Salvador, 12 de fevereiro de 2019.

Des. JOSÉ EDIVALDO ROCHA ROTONDANO

Presidente do Tribunal Regional Eleitoral da Bahia

ANEXO VIII

NSI-008 – Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR

1. Objetivo

1.1. Estabelecer as diretrizes para o funcionamento da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) do Tribunal Regional Eleitoral da Bahia.

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 em Redes Computacionais (ETIR) e seu do funcionamento.

2.3. Proteção do ambiente tecnológico do Tribunal.

3. Referências Normativas

3.1. 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.

3.2. 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 – APF.

3.3. 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 – APF.

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

4. Conceitos e definições

4.1. Agente responsável: 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 ~~pel~~o 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 redes de computadores.

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 computadores.

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 computadores.

4.5. Público Alvo: é o conjunto de pessoas, setores, órgãos ou entidades atendidas pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

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

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

5. Missão da ETIR

5.1. Facilitar e coordenar 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.

6. Público-alvo

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

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

6.3. Externamente, a ETIR relaciona-se com a ETIR da Justiça Eleitoral (ETIR/JE).

7. Modelo de Implementação

7.1. 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.

7.2. Devido ao modelo, via de regra, a ETIR desempenhará suas atividades, de forma reativa, sem, todavia, deixar de exercer ações proativas quando necessárias.

7.2.1. Os integrantes da ETIR deverão dedicar, 10% de sua jornada mensal de trabalho às ações proativas, conforme planejamento acordado com o Agente Responsável.

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

8. Estrutura Organizacional e Composição

8.1. A ETIR está administrativamente subordinada à Secretaria de Tecnologia da Informação.

8.2. O Gestor de Segurança da Informação, com o apoio do Agente Responsável da ETIR, deverá levantar a infraestrutura (pessoas e recursos 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.

8.2.1. As necessidades de infraestrutura e de desenvolvimento de competências e habilidades dos integrantes da ETIR serão apresentadas à Secretaria de Tecnologia da Informação e ao Comitê de Segurança da Informação.

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

? todos os servidores efetivos lotados na Seção de Infraestrutura Tecnológica;

? Chefe da Seção de Suporte ao Usuário;

? Chefe da Seção de Banco de Dados;

? Chefe da Seção de Soluções Corporativas; e

? Chefe da Seção de Microinformática.

8.3.1. O Agente Responsável da ETIR será o Chefe da Seção de Infraestrutura Tecnológica.

8.3.2. Os Chefes de Seção serão representados, em suas ausências, pelos respectivos substitutos legais, inclusive no tocante ao item 8.3.1.

8.4. Ao Agente Responsável caberá:

8.4.1. Gerenciar a Equipe e as atividades que realizar.

8.4.2. Acompanhar o processo de identificação e classificação de ativos de informação.

8.4.3. Acompanhar o registro dos eventos de segurança.

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

8.4.5. Elaborar os procedimentos internos a serem observados pela ETIR, com apoio da própria equipe.

8.4.6. Planejar e distribuir tarefas para a ETIR, inclusive as de caráter proativo.

8.4.7. Orientar os integrantes da Equipe para o fiel desempenho de suas atividades.

8.4.8. Efetuar as comunicações da ETIR às instâncias decisórias.

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

8.5. Caso necessário, poderão ser convocados outros servidores da Secretaria de Tecnologia da Informação e/ou de outras áreas do Tribunal para auxiliar a Equipe no desenvolvimento de suas atividades.

9. Autonomia

9.1. 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, se as recomendações não forem seguidas, no mínimo, ao Gestor de Segurança da Informação, aos Coordenadores das áreas técnicas envolvidas e ao Secretário de Tecnologia da Informação.

9.2. 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 9.1.

9.2.1. Quando o tratamento e resposta ao incidente afetar a imagem do Tribunal perante à Sociedade, a exemplo da interrupção de serviços prestados ao cidadão, ou impactar a execução de processos internos críticos, seu custo/benefício deverá ser avaliado em conjunto com as instâncias do item 9.1 e com a área responsável pelo serviço/processo.

9.2.2. 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.

10. Atribuições

10.1. Executar o processo de Gestão de Incidentes de Segurança em Redes Computacionais estabelecido na NSI-009.

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

10.3. Fornecer informações sobre a ocorrência ou prevenção de incidente em redes computacionais à Secretaria de Tecnologia da Informação e ao Comitê de Segurança da Informação e comunicar à ETIR/JE.

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

10.5. Apresentar ao Comitê de Segurança da Informação, semestralmente, nos meses de março e setembro, 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;

10.6. Implementar mecanismos de monitoramento e tratamento de incidentes em redes computacionais.

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

10.8. 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.

ANEXO IX

NSI-009 – 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 do Tribunal Regional Eleitoral da Bahia.

2. Motivações

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

2.2. Necessidade de tratar os incidentes em redes computacionais com respostas rápidas e eficientes.

2.3. Correto direcionamento e dimensionamento de recursos tecnológicos e humanos para prover uma Gestão de Incidentes de Segurança em Redes Computacionais com menor custo e maior qualidade.

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

3. Referências normativas

3.1. 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 – APF.

3.2. 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 – APF.

3.4. 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.

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

3.6. Norma Complementar nº 21/IN01/DSIC/GSIPR, de 8 de outubro de 2014, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta.

4. Conceitos e definições

4.1. 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 redes de computadores.

4.2. 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.

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 computadores.

4.4. Evento adverso: ocorrência relevante para a segurança da informação, identificada em um sistema, serviço ou rede, indicativa de possível violação da Política de Segurança da Informação, ~~ou~~ falha de controles ou representativa de situação desconhecida.

4.5. Incidente de segurança em redes computacionais: qualquer evento adverso, confirmado ou sob suspeita.

4.6. 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.

4.7. 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.

4.8. 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.

4.9. Usuários: magistrados e servidores ocupantes de cargo efetivo ou em comissão, requisitados e cedidos, desde que previamente autorizados, bem como empregados de empresas prestadoras de serviços terceirizados, consultores, estagiários, e outras pessoas que se encontrem a serviço da Justiça Eleitoral, utilizando em caráter temporário os recursos tecnológicos do TRE-BA.

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

5. Escopo

5.1. 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 da Bahia.

6. Diretrizes

6.1. 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.

6.2. Estão abrangidos por esta Norma os eventos, confirmados ou suspeitos, relacionados à segurança de sistemas ou redes computacionais, que comprometam o ambiente tecnológico do TRE-BA, 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.

6.3. 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.

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

7.1. O processo de Gestão de Incidentes de Segurança em Redes Computacionais é contínuo e composto pelas seguintes etapas:

a) Detecção e registro: compreende a detecção ou 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: compreende a 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: compreende a análise do incidente, com verificação da necessidade de outras ações, providências ou comunicações, e após seu cumprimento, o encerramento do incidente.

d) Avaliação de incidentes: compreende a avaliação do histórico de incidentes, com consolidação das informações e indicadores e verificação das oportunidades de melhoria e lições aprendidas.

7.1.1. O processo de Gestão de Incidentes de Segurança em Redes Computacionais deverá observar as diretrizes das Normas Complementares nº 08/IN01/DSIC/GSIPR e 21/IN01/DSIC/GSIPR.

7.1.2. A ETIR deverá recomendar, às áreas responsáveis, a implementação de diretrizes estabelecidas nas Normas indicadas no item 7.1.1.

7.2. O Tribunal poderá receber notificações externas (cidadão, CTIR.BR, CSIRT ou outras instituições) sobre incidentes (ocorridos ou suspeitos) por meio de sistemas gerenciadores de demandas, e-mail, telefone e outros canais de comunicação, que deverão ser remetidas à ETIR para o devido encaminhamento.

7.3. A notificação de incidente também poderá ser feita por qualquer usuário através da Central de Serviços de TIC ou pelo e-mail etir@tre-ba.jus.br.

7.3.1. Os usuários devem notificar, com brevidade, os incidentes de segurança da informação e vulnerabilidades de que tenham conhecimento ou suspeita.

7.3.2. 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 ou recursos tecnológicos.

7.4. 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 registro e encaminhamento devidos.

7.5. 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.

7.6. 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.

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

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

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

7.10. Quando houver indícios de ilícitos criminais durante o gerenciamento dos incidentes de segurança, o Comitê de Segurança da Informação e a Administração do TRE-BA deverão ser comunicados, para avaliação das providências cabíveis.

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

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

7.12.1 O relacionamento da ETIR com o Centro de Tratamento de Incidentes de Segurança de Computadores da Administração Pública Federal – CTIR Gov dar-se-á através da ETIR/JE.

7.13. 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.

7.14. 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.

7.15. O processo será revisto anualmente 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.

Decisões/Despachos

PROCESSO ADMINISTRATIVO DIGITAL Nº 1741/2019

Versa o presente expediente sobre autorização de deslocamento e concessão de diárias, tendo em vista a visita do Vice-Presidente e Corregedor Regional Eleitoral desta Corte, Des. Edmilson Jatahy Fonseca Júnior, ao Tribunal Superior Eleitoral a fim de tratar de assuntos atinentes à Justiça Eleitoral, no período de 12 a 14 de fevereiro de 2019, na Cidade de Brasília/DF.

Com efeito, a solicitação encontra amparo no art. 1º, §1º, c/c art. 4º, da Resolução TSE nº 23.323/2010, in verbis:

Art. 1º O magistrado ou servidor da Justiça Eleitoral que se afastar, a serviço, da jurisdição ou sede para outro ponto do território nacional ou para o exterior, em caráter eventual ou transitório, fará jus a passagens e diárias, destinadas a indenizar as despesas extraordinárias com pousada, alimentação e locomoção urbana, na forma prevista nesta resolução.

§ 1º Somente serão concedidas diárias a magistrados e servidores que estejam no efetivo exercício dos respectivos cargos, funções ou atividades equivalentes.

[...]

Art. 4º A concessão de diárias ficará condicionada à disponibilidade orçamentária da Justiça Eleitoral, e pressupõe, obrigatoriamente, a compatibilidade entre o motivo do deslocamento com o interesse público, as atribuições do cargo efetivo e as atividades desempenhadas no exercício da função comissionada ou do cargo em comissão. (Grifos aditados).

A SEAJE, por seu turno, manifesta-se no doc. nº 28170/19 pela concessão de duas diárias e meia, correspondente ao período de 12 a 14.2.2019, totalizando o montante de R$ 1.613,65 (um mil seiscentos e treze reais e sessenta e cinco centavos), conforme indicado no predito documento, em consonância com a Portaria TSE nº 247, publicada no DJE de 21/03/2016.

Do exposto, havendo disponibilidade orçamentária, autorizo o deslocamento e a emissão de nota de empenho, e, tendo em vista que o requerimento encontra abrigo nas normas vigentes, defiro o pedido de pagamento de diárias.

À ASSESP para publicação da presente decisão.

Após, à SEAAC para certificar a emissão das passagens após a retificação das datas do deslocamento.

Por fim, à SOF para adoção das providências pertinentes.

Salvador, 12 de fevereiro de 2019.

Des. JOSÉ EDIVALDO ROCHA ROTONDANO

Presidente do Tribunal Regional Eleitoral da Bahia

Convênios

TERMO DE PARCERIA E COOPERAÇÃO TÉCNICA Nº 1/2019

TERMO DE PARCERIA E COOPERAÇÃO TÉCNICA Nº 1/2019, firmado entre a 183ª Zona Eleitoral e o Município de Teixeira de Freitas/BA: 13876/2018. OBJETO: Cooperação entre os partícipes visando possibilitar a realização do cadastramento biométrico dos eleitores do Município de Teixeira de Freitas/BA. FUNDAMENTO LEGAL: Leis nºs 7.444/1985 e 9.454/1997, Resoluções TSE nºs 21.538/2003 e 23.335/2011. VIGÊNCIA: a partir da assinatura do convênio até 22.2.2019. ASSINATURA: 15.1.2019. SIGNATÁRIOS: Bel. Humberto José Marçal, pela 183ªZE, e Ronaldo Alves Cordeiro, pelo Município de Teixeira de Freitas.