TRIBUNAL REGIONAL ELEITORAL DE MATO GROSSO

PORTARIA Nº 47/2020

Institui a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do TRE-MT (ETIR/TRE-MT) e as políticas de Gestão de Incidentes de TIC e de Gestão de Riscos de TIC.

O **PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DE MATO GROSSO**, no uso das atribuições que lhe são conferidas pelo art. 19, XL do Regimento Interno deste Tribunal,

Considerando a Política de Segurança da Informação da Justiça Eleitoral (PSI-JE), aprovada pela Resolução TSE nº 23.501, de 19 de dezembro de 2016 e a ETIR/TSE instituída pela Portaria TSE nº 1.014 de 23 de novembro de 2018;

Considerando o disposto nos Acórdãos nº 866/2011, nº 594/2011, nº 7312/2010 e nº 2746/2010, do TCU Plenário, que determinam a instituição de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

Considerando a importância da adoção de boas práticas relacionadas à proteção da informação, preconizadas pelas Normas NBR ISO/IEC 27001:2013 e 27002:2005, e da análise de riscos pela NBR ISO/IEC 27005:2008;

Considerando o que consta no processo SEI nº 06788.2019-8,

RESOLVE:

Art. 1º Constituir a equipe de tratamento e resposta a incidentes em redes computacionais do TRE-MT (ETIR/TRE-MT), com a seguinte composição:

I - a(o) Gestor(a) de Segurança da Informação, cuja nomeação é disciplinada pela Portaria TRE-MT nº 101/2017, alterada pela Portaria TRE-MT nº 399/2017, que atuará como Coordenador(a) da ETIR;

II - a(o) Coordenador(a) de Infraestrutura Computacional;

III - a(o) Coordenador(a) de Soluções Coorporativas;

IV - a(o) Chefe da Seção de Gerência de Redes;

V - a(o) Chefe da Seção de Suporte Operacional;

VI - a(o) Chefe da Seção de Banco de Dados.

Art. 2º Estabelecer a Política de Gestão de Incidentes de Segurança em Redes Computacionais do TRE-MT que deverá ser observada e mantida pela ETIR/TRE-MT.

Art. 3º Instituir a gestão de riscos relativos à segurança da informação e designar como gestor(a) de risco de TIC a(o) titular da Secretaria de Tecnologia da Informação.

Parágrafo único. A(o) titular da Secretaria de Tecnologia da Informação poderá delegar a competência para gerir os riscos, objeto desta Portaria.

DOS CONCEITOS E DEFINIÇÕES

Art. 4º Para os efeitos desta Portaria e de seus anexos aplicam-se as seguintes definições:

I. Equipe de tratamento e resposta a incidentes em redes computacionais ETIR: grupo de pessoas com a responsabilidade de receber, analisar e responder as notificações e as atividades relacionadas a incidentes de segurança em redes computacionais;

II. Incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relativo a segurança dos sistemas de computação ou das redes computacionais;

III. Tratamento de incidentes de segurança em redes computacionais: serviço que consiste em receber, filtrar, classificar e responder as 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;

IV. Gestão de riscos relativos à segurança da informação: processo contínuo, aplicado a todo o Tribunal, que consiste no desenvolvimento de um conjunto de ações destinadas a identificar, analisar, avaliar, priorizar, tratar e monitorar riscos capazes de afetar o cumprimento dos objetivos organizacionais relativos ou que façam uso direto da tecnologia da informação.

DO OBJETIVO E COMPETÊNCIAS

Art. 5º A ETIR/TRE-MT tem como objetivo garantir o tratamento e a resposta a incidentes de segurança na rede computacional, no âmbito do Tribunal Regional Eleitoral de Mato Grosso.

Parágrafo único. As competências e a forma de organização da ETIR/TRE-MT estão previstas no Anexo I desta Portaria.

Art. 6º A gestão de incidentes de segurança em redes computacionais complementa as obrigações da ETIR/TRE-MT.

Parágrafo único. Os objetivos, conceitos, escopo e diretrizes para o tratamento de incidentes no Tribunal estão previstas no Anexo II desta Portaria.

Art. 7º A gestão de riscos relativos à segurança da informação constitui-se de ferramental imprescindível para as análises da ETIR/TRE-MT, com vistas a mitigar ou prevenir incidentes e deverá ser condição para a implantação de

controles.

Parágrafo único. O modelo (framework) a ser adotado para o tratamento de riscos relativos à segurança da informação está previsto no Anexo III desta Portaria.

Art. 8º Além das atribuições previstas no Anexo I desta Portaria, compete também à ETIR/TRE-MT:

I - formalizar à ETIR/TSE os incidentes de segurança em redes computacionais que envolvam ou que possam vir a envolver mais de um Tribunal Eleitoral;

II - atender às orientações da ETIR/TSE;

III - receber e acompanhar os direcionamentos da ETIR/TSE e atuar em conjunto com os demais Regionais nas atividades de tratamento do incidente de segurança nas redes computacionais que envolver mais de um Estado;

IV- promover o intercâmbio científico-tecnológico concernente à segurança de redes computacionais, no âmbito da Justiça Eleitoral e com outras instituições;

V - sugerir mecanismos que permitam a prevenção de incidentes de segurança de redes computacionais da Justiça Eleitoral;

VI - sugerir a capacitação no tema de tratamento de incidentes de segurança em redes computacionais e análise de riscos de TIC.

DAS DISPOSIÇÕES GERAIS

Art. 9º Os anexos desta portaria deverão ser periodicamente atualizados pelo Comitê Gestor de Tecnologia da Informação - CETI.

Art. 10 Os casos omissos serão resolvidos pelo Presidente do CETI e as dúvidas surgidas na aplicação deste normativo serão dirimidos pela(o) titular da Secretaria de Tecnologia da Informação do Tribunal Regional Eleitoral.

Art. 11 Esta portaria entra em vigor na data de sua publicação.

Cuiabá-MT, 03 de fevereiro de 2020.

Desembargador **GILBERTO GIRALDELLI**
Presidente

TRIBUNAL REGIONAL ELEITORAL DE MATO GROSSO

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

ANEXO I

ETIR/TRE-MT - Equipe de tratamento e resposta a incidentes em redes computacionais do Tribunal Regional Eleitoral de Mato Grosso.

1. Objetivo e motivação

1.1. O objetivo desta norma é estabelecer as diretrizes para o funcionamento da equipe de tratamento e resposta a incidentes em redes computacionais (ETIR) do Tribunal Regional Eleitoral de Mato Grosso, com vistas a:

1.1.1. Alinhar as normas, regulamentações e melhores práticas relacionadas à matéria;

1.1.2. Formalizar a equipe de tratamento e resposta a incidentes em redes computacionais (ETIR) e seu funcionamento;

1.1.3. Proteger o ambiente tecnológico do Tribunal.

2. Missão da ETIR

2.1. Facilitar e coordenar as atividades de tratamento e resposta a incidentes em redes computacionais, de modo a contribuir para a garantia da disponibilidade, integridade e confidencialidade das informações do Tribunal, bem como colaborar com o intercâmbio científico-tecnológico relacionado à segurança de redes computacionais no âmbito da Justiça Eleitoral.

3. Referências Normativas

3.1. Lei nº 12.965, de 23 de abril de 2014 – marco civil da internet no Brasil.

3.2. Lei nº 13.709, de 14 de agosto de 2018, Lei geral de proteção de dados – LGPD, que dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (marco civil da internet).

3.3. Instrução Normativa GSI/PR nº 1, de 13 de junho de 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.

3.4. Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 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.

3.5. Norma Complementar nº 08/IN01/DSIC/GSIPR, de 19 de agosto de 2010, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que disciplina o gerenciamento de incidentes de segurança em redes computacionais 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.

3.6. Resolução nº 23.501/2016 do Tribunal Superior Eleitoral - TSE, que institui a Política de Segurança da Informação no âmbito da Justiça Eleitoral.

3.7. Acórdãos nºs 866/2011, 594/2011, 7312/2010 e 2746/2010, todos do TCU Plenário, que determinam a instituição de equipe de tratamento e resposta a incidentes em redes computacionais. Normas técnicas: ISONBR/IEC 27001:2013, 27002:2005.

3.8. Normas técnicas relativas à gestão de risco, especialmente ISONBR/IEC 27005:2008.

4. Conceitos e definições

4.1. **Agente responsável/Coordenador:** servidor público ocupante de cargo efetivo incumbido de liderar e coordenar os trabalhos e as entregas da equipe de tratamento e resposta a incidentes em redes computacionais, bem como pelo relacionamento com entes internos e externos quanto às funções e ações da ETIR.

4.2. **Artefato malicioso:** 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 rede de dados.

4.3. **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 em redes de dados.

4.4. **Incidente de segurança em redes computacionais:** qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de dados e demais dispositivos interligados.

4.5. **Público Alvo:** é o conjunto de pessoas, setores, órgãos ou entidades atendidas pela ETIR-TRE-MT.

4.6. **Tratamento de incidentes de segurança em redes computacionais:** é o serviço que consiste em receber, filtrar, classificar e responder as 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.

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

4.8. **CETI**: Comitê Gestor de Tecnologia da Informação.

5. Público-alvo

5.1. O público-alvo da ETIR é formado por todos os usuários da rede de dados da Justiça Eleitoral que a acessa por meio das redes de dados deste Tribunal.

5.2. A ETIR relaciona-se internamente com as unidades da Secretaria de Tecnologia da Informação (STI) e com o Comitê Gestor de Tecnologia da Informação (CETI).

5.3. Externamente, a ETIR relaciona-se com a ETIR da Justiça Eleitoral (ETIR/JE) e demais atores, principalmente:

a) O Tribunal Superior Eleitoral;

b) Os demais Tribunais Regionais Eleitorais e o Ministério Público da União;

c) O Tribunal de Justiça e o Ministério Público do Estado de Mato Grosso;

d) Os órgãos e empresas vinculadas ao Poder Legislativo e ao Poder Executivo do Estado de Mato Grosso;

e) As autarquias, empresas públicas e os órgãos e repartições dos demais entes da federação.

6. Modelo de Implementação

6.1. A ETIR será composta por servidores da Secretaria de Tecnologia da Informação, que, além de suas funções regulares, desempenharão as atividades relacionadas ao tratamento e resposta a incidentes em redes computacionais.

6.2. Via de regra a ETIR desempenhará suas atividades de forma proativa e reativa quando necessário.

6.2.1. Os integrantes da ETIR deverão dedicar em torno de cinco por cento de sua jornada mensal de trabalho às ações e atividades proativas e preventivas, mediante planejamento prévio.

6.3. As atividades reativas da ETIR terão prioridade sobre aquelas desempenhadas por seus integrantes em suas unidades de lotação.

6.4. A ETIR contará com dois integrantes auxiliares sendo um da Secretaria de Gestão de Pessoas e outro da Secretaria de Administração e Orçamento que atuarão nas ações proativas e preventivas e que envolvem usuários e capacitação de pessoal, além da promoção de campanhas educativas.

7. Estrutura Organizacional e Composição

7.1. A ETIR está administrativamente subordinada à Secretaria de Tecnologia da Informação e será gerida pela(o) Gestor(a) de Segurança da Informação que constitui Agente Responsável pela ETIR.

7.2. Cabe ao agente responsável pela ETIR levantar a infraestrutura (recursos humanos, materiais e tecnológicos) necessária à prestação dos serviços oferecidos ao público-alvo, bem como propor os meios para a capacitação e o aperfeiçoamento técnico dos integrantes da equipe.

7.2.1. As necessidades de infraestrutura e de desenvolvimento de competências e habilidades dos integrantes da ETIR deverão, sempre que necessário, ser apresentadas ao CETI.

7.3. A ETIR deverá atuar como um grupo de trabalho permanente, formado por:

a) Gestor(a) de Segurança da Informação (Coordenador da ETIR);

b) a(o) Coordenador(a) de Infraestrutura Computacional (CIEC);

c) a(o) Coordenador(a) de Soluções Coorporativas (CSC);

d) a(o) Chefe da Seção de Gerência de Redes (SGR);

e) a(o) Chefe da Seção de Suporte Operacional (SSO) e

f) a(o) Chefe da Seção de Banco de Dados (SBD).

7.3.1. É facultativa a participação direta da(o) titular da Secretaria de Tecnologia da Informação na ETIR .

7.3.2. No caso de ausências, a(o)s titulares deverão ser representada(o)s pela(o)s respectiva(o)s substituta(o)s.

7.4. A(o) Chefe da SGR caberá:

a) Realizar e acompanhar o processo de identificação e classificação de ativos de informação;

b) Realizar e acompanhar o registro dos eventos de segurança;

c) Utilizar metodologia e ferramentas reconhecidas e recomendadas em referenciais técnicos quanto ao processo de coleta e preservação de evidências e

d) Informar os usuários sobre os procedimentos adotados em relação aos incidentes de segurança da informação por eles comunicados.

7.5. A(o) Coordenador(a) da ETIR:

a) Gerenciar a equipe e as atividades que realizar;
b) Acompanhar o processo de identificação e classificação de ativos de informação;

c) Acompanhar o registro dos eventos de segurança;

d) Elaborar os procedimentos internos a serem observados pela ETIR, com apoio da própria equipe;

e) Planejar e distribuir tarefas para a ETIR, inclusive as de caráter proativa e preventiva;

f) Orientar os integrantes da equipe para o fiel desempenho de suas atividades;

g) Encaminhar as comunicações da ETIR às instâncias decisórias e;

h) Assegurar que os usuários sejam informados sobre os procedimentos adotados em relação aos incidentes de segurança da informação por eles comunicados.

7.6. Caso necessário, o(a) titular da Diretoria-Geral poderá convocar outros servidores do Tribunal para auxiliar a ETIR no desenvolvimento de suas atividades.

8. Autonomia

8.1. A ETIR terá autonomia compartilhada, ou seja, recomendará os procedimentos a serem executados quando da detecção de fragilidades em redes e sistemas computacionais e apresentará as ações a serem tomadas ou as repercussões, no mínimo, a(o) titular da Secretaria de Tecnologia da Informação e, em forma de relatório, nas reuniões ordinárias do CETI.

8.1.1. Recebidas as recomendações, cabe a(o) titular da Secretaria de Tecnologia da Informação, ou a quem ele delegar, determinar os procedimentos necessários ou encaminhar a demanda ao CETI para melhor análise de deliberação.

8.2. Na ocorrência de ataques aos serviços de TIC do Tribunal, a ETIR poderá implementar ações visando à interrupção imediata do incidente em redes computacionais, tais como efetuar bloqueios e tornar indisponíveis os serviços afetados, comunicando, prontamente, as ações às instâncias indicadas no item 8.1.

8.2.1. Quando o tratamento e a resposta ao incidente afetar a imagem do Tribunal perante a Sociedade, a exemplo da interrupção de serviços prestados ao cidadão, ou impactar a execução de processos internos críticos, o CETI deverá ser convocado pela(o) titular da Diretoria-Geral para análise conjunta das respostas aos incidentes.

8.2.2. Posteriormente, assim que o evento estiver controlado, a ETIR deverá emitir relatório recomendando as ações para sanar, em definitivo, as falhas que propiciaram o incidente, bem como dar conhecimento do ocorrido ao CETI.

9. Atribuições

9.1. Executar o processo de gestão de incidentes de segurança em redes computacionais estabelecido na Política de Segurança da Informação e nas suas normas anexas.

9.1.1. Os processos de monitoramento, documentação e registos diários poderão ser terceirizados desde que controlados por integrantes da ETIR.

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

9.3. Fornecer informações sobre a ocorrência ou prevenção de incidente em redes computacionais e comunicar à ETIR/JE.

9.4. Manter os registros dos incidentes em redes computacionais relacionados aos ativos de tecnologia da informação e comunicação.

9.5. Apresentar ao CETI, semestralmente, relatório estatístico dos incidentes de segurança ocorridos no período, com os respectivos tratamentos adotados, visando à elaboração de estudos de melhoria dos mecanismos e controles de segurança ou para subsidiar decisões estratégicas sobre segurança da informação.

9.6. Definir os mecanismos de monitoramento e de tratamento de incidentes em redes computacionais para serem implantados pela Seção de Gerência de Redes - SGR.

9.7. Divulgar alertas ou advertências diante da ocorrência de um incidente em redes computacionais ou, de forma proativa e preventiva, em face de vulnerabilidades conhecidas que possam gerar impactos nas atividades do público-alvo.

9.8. Interagir com outras equipes de tratamento e resposta a incidentes em redes computacionais e órgãos relacionados, bem como participar de eventos nacionais e internacionais acerca do tema.

TRIBUNAL REGIONAL ELEITORAL DE MATO GROSSO

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

ANEXO II

Gestão de incidentes de segurança em redes computacionais

1. Objetivo

1.1. Estabelecer o processo de gestão de incidentes de segurança em redes computacionais no âmbito desta Justiça Especializada.

1.2. Alinhar as normas, regulamentações e melhores práticas, relacionadas à matéria.

1.3. Tratar os incidentes no meio ambiente digital, relacionado ao Tribunal Regional Eleitoral de Mato Grosso, com respostas rápidas e eficientes.

1.4. Direcionar e dimensionar os recursos (tecnológicos e humanos) para prover uma gestão de incidentes de segurança em redes computacionais com menor custo e maior qualidade.

1.5. Formalizar um processo sistemático para gerenciamento dos incidentes em redes computacionais, provendo insumos para minimizar e/ou evitar eventos futuros.

2. Referências normativas

2.1. Resolução nº 23.501/2016 do Tribunal Superior Eleitoral - TSE, que institui a Política de Segurança da Informação no âmbito da Justiça Eleitoral.

2.2. 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 no âmbito da organização.

2.3. Norma Técnica ABNT NBR ISO/IEC 27002:2005, que fornece diretrizes para práticas de gestão de segurança da informação.

2.4. Norma Técnica ABNT NBR ISO/IEC 27005:2008, que fornece diretrizes para gestão de riscos em tecnologia da informação.

3. Conceitos e definições

a) **Artefato malicioso:** 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 rede de dados.

b) **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 com acesso aos mesmos.

c) **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 em rede de dados.

d) **Evento adverso:** ocorrência relevante para a segurança da informação, identificada em um sistema, em um serviço ou em uma rede, indicativa de possível violação da Política de Segurança da Informação, de falhas nos controles ou de situação desconhecida.

e) **Incidente de segurança em redes computacionais:** Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

f) **Medida de contenção:** controle e/ou ação para evitar que danos causados por um determinado incidente continuem aumentando com o passar do tempo. Além disso, visa o restabelecimento do sistema/serviço afetado, mesmo que não seja em sua capacidade total.

g) **Medida de solução:** controle e/ou ação tomada para sanar vulnerabilidades e problemas que sejam a causa-raiz de um ou mais incidentes de segurança em redes computacionais.

h) **Tratamento de incidentes de segurança em redes computacionais:** é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas, bem como realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

i) **Usuários:** magistrados e servidores ocupantes de cargo efetivo ou em comissão, requisitados, cedidos, estagiários, terceirizados (empregados de empresas prestadoras de serviços) e pessoal a serviço da Justiça Eleitoral, desde que previamente autorizados, utilizando em caráter temporário ou não os recursos tecnológicos da Justiça Eleitoral no Estado de Mato Grosso.

j) **Vulnerabilidade:** qualquer fragilidade dos sistemas computacionais e rede de dados que permitam a exploração maliciosa e acessos indesejados ou não autorizados.

4. Escopo

4.1. A Gestão de Incidentes de Segurança em Redes Computacionais, definida nesta norma, tem seu escopo limitado às situações relacionadas ao ambiente, ativos e processos de TIC que suportam os principais processos de negócio do Tribunal Regional Eleitoral de Mato Grosso.

5. Diretrizes

5.1. A gestão de incidentes de segurança em redes computacionais tem de assegurar que incidentes na rede computacional sejam identificados, registrados e avaliados em tempo hábil, com a tomada de medidas de contenção e/ou solução adequadas.

5.2. Estão abrangidos por esta norma os eventos, confirmados ou suspeitos, relacionados à segurança de sistemas ou redes computacionais que comprometam o ambiente tecnológico do Tribunal, seus ativos, informações e processos de negócio, bem como aqueles que contrariem a Política de Segurança da Informação, e dos quais decorram interrupção ou indisponibilidade de serviço essencial ao desempenho das atividades, vulnerabilidades de segurança, divulgação, alteração ou destruição de informações e/ou prática de ato definido como crime ou infração administrativa.

5.3. O Tribunal providenciará dispositivos de monitoramento, ferramentas de segurança e detecção de intrusão, a fim de subsidiar a gestão de incidentes de segurança em redes computacionais.

6. Processo de Gestão de Incidentes de Segurança em Redes Computacionais

6.1. O processo de gestão de incidentes de segurança em redes computacionais é contínuo e composto das seguintes etapas:

a) Detecção e registro: compreende a detecção ou o recebimento de notificação de incidente de segurança em redes computacionais, seu registro e obtenção das autorizações necessárias para o encaminhamento da investigação;

b) Investigação e contenção: refere-se à investigação e tratamento do incidente, coleta e preservação de evidências, comunicação às áreas afetadas, proposição e aplicação de ações de contenção, quando necessárias.

c) Encerramento: diz da fase de análise do incidente, com a verificação da necessidade de ações adicionais, providências ou comunicações, e, após o seu cumprimento, a finalização do incidente.

d) Avaliação de incidentes: trata da avaliação histórica de incidentes havidos, com a consolidação das informações, os indicadores e a verificação das oportunidades de melhoria e aprendizados resultantes da experiência.

6.1.1. O processo de gestão de incidentes de segurança em redes computacionais deverá observar as melhores práticas do mercado e deverá ser complementado pela atuação da ETIR.

6.2. O Tribunal poderá receber notificações externas dos cidadãos, CTIR GOV (Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo), CSIRT Cert (Grupos de Resposta a Incidentes de Segurança em Computadores) ou outras instituições correlatas, bem como por meio da Ouvidoria e de outras ETIR's, sobre incidentes ocorridos ou suspeitos, por meio de sistemas gerenciadores de demandas, e-mail, telefone e outros canais de comunicação. Em quaisquer casos, tais comunicados deverão ser remetidas à ETIR para análise e acompanhamento.

6.2.1. O repasse das informações deverá ser feito por meio do endereço eletrônico oficial da ETIR/TRE-MT: etir@tre-mt.jus.br.

6.2.2. Esse endereço eletrônico deverá corresponder a um grupo de usuários responsáveis por receber as informações, além dos membros integrantes da ETIR.

6.2.3. O endereço eletrônico da ETIR poderá ser divulgado para facilitar o recebimento de informações sobre incidentes, oriundas de qualquer usuário ou público externo. Os assuntos não relacionados à atuação da ETIR, recebidos por e-mail, serão direcionados à Ouvidoria Eleitoral.

6.3. Os usuários devem notificar, com brevidade, os incidentes de segurança da informação e vulnerabilidades de que tenham conhecimento ou suspeita, sob pena de cometimento de crime de omissão.

6.4. Vulnerabilidades ou fragilidades suspeitas não poderão ser objeto de teste ou prova pelos usuários sob o risco de violar a Política de Segurança da Informação e/ou provocar danos aos serviços ourecursos tecnológicos.

6.5. As equipes da Secretaria de Tecnologia da Informação, responsáveis pelo monitoramento dos ativos, serviços e sistemas deverão notificar os incidentes a eles relacionados à ETIR, para os registros e os encaminhamentos devidos.

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

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

6.8. A ETIR deverá, em conjunto com outras áreas ou pessoas e quando necessário, investigar o incidente e artefatos maliciosos, propor e implementar as ações de contenção, comunicar as áreas afetadas e coletar os dados necessários.

6.9. A coleta de evidência dos incidentes de segurança em redes computacionais deverá ser realizada pela ETIR ou por pessoal competente autorizado.

6.10. Quando o incidente de segurança em redes computacionais decorrer de suspeita de descumprimento da Política de Segurança da Informação ou houver indícios de infração, será observado o sigilo durante todo o processo, ficando as evidências, informações e demais registros restritos aos envolvidos na investigação.

6.10.1. Terminada a investigação, as informações deverão ser encaminhadas a(o) titular da Secretaria de Tecnologia da Informação. Em sendo integrante da ETIR, as informações deverão ser encaminhadas a(o) titular da Diretoria-Geral.

6.10.2. Quando houver indícios de ilícitos criminais durante o gerenciamento dos incidentes de segurança, a ETIR, juntamente com a(o) titular da Secretaria de Tecnologia da Informação, deverá encaminhar as informações a(o) titular da Diretoria-Geral.

6.11. O encerramento do incidente de segurança em redes computacionais será realizado pela ETIR, com comunicação a todas as áreas interessadas.

6.12. A ETIR relacionar-se-á com a ETIR/TSE, mantendo-a atualizada quanto às ocorrências de incidentes de segurança em redes computacionais e quanto às respectivas ações de tratamento.

6.12.1. O relacionamento da ETIR com o Centro de Tratamento de Incidentes de Segurança de Computadores da Administração Pública Federal - CTIR Gov dar-se-á por intermédio da ETIR/TSE.

6.13. A avaliação do processo de gestão de incidentes de segurança em redes computacionais ocorrerá através do histórico de incidentes, com verificação das oportunidades de melhoria.

6.14. O desenho do processo de gestão de incidentes de segurança em redes computacionais, a descrição das atividades, os respectivos papéis e responsabilidades dos envolvidos no processo, bem como os modelos de documentos a serem utilizados nas etapas do processo, serão publicados no Portal de Governança do Tribunal, após aprovação pelo Comitê de Segurança da Informação ou pelo CETI.

6.15. O processo será anualmente revisto ou, em menor prazo, quando necessário, e eventuais alterações propostas nos documentos acima indicados serão objeto de imediata divulgação na forma do item anterior, após aprovação pelo Comitê de Segurança da Informação ou pelo CETI.

TRIBUNAL REGIONAL ELEITORAL DE MATO GROSSO

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

ANEXO III

Gestão de riscos relativos à segurança da informação

1. OBJETIVO E MOTIVAÇÃO

1.1. A Resolução nº 211 do Conselho Nacional de Justiça que Institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário elenca, em seu artigo 12, II, "c", a gestão de riscos relacionada ao macroprocesso de segurança da informação como procedimento obrigatório.

1.2. Embora possa parecer que a gestão estratégica de riscos de tecnologia da informação e comunicação pressuponha a implantação do processo correlato em nível organizacional e que não haja como falar-se em sua implementação sem antes mapear e controlar os macroprocessos institucionais; acredita-se que, partindo-se do que já realizou o CNJ e o TSE por meio de seus respectivos planejamentos estratégicos e apoiado pelo planejamento estratégico deste Tribunal, passa a ser possível a gestão simplificada dos riscos atinentes, exclusivamente, à TIC e seus processos correlatos de forma independente.

1.3. Além disso, urge providências a fim de assegurar a continuidade do negócio e garantir a disponibilidade dos serviços de TIC, subprocessos do macroprocesso "Segurança da Informação", para os quais o mapeamento e o controle dos riscos é de fundamental importância. Em processos desta natureza é sempre preciso levar em conta a limitação dos recursos financeiros e humanos, isso porque, neste caso, o controle somente se justifica se economicamente viável for.

1.4. Por isso, foi preciso customizar um *framework*, baseado em COBIT (*control objectives for information and related technology*) e nas normas ISO 27005, 31000 e 38500, aceito pelos principais órgãos de controle interno e externo do mundo para atender à necessidade de catalogar e gerenciar o máximo de riscos possíveis observando apenas os principais processos operacionais, estratégicos e de negócio relacionados à Segurança da Informação tratando-se, por hora, os riscos relacionados aos demais processos ou aqueles não mapeados como aceitos de forma passiva.

2. RESULTADO ESPERADO

2.1. O primeiro resultado prático é a criação de um catálogo de riscos conhecidos. A partir dele, poder-se-á justificar os investimentos em TIC ou alterar a estratégia de contratação do Tribunal.

2.2. Em seguida, a partir do tratamento dado, observar-se-ão os efeitos sobre o plano de continuidade do negócio, bem como sobre a disponibilidade dos serviços de TIC, dando amplo conhecimentos aos riscos a que a instituição se encontra exposta.

2.3. Por fim, o processo de gestão de risco como um todo permitirá o planejamento da infraestrutura de TIC, *compliance* e *accountability*.

2.4. O processo deverá estar em operação em até 180 dias após a aprovação do *framework*.

3. FRAMEWORK: FORMA DE IMPLANTAÇÃO

3.1. Este *framework* não se resume apenas à segurança da informação e pode ser utilizado para os processos de gestão de riscos de projetos de TIC e contratações diversas.

3.2. O modelo prevê o cadastramento de qualquer risco de TIC, estratégico ou não.

3.3. Os riscos cadastrados e seus eventuais tratamentos poderão ser compartilhados entre Tribunais por conta da similaridade dos processos internos.

3.4. A unidade responsável pela análise poderá utilizar-se de ferramentas de mercado ou especialmente desenvolvida para realização do gerenciamento de risco.

3.5. Cada unidade da STI poderá realizar sua própria análise de riscos sobre os processos em que atua. A Secretaria de Tecnologia da Informação deverá realizar a análise de riscos de forma geral sobre todos os processos de TIC, podendo delegar a atribuição.

3.6. Detalhamento e conceitos

a) Risco: segundo a ABNT NBR ISO/IEC 38.500:2009 é a combinação da probabilidade de um evento e suas consequências.

b) Risco (em sentido amplo): evento qualificado ou conjunto de eventos capaz de afetar positivamente (oportunidade) ou negativamente (ameaça) os objetivos, processos de trabalho e iniciativas do Tribunal relativamente à segurança da informação.

c) Risco inerente: risco antes da implantação de um controle.

d) Risco residual: risco eventualmente remanescente após a implantação de um controle ou resultante da eficácia, ainda que parcial, de um tratamento.

e) Controle: medida que altera o impacto do risco, tal como: um processo, uma política, um dispositivo, uma prática ou ação etc.

f) Evento: ocorrências internas ou externas que podem causar impacto negativo ou positivo.

g) Gestão de riscos: processo contínuo, aplicado a toda a organização, voltado para o desenvolvimento de um conjunto de ações destinadas a identificar, analisar, avaliar, priorizar, tratar e monitorar riscos, capazes de afetar o cumprimento dos objetivos organizacionais. Entretanto, para esta norma, o escopo se restringe a eventos que podem impactar a segurança da informação no TRE-MT.

h) Impacto: efeito resultante da ocorrência de um evento correlacionado a um risco.

i) Grau de risco: é o produto das variáveis impacto versus probabilidade do risco.

j) Probabilidade: possibilidade de ocorrência do evento que afete um risco gerenciado.

k) Vulnerabilidade: ausência, inadequação ou deficiência em uma fonte de risco, a qual pode vir a contribuir com a concretização de um evento indesejado.

l) Aceitação do risco: grau de risco a que se está disposto a aceitar ou cujo controle não apresenta viabilidade técnica ou econômica.

3.7. Objetivos

a) Aprimorar ou instituir os controles internos relacionados a eventos que possam impactar em riscos à segurança da informação.

b) Possibilitar, por meio de uma visão sistêmica, uma abordagem explícita da incerteza em um processo padronizado e transparente;

c) Formalizar e reconhecer a existência de riscos não tratados, residuais e mitigados.

d) Aprimorar a tomada de decisão sustentando-a com dados técnicos e objetivos.

3.8. Operacionalização

3.8.1. Subprocessos

a) Estabelecimento do escopo: consiste na definição dos parâmetros externos e internos relativos à segurança da informaçãorelacionados ao contexto de exposição mais frequente à risco. A STI deverá desenhar os principais processos com incidência relativa à disponibilidade e à continuidade do negócio ou eles poderão ser observados pelas unidades internas por meio do Planejamento Estratégico de TIC e do Plano Diretor de TIC.

b) Identificar os riscos: envolve a realização de um inventário descritivo dos riscos relacionados aos principais processos mapeados.

c) Analisar os riscos: diz respeito à compreensão da natureza dos eventos correlacionados e seus prováveis impactos. Estabelece-se o grau de risco por meio da combinação da probabilidade de ocorrência multiplicada pelos prováveis impactos.

d) Avaliação dos riscos: nesta fase o controle ou a aceitação do risco deve ser estabelecido.

e) Tratamento dos riscos: caso o risco seja passível de controle, as medidas de resposta deverão ser documentadas e, em seguida, implementadas. Em não sendo, deverá ser aceito o risco ou rapidamente comunicado.

f) Monitoramento: as unidades de controle interno e externo devem, periodicamente, monitorar o processo de gestão de riscos e sua efetividade. A (o) s gestores de riscos devem avaliar o risco em si, a ocorrência de eventos e propor ou aplicar medidas de correção.

g) Comunicação: consiste em tornar transparente para a organização tanto os riscos, quanto os controles, bem como o processo e suas etapas. A comunicação deve ser constante e a publicação dos resultados periódica e clara.

h) Retroalimentação: consiste em tratar o processo de gestão de risco de forma cíclica com periodicidade, por exemplo, bienal. A cada ciclo, uma nova análise deve ser iniciada, aproveitando-se a aprendizagem do ciclo anterior.

i) Grau de maturidade: a cada ciclo, analisar e documentar o grau de maturidade da gestão de riscos da unidade de TIC.

4. FRAMEWORK: IMPLANTAÇÃO

4.1. Após a aprovação dos atos normativos, no prazo assinalado, o processo de análise de risco deverá ser implantado e obedecerá às etapas descritas abaixo.

4.2. Etapa 01:

4.2.1. As atividades envolvidas nesta etapa serão agrupadas por contextos:

a) MAPEAR PROCESSOS PRINCIPAIS: trata-se da escolha dos processos que serão analisados em busca de eventos que possuam impactos que possam significar riscos. Aos demais não mapeados, será atribuída a condição de risco e denominada a aceitação.

b) IDENTIFICAR RISCOS: Identificação e cadastramento dos riscos.

c) ADMINISTRAR RISCOS: Tratamento dos riscos. Realiza-se o cálculo do grau de risco e documentam-se as respostas aos riscos.

d) GERIR RISCO: encaminham-se as respostas aos riscos para as unidades responsáveis pela implementação, realiza-se o monitoramento dos riscos, publicam-se os resultados.

4.3. Etapa 02:

4.3.1. Definição da(o) Gestor(a) de Risco:

a) Trata-se de uma pessoa responsável por um único risco ou por um conjunto de riscos relacionados ou afins.

b) A(o) gestor(a) do processo de gestão de risco não pode ser confundida(o) com o gestor(a) do risco. Esta última(o) está relacionada(o) com o processo mapeado, de onde se identificou o risco e a(o) primeir(a)o é a(o) gestor(a) de toda a atividade em nível organizacional, ou seja, a(o) titular da Secretaria de Tecnologia da Informação ou outra(o) por delegação indicada(o).

c) Além do grupo responsável pela Governança de TIC, caberá ao gestor(a) o monitoramento do risco, sendo este último o responsável direto pelo detalhamento da atividade.

d) Caberá ao gestor(a) a definição da periodicidade de monitoramento obedecendo a diretrizes e macroprocessos da equipe de Governança da TIC (CETI).

4.4. Etapa 03:

4.4.1. Levantamento dos possíveis eventos. Os eventos são identificados e relacionados aos riscos previamente cadastrados, podendo existir mais de um evento possível para um risco e um evento guardar relação com vários riscos.

4.5. Etapa 04:

4.5.1. Categorização do risco. Os riscos são identificados e agrupados em categorias, com vistas a facilitar o seu gerenciamento, a princípio são classificados em:

a) estratégicos: aqueles que podem afetar a tomada de decisão e que se não tratados podem afetar negativamente o alcance dos objetivos da organização;

b) operacionais: os que afetam o desempenho e a qualidade das atividades operacionais de TIC, entretanto, com impacto sobre onegócio como um todo e, por isso, normalmente devem ser tratados, transferidos ou mitigados, mas não poderão ser aceitos por conta do impacto;

c) reputação ou imagem: podem alcançar a imagem da unidade de TIC e podem ser aceitos. Os riscos que podem afetar a organização não poderão ser aceitos;

d) conformidade: podem ser aceitos se a norma não for obrigatória.

4.6. Etapa 05:

4.6.1. Análises:

a) A **análise qualitativa** ou análise empírica dos riscos: processo de avaliar a probabilidade de ocorrência de um evento e o impacto causado por ele. O que se traduz em um risco identificado. Ela se baseia no julgamento e na intuição, mensurados conforme a experiência da(o) gestor(a) do risco.

b) A **análise quantitativa:** análise com base em uma escala numérica ou de valores (quando mensurável) capaz de traduzir a intensidade do risco.

4.6.2. A avaliação do grau de risco é obtida a partir da estimativa de:

a) probabilidade de ocorrência de um evento;

b) gravidade do impacto ou de seus efeitos ou de suas consequências;

4.6.3. O nível do risco, criticidade ou grau é a magnitude do risco. Ele será expresso pelo resultado da multiplicação dos pesos das variáveis estimadas probabilidade (4.6.2.a) versus impacto (4.6.2.b), conforme a relação exemplificativa de pesos a seguir:

a) Probabilidade: muito baixa, peso 1; baixa, peso 3; moderada, peso 5; alta, peso 7; muito alta, peso 9.

b) Impacto: insignificante, peso 1; baixo, peso 3; moderado, peso 5; relevante, peso 7; catastrófico, peso 9.

4.7. Etapa 06:

4.7.1. Calcular a criticidade ou grau de risco: probabilidade multiplicada pelo impacto.

4.7.2. A criticidade obtida deverá ser posicionada em uma classificação adequada para orientar o tratamento padronizado em resposta aos riscos: baixa, moderada, elevada ou extrema, entre outras.

4.8. Etapa 07:

4.8.1. Respostas aos Riscos:

a) **Tratar, prevenir ou evitar**: aplicável a riscos de alto grau. Não devem ser aceitos.

b) **Transferir:** processo onde a responsabilidade pela resposta ao evento é delegada ou transferida para um terceiro.

c) **Compartilhar:** tal como na transferência; aqui, parte do risco (residual) ainda permanece na organização.

d) **Mitigar**: iniciativas visando reduzir ou minimizar a probabilidade de ocorrência de um evento ou mesmo o seu impacto.

e) **Contingenciar:** forma de aceitação do risco de modo ativo, mediante um plano de contingência ou de contramedidas.

f) **Aceitar:** Aceita-se passivamente o risco e seus prováveis impactos.

4.8.2. A organização deverá estabelecer o padrão de resposta a ser adotado de acordo com a criticidade calculada dos riscos gerenciados.

4.9. Etapa 08:

4.9.1. Cumpridas as etapas anteriores, a(o) titular da Secretaria de TI deverá reunir as informações relativas aos riscos e periodicamente apresentá-las ao CETI (Comitê Estratégico de Tecnologia da Informação) para priorização dos controles e conhecimento dos riscos, facultando-se a auditoria à unidade de Controle Interno desta Corte quando a ela convier.