbito deste Tribunal. (alterado pela Portaria GP.TRT4 nº 4.095/2023)

2. Motivações

2.1. Alinhamento às normas, regulamentações e melhores práticas, relacionadas à matéria.

2.2. Necessidade de tratar os incidentes de segurança da informação com resposta rápida e eficiente.

2.3. Correto direcionamento e dimensionamento de recursos tecnológicos e humanos para prover uma Gestão de Incidentes de Segurança da Informação com menor custo e maior qualidade.

2.4. Formalização de um processo para gerenciamento dos incidentes de segurança da informação, provendo insumos para minimizar e/ou evitar eventos adversos futuros. (alterado pela Portaria GP.TRT4 nº 4.095/2023)

3. Referências normativas (alterado pela Portaria GP.TRT4 nº 4.095/2023)

3.1. Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão de Segurança da Informação e Comunicações na Administração Pública Federal.

3.2. Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14.08.2009, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

3.3. Norma Complementar nº 08/IN01/DSIC/GSIPR, de 14.08.2010, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que disciplina o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais – ETIR dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

3.4. Norma Técnica ISO/IEC 27000:2018, que especifica conceitos e definições relacionados às normas de segurança da informação.

3.5. Norma ABNT NBR ISO/IEC 27002:2022, que fornece um conjunto de referência de controles genéricos de segurança da informação;

3.6. Norma ABNT NBR ISO/IEC 27035-3:2021 que fornece diretrizes para operações de resposta a incidentes de TIC;

3.7. Resolução CNJ nº 396, de 07 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

3.8. Norma Complementar nº 21/IN01/DSIC/GSIPR, de 10.10.2014, do Departamento de Segurança da Informação e Comunicações da Presidência da República, 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.

4. Conceitos e definições

4.1. Artefato malicioso: é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores.

4.2. Ativos de Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

4.3. Usuários: magistrados e servidores ocupantes de cargo efetivo ou em comissão, requisitados e cedidos, desde que previamente autorizados, empregados de

empresas prestadoras de serviços terceirizados, consultores, estagiários, e outras pessoas que se encontrem a serviço da Justiça do Trabalho, utilizando em caráter temporário os recursos tecnológicos do TRT.

4.4. Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR: Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores.

4.5. Evento de segurança da informação: ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

4.6. Incidente de segurança da informação: é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

4.7. Medida de contenção: controle e/ou ação tomada para evitar que danos causados por um determinado incidente continuem aumentando com o passar do tempo. Além disso, tais medidas visam o restabelecimento do sistema/serviço afetado, mesmo eu não seja em sua capacidade total. (alterado pela Portaria GP.TRT4 nº 6.493/2019)

4.8. Medida de erradicação: controle e/ou ação tomada para sanar vulnerabilidades e problemas que sejam a causa-raiz de um ou mais incidentes de segurança da informação. (alterado pela Portaria GP.TRT4 nº 4.095/2023)

4.9. Medidas de recuperação: conjunto de ações para restabelecer o ambiente ao estado normal, situação na qual se encontrava antes do incidente, contemplando medidas de melhoria observadas no tratamento do evento adverso. (alterado pela Portaria GP.TRT4 nº 4.095/2023)

4.10. Tratamento de Incidentes de Segurança em Redes Computacionais: é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações

que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências. (alterado pela Portaria GP.TRT4 nº 4.095/2023)

4.11. Vulnerabilidade: fragilidade de um ativo ou controle que pode ser explorado por uma ameaça. (alterado pela Portaria GP.TRT4 nº 4.095/2023)

4.12. CTIR GOV: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações – DSIC do Gabinete de Segurança Institucional da Presidência da República – GSI. (incluído pela Portaria GP.TRT4 nº 4.095/2023)

5. Escopo

5.1. A Gestão de Incidentes de Segurança da Informação, definida nesta norma, tem seu escopo limitado às situações relacionadas ao ambiente, ativos, projetos e processos de TIC. (alterado pela Portaria GP.TRT4 nº 4.786/2020)

6. Diretrizes

6.1. A Gestão de Incidentes de Segurança da Informação tem como principal objetivo assegurar que incidentes de segurança da informação sejam identificados, registrados e avaliados em tempo hábil, com a tomada de medidas de contenção, erradicação e recuperação adequadas. (alterado pela Portaria GP.TRT4 nº 4.095/2023)

6.2. Estão abrangidos por esta norma os eventos, confirmados ou suspeitos, relacionados à segurança de sistemas ou redes computacionais, que comprometam o ambiente tecnológico do TRT, seus ativos, informações e processos de negócio, bem como aqueles que contrariem a Política de Segurança da Informação deste Tribunal, e dos quais decorram interrupção, parcial ou total, de serviço essencial ao desempenho das atividades, vulnerabilidades de segurança, divulgação, alteração ou destruição de informações e/ou prática de ato definido como crime ou infração administrativa. (alterado pela Portaria GP.TRT4 nº 6.493/2019)

6.3. O Tribunal providenciará dispositivos de monitoramento, ferramentas de segurança e detecção de intrusão, a fim de subsidiar a Gestão de Incidentes de Segurança da

Informação.

7. O processo de Gestão de Incidentes de Segurança da Informação

7.1. O processo de Gestão de Incidentes de Segurança da Informação é contínuo e aplicado na implementação e operação do Sistema de Gestão de Segurança da Informação (SGSI).

7.2. O processo de Gestão de Incidentes de Segurança da Informação é composto pelas seguintes etapas: (alterado pela Portaria GP.TRT4 nº 4.095/2023)

7.2.1. **Preparação**: consiste no conjunto de atividades pró-ativas, para mapeamento e proteção do ambiente tecnológico, como implantação de mecanismos para auxílio à detecção de incidentes, elaboração de planos de resposta a incidentes, dentre outros. (alterado pela Portaria GP.TRT4 nº 4.095/2023)

7.2.2. **Detecção e Análise**: compreende a detecção ou recebimento de informação sobre eventos maliciosos suspeitos, a investigação do ocorrido, para determinar se de fato é um incidente, avaliação da extensão e do impacto do incidente e a comunicação do evento. (alterado pela Portaria GP.TRT4 nº 4.095/2023)

7.2.3. **Contenção, erradicação e recuperação**: compreende o conjunto de atividades necessárias para a contenção e erradicação de um incidente, bem como as ações necessárias à recuperação do ambiente tecnológico à operação normal. (alterado pela Portaria GP.TRT4 nº 4.095/2023)

7.2.4. **Atividades pós-incidente**: consistem nas tarefas relacionadas realizadas após o encerramento do incidente, que visam ao aperfeiçoamento na deteção e resposta dadas, além dos processos realizados durante todo o tratamento. (alterado pela Portaria GP.TRT4 nº 4.095/2023)

7.3. Os incidentes, notificados ou detectados, devem ser objeto de registro, com a finalidade de assegurar a manutenção do histórico e auxiliar na geração de indicadores.

7.4. A notificação de incidente, suspeito ou confirmado, poderá ser feita por qualquer usuário, sem necessidade de prévia autorização do gestor, através do formulário de solicitação de atendimento da Central de Serviços ou diretamente à Coordenadoria

de Segurança da Informação e Proteção de Dados, pelo telefone ou pelo e-mail setic.csipd@trt4.jus.br, que a reportará Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação. (alterado pela Portaria GP.TRT4 nº 4.095/2023).

7.5. Os usuários devem notificar, o mais breve possível, os incidentes de segurança da informação e vulnerabilidades de que tenham conhecimento (observada ou suspeita).

7.6. Vulnerabilidades ou fragilidades suspeitas não deverão ser objeto de teste ou prova pelos usuários, sob o risco de violar a política de segurança da informação e/ou provocar danos aos serviços ou recursos tecnológicos.

7.7. As equipes da Secretaria de Tecnologia da Informação responsáveis pelo monitoramento dos ativos, serviços e sistemas devem notificar os incidentes a eles relacionados à Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação, para o devido registro e encaminhamento. (alterado pela Portaria GP.TRT4 nº 7.137/2017)

7.8. O Tribunal poderá receber notificações externas (CTIR.BR, CSIRT ou outras entidades) sobre incidentes (ocorridos ou suspeitos) por meio de sistemas gerenciadores de demandas, e-mail, telefone, etc, que deverão ser remetidas à Coordenadoria de Segurança da Informação e Proteção de Dados, para o devido encaminhamento. (alterado pela Portaria GP.TRT4 nº 4.095/2023)

7.9. O tratamento da informação deve ser realizado de forma a viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação, com retorno das operações à normalidade no menor prazo possível, bem como evitar futuras ocorrências, com a proposição de ações de solução, quando existentes.

7.10. A Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação deve conduzir, apoiada pelas outras áreas da SETIC, investigação do incidente e de artefatos maliciosos, propondo e implementando as ações de contenção, erradicação e recuperação, comunicando as áreas afetadas e coletando os dados necessários. (alterado pela Portaria GP.TRT4 nº 4.095/2023)

7.11. A coleta de evidência dos incidentes de segurança da Informação deve ser realizada

pela Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação ou por pessoal competente e por ela autorizado. (alterado pela Portaria GP.TRT4 nº 7.137/2017)

7.12. Quando o incidente de segurança da informação decorrer de suspeita de descumprimento da Política de Segurança da Informação, será observado o sigilo durante todo o processo, ficando as evidências, informações e demais registros restritos aos envolvidos na investigação.

7.13. Quando houver indícios de ilícitos criminais durante o gerenciamento dos incidentes de segurança, o Comitê de Segurança da Informação e Proteção de Dados e a Administração do TRT deverão ser comunicados, para avaliação das providências cabíveis. (alterado pela Portaria GP.TRT4 nº 4.920/2022)

7.14. O encerramento do incidente de segurança da informação será realizado pelo coordenador da ETIR, com comunicação a todas as áreas interessadas e ao Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal (CTIR.BR) na forma e nos casos definidos pelo referido órgão. (alterado pela Portaria GP.TRT4 nº 4.742/2024)

7.15. A avaliação do processo de gestão de incidentes de segurança da informação ocorrerá por meio do histórico de incidentes, com verificação das oportunidades de melhoria. (alterado pela Portaria GP.TRT4 nº 4.095/2023)

7.16. O desenho do processo de Gestão de Incidentes de Segurança da Informação, a descrição das atividades, os respectivos papéis e responsabilidades dos envolvidos no processo, bem como os modelos de documentos a serem utilizados nas etapas do processo, serão publicados no Portal de Governança de TI, após aprovação pela Presidência.

8. Atualização da norma

8.1. As diretrizes previstas na presente norma serão atualizadas sempre que alterados os procedimentos da Gestão de Incidentes de Segurança da Informação, observada a periodicidade prevista para a revisão da Política de Segurança da Informação.