PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO

PORTARIA GP.TRT4 Nº 4.095, DE 20 DE JULHO DE 2023.

Altera a Portaria GP.TRT4 nº 4.772/2008, a qual institui a Política de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 4ª Região, e dá outras providências.

O PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a revisão e atualização realizada na Política de Segurança da Informação, instituída pela Portaria GP.TRT4 n° 4.772/2008 da Presidência deste Tribunal, de acordo com o artigo 1º, § 1º, da referida norma;

CONSIDERANDO o que consta nos Processos Administrativos PROADs nºs 7248/2019, 7264/2019, 7268/2019 e 11519/2020,

RESOLVE:

Art. 1º Alterar os incisos VII e VIII do artigo 1º, § 2º, das Diretrizes Gerais da Portaria GP.TRT4 nº 4.772/2008, que passam a vigorar com as seguintes redações:

> VII – Norma ABNT NBR ISO/IEC 27001:2022, que estabelece os requisitos para um Sistema de Gestão da Segurança da Informação;
>
> VIII - Norma ABNT NBR ISO/IEC 27002:2022, que fornece um conjunto de referência de controles de segurança da informação;

Art. 2º Alterar o *caput* dos artigos 4º, 5º, 7º e Parágrafo único, 10, 11, 14-A e 14-B das Diretrizes Gerais da Portaria GP.TRT4 nº 4.772/2008, que passam a vigorar com as

seguintes redações:

> **Art. 4º** O uso adequado dos recursos de tecnologia da informação visa a contribuir para a efetividade e a continuidade da prestação jurisdicional deste Tribunal.
>
> **Art. 5º** A utilização dos recursos de tecnologia da informação será monitorada, com a finalidade de detectar a ocorrência de eventos de segurança cibernética suspeitos e divergências entre as normas que integram a Política de Segurança da Informação e os registros de eventos monitorados, fornecendo evidências nos casos de incidentes de segurança.
>
> [...]
>
> **Art. 7º** As informações, sistemas e métodos tratados pelos usuários, no exercício de suas funções, independentemente da forma de tratamento, são propriedade do Tribunal e serão utilizadas exclusivamente para fins relacionados às atividades a ele afetas.
>
> ***Parágrafo único*.** Quando as informações, sistemas e métodos forem tratados por terceiros para uso exclusivo do Tribunal, ficam os criadores obrigados ao sigilo permanente de tais produtos, sendo vedada a sua reutilização em projetos para outrem.
>
> [...]
>
> **Art. 10.** A Coordenadoria de Segurança da Informação e Proteção de Dados, vinculada à Secretaria de Tecnologia da Informação e Comunicações, tem por objetivo prover soluções de segurança que agreguem valor aos serviços

> prestados pelo Tribunal Regional do Trabalho da 4ª Região, pautadas na conscientização e no comprometimento de seus usuários para a preservação da confidencialidade, da integridade e da disponibilidade das informações, a segurança nas operações e a excelente imagem perante a sociedade.
>
> **Art. 11.** As atribuições da Coordenadoria de Segurança da Informação e Proteção de Dados são definidas pela Portaria GP.TRT4 nº 486/2023 e suas atualizações, que regulamenta as atribuições e responsabilidades da Secretaria de Tecnologia da Informação e Comunicações.
>
> [...]
>
> **Art. 14-A.** É criada a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR, subordinada à Secretaria de Tecnologia da Informação e Comunicações e coordenada pela Coordenadoria de Segurança da Informação e Proteção de Dados.
>
> **Art. 14-B.** As atribuições da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR, sua estrutura, bem como a designação de seus integrantes são regulados no Anexo 7 desta Portaria.

Art. 3º Alterar os subitens 3.2, 3.3, 4.5, 4.6, 5.3.1, 5.3.3 e 5.3.4 do Anexo I da Portaria GP.TRT4 nº 4.772/2008, que passam a vigorar com as seguintes redações:

> 3.2 Norma Técnica ABNT NBR ISO/IEC 27001:2022, que estabelece os requisitos para um Sistema de Gestão de Segurança da Informação;
>
> 3.3. Norma ABNT NBR ISO/IEC 27002:2022, que fornece

um conjunto de referência de controles de segurança da informação.

[…]

4.5. Serviço - produto disponibilizado na internet, como mídia *streaming*, por exemplo, cujo acesso se dá por meio de navegador web ou por aplicativo (conhecidos também como *app*).

4.6. Sítio - É um conjunto de páginas *web* organizadas a partir de um URL básico, onde fica a página principal, e geralmente são armazenadas numa única pasta ou subpastas relacionadas no mesmo diretório de um servidor.

[...]

5.3.1. Acessar conteúdo considerado ofensivo, ilegal, impróprio ou incompatível com as atividades funcionais tais como: pornografia, pedofilia, racismo, jogos e páginas de distribuição e de compartilhamento de software.

[...]

5.3.3. Utilizar programas e/ou acessar sítios/serviços de áudio e vídeo em tempo real ou sob demanda, exceto aqueles homologados pelo TRT4 ou autorizados pelo Comitê de Segurança da Informação e Proteção de Dados.

5.3.4. Acessar sítios ou serviços que possam comprometer de alguma forma a confidencialidade, integridade ou disponibilidade do ambiente tecnológico e informações do TRT.

Art. 4º Incluir os subitens 4.7. e 5.2.1.1 no Anexo I da Portaria GP.TRT4 nº 4.772/2008, com as seguintes redações:

> 4.7. Situação de contingência - estado ou condição na qual exista a ocorrência de falha/problema, em um ou mais recursos tecnológicos, que reduzam a capacidade dos sistemas e serviços que suportam a atividade da organização.
>
> […]
>
> 5.2.1.1. A eventual ausência de mecanismos de controle de acesso à internet em equipamentos fora das dependências da Justiça do Trabalho não exime o usuário do dispositivo tecnológico de observar as regras e boas práticas definidas nesta norma.

Art. 5º Alterar os subitens 4.2, 4.3, 5.6, 5.8.3 e 8.1 do Anexo II da Portaria GP.TRT4 nº 4.772/2008, que passam a vigorar com as seguintes redações:

> 4.2. Norma Técnica ABNT NBR ISO/IEC 27001:2022, que estabelece os requisitos para um Sistema de Gestão de Segurança da Informação;
>
> 4.3. Norma ABNT NBR ISO/IEC 27002:2022, que fornece um conjunto de referência de controles de segurança da informação.
>
> [...]
>
> 5.6. No caso de alteração de endereço eletrônico, o endereço antigo será mantido na forma de *alias* pelo período de até doze meses, a contar da alteração, ou permanentemente, em casos excepcionais e devidamente justificados.

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO

[...]

5.8.3. A caixa postal institucional da unidade terá um único endereço de correio eletrônico, cujo identificador será formado pela denominação da unidade ou por sigla que permita a sua identificação, precedida pela sigla da unidade a qual pertence (ex.: segesp.digesp@trt4.jus.br, segesp.aposentadoria@trt4.jus.br).

[…]

8.1. O uso do correio eletrônico será monitorado por meio de ferramentas com o intuito de impedir o recebimento de *spam*, *hoax*, *phishing*, mensagens contendo vírus e outros arquivos que coloquem em risco a segurança do ambiente tecnológico do Tribunal ou que contenham conteúdo impróprio.

Art. 6º Incluir a letra “p” ao subitem 7.7 do Anexo II da Portaria GP.TRT4 nº 4.772/2008, com a seguinte redação:

[...]

p) dados pessoais, sensíveis ou não, que não estejam vinculados às atividades de trabalho e devidamente adequados às legislações vigentes.

Art. 7º Excluir o subitem 4.4. do Anexo II da Portaria GP.TRT4 nº 4.772/2008.

Art. 8º Alterar a íntegra do item 3 do Anexo III da Portaria GP.TRT4 nº 4.772/2008, que passa a vigorar com a seguinte redação:

3. Referências normativas

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. Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.

3.3. Instrução Normativa GSI/PR nº 5, de 31 de agosto de 2021, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.

3.4. Norma Complementar 12/IN01/DSIC/GSIPR, de 30 de janeiro de 2012, que estabelece diretrizes para o Uso de Dispositivos Móveis nos Aspectos relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal.

3.5. Norma Complementar nº 21/IN01/DSIC/GSIPR, de 08 de outubro de 2014, 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.

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

3.7. Norma Técnica ABNT NBR ISO/IEC 27001:2022, que estabelece os requisitos para um Sistema de Gestão de Segurança da Informação.

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

3.9. Portaria GP.TRT4 nº 3.244/2021, de 25 de novembro de 2021, que estabelece normas gerais sobre administração de materiais de consumo e bens permanentes no âmbito do Tribunal Regional do Trabalho da 4ª Região.

3.10. Resolução CSJT nº 164, de 18 de março de 2016, que disciplina o uso e a concessão de certificados digitais institucionais no âmbito da Justiça do Trabalho de primeiro e segundo graus.

Art. 9º Alterar os subitens 5.1.1., 5.1.5., 5.2.5.1., 5.2.6.2. e a íntegra do 5.3. do Anexo III da Portaria GP.TRT4 nº 4.772/2008, que passam a vigorar com as seguintes redações:

5.1.1. O uso adequado dos recursos de tecnologia da informação visa a contribuir para a efetividade e a continuidade das atividades desenvolvidas neste Tribunal.

[...]

5.1.5. Não será fornecido suporte a equipamentos particulares (por exemplo: computadores, *notebooks, smartphones* e *tablets*), seja quanto à instalação e configuração de sistemas ou aplicativos, ainda que disponibilizados pelo TRT4, seja quanto às questões relacionadas à conexão à rede sem-fio.

[...]

5.2.5.1. É permitida a conexão de dispositivos móveis particulares nas redes sem-fio administradas pelo TRT4,

desde que por meio da autenticação utilizando a credencial do usuário (usuário e senha).

[...]

5.2.6.2. É proibido o armazenamento, em qualquer diretório na rede do Tribunal ou nas soluções baseadas em nuvem, sob pena de serem excluídos pela SETIC, sem anuência do usuário, de arquivos não relacionados ao trabalho, tais como:

a) fotos, músicas e filmes de qualquer formato;
b) programas não homologados ou não licenciados;
c) programas de conteúdo prejudicial à segurança do parque computacional deste Tribunal.

5.3. Nuvem corporativa

5.3.1. Ao armazenamento de arquivos na nuvem corporativa aplicam-se as regras previstas no item 5.2.6.2.

5.3.2. Os arquivos armazenados na nuvem corporativa deverão ser vinculados (ter como proprietário) à caixa postal institucional da unidade, quando existente, ou outra designada pelo gestor da unidade para tal fim.

5.3.3. Nos casos de relotação ou afastamentos previstos no Anexo 2 desta Política (casos de exclusão da caixa postal), o gestor deverá solicitar ao servidor ou estagiário, de forma antecipada, sempre que possível, a verificação da existência de arquivos que digam respeito às atividades da unidade e que permaneçam na propriedade do servidor/estagiário, para que sejam transferidos para a caixa postal institucional da unidade ou outra designada pelo gestor.

5.3.3.1. Caso persistam arquivos vinculados à caixa postal institucional do servidor/estagiário quando de sua exclusão, eles serão transferidos para a caixa postal institucional da unidade, ou outra designada pelo gestor, para triagem e definição da necessidade ou não de manutenção dos arquivos.

5.3.4. Nos casos de exclusão da caixa postal institucional de magistrados (exceto a hipótese de falecimento), será dada ciência, de forma antecipada, sobre a necessidade de transferência ou *download* dos arquivos armazenados na nuvem, sob pena de serem excluídos juntamente com a caixa postal.

5.3.5. Nos casos de exclusão da caixa postal institucional de unidade, os arquivos serão transferidos para a conta da unidade designada como nova responsável pelas atividades ou para servidor designado para tal fim.

5.3.6. A SETIC não garante a recuperação de caixas postais, mensagem de e-mails e arquivos armazenados na solução em nuvem excluídos há mais de 30 dias.

Art. 10. Incluir o inciso IV no subitem 6.1.2. do Anexo III da Portaria GP.TRT4 nº 4.772/2008, com a seguinte redação:

IV) a inclusão, alteração ou remoção de acessos decorrentes da alteração do regime de trabalho (presencial ou teletrabalho).

Art. 11. Incluir o subitem 6.2.4.1. do Anexo III da Portaria GP.TRT4 nº 4.772/2008, com a seguinte redação:

6.2.4.1. Por questões de segurança, a SETIC poderá

exigir a autenticação de multifator para realização do acesso aos recursos tecnológicos.

Art. 12. Excluir o subitem 5.5.2.1 do Anexo III da Portaria GP.TRT4 nº 4.772/2008.

Art. 13. Alterar o subitem 6.1.8., acrescentando a este o subitem 6.1.8.1., e os subitens 6.1.9. e 6.1.10. do Anexo III da Portaria GP.TRT4 nº 4.772/2008, que passam a vigorar com as seguintes redações:

6.1.8. O privilégio de administrador na estação de trabalho é restrito aos membros da equipe técnica da SETIC que necessitem de acesso privilegiado para o desempenho das atividades funcionais.

6.1.8.1. Nos computadores portáteis disponibilizados pelo Tribunal aos magistrados, estes terão privilégio de administrador local.

6.1.9. Os acessos privilegiados aos sistemas e serviços de TIC serão concedidos aos membros da equipe técnica da SETIC, sempre que necessários ao desempenho das atividades funcionais, de modo a permitir a gestão e configuração do ambiente tecnológico.

6.1.9.1. É responsabilidade da chefia imediata solicitar a concessão, a alteração e a remoção dos acessos privilegiados dos seus subordinados.

6.1.9.2. Os acessos concedidos deverão ser revisados pelo menos uma vez ao ano.

6.1.10. As solicitações de acessos de prestadores de serviço aos recursos tecnológicos do TRT4 terão caráter temporário e deverão ser acompanhadas da respectiva justificativa, bem como do prazo previsto para a

realização das atividades.

6.1.10.1. No caso do prestador de serviço necessitar de acesso privilegiado, as regras observarão o disposto no item 6.1.9.

Art. 14. Excluir o subitem 6.1.11. do Anexo III da Portaria GP.TRT4 nº 4.772/2008.

Art. 15. Alterar os subitens 4.2. e 4.3. do Anexo IV da Portaria GP.TRT4 nº 4.772/2008, que passam a vigorar com as seguintes redações:

4.2. Norma Técnica ABNT NBR ISO/IEC 27001:2022, que estabelece os requisitos para um Sistema de Gestão de Segurança da Informação.

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

Art. 16. Alterar os subitens 4.3., 4.5, 4.6, 10.2, 10.3 e 10.5.3 do Anexo VI da Portaria GP.TRT4 nº 4.772/2008, que passam a vigorar com as seguintes redações:

4.3. Norma Técnica ABNT NBR ISO/IEC 27005:2019, que fornece diretrizes para o processo de gestão de riscos de Segurança da Informação.

[...]

4.5. Norma Técnica ABNT NBR ISO/IEC 27001:2022, que estabelece os requisitos para um Sistema de Gestão de Segurança da Informação.

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

[…]

10.2. O processo de GRSIC-TRT4 está baseado nas definições constantes nas normas técnicas ABNT NBR ISO/IEC 27005:2019 e ABNT NBR ISO/IEC 31000:2018 e na Instrução Normativa GSI/PR nº 3.

10.3. Os riscos serão avaliados a partir da: a) **Probabilidade**, que é a possibilidade de algum evento adverso ocorrer, podendo gerar impacto negativo. A escala é definida em quatro níveis: raro, possível, provável ou iminente; b) **Impacto**, que é a medida do dano ocasionado caso o evento adverso concretize-se. A escala é definida em quatro níveis: perceptível, moderado, crítico ou catastrófico. Desta forma os riscos são analisados com base em duas variáveis (probabilidade e impacto). O produto dessas duas variáveis determina o nível do risco, conforme mapa a seguir:

	1 - Raro	**2 - Possível**	**3 - Provável**	**4 - Iminente**
1 - Perceptível	1	2	3	4
2 - Moderado	2	4	6	8
3 - Crítico	3	6	9	12
4 - Catastrófico	4	8	12	16

Classificação do Risco	**Valores do RISCO**
Muito baixo	1 a 2
Baixo	3 a 4
Médio	6 a 8
Alto	9 a 12
Muito alto	16

[...]

10.5.3. Tratamento dos Riscos - compreende a implementação das ações do Plano de Tratamento de Riscos.

Art. 17. Alterar a íntegra do item 5 do Anexo VI da Portaria GP.TRT4 nº 4.772/2008, que passa a vigorar com a seguinte redação:

5.1. Ameaça - causa potencial de um incidente indesejado, que pode resultar em danos a um sistema ou organização;

5.2. Análise de riscos - processo para compreender a natureza do risco e determinar o nível de risco;

5.3. Avaliação de riscos - processo de comparação dos resultados da análise de risco com critérios de risco para determinar se o risco e/ou sua magnitude são aceitáveis ou toleráveis;

5.4. 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;

5.5. Comunicação do risco - conjunto de processos contínuos e iterativos que uma organização realiza para fornecer, compartilhar ou obter informações e para dialogar com as partes interessadas sobre o gerenciamento de riscos;

5.6. Estimativa de riscos - processo utilizado para atribuir valores à probabilidade e às consequências de um risco;

5.7. Evitar risco - forma de tratamento de risco pela qual se decide não realizar a atividade, a fim de não se

envolver ou agir de forma a se retirar de uma situação de risco;

5.8. Evento adverso - ocorrência ou alteração negativa de um conjunto de circunstâncias;

5.9. Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC–TRT4) – conjunto de atividades que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

5.10. Gestão de Riscos em Projetos de TIC – conjunto de atividades que envolve a identificação, a análise, o planejamento de respostas, o monitoramento e o controle de riscos de um projeto.

5.11. Gestão de Riscos em Processos de TIC – conjunto de atividades, estabelecidas de acordo com as peculiaridades ou normatividades que regem cada processo, que visam a identificar e minimizar ou eliminar os riscos.

5.12. Identificação de riscos – processo para localizar, listar e caracterizar elementos do risco.

5.13. Impacto - é a medida do dano ocasionado caso o evento adverso concretize-se;

5.14. Probabilidade - é a possibilidade de algum evento adverso ocorrer.

5.15. Reduzir risco – forma de tratamento de risco pela

qual se decide realizar a atividade, adotando ações para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco;

5.16 Reter risco – forma de tratamento de risco pela qual se decide realizar a atividade, assumindo as responsabilidades caso ocorra o risco identificado;

5.17. Riscos de Segurança da Informação e Comunicações – potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

5.18. Transferir risco – uma forma de tratamento de risco pela qual se decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco;

5.19. Tratamento dos riscos – processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco;

5.20. Vulnerabilidade - fragilidade de um ativo ou controle que pode ser explorada por uma ou mais ameaças.

Art. 18. Alterar o título do Anexo VII da Portaria GP.TRT4 nº 4.772/2008, que passa a vigorar com a seguinte redação:

NSI007 – Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação – ETIR

Art. 19. Alterar os subitens 1.1., 2.2., 4.5., 5, 6.1., 6.2., 6.3., 7.1., 8.1., 8.2. e 9.1. do Anexo VII da Portaria GP.TRT4 nº 4.772/2008, para substituir a sigla ETRI por ETIR.

Art. 20. Incluir os subitens 3.5 e 3.6 no Anexo VII da Portaria GP.TRT4 nº 4.772/2008, com as seguintes redações:

> 3.5. Norma ABNT NBR ISO/IEC 27002:2022, que fornece um conjunto de referência de controles genéricos de segurança da informação.
>
> 3.6. Resolução CNJ nº 396, de 07 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

Art. 21. Alterar a íntegra dos itens 4 e 10 do Anexo VII da Portaria GP.TRT4 nº 4.772/2008, que passam a vigorar com as seguintes redações:

> **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. Comunidade ou Público Alvo: é o conjunto de pessoas, setores, órgãos ou entidades atendidas pela Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação.
>
> 4.3. CPTRIC-PJ: Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário, que tem por objetivo prover canal oficial de ações preventivas e corretivas, em caso de ameaças ou de ataques cibernéticos.
>
> 4.4. 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.

4.5. Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação – ETIR: Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança da informação.

4.6. Incidente de segurança da informação: Um único ou uma série de eventos indesejados ou inesperados de segurança da informação que têm uma probabilidade significativa de colocar em perigo as operações da instituição e ameaçar a segurança da informação.

4.7. Tratamento de Incidentes de Segurança da Informação: conjunto de processos para detectar, relatar, avaliar, responder, lidar e aprender com incidentes de segurança da informação.

4.8. 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.

4.9. Vulnerabilidade: fragilidade de um ativo ou controle que pode ser explorada por uma ou mais ameaças.

[...]

10. Atribuições

10.1. Planejar, em conjunto com outras áreas da SETIC, ações para a prevenção de incidentes cibernéticos e de dados pessoais.

10.2. Responder e tratar os incidentes de segurança da informação e de dados pessoais no âmbito do TRT4;

10.3. Receber e analisar as informações sobre vulnerabilidades, artefatos maliciosos e tentativas de intrusão, com definição de estratégias e ações para sua detecção ou correção;

10.4. Fornecer informações, aos envolvidos, sobre a ocorrência e, ao público interno, orientações de prevenção de incidentes de segurança da informação.

10.5. Manter os registros dos incidentes de segurança da informação e de dados pessoais no âmbito do TRT4;

10.6. Divulgar alertas ou advertências diante da ocorrência de um incidente de segurança da informação ou de dados pessoais ou, de forma proativa, em face de vulnerabilidades e incidentes conhecidos e que possam gerar impactos nas atividades dos usuários;

10.7. Interagir com outras equipes e órgãos relacionados ao tratamento de incidentes de segurança, participação em fóruns e redes nacionais e internacionais.

Art. 22. Alterar os subitens 5.1, 6.3, 7.1, 8.1 e 9.1 do Anexo VII da Portaria GP.TRT4 nº 4.772/2008, que passam a vigorar com as seguintes redações:

5.1. Prover capacidade adequada para prevenção,

resposta e tratamento de incidentes de segurança da informação e de dados pessoais no âmbito do TRT4.

[...]

6.3. Externamente, a ETIR se relaciona com o Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR.GOV), Polícia Federal, Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (CPTRIC-PJ) do CNJ, dentre outros.

[...]

7.1. A ETIR será composta por servidores da Secretaria de Tecnologia da Informação e Comunicações, que, além de suas funções regulares, desempenharão as atividades relacionadas à prevenção, ao tratamento e à resposta a incidentes de segurança da informação e de dados pessoais.

[...]

8.1. A ETIR é subordinada à Secretaria de Tecnologia da Informação e Comunicações e é coordenada pela Coordenadoria de Segurança da Informação e Proteção de Dados.

[...]

9.1. A autonomia da ETIR é compartilhada. A equipe recomendará, no mínimo, aos Coordenadores das áreas técnicas envolvidas e à Diretoria da Secretaria de Tecnologia da Informação e Comunicações, os procedimentos de prevenção, de tratamento e de resposta a serem executados e/ou as medidas de recuperação

durante um ataque e apresentará as ações a serem tomadas (ou as repercussões se as recomendações não forem seguidas). De acordo com a gravidade do incidente, a proposição deverá, ainda, ser submetida ao Comitê de Segurança da Informação e Proteção de Dados e/ou à Presidência do Tribunal. As ações serão sempre definidas em conjunto com as instâncias consultadas.

Art. 23. Alterar os subitens 1.1., 2.4., 6.1., 7.4., 7.8., 7.10. e 7.15. do Anexo VIII da Portaria GP.TRT4 nº 4.772/2008, que passam a vigorar com as seguintes redações:

1.1. Estabelecer as diretrizes e definir o processo de Gestão de Incidentes de Segurança da Informação no âmbito deste Tribunal.

[...]

2.4. Formalização de um processo para gerenciamento dos incidentes de segurança da informação, provendo insumos para minimizar e/ou evitar eventos adversos futuros.

[...]

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.

[...]

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.

[...]

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.

[...]

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.

[…]

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.

Art. 24. Alterar a íntegra do item 3 e os subitens 4.8, 4.9, 4.10 e 4.11 do Anexo VIII da

Portaria GP.TRT4 nº 4.772/2008, que passam a vigorar com as seguintes redações:

3. Referências normativas

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.

[...]

4.8. 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.

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.

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.

4.11. Vulnerabilidade: fragilidade de um ativo ou controle que pode ser explorado por uma ameaça.

Art. 25. Alterar os subitens 7.2., 7.2.1., 7.2.2., 7.2.3 e 7.2.4. do Anexo VIII da Portaria GP.TRT4 nº 4.772/2008, que passam a vigorar com as seguintes redações:

7.2. O processo de Gestão de Incidentes de Segurança da Informação é composto pelas seguintes etapas:

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.

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.

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.

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.

Art. 26. Incluir o subitem 4.12. no Anexo VIII da Portaria GP.TRT4 nº 4.772/2008, com a seguinte redação:

> 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.

Art. 27. Excluir o subitem 7.17. do Anexo VIII da Portaria GP.TRT4 nº 4.772/2008.

Art. 28. Alterar os subitens 2.3., 3.2., 3.3. e 5.1.1. do Anexo X da Portaria GP.TRT4 nº 4.772/2008, que passam a vigorar com as seguintes redações:

> 2.3. Manutenção de um nível adequado de resiliência dos serviços e sistemas de TIC críticos frente a eventos que possam causar sua interrupção, contribuindo para contínua melhoria da prestação jurisdicional.
>
> [...]
>
> 3.2. Norma ABNT NBR ISO/IEC 27001:2022, que estabelece os requisitos para um Sistema de Gestão da Segurança da Informação.
>
> 3.3. Norma ABNT NBR ISO/IEC 27002:2022, que fornece um conjunto de referência de controles genéricos de segurança da informação.
>
> [...]
>
> 5.1.1. Reduzir o risco de interrupções dos serviços e sistemas de TIC que suportam as atividades críticas do

TRT4, minimizando o impacto decorrente de tais eventos adversos.

Art. 29. Incluir o subitem 3.5 no Anexo X da Portaria GP.TRT4 nº 4.772/2008, com a seguinte redação:

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

Art. 30. Republique-se a Portaria GP.TRT4 nº 4.772/2008, com as alterações ora promovidas.

Art. 31. Esta Portaria entra em vigor na data de sua publicação.