PORTARIA Nº 4.786 DE 22 DE DEZEMBRO DE 2020.

Altera a Portaria 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.

A 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 n° 4.772/2008 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 Incluir os incisos XIII e XIV, no parágrafo 2º, do Art. 1º, das Diretrizes Gerais da Portaria nº 4.772/2008, com as seguintes redações:

"XIII - Decreto nº 10.222, de 05 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética.

XIV - ISO/IEC 27000:2018, que define uma visão geral sobre sistemas de gestão de segurança da informação e de termos e conceitos utilizados."

Art. 2º Alterar o Art. 2º das Diretrizes Gerais da Portaria nº 4.772/2008, que passa a ter a nova redação:

"Art. 2º Para os efeitos deste Ato aplicam-se as seguintes definições:

Auditoria - processo sistemático, independente e documentado para obter evidências de auditoria e avaliá-las objetivamente para determinar em que medida os critérios de auditoria são atendidos;

Confidencialidade: propriedade de que as informações não são disponibilizadas ou divulgadas a indivíduos, entidades ou processos não autorizados;

Disponibilidade: propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada;

Integridade: propriedade de precisão e completude;

Plano de Continuidade da Prestação dos Serviços: conjunto de ações de prevenção e procedimentos de recuperação a serem seguidos para proteger os processos críticos de trabalho contra efeitos de falhas de equipamentos, acidentes, ações intencionais ou desastres naturais significativos, assegurando a disponibilidade das informações.

Recurso de tecnologia de informação: qualquer equipamento, dispositivo, serviço, infraestrutura ou sistema de processamento da informação, instalações físicas que os abriguem.

Segurança da Informação: conjunto de ações, controles e medidas para assegurar a preservação da confidencialidade, disponibilidade e integridade da informação

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.”

Art. 3º Alterar o Art. 11 das Diretrizes Gerais da Portaria nº 4.772/2008, que passa a ter a seguinte redação:

"As atribuições do Escritório de Segurança da Informação são definidas pela Portaria nº 7.596/2014 e suas atualizações, que regulamenta as atribuições e responsabilidades da Secretaria de Tecnologia da Informação e Comunicações."

Art. 4º Incluir o item 5.3.1.1 no Anexo 1 da Portaria nº 4.772/2008, com a seguinte redação:

"5.3.1.1 A restrição de que trata o item 5.3.1 pode ser flexibilizada: por razão de trabalho, desde que, previamente, autorizada pelo Comitê de Segurança da Informação."

Art. 5º Alterar os itens 5.3.1, 5.3.2 e 5.3.3 do Anexo 1 da Portaria nº 4.772/2008, que passam a ter as seguintes redações:

"5.3.1 Acessar páginas de 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."

"5.3.2 Utilizar programas de troca de mensagens em tempo real (bate-papo) ou programas para troca de conteúdo via rede ponto-a-ponto (*peer-to-peer*), exceto programas homologados pelo TRT4 ou autorizados pelo Comitê de Segurança da Informação."

"5.3.3 Utilizar programas e/ou acessar páginas de áudio e vídeo em tempo real, ou sob demanda, exceto programas homologados pelo TRT4 ou autorizados pelo Comitê de Segurança da Informação."

Art. 6º Incluir os itens 3.14, 5.7.1.6.1, e 5.8.4.2 no Anexo 2 da Portaria nº 4.772/2008, com as seguintes redações:

"3.14 *Alias* - endereço eletrônico alternativo para uma conta de correio eletrônico. Pode ser usado para exibir um endereço genérico ou temporário para o público."

"5.7.1.6.1 Não ocorrerá a exclusão da caixa postal institucional pessoal nos casos de licenças."

“5.8.4.2 Findada a necessidade para a qual a caixa postal institucional da unidade foi criada, o responsável pelo gerenciamento deverá informar à SETIC para a exclusão da caixa postal.”

Art. 7º Alterar os itens 3.3, 3.5, 3.8, 3.13, 5.7.1.2, 5.7.1.6, 5.7.1.7. 5.7.1.8, 5.7.1.8.1, 5.7.2.1, 5.7.2.2, 5.8.4, 7.2, 7.5, 7.7 letras g, n, e o do item 7.7, 7.8.1, e 8.1 no Anexo 2 da Portaria nº 4.772/2008, com as seguintes redações:

"3.3. Lista de distribuição – agrupamento de diversos endereços eletrônicos, representado por um endereço eletrônico específico, que permite a distribuição conjunta de uma mensagem eletrônica a todos os seus integrantes”

"3.5. Identificador – parte inicial do endereço eletrônico, localizada antes do símbolo arroba (@), que o diferencia das demais caixas postais e identifica seu usuário, setor, ou finalidade.”

"3.8. Usuário de correio eletrônico – magistrado, servidor e ou estagiário que utiliza alguma caixa postal eletrônica."

"3.13. *Hoax* – mensagem eletrônica encaminhada a muitos destinatários, e de conteúdo geralmente alarmante e com pouca ou nenhuma veracidade, cujo objetivo é a propagação de boatos e informações distorcidas.”

"5.7.1.2. A criação de caixa postal institucional pessoal de servidor ou magistrado será feita pela SETIC após a notificação de seu ingresso pela SEGESP.”

"5.7.1.6. A caixa postal institucional pessoal de magistrados e/ou servidores será excluída definitivamente nos casos de falecimento, exoneração, demissão, redistribuição, aposentadoria, remoção, permuta de magistrado, vacância por posse em outro cargo inacumulável e cedência permanente a outro órgão ou retorno à origem.”

"5.7.1.7. Ocorridos os fatos descritos no item anterior, incumbe à Secretaria de Gestão de Pessoas comunicá-los à Secretaria de Tecnologia da Informação e Comunicações, no prazo de até 5 dias da publicação do Ato respectivo, exceto nos casos de demissão, quando a comunicação deverá ocorrer de imediato à ciência

do afastamento pela Secretaria de Gestão de Pessoas."

"5.7.1.8. Nos casos de demissão haverá suspensão imediata da caixa postal institucional, a partir da comunicação da Secretaria de Gestão de Pessoas."

"5.7.1.8.1. A exclusão da caixa postal será realizada somente após comunicada pela Secretaria de Gestão de Pessoas a decisão administrativa definitiva (que equivale ao trânsito em julgado)."

"5.7.2.1. O gestor da unidade poderá solicitar, por escrito, à SETIC, a criação de caixa postal institucional pessoal ao estagiário somente quando houver essa necessidade para o serviço a ser desempenhado."

"5.7.2.2. O envio de mensagens por estagiários será restrito a endereços eletrônicos mantidos pelo TRT. Quando for expressamente solicitado, com a devida justificativa pelo gestor da unidade a que vinculados, será permitido o envio a endereços externos."

"5.8.4. Em casos excepcionais, devidamente justificados, e a critério da Presidência, poderão ser criadas caixas postais institucionais a fim de atender comissões, grupos de trabalho ou núcleos formalmente constituídos, bem como demandas de trabalho específicas e eventos temporários."

"7.2. O acesso ao correio eletrônico a partir de estações de trabalho fornecidas pelo Tribunal será feito apenas a partir do navegador de internet."

"7.5. O envio de mensagem eletrônica para lista de distribuição que englobe elevado número de endereços eletrônicos é permitido em caráter excepcional ou a unidades administrativas, autorizado pela Presidência."

"7.7. (...):
(...)

g) *malwares*;

(...)

n) *Spam, phishing e hoax*;

o) materiais criptografados, exceto nos casos em que as informações da mensagem necessitem proteção quanto ao sigilo."

"7.8.1. A SETIC não garante a recuperação de mensagens de e-mails ou de caixas postais excluídos há mais de 20 dias."

"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 da infraestrutura tecnológica do Tribunal ou que contenham conteúdo impróprio."

Art. 8º Alterar o item 7.6. no Anexo 2 da Portaria nº 4.772/2008, com a seguinte redação:

"7.6. É de responsabilidade do usuário:

a. eliminar periodicamente as mensagens eletrônicas contidas nas caixas postais;

b. manter exclusivo o acesso à sua caixa postal institucional pessoal, não compartilhando a respectiva senha e/ou delegando o acesso a terceiros.

c. informar ao Escritório de Segurança da Informação o recebimento de mensagem que contrarie o disposto no item 7.7."

Art. 9º Incluir os itens 5.3.7 e 6.1.9.1 no Anexo 3 da Portaria nº 4.772/2008, com as seguintes redações:

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

"6.1.9.1. Nos computadores portáteis disponibilizados pelo Tribunal aos magistrados e servidores, estes terão privilégio de administrador local."

Art. 10 Alterar os itens 4.2, 5.4.1, 5.4.2, e 6.1.11 no Anexo 3 da Portaria nº 4.772/2008,

com as seguintes redações:

"4.2 Controle de acesso: métodos para garantir que o acesso aos ativos seja autorizado e restrito com base no negócio e em segurança."

"5.4.1 O fornecimento de equipamentos a magistrados e servidores, quando autorizado, está condicionado às necessidades de trabalho e à responsabilização formal a partir de seu recebimento."

"5.4.2 Os computadores portáteis são fornecidos com instalação padrão desenvolvida pelo TRT4, composta por softwares e aplicativos necessários ao desempenho das funções de trabalho, além de softwares para proteção, monitoramento e auditoria do equipamento."

"6.1.11 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.

6.1.11.1 No caso do prestador de serviço necessitar de acesso privilegiado, as regras observarão o disposto no item 6.1.10."

Art. 11 Alterar o item 3 no Anexo 3 da Portaria nº 4.772/2008, que passa a ter a seguinte redação:

3. Referências normativas

3.1. Manual de Instruções para Certificação Digital, produzido pela Seção de Apoio Administrativo, vinculada à SEGESP.

3.2. Norma Complementar 01/IN01/DSIC/GSIPR, de 15 de outubro de 2008, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre a Gestão de Segurança da Informação e Comunicações, no âmbito da Administração Pública Federal, direta e indireta.

3.3. Norma Complementar nº 07/IN01/DSIC/GSIPR (Revisão 01), de 15.07.2014, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece diretrizes para a implementação de controles de acesso à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

3.4. Norma Complementar 10/IN01/DSIC/GSIPR, de 30 de janeiro de 2012, que estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação nos Aspectos Relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal.

3.5. 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.

3.6. Norma Complementar 14/IN01/DSIC/GSIPR, de 30 de janeiro de 2012, que estabelece diretrizes relacionadas à Segurança da Informação e Comunicações para o Uso de Computação em Nuvem nos órgãos e entidades da Administração Pública Federal.

3.7. 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.

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

3.9. Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.

3.10. Norma Técnica ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação.

3.11. Portaria nº 4.646, de 16 de agosto de 2018, da Presidente do TRT da 4ª Região, que regulamenta o desfazimento de bens móveis no âmbito da Justiça do Trabalho da 4ª Região.

3.12. 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. 12 Excluir o item 6.1.12. no Anexo 3 da Portaria nº 4.772/2008.

Art. 13 Alterar os itens 3 e 5 no Anexo 4 da Portaria nº 4.772/2008, que passam a ter as seguintes redações:

"**3. Conceitos e definições**

3.1. *Backup* tipo "*archive*" – é o utilizado pelos *backups* mensais e anuais, tem retenção maior, mas só contém a versão do arquivo no momento do *archive*.

3.2. *Backup* tipo "backup" – é o ordinário, utilizado nos *backups* diários, com retenção menor, mas que contém versões diárias dos arquivos (possibilita o *backup* de várias versões e a navegação por estas versões).

3.3. *Backup* completo – são copiados todos os arquivos existentes no momento do backup.

3.4. *Backup* em fita - mídia magnética. Pode ser movida para cofre resistente a fogo.

3.5. *Backup* incremental – somente os arquivos novos ou modificados desde o último *backup* são transmitidos.

3.6. Disco rígido - Dispositivo de armazenamento local de dados utilizados

pelos computadores.

3.7. Equipamento servidor - Computador com alta capacidade de armazenamento e processamento, destinado ao provimento de serviços e sistemas de TIC.

3.8. Produto, sistema ou serviço - soluções tecnológicas que demandam a salvaguarda de dados por ele utilizados;

3.9. Responsável pelo produto, sistema ou serviço - magistrado, servidor ou área de negócio que responde e/ou define os requisitos da solução.

3.10. RPO (*Recovery-Point Objective*) – o quanto é necessário voltar no tempo para encontrar um *backup* dos dados, ou seja, o tempo máximo de perda de dados.

3.11. RTO (*Recovery-Time Objective*) – tempo estimado para restaurar os dados ou para tornar os sistemas operacionais novamente.

3.12. Versão ativa – é a última versão do arquivo no backup.

3.13. Versão de arquivos – sempre que um arquivo for criado/alterado/apagado, é criada uma nova versão deste arquivo no backup.

3.14. Versão(ões) inativa(s) – versão(ões) anterior(es) à última versão do arquivo no backup.

3.15. *Virtual Tape Library* (VTL) - tecnologia que emula fitas magnéticas em disco, o que garante gravação e restauração em alta velocidade. No TRT há duas soluções de VTL, em locais físicos distintos, para fins de continuidade e disponibilidade.”

"**5. Procedimentos de *backup***

5.1 O responsável pelo produto, sistema ou serviço deve solicitar formalmente à

Coordenadoria de Infraestrutura Tecnológica a inserção de dados ao sistema de backup, previamente à entrada em operação de tais soluções.

5.1.1 Cabe ao responsável pelo produto, sistema ou serviço, definir, com apoio da SETIC, os requisitos para realização do backup, tais como: os dados que devem estar contemplados no backup, tempo de retenção, RTO, RPO, dentre outros.

5.1.2 Em caso de alteração dos requisitos para realização do backup, o responsável deverá atualizar a Coordenadoria de Infraestrutura Tecnológica das novas demandas, para correta salvaguarda das informações.

5.2 Os procedimentos de *backup* realizados pela SETIC serão executados por soluções automatizadas, seguindo especificações técnicas definidas pela equipe técnica responsável, em conformidade com a presente política, abrangendo os dados armazenados no ambiente tecnológico disponibilizado pelo TRT.

5.3 O *backup* dos dados armazenados nos servidores das unidades do interior do Estado será realizado diariamente, à noite.

5.4 Os dados armazenados no disco rígido de estações de trabalho ou de notebooks não serão objeto de *backup* de dados. Nesse sentido, sua recuperação não é garantida em casos de indisponibilidade causados por erros de hardware no disco rígido, apagamentos acidentais ou intencionais, falhas no sistema operacional, ação de códigos maliciosos, dentre outros.

5.5 Os dados objeto de *backup* tipo "*archive"* serão armazenados, ao final do processo, em dois locais: uma cópia no conjunto de fitas primárias, disponíveis para restaurações, e a outra cópia no conjunto de fitas secundárias, armazenadas no cofre.

5.6 A periodicidade, o tempo de retenção, o RPO e o RTO dos *backups* observarão as seguintes regras (excetuados os dados do PJe-JT, que possui regramento próprio):

Tipo de Backup		**Arquivos armazenados em diretórios de rede na Capital**	**Arquivos armazenados em diretórios de rede do interior e dados do inFOR do interior**	**Dados dos sistemas armazenados no Banco de Dados da Capital (NovaJus4, inFOR Capital, e-Revista e Sistemas Administrativos)**
***Backup* Intradiário**	**Dias e horários**	Todos os dias, às 10h, 13h, 15h e 18h.	N/A	Todos os dias, a cada duas horas.
	Retenção	Versões objeto do *backup* serão retidas por três (3) dias.	N/A	A versão objeto de *backup* tem retenção de quinze (15) dias.
***Backup* diário (tipo backup)**	**Dias e horários**	Todos os dias, com início às 22h.	Todos os dias, com início às 10h.	Completo, todos os dias.
	Retenção	Quinze (15) últimas versões do arquivo, desde que as versões inativas estejam dentro de um prazo de 30 dias. No caso de arquivos deletados, a última versão será mantida pelo prazo de 60 dias.	Trinta (30) últimas versões do arquivo, desde que as versões inativas estejam dentro de um prazo de 30 dias. No caso de arquivo deletados, a última versão será mantida pelo prazo de 60 dias.	A versão objeto de *backup* tem retenção de quinze (15) dias.
***Backup* semanal (tipo archive)**	**Dias e horários**	N/A	N/A	N/A
	Retenção	N/A	NA	N/A
***Backup* mensal (tipo archive)**	**Dias e horários**	Terceiro final de semana de cada mês	Terceiro final de semana de cada mês	Primeiro final de semana de cada mês
	Retenção	A versão dos arquivos objeto do *backup* será retida pelo período de seis (6) meses.	A versão dos arquivos objeto do *backup* será retida pelo período de seis (6) meses.	A versão objeto de *backup* será retida pelo período de quinze (15) meses.
***Backup* anual (tipo archive)**	**Dias e horários**	Durante o recesso	Durante o recesso	Durante o recesso
	Retenção	A versão dos arquivos objeto do *backup* será retida pelo período de cinco (5) anos.	A versão dos arquivos objeto do *backup* será retida pelo período de cinco (5) anos.	A versão objeto do *backup* será retida pelo período de dez (10) anos.
RPO (tempo máximo de perda dos dados)		10 horas	24 horas	2 horas
RTO (tempo estimado para a restauração)		Imediato para restaurações pontuais. 30 horas para restauração completa.	2 horas	28 horas

5.7. A periodicidade, o tempo de retenção, o RPO e o RTO dos *backups* dos dados relativos ao PJe-JT observarão as seguintes regras:

5.7.1. O RPO e o RTO abaixo indicados referem-se à tecnologia de backup conhecida como *Virtual Tape Library*, que atua como primeira e segunda instâncias de salvaguarda dos dados e, também, a uma terceira instância, que é o backup em fita magnética, utilizada para fins históricos.

Tipo de Backup	**BANCO DE DADOS POSTGRES**	
***Backup* diário VTL**	**Dias e horários**	Completo, todos os dias.
	Retenção	A versão objeto do *backup* será retida pelo período de quinze (15) dias.
Backup semanal (tipo archive) Tape	**Dia**	Todo final de semana que não coincidir com o backup mensal
	Retenção	15 dias
***Backup* mensal (tipo *archive*) Tape**	**Dia**	Primeiro final de semana de cada mês
	Retenção	A versão objeto do *backup* será retida pelo período de um (1) ano
***Backup* anual (tipo *archive*) Tape**	**Dia**	Em janeiro do ano seguinte, entre os dias 1º e 28, preferencialmente no primeiro domingo.
	Retenção	A versão objeto do *backup* será retida pelo período de cinco (5) anos.
VTL - RPO (tempo máximo de perda dos dados)	2 horas	
VTL - RTO (tempo estimado para a restauração)	19 horas	
RPO (tempo máximo de perda dos dados) Tape	1 semana	
RTO (tempo estimado para a restauração) Tape	19h + procedimentos de inserção das fitas	

5.8. No caso de serviços armazenados em nuvem, a responsabilidade pelo *backup* será da prestadora de serviços, assegurado um prazo de retenção de, no mínimo, 30 dias.

5.9. As mídias de backup, quando transportadas, deverão ser protegidas de extravio e de eventos que possam causar dano físico.

5.9.1. A movimentação de mídias de *backup* deverá ser realizada por servidor designado, com registro, no mínimo, da identificação da mídia e a data e hora da movimentação."

Art. 14 Alterar o item 7.2 no Anexo 4 da Portaria nº 4.772/2008, com a seguinte redação:

"7.2 Os testes serão baseados em dados pré-selecionados que garantam a efetividade, eficiência e confiabilidade do procedimento, na periodicidade e forma estabelecidas no quadro que segue:"

Grupo de *backup*	**Equipes responsáveis pela recuperação**	**Periodicidade**	**Recuperação**	**Equipe responsável pela validação**	**Validação**
Arquivos armazenados em diretórios de rede na Capital	SGBD	Mensal	Restaurar versão do dia anterior de alguns arquivos do volume lógico (drive) sendo testado.	SST	Por amostragem, verificar a integridade de alguns arquivos recuperados.
	SST	Mensal	Utilizando o recurso "Versões Anteriores", restaurar versão do dia anterior de arquivos das cópias intradiárias	SST	Por amostragem, verificar a integridade de alguns arquivos recuperados.
Arquivos armazenados em diretórios de rede do interior	SGBD	Mensal	Restaurar a versão mais recente de alguns arquivos de uma localidade do interior. Alternar localidade a cada teste.	SRT	Por amostragem, verificar a integridade de alguns arquivos recuperados.
Dados do inFOR do interior	SGBD	Semestral	Restaurar versão do dia anterior da base de dados do inFOR de uma das localidades do interior. Alternar localidade a cada teste.	CDS	Testar, por amostragem, o funcionamento adequado do sistema em relação a determinado processo em uma unidade do interior.

Dados dos sistemas armazenados no Banco de Dados da Capital	SGBD	Bimestral	Restaurar versão do dia anterior de uma das tablespaces da base de produção, alternando a cada teste o sistema (inFOR, NovaJus4, Folha, RH, PJ4, System) envolvido.	CDS	Testar, por amostragem, o funcionamento adequado do sistema cujas tablespaces foram recuperadas. Testar inFOR, NovaJus4 e ADMEletrônico em relação a determinado processo. Testar sistemas RH e Folha em relação a determinado servidor.
PJe	SGDB	Mensal	Restaurar para base de BUGFIX e para a base de testes (TST) ou de Treinamento (TRN) do PJe a base de produção.	Equipe de apoio do PJe	Testar a integridade dos dados e funcionamento da base restaurada, mediante sua utilização para homologação de novas versões do PJe.

Art. 15 Alterar o item 2.1 inciso VII no Anexo 5 da Portaria nº 4.772/2008, com a seguinte redação:

"VII - solicitar ao Escritório de Segurança da Informação, quando necessário, a realização de auditorias extraordinárias acerca do uso dos recursos de tecnologia da informação do Tribunal;"

Art. 16 Alterar o item 3 no Anexo 5 da Portaria nº 4.772/2008, que passa a ter a seguinte redação:

"**3. Funcionamento do Comitê**

3.1. Nos impedimentos ou afastamentos do Presidente do Comitê de Governança de Tecnologia da Informação e Comunicações, o Comitê de Segurança da Informação será presidido pelo Juiz Auxiliar da Presidência.

3.2. As deliberações do Comitê de Segurança da Informação poderão ser realizadas por meio de reunião presencial ou remota, ou por outro meio eletrônico.

3.3. O quorum mínimo para deliberação é de quatro membros.

3.3.1 Havendo empate nos votos de deliberação, caberá ao

Presidente do Comitê a decisão final sobre a questão deliberada.

3.4. Compete ao Presidente a convocação para as reuniões.

3.4.1 Poderão ser convidados para a reunião magistrados e/ou servidores não integrantes do Comitê, para esclarecimentos porventura necessários.

3.4.1.1. Membros não integrantes não terão direito a voto nas deliberações do Comitê de Segurança da Informação.

3.4.2. A pauta da reunião e os respectivos documentos serão previamente disponibilizados aos integrantes do Comitê e aos demais convidados para a reunião.

3.4.3. A reunião será registrada em ata, a qual deve ser aprovada por todos os integrantes do Comitê presentes na reunião, em expediente administrativo eletrônico classificado como sigiloso, quando necessário.

3.5. As deliberações do Comitê de Segurança da Informação serão registradas e mantidas, em caráter permanente, pelo Escritório de Segurança da Informação."

Art. 17 Incluir o item 4.8. do Anexo 6 da Portaria nº 4.772/2008, com a seguinte redação:

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

Art. 18 Alterar os itens 5.1. a 5.3, 5.6., e 5.18. do Anexo 6 da Portaria nº 4.772/2008, que passam a ter as seguintes redações:

"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;"

"5.6. 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;"

"5.18. Vulnerabilidade – fragilidade de um ativo ou controle que pode ser explorada por uma ou mais ameaças."

Art. 19 Alterar o item 10 no Anexo 6 da Portaria nº 4.772/2008, que passa a ter a seguinte redação:

"**10. Gestão de riscos em Segurança da Informação e Comunicações (GRSIC-TRT4)**

10.1. O processo de GRSIC-TRT4 é contínuo, fornecendo subsídios e integrando-se à implantação e operação do Sistema de Gestão de Segurança da Informação.

10.2. O processo de GRSIC-TRT4 está baseado nas definições constantes nas normas técnicas ABNT NBR ISO/IEC 27005:2011 e ABNT NBR ISO/IEC 31000:2018 e na Norma Complementar nº 04/IN01/DSIC/GSIPR.

10.3. Os critérios para avaliação do risco levam em consideração o "PSR": a) **Probabilidade**, que é a possibilidade de uma vulnerabilidade ser explorada por uma ou mais ameaça(s), ocasionando um incidente de segurança; b) **Severidade**, que é a consequência para o ativo de informação caso um incidente ocorra; e c) **Relevância**, que é a importância do ativo de informação para os processos de negócio aos quais ele está relacionado. Desta forma, a avaliação de riscos é realizada através do produto de três variáveis (probabilidade, severidade e relevância). A partir do valor obtido, o risco é classificado de acordo com a tabela a seguir:

Classificação do Risco	Valores do "PSR"
Muito baixo	1 a 6
Baixo	8 a 16
Médio	18 a 30
Alto	32 a 50
Muito alto	60 a 125

10.4. O tratamento dos riscos será definido de acordo com as necessidades levantadas pelas partes interessadas, regulamentações e legislações vigentes, avaliação técnica e análise custo/benefício.

10.5. O processo de GRSIC-TRT4 é composto pelas etapas descritas a seguir:

10.5.1 Contextualização - compreende a definição e aprovação do contexto da análise e avaliação de riscos a ser realizada, com a identificação de seu propósito, escopo, limites e partes interessadas.

10.5.2 Análise e Avaliação dos Riscos - compreende o mapeamento dos ativos, identificação, análise e avaliação dos riscos, bem como a elaboração e aprovação do Plano de Tratamento dos Riscos.

10.5.3 Tratamento dos Riscos - compreende a implementação das ações do Plano de Tratamento de Riscos, seu monitoramento e apresentação dos resultados.

10.5.4 Melhoria contínua - compreende a realização da análise crítica pela Administração, com avaliação dos resultados e das propostas de melhoria apresentadas.

10.6. O desenho do processo de Gestão de Riscos de Segurança da Informação, a descrição das atividades, respectivos papéis e

responsabilidades dos envolvidos no processo, bem como demais documentos relacionados, serão publicados no Portal de Governança de TI, após aprovação pela Presidência.

10.7. O processo será revisto anualmente ou em menor prazo, quando necessário, e eventuais alterações propostas nos documentos acima indicados serão, após aprovação pela Presidência deste TRT, objeto de imediata divulgação na forma do item anterior."

Art. 20 Incluir o item 3.4 no Anexo 7 da Portaria nº 4.772/2008, com a seguinte redação:

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

Art. 21 Alterar os itens 5.1, 6.1, 8.2, 8.3 e 8.4 do Anexo 7 da Portaria nº 4.772/2008, com as seguintes redações:

"5.1 Prover capacidade adequada para resposta e tratamento de incidentes de segurança da informação em ambiente tecnológico."

"6.1 O público-alvo da ETRI é formado por todos os usuários do ambiente tecnológico deste Tribunal."

"8.2 A ETRI é composta por servidores da Secretaria de Tecnologia da Informação e Comunicações, sendo:

- assistente-chefe do Escritório de Segurança da Informação;
- coordenador(a) da Coordenadoria de Desenvolvimento de Sistemas;
- coordenador(a) da Coordenadoria de Atendimento a Usuários;
- os(as) assistentes-chefes da Coordenadoria de Infraestrutura Tecnológica;
- coordenador(a) da Coordenadoria de Implantação de Sistemas;"

8.3 Para cada uma das posições o substituto formalmente designado será o suplente;

8.4 Caso necessário, deverão ser convocados outros servidores da Secretaria de Tecnologia da Informação e Comunicações e/ou servidores de outras áreas do Tribunal (jurídica, gestão de pessoas, comunicação social, etc.) para auxiliar a equipe no desenvolvimento de suas atividades."

Art. 22 Alterar os itens 4, 9, 10, 11 no Anexo 7 da Portaria nº 4.772/2008, que passam a ter 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 **Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação – ETRI**: Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança da informação.

4.4 **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.

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

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

"9. Autonomia

9.1 A autonomia da ETRI 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 a serem executados 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/ou à Presidência do Tribunal. As ações serão sempre definidas em conjunto com as instâncias consultadas.

10. Atribuições

10.1 Investigar e propor ações de contenção para os incidentes de segurança da informação relacionados aos ativos de tecnologia de informação;

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

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

10.4. Manter os registros dos incidentes de segurança da informação relacionados aos ativos de tecnologia da informação;

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

10.6. Interagir com outras equipes e órgãos relacionados ao tratamento de

incidentes de segurança, participação em fóruns e redes nacionais e internacionais.

11. Atualização da Norma

11.1. O disposto na presente norma será atualizado sempre que alterados os procedimentos de controle de acesso à internet, observada, ainda, a periodicidade prevista para a revisão da Política de Segurança da Informação."

Art. 23 Excluir o item 12 no Anexo 7 da Portaria nº 4.772/2008.

Art. 24 Incluir o item 3.7. no Anexo 8 da Portaria nº 4.772/2008, com a seguinte redação:

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

Art. 25 Alterar os itens 4.10, 5.1, 7.4, 7.10, e 7.14 do Anexo 8 da Portaria nº 4.772/2008, com as seguintes redações:

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

"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."

"7.4 A notificação de incidente 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 ao Escritório de Segurança da Informação, pelo telefone ou pelo e-mail setic.esi@trt4.jus.br, que a reportará à Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação."

"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 artefatos maliciosos, propondo e implementando as ações de

contenção, comunicando as áreas afetadas e coletando os dados necessários."

"7.14 O encerramento do incidente de segurança da informação será realizado pelo Escritório de Segurança da Informação, 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."

Art. 26 Alterar os itens 4.3, 4.7, e 4.11 no Anexo 10 da Portaria nº 4.772/2008, com as seguintes redações:

"4.3 Continuidade de negócios: capacidade de um órgão ou entidade de, quando ocorrer algum incidente de interrupção, manter suas operações em um nível aceitável, previamente definido, minimizando os impactos e recuperando perdas de ativos da informação das atividades críticas."

"4.7 Plano de Continuidade: Conjunto de procedimentos documentados que orientam a organização, após a interrupção, em como responder, recuperar, retomar e restaurar para um nível predefinido de operação, composto por Plano de Continuidade Operacional e Plano de Recuperação de Desastres."

"4.11 RPO (*Recovery Point Objective*): ponto em que a informação usada por uma atividade deve ser restaurada para permitir a operação da atividade na retomada."

Art. 27 Republique-se a Portaria nº 4.772/2008, com as alterações ora efetuadas.

Art. 28 Esta Portaria entra em vigor na data de sua publicação.

Documento assinado digitalmente

CARMEN IZABEL CENTENA GONZALEZ

Presidente do TRT da 4ª Região/RS