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.