TRIBUNAL REGIONAL ELEITORAL DO MARANHÃO

INSTRUÇÃO NORMATIVA Nº 6, DE 27 JUNHO DE 2022

Dispõe sobre regras e procedimentos empregados pela Equipe de Tratamento e Resposta a Incidentes em Redes computacionais da Justiça Eleitoral do Maranhão.

A PRESIDÊNCIA DO TRIBUNAL REGIONAL ELEITORAL DO MARANHÃO, no uso das atribuições que lhe são conferidas pelo art. 29 do Regimento Interno deste Tribunal, considerando a Resolução TSE nº 23.644/2021, a Resolução TRE-MA nº 9.888/2021, que adota a Resolução TSE nº 23.644/2021 como Política de Segurança da Informação do TRE-MA, a Portaria 738 de 14 de novembro de 2017, que cria a ETIR, a Resolução CNJ nº 396, de 7 de julho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), bem como a Portaria 162, de 10 de junho de 2021, que aprova protocolos e manuais criados pela Resolução 396/202,

RESOLVE:

Art. 1º Esta instrução normativa dispõe sobre regras e procedimentos empregados pela Equipe de Tratamento e Resposta a Incidentes em Redes computacionais da Justiça Eleitoral do Maranhão, com o intuito de elevar o nível de segurança das infraestruturas críticas.

Art. 2º Para fins desta Instrução Normativa entende-se por:

I - Central-TI - unidade destinada ao atendimento dos usuários dos serviços de Tecnologia da Informação - TI, único ponto de contato entre o provedor de serviço e os usuários;

II - ETIR - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais da Justiça Eleitoral do Maranhão, com atribuições definidas pela Resolução 23.644/2021 e pela portaria Resolução CNJ 396/2021, e integrantes definidos pela Portaria da Presidência n. 738, de 14 de novembro de 2017;

III - incidente de segurança de rede: qualquer evento, ainda que suspeito, que viole a política de segurança da informação ou possa comprometer a segurança computacional;

IV - artefatos maliciosos: qualquer tipo de arquivo suspeito enviado para análise, e-mail suspeitos de spam, equipamento; e

V - Indicadores de Comprometimento (IOC): são indicadores (impressão de telas, mensagens, arquivos, etc.) que comprovem que ouve uma violação de segurança.

Art. 3º A missão da ETIR é:

I - receber, analisar, classificar, tratar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores, além

de armazenar registros para formação de séries históricas como insumo estatístico e para fins de auditoria no âmbito da Justiça Eleitoral do Maranhão;

Art. 4º A ETIR será responsável por:

I - coletar e preservar as mídias de armazenamento e registros de eventos dos dispositivos afetados ou as suas respectivas imagens forenses, os dados voláteis armazenados nos dispositivos computacionais, como a memória principal (memória RAM);

II - coletar e armazenar, nos casos de inviabilidade de preservação das mídias de armazenamento, cópia dos arquivos afetados pelo incidente, tais como: logs, configurações do sistema operacional, arquivos do sistema de informação, e outros julgados necessários, mantendo-se a estrutura de diretórios original e os "metadados" desses arquivos, como data, hora de criação e permissões. Caso não seja possível preservar as mídias deve-se fazer constar em relatório os procedimentos adotados;

III - caberá à ETIR elaborar o Processo de Tratamento e Resposta a Incidentes em Redes Computacionais no âmbito do Tribunal Eleitoral;

IV - comunicar a ocorrência de incidentes em redes de computadores aos Centros de Tratamento de Incidentes ligados a entidades de governo, ao Centro de Tratamento de Incidentes em Redes Computacionais do Poder Judiciário e ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - CERT.br, sempre que a cooperação seja necessária para prover uma melhor resposta ao incidente;

V - comunicar com as equipes congêneres de outros Tribunais Eleitorais para o tratamento de incidentes de segurança comuns aos tribunais envolvidos;

VI - observar os protocolos de Prevenção Incidentes, Gerenciamento de Crise e Investigação de Ilícitos contidos na portaria 162 CNJ; e

VII - acionar, em caso de crise, o Comitê de Crise Cibernética.

Art. 5º No modelo de implementação da ETIR-MA não existirá um grupo exclusivamente dedicado às funções de tratamento e respostas a incidentes. A Equipe atuará de forma reativa e será formada a partir dos membros das equipes de TI do próprio TRE-MA, que além de suas funções regulares passarão a desempenhar as atividades relacionadas ao tratamento e resposta a incidentes em redes computacionais.

Art. 6º A ETIR terá como público-alvo as unidades internas da Secretaria e as Zonas Eleitorais do TRE-MA prestando prioritariamente os seguintes serviços:

I - análise de vulnerabilidade;

II - elaboração e divulgação de alertas e avisos;

III - análise de artefatos maliciosos;

IV - prospecção ou monitoramento de novas tecnologias que minimizem ou evitem incidentes de segurança em redes computacionais;

V - avaliação de segurança em redes computacionais;

VI - detecção de intrusão; e

VII - disseminação de informações relacionadas à segurança em redes computacionais. Parágrafo único. As demandas que não se encaixem nas hipóteses

previstas no caput deste artigo serão encaminhadas ao Secretário de Tecnologia da Informação e Comunicação. Da classificação e priorização dos chamados e incidentes.

Art. 7º Todos os chamados deverão ser classificados de acordo com um dos seguintes graus de sigilo:

I - restrito: para informações sigilosas, cujo conhecimento será privativo da ETIR e cuja circulação ficará restrito aos seus membros;

II - parcialmente restrito: quando, em virtude de certo grau de restrição, o intercâmbio de informações se restringir a entidades de alta confiabilidade ou com outras unidades do TRE-MA; ou

III - público: quando as informações puderem ser irrestritamente divulgadas.

Art. 8º Todos os chamados serão categorizados de acordo com um dos seguintes níveis de gravidade:

I - altíssimo: para incidentes que exijam resposta imediata em razão da indisponibilidade de algum serviço, como previstos nos incisos I e II do art. 9º desta Instrução Normativa;

II - alto: para incidentes que tenham potencial de configurar a hipótese prevista no inciso I do caput deste artigo ou caracterizar o disposto nos incisos III e V do art. 9º desta Instrução Normativa; e

III - baixo: para incidentes de baixo impacto ou poder destrutivo, tais como, os descritos nos incisos IV, VI e VII do art. 9º desta Instrução Normativa.

Parágrafo único. Os chamados categorizados como de altíssima gravidade preferirão os de alta e baixa e serão prontamente atendidos.

Art. 9º O incidente subordinar-se-á a uma das seguintes classificações:

I - código malicioso: quando houver alguma infeção por vírus, trojans, worms, spyware, dialler;

II - disponibilidade: quando houver ataques tipo DoS/DDoS ou sabotagem que acarretem indisponibilidade de serviços;

III - coleta de informação: quando houver tentativa de obter informações de rede e serviços de rede por meio de engenharia social, “SCAN”, “SNIFFING” (observação de tráfego de rede), “PHISHING”;

IV - tentativa de intrusão: quando se tentar explorar vulnerabilidades já conhecidas e novas vulnerabilidades ou em caso de tentativa irregular de login;

V - segurança da informação: quando houver acesso não autorizado a informação, modificação/remoção não autorizada de recursos, inclusive por métodos de interceptação;

VI - fraude: quando houver utilização ilegítima de nome de terceiros, acesso não autorizado com o objetivo de fazer passar por outra pessoa ou entidade, violação de direitos autorais;

VII - conteúdo abusivo: utilização de spam, assédio sexual, pornografia infantil, racismo e apologia à violência;

VIII - intrusão: quando houver comprometimento de aplicações ou contas de acesso com ou sem privilégio; ou

IX - outros: quando se tratar de novos incidentes que ainda não foram classificados.

Da abertura do chamado

Art. 10º A abertura de chamado para resolução de incidentes de redes deverá conter, no mínimo:

I - a classificação do chamado, de início categorizado como restrito, nos termos do disposto no inciso I do caput do art. 6º desta Instrução;

II - a classificação do incidente, segundo o disposto no art. 8º desta Instrução;

III - o nível de gravidade do chamado, de acordo com o previsto no art. 7º da presente Instrução;

IV - a data e hora em que o incidente foi percebido;

V - o nome do interessado, e-mail, telefone, local de trabalho;

VI - breve relato em que se informe como o incidente foi percebido, se ainda persiste, que sintomas apresenta e quais equipamentos foram afetados;

VII - eventual notificação acerca da perda de dados;

VIII - eventual notificação acerca de ocorrência de quebra de segurança e sua localização;

IX - informação acerca de indisponibilidade de serviço;

X - descrição pormenorizada de vazamento de dados ou informações sigilosas;

XI - informação sobre eventual dano à imagem do TRE; e

XII - evidências documentais, como, arquivos de log, fotos, emails.

Da documentação dos procedimentos e troca de informações

Art. 11. A ETIR deverá documentar os procedimentos operacionais para os incidentes a fim de guiar suas atividades com pelo menos as seguintes informações:

I - objetivo, âmbito de aplicação e providências preliminares;

II - classificação do incidente, nos termos do disposto no art. 9º desta Instrução;

III - etapas essenciais de execução, contendo as ações a serem realizadas;

IV - indicação de como e onde as informações levantadas serão armazenadas ou documentadas;

V - nome autor do procedimento;

VI - a versão do arquivo de procedimento;

VII - data e hora da última atualização;

VIII - a forma de comunicação do procedimento; e

IX - plano de resposta ao incidente.

Art. 12. A ETIR do TRE-MA ao trocar informações com outras ETIRs, deverá utilizar o padrão IODEF (Incident Object Description Exchange Format) que compreende os seguintes campos:

I - identificador do incidente: número atribuído ao incidente pela ETIR que gerou o documento IODEF;

II - identificador alternativo: número utilizado por outra ETIR para referenciar o incidente descrito no documento;

III - atividades relacionadas: números de incidentes que estejam relacionados;

IV - momento da detecção: o momento no qual o incidente foi detectado pela primeira vez;

V - início do incidente: momento em que se iniciou o incidente;

VI - fim do incidente: momento em que se finalizou o incidente;

VII - momento da divulgação: momento em que se divulgou o incidente;

VIII - descrição: descrição do incidente;

IX - avaliação do impacto: a caracterização do impacto do incidente;

X - método: a técnica utilizada pelo atacante no incidente;

XI - contato: informações de contato das partes envolvidas no incidente;

XII - dados do evento: descrição dos eventos que compreendem o incidente;

XIII - histórico: log de eventos significantes ou ações que ocorreram durante o curso do manuseio do incidente; e

XIV - dados adicionais: qualquer dado necessário para complementar.

Da divulgação das informações

Art. 13. A divulgação ou comunicação de qualquer informação sobre incidente de segurança deverá ser realizada pelo Secretário de TIC, com prévia autorização do Diretor Geral, e auxílio da COIMC caso necessário.

§ 1º Não poderão ter suas informações divulgadas os incidentes:

I - classificados com grau restrito e parcialmente restrito;

II - cujo conteúdo do incidente seja classificado como Sigiloso; e

III - em fase de investigação.

§ 2º Depende de autorização prévia e expressa de terceiros envolvidos a divulgação de incidentes de segurança que lhes digam respeito.

Do processo de tratamento e resposta a incidentes

Art. 14. O início do tratamento iniciará com a fase de detecção, onde haverá a comunicação de incidentes ou solicitação de algum serviço relativo a segurança da informação, que poderá ser realizada por meio:

I - da Central - TI, em se tratando do público interno da Justiça Eleitoral

do Maranhão;

II - da Ouvidoria, no caso do público externo da Justiça Eleitoral do Maranhão; e

III - da ETIR.

§ 1º A Ouvidoria encaminhará à ETIR, por meio da Central - TI, os chamados externos relativos a incidentes de segurança da informação.

§ 2º O chamado será classificado inicialmente pela Central - TI como restrito e poderá ter sua classificação alterada pela ETIR.

Art. 15. Antes de iniciar a análise, a ETIR realizará a triagem, para saber se o incidente é real e se é de sua alçada.

Art. 16. Em caso afirmativo, proceder-se-á à análise do incidente, que consistirá, no mínimo, das seguintes etapas

I - verificação: consiste na verificação se o incidente é real. Ocorre nova verificação se o incidente está no escopo de tratamento da ETIR-MA;

II - classificação e priorização: consiste em nova classificação e priorização dos chamados e incidentes; e

III - designação: em que se define a área ou o profissional mais adequado para tratar o incidente.

Art. 17. Concluída a análise do incidente, passar-se-á à fase de tratamento do chamado, que compreende pelo menos as seguintes etapas:

I - análise de dados: objetiva recolher toda informação possível e nivelar o conhecimento sobre o incidente entre os membros da equipe, incluindo a notificação das partes mais afetadas, coleta de dados, análise de logs, requisição de informações adicionais, análise de sistemas de monitoramento;

II - busca de solução: subsequente ao nivelamento do conhecimento, compreende a aplicação de brainstorm, bem como pesquisa base de soluções;

III - implementação da solução: compreende a execução da solução encontrada; e

IV - erradicação e recuperação: consiste na erradicação do incidente e restabelecimento dos serviços afetados.

Art. 18. Após o restabelecimento dos serviços o chamado entra na fase de finalização, em que se procederá à sua classificação final, ao registro das lições aprendidas e ao efetivo arquivamento.

Art. 19º A ETIR adotará o modelo de autonomia compartilhada e trabalhará em acordo com os outros setores da organização a fim de participar do processo de decisão sobre quais medidas devem ser adotadas durante o tratamento e recuperação de incidentes de segurança.

Parágrafo único. Durante um incidente de segurança, a ETIR executará as medidas técnicas necessárias para interromper o incidente e preservar as evidências relacionadas, e aguardando pela deliberação de níveis superiores de gestão quanto à recuperação e tratamento do incidente conforme o seu nível de gravidade e impacto.

Art. 20. Esta Instrução Normativa entra em vigor na data de sua assinatura.

Cientifique-se. Publique-se. Cumpra-se

Desa. ÂNGELA MARIA MORAES SALAZAR
Presidenta

São Luís, 27 de junho de 2022.

Documento assinado eletronicamente por **ANGELA MARIA MORAES SALAZAR**, **Presidente**, em 30/06/2022, às 19:02, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-ma.jus.br/autenticar informando o código verificador **1649057** e o código CRC **06DECC3E**.

0003374-55.2022.6.27.8000	1649057v8