PORTARIA Nº 7.137 DE 21 DE DEZEMBRO DE 2017.

Altera a Portaria nº 4.772/2008, que 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 da Presidência deste Tribunal, de acordo com o artigo 1º, § 1º, da referida norma;

CONSIDERANDO as alterações regimentais aprovadas por meio da Resolução Administrativa n° 50/2017, que conferiu nova denominação à Comissão de Informática, passando a denominá-la Comitê de Governança de Tecnologia da Informação e Comunicações;

CONSIDERANDO os integrantes eleitos para compor o Comitê de Governança de Tecnologia da Informação e Comunicações nos próximos 02 anos, nos termos da Ata nº 12/2017 da Sessão Extraordinária e Plenária do TRT da 4ª Região, de 30-10-2017;

CONSIDERANDO as alterações no quadro de gestores do Tribunal Regional do Trabalho da 4ª Região, a contar de 15-12-2017;

CONSIDERANDO o que consta nos Processos Administrativos nº 0003394-28.2013.5.04.0000, 0004550-85.2012.5.04.0000, 0003230-29.2014.5.04.0000, 0000829-57.2014.5.04.0000 e 0008345-31.2014.5.04.0000,

RESOLVE:

Art. 1º Alterar os itens 5.3.2, 5.3.3, 5.4.1, 5.7 e 6.1 do Anexo 1 da Portaria 4.772/2008, que passam a ter a seguinte redação:

> “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 os 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 os autorizados pelo Comitê de Segurança da Informação."

"5.4.1. A liberação de acesso a sítios e serviços bloqueados, mas necessários ao desempenho das atribuições funcionais do usuário, dependerá de solicitação, devidamente justificada, à Secretaria de Tecnologia da Informação e Comunicações, que a submeterá, quando for o caso, ao Comitê de Segurança da Informação, para deliberação."

"5.7. As medidas identificadas no item anterior, quando implementadas, serão comunicadas à Seção de Atendimento aos Usuários, a fim de possibilitar o repasse de informações aos usuários interessados."

"6.1. Por motivos de segurança, todo acesso à internet será monitorado, e os registros serão mantidos pela Secretaria de Tecnologia da Informação e Comunicações."

Art. 2º Alterar o Anexo 4 da Portaria 4.772/2008, que passa a ter a seguinte redação:

ANEXO 4

NSI004 – Procedimentos de backup e recuperação de dados

1. **Objetivo**

   1.1. Estabelecer diretrizes e padrões para os procedimentos de backup, testes e recuperação de dados realizados pela Secretaria de Tecnologia da Informação e Comunicações, no âmbito do Tribunal Regional do Trabalho da 4ª Região.

2. **Motivações**

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

   2.2. Garantia de que a salvaguarda das informações seja realizada de forma otimizada, atendendo às necessidades do Tribunal.

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 transmitidos todos os arquivos existentes no momento do backup.

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

3.5. Disco rígido local - Dispositivo de armazenamento de dados utilizados pelos computadores pessoais.

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

3.7. 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.

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

3.9. Tivoli Storage Manager (TSM) Server – é o equipamento servidor de backup, que gerencia todos os backups realizados.

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

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

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

4. Referências Normativas

4.1. Instrução Normativa GSI/PR nº 1, de 13.06.2008, do Gabinete de Segurança Institucional da Presidência da República, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

4.2. 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 da organização.

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

5. Procedimentos de backup

5.1. Os procedimentos de backup realizados pela SETIC serão executados de forma automática e abrangem os dados gravados nos diretórios de rede privativos de cada unidade judiciária e administrativa do Tribunal e nos sistemas computacionais disponibilizados pelo TRT.

5.2. O backup dos dados das unidades do interior do Estado será realizado a partir do repositório centralizado em Porto Alegre, após a sincronização dos equipamentos-servidores de cada Foro, realizada ao final de cada dia.

5.3. Os dados armazenados em discos rígidos locais não serão copiados e não será garantida sua recuperação em caso de erro físico nas mídias de gravação ou instabilidade no sistema operacional instalado na máquina.

5.4. 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.

5.5. 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 5h.	Completo, todos os dias.
	Retenção	Quinze (15) últimas versões do arquivo,	Trinta (30) últimas versões do arquivo,	A versão objeto de backup tem retenção

		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.	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.	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	Último 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 seis (6) 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	

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

Tipo de Backup	**ARQUIVOS DE CONFIGURAÇÃO DO APACHE (Interno e Externo)**	**ARQUIVOS DE CONFIGURAÇÃO DO JBOSS**	**BANCO DE DADOS POSTGRES**	
Backup diário	**Dias e horários**	Incremental, de segunda a sexta-feira, com início às 21h.	Incremental, de segunda a sexta-feira, com início às 21h.	Completo, todos os dias.
	Retenção	A versão objeto do backup será retida pelo período de trinta	A versão objeto do backup será retida pelo período de trinta	A versão objeto do backup será retida pelo período de

		(30) dias.	(30) dias.	quinze (15) dias.
Backup mensal (tipo *archive*)	**Dia**	Segundo domingo do mês	Segundo domingo do mês	Segundo domingo do mês
	Retenção	A versão objeto do backup será retida pelo período de um (1) ano	A versão objeto do backup será retida pelo período de um (1) ano	A versão objeto do backup será retida pelo período de um (1) ano
Backup anual (tipo *archive*)	**Dia**	Em janeiro do ano seguinte, entre os dias 1º e 28, preferencialmente no primeiro domingo.	Em janeiro do ano seguinte, entre os dias 1º e 28, preferencialmente no primeiro domingo.	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.	A versão objeto do backup será retida pelo período de cinco (5) anos.	A versão objeto do backup será retida pelo período de cinco (5) anos.
RPO (tempo máximo de perda dos dados)	24 horas	24 horas	02 horas	
RTO (tempo estimado para a restauração)	1 hora	4 horas	19 horas	

5.7. 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.

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

5.8.1. 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.

6. Recuperação de dados

6.1. A recuperação de dados e arquivos, sempre que não puder ser realizada pelo próprio usuário, será solicitada à Secretaria de Tecnologia da Informação e Comunicações, por meio da Seção de Atendimento ao Usuário.

7. Testes de recuperação de dados

7.1. Periodicamente serão realizados testes de recuperação de dados.

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	SST/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.
Arquivos armazenados em diretórios de rede do interior	SRT/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.	SGBD/ 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.

7.3. Os resultados dos testes serão validados, de forma documentada, pelas equipes identificadas no quadro anterior.

7.4. Se restaurações de dados forem realizadas em períodos iguais ou menores que os definidos para os testes, a equipe responsável pela execução dos testes poderá, a partir dos resultados obtidos, considerar que tais ações têm validade como teste naquele período.

8. **Atualização da Norma**

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

Art. 3º Alterar o item 1, os incisos I e III do item 2, o item 3.1 do Anexo 5 da Portaria n° 4.772/2008, que passam a ter a seguinte redação:

"**1. Integrantes do Comitê**

Observado o disposto no art. 8º da Portaria no 4.772/2008, o Comitê de Segurança da Informação será composto pelos seguintes integrantes:

–CLAUDIO ANTONIO CASSOU BARBOSA, Desembargador Presidente do Comitê de Governança de Tecnologia da Informação e Comunicações;

– EVANDRO LUIS URNAU, magistrado de 1° Grau, indicado pelo Comitê de Governança de Tecnologia da Informação e Comunicações;

– ELISABETE SANTOS MARQUES, Juíza Auxiliar da Presidência;

– CLOCEMAR LEMES SILVA, Juiz Auxiliar da Corregedoria Regional;

– BÁRBARA BURGARDT CASALETTI, Diretora-Geral;

– ONÉLIO LUIS SOARES DOS SANTOS, Secretário-Geral Judiciário;

– NATACHA MORAES DE OLIVEIRA, Diretora da Secretaria de Tecnologia da Informação e Comunicações."

"**2. Competências do Comitê**

I - elaborar e submeter à Presidência do Tribunal, ouvido o Comitê de Governança de Tecnologia da Informação e Comunicações, propostas de normas e políticas de uso dos recursos de informação.

[...]

III - estabelecer diretrizes e definições estratégicas para as ações e projetos relacionados à Segurança da Informação."

"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."

Art. 4º Alterar os itens 8.3, 9.2, 9.3, 10 e 11.1 do Anexo 6 da Portaria 4.772/2008, que passam a ter a seguinte redação:

"8.3. A gestão de riscos em projetos é realizada pelo Gerente do Projeto e monitorada pelo Escritório de Projetos da Secretaria de Tecnologia da Informação e Comunicações. "

"9.2. As atividades inerentes à gestão de riscos nos processos de TIC devem observar as diretrizes desta norma e outras específicas relacionadas ao processo. "

"9.3. A gestão de riscos em processos de TIC é monitorada pelo Escritório de Processos de TIC. "

"**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 e da Gestão de Continuidade de Negócios.

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 31000:2009 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, 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 de 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.Considerando as políticas praticadas pelo TRT da 4ª Região, não há riscos passíveis de serem tratados através da estratégia de transferência de riscos.

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

10.6.1. 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.

10.6.2. 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.

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

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

10.7. 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.

10.8. 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. ”

“11.1. As diretrizes previstas na presente norma serão atualizadas sempre que alterados os procedimentos de Gestão de Riscos de TIC, observada a periodicidade prevista para a Política de Segurança da Informação. ”

Art. 5º Alterar o Anexo 7 da Portaria 4.772/2008, que passa a ter a seguinte redação:

ANEXO 7

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

1. Objetivos

1.1. Estabelecer as diretrizes para o funcionamento da Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETRI) do Tribunal Regional do Trabalho da 4ª Região.

2. Motivações

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

2.2. Necessidade de formalização da Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETRI) e seu funcionamento.

2.3. Proteção do ambiente tecnológico do Tribunal.

3. Referências Normativas

3.1. Instrução Normativa GSI/PR nº 1, de 13.06.2008, do Gabinete de Segurança Institucional da Presidência da República, a qual disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

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. Portaria nº 4.772/2008, da Presidência do TRT da 4ª Região, que institui a Política de Segurança da Informação no âmbito deste Tribunal.

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 em redes de computadores;

4.4. Incidente de segurança da informação: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

4.5. Tratamento de Incidentes de Segurança da Informação: 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;

4.6. Vulnerabilidade: qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados.

5. Missão da ETRI

5.1. Coordenar as atividades de tratamento e resposta a incidentes de Segurança da Informação, a fim de contribuir para a garantia da disponibilidade, integridade e confidencialidade das informações.

6. Público-alvo

6.1. O público-alvo da ETRI é formado por todos os usuários da rede de computadores e sistemas deste Tribunal.

6.2. A ETRI relaciona-se, internamente, com as diversas unidades da Secretaria de Tecnologia da Informação e Comunicações e com o Comitê de Segurança da Informação.

6.3. Externamente, a ETRI se relaciona com o Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil – Cert.br e outros órgãos do Poder Judiciário Federal.

7. Modelo de Implementação

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

8. Estrutura Organizacional e Composição

8.1. A ETRI é subordinada à Secretaria de Tecnologia da Informação e Comunicações e é coordenada pelo Escritório de Segurança da Informação.

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

- um representante do Escritório de Segurança da Informação;
- um representante da Coordenadoria de Desenvolvimento de Sistemas;
- um representante da Coordenadoria de Atendimento a Usuários
- um representante da Seção de Suporte Técnico
- um representante da Seção de Redes e Telecomunicações
- um representante da Seção de Gerenciamento de Banco de Dados

8.2.1. Para cada uma das posições será designado um suplente.

8.3. Caso necessário, poderão 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.

9. Integrantes

9.1. São membros titulares:

- CLEONICE SANTOS CONDOTTA, representante do Escritório de Segurança da Informação;
- ANDRÉ SOARES FARIAS, representante da Coordenadoria de Desenvolvimento de Sistemas;
- DIEGO FRAGA CONTESSA, representante da Coordenadoria de Atendimento a Usuários;
- FELIPE BOHM DA CUNHA, representante da Seção de Suporte Técnico;
- GUSTAVO ADOLFO KELLERMANN, representante da Seção de Redes e Telecomunicações;
- ERIC GUATIMOZIN SILVA, representante da Seção de Gerenciamento de Banco de Dados.

9.2. São membros suplentes:

- LUCAS POZATTI - suplente do representante do Escritório de Segurança da Informação;
- FÁBIO DE OLIVEIRA GARCIA, suplente do representante da Coordenadoria de Desenvolvimento de Sistemas;
- ANA LÚCIA MOREIRA, suplente do representante da Coordenadoria de Atendimento a Usuários.
- ANDRÉ LUIZ LIVI, suplente do representante da Seção de Suporte Técnico;
- ERNANI SOARES KERN, suplente do representante da Seção de Redes e Telecomunicações;
- EVANDRO BASSANESI, suplente do representante da Seção de Gerenciamento de Banco de Dados

10. Autonomia

10.1. 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.

11. Atribuições

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

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

11.3. Fornecer informações e orientações sobre a ocorrência ou prevenção de incidente de segurança da informação;

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

11.5. Divulgar 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; e

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

12. Atualização da Norma

12.1. 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. 6º Incluir os itens 3.6. e 4.11 e alterar os itens 7.4., 7.7., 7.10., 7.11. e 7.17 do Anexo 8 da Portaria 4.772/2008, que passam a ter a seguinte redação:

"3.6. Norma Complementar nº 21/IN01/DSIC/GSIPR, 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."

"4.11. 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; ”

“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 os reportarão à Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação. ”

“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.”

“7.10. A Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação deve, em conjunto com as outras áreas da SETIC, investigar o incidente e artefatos maliciosos, propondo e implementando as ações de contenção, comunicando as áreas afetadas e coletando os dados necessários.”

“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.”

“7.17. 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. 7º Alterar o item 6.3 do Anexo 10 da Portaria n° 4.772/2008, que passa a ter a seguinte redação:

“6.3. 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. 8° Alterar os incisos I e II do artigo 8° da Portaria n° 4.772/2008, que passam a vigorar com seguinte redação:

“I – o Desembargador Presidente do Comitê de Governança de Tecnologia da Informação e Comunicações, que o presidirá;

II – um magistrado de 1º Grau, indicado pelo Comitê de Governança de Tecnologia da Informação e Comunicações;"

Art. 9º Republique-se a Portaria nº 4.772/2008, com as alterações ora efetuadas.

Art. 10. Esta Portaria entra em vigor na data de sua publicação.

Vania Cunha Mattos
Presidente do TRT da 4ª Região/RS