Art. 2º Registre-se. Publique-se.

Documento assinado eletronicamente por GILBERTO DE PAULA PINHEIRO, Presidente, em 20/09/2022, às 08:43, conforme art. 1º, III, "b", da Lei 11.419/2006.

PORTARIA PRESIDÊNCIA Nº 231/2022 TRE-AP/PRES/ASPRES

Reinstitui a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do Tribunal Regional Eleitoral do Amapá (ETIR/TRE-AP)

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO AMAPÁ, no uso de suas atribuições legais definidas pelo Regimento Interno desta Corte e,

CONSIDERANDO a Política de Segurança da Informação do Tribunal Regional Eleitoral do Amapá (PSI-TRE/AP), aprovada pela Resolução TRE nº 570, de 20 de maio de 2022;

CONSIDERANDO a Política de Segurança da Informação da Justiça Eleitoral (PSI-JE), aprovada pela Resolução TSE nº 23.644, de 1 de julho de 2021;

CONSIDERANDO a Resolução CNJ nº 370/2021, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário;

CONSIDERANDO a Resolução CNJ nº 396/2021, que institui a Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário;

CONSIDERANDO a Portaria TRE-AP nº 281/2021, que Institui o Protocolo de Gerenciamento de Crises Cibernéticas no âmbito do Tribunal Regional Eleitoral do Estado do Amapá;

CONSIDERANDO a Portaria CNJ nº 162/2021, que aprova Protocolos e Manuais criados pela Resolução CNJ nº 396/2021;

CONSIDERANDO a importância da adoção de boas práticas relacionadas à proteção da informação preconizadas pelas normas ISO NBR/IEC 27001:2013 e 27002:2013;

CONSIDERANDO a necessidade de se definir a responsabilidade por receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança da informação;

CONSIDERANDO a importância da adoção de boas práticas relacionadas à segurança e sigilo dos dados de que trata a lei n° 13.709 de agosto de 2018 no tratamento de dados pessoais;

CONSIDERANDO que, diante da premissa de garantir e incrementar a segurança da informação e comunicações no Tribunal Regional Eleitoral do Amapá, existe a necessidade de apoiar a condução da Política de Segurança Institucional (PSI) em vigor neste Tribunal;

CONSIDERANDO que a estratégia de segurança da informação é composta por várias camadas, dentre elas a criação de Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais (ETIR), mundialmente conhecido como CSIRT® (do inglês "Computer Security Incident Response Team"), cuja adoção por diversas instituições cresce de forma notória;

CONSIDERANDO que a ETIR visa garantir o cumprimento da missão institucional do Tribunal Regional Eleitoral do Amapá através das atividades de tratamento e respostas aos incidentes de segurança da informação, buscando minimizar vulnerabilidades e ameaças que possam comprometer o negócio do Tribunal.

RESOLVE:

Artigo 1º Reinstituir a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do Tribunal Regional Eleitoral do Amapá (ETIR/TRE-AP).

Art. 2º A ETIR/TRE-AP terá como membros os titulares das unidades abaixo relacionadas ou seus respectivos substitutos legais:

I - Seção de Cibersegurança (Coordenador);

II - Seção de Gestão de Serviços e Microinformática;

III - Seção de Desenvolvimento de Sistemas;

IV - Seção de Administração de Sistemas e Banco de Dados;

V - Seção de Gestão de Infraestrutura e Redes de Comunicação.

Art. 3º Os eventuais substitutos dos titulares das funções que compõem a ETIR atuarão como suplentes.

Art. 4º Disciplinar a criação de Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais (ETIR) no âmbito do Tribunal Regional Eleitoral do Amapá.

DAS DEFINIÇÕES

Art. 5º Para os efeitos desta portaria são estabelecidos os seguintes conceitos e definições:

I - Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais (ETIR): Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

II - Coordenador: Servidor Público ocupante de cargo efetivo carreira do Tribunal Regional Eleitoral do Amapá incumbido de coordenar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR);

III - Comunidade ou Público Alvo: é o conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais (ETIR);

IV - CTIR-GOV: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações - Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República - GSI;

V - CPTRIC-PJ: Centro de Prevenção, Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores do Poder Judiciário;

VI - Incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à informação ou dos sistemas de computação ou das redes de computadores;

VII - Serviço: é o conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais;

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

IX - 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.

X - Detecção de intrusão: serviço que consiste na análise do tráfego de redes e de histórico de dispositivos que detectam as tentativas de intrusões em redes de computadores, com vistas a identificar e iniciar os procedimentos de resposta a incidentes de segurança em redes computacionais, com base em eventos com características pré-definidas, que possam levar a uma possível intrusão.

XI - Tratamento de artefatos maliciosos: serviço que consiste em receber informações ou cópia de artefato malicioso que foi utilizado no ataque, ou em qualquer atividade desautorizada ou maliciosa. Uma vez recebido, o mesmo deve ser analisado, ou seja, deve-se buscar a natureza do artefato, seu mecanismo, versão e objetivo, para que seja desenvolvida, ou pelo menos sugerida, uma estratégia de detecção, remoção e defesa.

XII - Tratamento de incidentes de segurança em redes computacionais: 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.

XIII - Tratamento de vulnerabilidades: serviço que consiste em receber informações sobre vulnerabilidades, quer sejam em hardware ou software, objetivando analisar sua natureza, mecanismo e suas consequências e desenvolver estratégias para detecção e correção.

DA RESPONSABILIDADE

Art. 6º Cabe ao Coordenador criar os procedimentos internos, gerenciar as atividades, distribuir tarefas para a Equipe ou Equipes que compõem a ETIR e ser a interface com o CTIR-GOV e com o CPTRIC-PJ.

Parágrafo único. Para fins de cumprimento dos objetivos estabelecidos nesta portaria, cabe ao Coordenador reportar os incidentes de segurança cibernética que detectar ao CPTRIC-PJ.

DO MODELO DE IMPLEMENTAÇÃO

Art. 7º A ETIR será formada pelos membros indicados no artigo 2º, que, além de suas funções regulares, passarão a desempenhar as atividades relacionadas ao tratamento e resposta a incidentes de segurança da informação da rede interna do Tribunal Regional Eleitoral do Amapá.

Art. 8º A Equipe desempenhará suas atividades, via de regra, de forma reativa, sendo desejável, porém, que o Coordenador da ETIR atribua responsabilidades para que os seus membros exerçam atividades proativas.

DA ESTRUTURA ORGANIZACIONAL

Art. 9º A ETIR ficará subordinada à Coordenadoria de Infraestrutura, da Secretaria de Tecnologia da Informação do Tribunal Regional Eleitoral do Amapá.

Art. 10 São atribuições do Coordenador da ETIR:

I - Coordenar o planejamento, implementação e manutenção da infraestrutura necessária à ETIR;

II - Garantir que os incidentes de segurança da informação no âmbito Tribunal Regional Eleitoral do Amapá sejam monitorados e analisados criticamente;

III - Adotar procedimentos de feedback para assegurar que os usuários que comuniquem incidentes de segurança da informação e comunicações na rede interna de computadores sejam informados dos procedimentos adotados;

IV - Apoiar os treinamentos relacionados à Segurança da Informação e Comunicações fornecendo casos práticos de incidentes de segurança na rede interna de computadores, garantindo a confidencialidade e os devidos níveis de sigilo, sobre o que poderia acontecer, como reagir a tais incidentes e como evitá-los no futuro.

Art. 11 É competência da Coordenadoria de Infraestrutura da Secretaria de Tecnologia da Informação apoiar o Tribunal Regional Eleitoral do Amapá nas atividades de capacitação e tratamento de incidentes de segurança.

Art. 12 É de competência da ETIR:

I - Recolher provas o quanto antes após a ocorrência de um incidente de Segurança da Informação e Comunicações na rede interna de computadores;

II - Executar análise crítica sobre os registros de falhas para assegurar que elas foram satisfatoriamente resolvidas;

III - Investigar as causas dos incidentes de Segurança da Informação e Comunicações na rede interna de computadores;

IV - Implementar mecanismos para permitir a quantificação e monitoração dos tipos, volumes e custos de incidentes e falhas de funcionamento;

V - Indicar a necessidade de controles aperfeiçoados ou adicionais para limitar a frequência, os danos e o custo de futuras ocorrências de incidentes.

Art. 13 Caso necessário, poderão ser convocados para comporem a ETIR os membros da Comissão e Segurança da Informação ou os Membros do Comitê de Crise.

DA AUTONOMIA DA ETIR

Art. 14 A ETIR/TRE-AP tem autonomia compartilhada, ou seja, participará do resultado da decisão recomendando os procedimentos a serem executados ou as medidas de recuperação durante a identificação de uma ameaça e debaterá as ações a serem tomadas, seus impactos e a repercussão caso as recomendações não sejam seguidas.

Parágrafo único. Durante um incidente de segurança, se justificável, a equipe poderá tomar a decisão de executar as medidas de recuperação sem aguardar pela aprovação de níveis superiores de gestão, porém, comunicando à Diretoria Geral para ciência das ações tomadas.

DO TRATAMENTO DE DADOS PESSOAIS

Art. 15 A equipe da ETIR observará os fundamentos da proteção de dados pessoais previstos no artigo 2º da lei 13.709 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), durante todo o ciclo de vida de um incidente de segurança.

Art. 16 A ETIR seguirá as orientações de segurança no tratamento de dados pessoais, conforme artigo 46 e 47 da Lei Geral de Proteção de Dados Pessoais, durante os incidentes de segurança da informação.

Art. 17 Quando se fizer necessário, a ETIR observará a prerrogativa de que trata o inciso III do artigo 4º da Lei Geral de Proteção de Dados Pessoais.

Art. 18 Quando apropriado, a equipe da ETIR deverá observar as orientações e normas oriundas do Comitê Gestor de Proteção de Dados, que implementará programa de governança em privacidade de dados em incidentes de segurança da informação, conforme artigo 50 da Lei Geral de Proteção de Dados Pessoais.

Art. 19 O Coordenador da ETIR encaminhará ao Gestor de Segurança da Informação e ao Encarregado de Dados Pessoais relatório resumido de todos os incidentes categorizados como graves que envolvam dados pessoais, tão logo a gravidade do incidente seja definida.

DAS DISPOSIÇÕES GERAIS

Art. 20 A Equipe deve ser composta por servidores públicos ocupantes de cargo efetivo de carreira com perfil técnico compatível.

Art. 21 A ETIR observará padrões e procedimentos técnicos e normativos no contexto de tratamento de incidentes de segurança em rede orientados pelo CTIR-GOV e CPTRIC-PJ.

Art. 22 A ETIR poderá usar as melhores práticas de segurança da informação, desde que não conflitem com os dispositivos desta Norma Complementar.

Art. 23 A ETIR deverá comunicar de imediato a ocorrência de todos os incidentes de segurança ocorridos na sua área de atuação ao CPTRIC-PJ, conforme padrão definido por esse Órgão, a fim de permitir a geração de estatísticas e soluções integradas para o Poder Judiciário.

Art. 24 Os casos omissos e as dúvidas surgidas na aplicação desta Portaria serão dirimidos pelo titular da Secretaria de Tecnologia da Informação, com anuência do Diretor Geral do Tribunal Regional Eleitoral do Amapá.

Art. 25 Este normativo deverá ser revisado periodicamente, em intervalos de, no máximo, três anos.

Art. 26 Esta portaria revoga a Portaria Presidência nº 244/2018.

Art. 27 Esta Portaria entra em vigor na data de sua publicação.

Documento assinado eletronicamente por GILBERTO DE PAULA PINHEIRO, Presidente, em 18/09/2022, às 18:50, conforme art. 1º, III, "b", da Lei 11.419/2006.

PORTARIA PRESIDÊNCIA Nº 229/2022 TRE-AP/PRES/ASPRES

Institui o Protocolo de Prevenção de Incidentes Cibernéticos no âmbito do Tribunal Regional Eleitoral do Amapá.

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO AMAPÁ, no uso de suas atribuições legais e regimentais,