PODER JUDICIÁRIO
TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO

PORTARIA Nº 6.137, DE 10 DE OUTUBRO DE 2014.

Altera a Portaria nº 4.772/2008, a qual instituiu a Política de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 4ª Região.

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

CONSIDERANDO o que consta nos processos administrativos eletrônicos nº 0000829-57.2014.5.04.0000 (PA) e 0003230-29.2014.5.04.0000 (PA),

RESOLVE:

Art. 1º Alterar os artigos 14, 14-A e 14-B da Portaria nº 4.772/2008, que passam a ter a seguinte redação:

> **Art. 14.** As normas complementares às diretrizes gerais definidas na Política de Segurança da Informação deste Tribunal serão editadas sob a forma de Anexos, que integrarão a presente Portaria.
>
> **Art. 14-A.** É criada a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETRI, subordinada à Secretaria de Tecnologia da Informação e Comunicações e coordenada pelo Escritório de Segurança da Informação.
>
> **Art. 14-B.** As atribuições da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETRI, sua estrutura, bem como a designação de seus integrantes são regulados no Anexo 7 desta Portaria.

Art. 2° Incluir o Anexo 6 (NSI006 – Gestão de Riscos de Tecnologia da Informação e Comunicações) na Portaria nº 4.772/2008, com a seguinte redação:

ANEXO 6
NSI006 – Gestão de Riscos de Tecnologia da Informação e Comunicações

1. Objetivos

Estabelecer as diretrizes da gestão de riscos relacionada ao ambiente tecnológico no âmbito deste Tribunal, aos projetos e processos de Tecnologia da Informação e Comunicações (TIC), e definir o processo de Gerenciamento de Riscos de Segurança da Informação e Comunicações do TRT da 4ª Região (GRSIC-TRT4).

2. Aplicabilidade

Este documento aplica-se a todas as unidades pertencentes à Secretaria de Tecnologia da Informação e Comunicações, responsáveis por gerenciar, manipular e operar informações, projetos, processos, produtos e serviços relacionados à área de TIC no âmbito do TRT da 4ª Região.

3. Motivações

3.1. Necessidade de um processo sistemático para gerenciar riscos referentes à Segurança da Informação e Comunicações (SIC), projetos e processos de TIC, provendo insumos para aumentar a proteção contra eventos indesejados.

3.2. Correto direcionamento de esforços e investimentos financeiros, tecnológicos e humanos.

3.3. Conformidade com normatizações e regulamentações relacionadas ao assunto.

4. Referências normativas

4.1. Decreto nº 3.505/2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

4.2. Resolução CNJ nº 90/2009, que dispõe sobre os requisitos de nivelamento de Tecnologia da Informação no âmbito do Poder Judiciário.

4.3. 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.

4.4. Norma Complementar nº 04/IN01/DSIC/GSIPR (Revisão 01), de 15.02.2013**,** do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações –

GRSIC nos órgãos ou entidades da Administração Pública Federal – APF, direta e indireta.

4.5. Norma Técnica ABNT NBR ISO/IEC 27005:2011, que fornece diretrizes para o processo de gestão de riscos de Segurança da Informação.

4.6. Norma Técnica ABNT NBR ISO 31000:2009, que fornece princípios e diretrizes genéricas para a gestão de riscos.

4.7. Norma ABNT NBR ISO/IEC 27002:2013, que trata de Código de Prática para a Gestão da Segurança da Informação.

4.8. 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.

4.9. Norma Técnica ABNT ISO GUIA 73:2009, que fornece as definições de termos genéricos relativos à gestão de riscos.

5. Conceitos e definições

5.1. **Ameaça** – conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou uma organização;

5.2. **Análise de riscos** – uso sistemático de informações para identificar fontes e estimar o risco;

5.3. **Análise/avaliação de riscos** – processo completo de análise e avaliação de riscos;

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. **Avaliação de riscos** – processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;

5.6. **Comunicação do risco** – troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e as outras partes interessadas;

5.7. **Estimativa de riscos** – processo utilizado para atribuir valores à probabilidade e às consequências de um risco;

5.8. **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;

5.9. **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. **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;

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

5.15. **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;

5.16. **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;

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

5.18. **Vulnerabilidade** – conjunto de fatores internos ou causa potencial de um incidente indesejado que podem resultar em risco para um sistema ou uma organização, os quais podem ser evitados por uma ação interna de Segurança da Informação.

6. Escopo

A Gestão de Riscos, definida por esta Norma, tem seu escopo limitado às medidas protetivas dos ativos de informação, bem como dos projetos e

processos relacionados à área de TIC, que suportam os principais processos de negócio do TRT da 4ª Região.

7. Diretrizes

7.1. A Gestão de Riscos leva em consideração as definições do Planejamento Estratégico Institucional e do Planejamento Estratégico de TIC e está alinhada à Política de Segurança da Informação deste Tribunal.

7.2. A Gestão de Riscos é abordada de forma sistemática, com o objetivo de manter os riscos em níveis aceitáveis para cada projeto, processo e/ou serviço analisado.

7.3. Os riscos são analisados e avaliados em função de sua relevância para os principais processos de negócio deste Tribunal e são tratados de forma a assegurar respostas tempestivas e efetivas.

8. Gestão de riscos em projetos de TIC

8.1. A gestão e comunicação de riscos em projetos de TIC são definidas na metodologia de gerenciamento de projetos adotada e têm como objetivo aumentar a probabilidade e o impacto dos eventos positivos e reduzir a probabilidade e o impacto dos eventos negativos no projeto.

8.2. As atividades inerentes ao gerenciamento de riscos em projetos relacionados à TIC devem observar o disposto na metodologia de gerenciamento de projetos adotada.

8.3. A gestão de riscos em projetos é monitorada pelo Escritório de Projetos da Secretaria de Tecnologia da Informação e Comunicações.

9. Gestão de riscos em processos de TIC

9.1. A gestão e comunicação de riscos em processos de TIC são definidas na especificação de cada processo e visam à identificação e ao controle dos eventos que possam comprometer seus objetivos, contribuindo para sua melhoria.

9.2. As atividades inerentes à gestão de riscos nos processos de TIC (por exemplo: contratação, desenvolvimento, etc.) devem observar as diretrizes desta norma e outras específicas relacionadas ao processo.

9.3. A gestão de riscos em processos de TIC é monitorada pela Seção de Governança 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. Considera-se como **Impacto**, o produto da Severidade e da Relevância. 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. Os riscos classificados como "Baixo" ou "Muito Baixo" são aceitos pela Presidência do TRT da 4ª Região (conforme item 10.7.2).

10.4.1. A aceitação do risco, neste caso, não significa negligenciá-lo, mas reconhecer sua existência e acompanhá-lo, de forma a evitar ser surpreendido por sua concretização.

10.4.2. Os demais riscos serão tratados de acordo com as necessidades levantadas pelas partes interessadas,

pelas regulamentações e legislações vigentes e pela 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. Definições preliminares – compreende a definição do escopo da avaliação de riscos a ser executada e a identificação das partes interessadas, considerando os critérios para classificação e aceitação de riscos definidos nos itens 10.3 e 10.4, respectivamente.

10.6.1.1. O escopo pode abranger o Tribunal como um todo, um segmento, um processo, um sistema, um recurso ou um ativo de informação.

10.6.1.2. O escopo é definido considerando-se prioritariamente os principais serviços que suportam os processos de negócio do TRT da 4ª Região.

10.6.2. Análise/Avaliação dos riscos – compreende:

10.6.2.1. Mapeamento dos ativos de informação no âmbito do escopo definido;

10.6.2.2. Identificação dos riscos: identificação de ameaças, vulnerabilidades e dos controles de SIC já existentes, relacionados aos ativos mapeados;

10.6.2.3. Análise dos riscos: informar valores para probabilidade, severidade e relevância de cada risco para o escopo analisado;

10.6.2.4. Avaliação dos riscos: determinar, considerando os itens 10.3 e 10.4, se os riscos são aceitáveis ou se requerem tratamento, comparando-se a estimativa de riscos com os critérios estabelecidos na fase anterior; e

10.6.2.5. Relação dos riscos que requeiram tratamento, priorizando-os de acordo com os critérios estabelecidos na fase anterior.

10.6.3. Plano de Tratamento de Riscos – compreende a elaboração de plano visando à definição das formas de tratamento dos riscos, de implantação de controles e dos responsáveis por sua implementação, considerando as restrições organizacionais, estruturais, tecnológicas e técnicas, os requisitos

normativos e/ou legais, os controles de SIC existentes e implementados e a análise custo/benefício.

10.6.3.1. Para cada risco levantado, deve ser definida a estratégia de tratamento: mitigar (reduzir), evitar ou reter.

10.6.3.2. Para cada tratamento, devem ser definidas as tarefas a serem realizadas, o responsável pela execução do tratamento e o prazo de execução;

10.6.3.3. Considerando a definição da estratégia de tratamento e do(s) controle(s) a ser(em) implementado(s), deve ser informado, para cada risco levantado, o risco residual.

10.6.4. Aceitação de riscos – nesta fase, são verificados os resultados do processo executado, considerando o Plano de Tratamento de Riscos aprovado, e os riscos residuais, aceitando-os formalmente ou submetendo-os a nova avaliação.

10.6.5. Implementação do Plano de Tratamento de Riscos: após a aceitação dos riscos, as ações de SIC contidas no Plano aprovado devem ser executadas e implantadas.

10.6.6. Monitoramento e análise crítica: esta fase tem por objetivo monitorar os riscos levantados e detectar possíveis falhas nos resultados, nos controles implementados e na eficácia da GRSIC-TRT4.

10.6.6.1. Monitoramento dos riscos: os riscos devem ser regularmente monitorados e analisados criticamente, a fim de verificar mudanças relativas aos critérios de avaliação e de aceitação dos riscos, aos processos/fluxos suportados pela área de TIC, aos ativos de informação, às ações de segurança da informação e aos fatores do risco (ameça, vulnerabilidade, probabilidade e impacto);

10.6.6.2. Monitoramento do processo de GRSIC-TRT4: o processo deve ser monitorado e analisado criticamente, com o objetivo de mantê-lo alinhado às normas relacionadas à matéria e às necessidades do TRT da 4ª Região.

10.6.7. Melhoria do processo de GRSI-TRT4 – a cada dois anos ou sempre que necessário, o processo deverá ser revisto, e, se for o caso, encaminhada proposta à Presidência, após parecer do Comitê de Segurança

da Informação, a fim de implementar eventuais melhorias identificadas, executando-se as ações corretivas ou preventivas aprovadas, assegurando que as melhorias atinjam os objetivos pretendidos.

10.6.8. Comunicação do Risco: as unidades da Secretaria de Tecnologia da Informação e Comunicações, o Comitê de Segurança e a Presidência devem ser consultados ou informados nas diversas fases da gestão de riscos.

10.7. Responsabilidades da GRSIC-TRT4

10.7.1. O Escritório de Segurança da Informação, em conjunto com a Diretoria da Secretaria de Tecnologia da Informação e Comunicações, é responsável por gerenciar e coordenar as atividades inerentes ao processo de GRSIC no âmbito do TRT da 4ª Região especificadas no item 10.6.

10.7.2. Cabe à Presidência do TRT da 4ª Região, após manifestação do Comitê de Segurança da Informação, aprovar formalmente os seguintes documentos: definições preliminares da análise de GRSIC-TRT4 (subitem 10.6.1), o documento de aceitação de riscos (subitem 10.6.4) e o relatório de melhorias a serem implantadas/executadas (subitem 10.6.7).

Art. 3º Incluir o Anexo 7 (NSI007 – Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETRI) na Portaria nº 4.772/2008, com a seguinte redação:

ANEXO 7
NSI007 – Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETRI

1. Missão

Apoiar as atividades de tratamento e resposta a incidentes em redes computacionais, a fim de contribuir para a garantia da disponibilidade e da segurança na prestação de serviços do Tribunal.

2. Referências Normativas

2.1 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.
2.2 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.
2.3 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.
2.4 Portaria nº 4.772/2008, da Presidência do TRT da 4ª Região, que institui a Política de Segurança da Informação no âmbito deste Tribunal.

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

4. Modelo de Implementação
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 em redes computacionais.

5. Estrutura Organizacional e Composição
A ETRI é subordinada à Secretaria de Tecnologia da Informação e Comunicações e é coordenada pelo Escritório de Segurança da Informação.
A ETRI é composta por servidores da Secretaria de Tecnologia da Informação e Comunicações, sendo: um administrador de redes, um administrador de banco de dados, um analista de suporte (atendimento) e um analista de sistemas.
Para cada uma das posições será designado um suplente.

Caso necessário, poderão ser convocados servidores de outras áreas do Tribunal (jurídica, gestão de pessoas, comunicação social, etc.) para auxiliar a equipe no desenvolvimento de suas atividades.

6. Integrantes

A ETRI é composta pelos seguintes integrantes:

Membros Titulares:

– ANDRÉ SOARES FARIAS, analista de sistemas;
– FELIPE BOHM DA CUNHA, administrador de redes;
– ERIC GUATIMOZIN SILVA, administrador de banco de dados;
– DENILSON RIBEIRO DE QUADROS, analista de suporte (atendimento).

Membros Suplentes:

– FÁBIO DE OLIVEIRA GARCIA, suplente do analista de sistemas;
– ANDRÉ LUIZ LIVI, suplente do administrador de redes;
– EVANDRO BASSANESI, suplente do administrador de banco de dados;
– DIEGO FRAGA CONTESSA, suplente do analista de suporte (atendimento).

7. Autonomia

A autonomia da ETRI é compartilhada. A equipe recomendará, no mínimo, aos Coordenadores das áreas técnicas envolvidas, à Diretoria da Secretaria de Tecnologia da Informação e Comunicações e ao Escritório de Segurança da Informação, 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 à Presidência do Tribunal. As ações serão sempre definidas em conjunto com as instâncias consultadas.

8. Atribuições

São atribuições da ETRI:

I – opinar sobre assuntos relacionados a tratamento e resposta a incidentes em redes computacionais;

II – propor as metodologias e os processos específicos para tratamento e resposta a incidentes em redes computacionais, tais como análise, avaliação de riscos e vulnerabilidades;

III – prover ações de monitoria, auditoria e registro de dados em redes computacionais;

IV – participar na elaboração de planos de continuidade;

V – analisar tecnicamente e monitorar incidentes de segurança da informação;

VI – realizar testes e verificações em sistemas e serviços de redes computacionais;

VII – participar de investigações de incidentes de segurança da informação;
VIII – identificar e avaliar os riscos decorrentes da implementação de mudanças no ambiental computacional.

Art. 4º Republique-se a Portaria nº 4.772/2008, com as alterações promovidas pela presente.

Art. 5º Esta Portaria entra em vigor na data de sua publicação.

CLEUSA REGINA HALFEN
Presidente do TRT da 4ª Região/RS