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,

CONSIDERANDO a necessidade de se garantir procedimentos adequados para a gestão da segurança cibernética no âmbito do Tribunal Regional do Amapá;
CONSIDERANDO os termos da Resolução CNJ n.° 396/2021, que "Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ)", e que apresenta diversos controles mínimos e medidas a serem adotadas pelos órgãos do Judiciário;
CONSIDERANDO os termos do Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário - Anexo II da Portaria CNJ n.º 162 de 10/6/2021 -, que aprovou os Protocolos e Manuais criados pela Resolução CNJ nº 396/2021;
CONSIDERANDO que a segurança cibernética é um empreendimento coletivo;
CONSIDERANDO para melhor detectar, conter e eliminar ataques cibernéticos e minimizar eventuais impactos na operação, assegurando o funcionamento dos sistemas críticos do Tribunal Regional Eleitoral do Amapá (TRE-AP), sobretudo em ambiente de constante ameaça, faz-se necessário possuir mecanismos de respostas e prevenção;
CONSIDERANDO que o tratamento de incidentes contempla funções de preparação, identificação, contenção, erradicação, recuperação e lições aprendidas;
RESOLVE:
Artigo 1º Instituir o Protocolo de Prevenção de Incidentes Cibernéticos no Tribunal Regional Eleitoral do Amapá (PPINC/TRE-AP).
Parágrafo único. O Protocolo previsto no caput possui caráter subsidiário, orientador, suplementar e deve ser interpretado em conjunto com a Política de Segurança da Informação do TRE-AP, prevista na Resolução TRE nº 570/2022.
CAPÍTULO I
DAS FUNÇÕES BÁSICAS
Art. 2º Para os efeitos deste normativo, são funções básicas do Protocolo de Prevenção de Incidentes Cibernéticos do Tribunal Regional Eleitoral do Amapá (PPINC/TRE-AP): identificar, proteger, detectar, responder e recuperar, nos seguintes termos:
I - identificar: entendimento organizacional para gerenciar o risco direto e/ou indireto de ataques cibernéticos a sistemas, pessoas, ativos, dados e recursos. Permite ao órgão avaliar os recursos que suportam funções críticas e os riscos relacionados. São medidas de concentração e priorização dos esforços na gestão de ativos, ambiente de negócios, governança, avaliação de riscos e estratégia de gestão de riscos;
II - proteger: desenvolvimento e implementação de salvaguardas que assegurem a proteção de dados, inclusive pessoais, e de ativos de informação, bem como a prestação de serviços críticos;
III - detectar: desenvolvimento e implementação de atividades adequadas à descoberta oportuna de eventos ou à detecção de incidentes de segurança cibernética. Estão contempladas ações de monitoramento contínuo de segurança, processos de detecção de anomalias e eventos;
IV - responder: desenvolvimento e implementação de atividades apropriadas à adoção de medidas em incidentes cibernéticos detectados. Nessa categoria, são incluídos os planos de resposta, de comunicações, de análise, de mitigação e de melhorias;
V - recuperar: desenvolvimento, implementação e manutenção dos planos de resiliência e de restauração de quaisquer capacidades ou serviços que foram prejudicados em razão de incidentes de segurança cibernética.
CAPÍTULO II
DOS PRINCÍPIOS CRÍTICOS
Art. 3º O Protocolo de Prevenção de Incidentes Cibernéticos do Tribunal Regional Eleitoral do Amapá (PPINC/TRE-AP) contemplará um conjunto de princípios críticos que assegurem a construção de sistema de segurança cibernética eficaz.
Art. 4º Para os efeitos deste normativo, são considerados os seguintes princípios críticos:

I - base de conhecimento de defesa: consiste no uso de informações e conhecimento de ataques reais que comprometeram sistemas. Informações conseguidas por meio de interação e de cooperação com outras equipes de tratamento a incidentes e respostas. Tem por propósito fornecer bases fundamentais ao aprendizado contínuo com apoio em eventos ocorridos. Apoia a construção de defesas eficazes e práticas.

II - priorização: foco prioritário na formação, na revisão de controles/acessos, nos processos e na disseminação da cultura de segurança cibernética. Contribui para a redução de riscos e para a proteção contra as ameaças mais sensíveis e que encontram viabilidade em sua célere implementação.

III - instrumentos de aferição e métricas: definição e estabelecimento de métricas comuns que fornecem linguagem compartilhada e de compreensão abrangente para magistrados, servidores, colaboradores, prestadores de serviços, especialistas em tecnologia da informação, auditores e demais atores do sistema de segurança. Permite a medição da eficácia das medidas de segurança dentro da organização. Fornece insumos para que os ajustes necessários, quando identificados, possam ser implementados de forma célere.

IV - diagnóstico contínuo: processo de trabalho que realiza continuamente medição para testar e validar a eficácia das ações de segurança atuais e contribui para a definição de prioridades e para os próximos passos a serem tomados.

V - formação, capacitação e conscientização: processos formais de educação continuada com a inclusão em planos de capacitação que contemplem a disseminação, a formação, a conscientização e a instrução para todos os atores envolvidos em atividades diretas ou indiretas que contribuam para a cultura de segurança cibernética dentro da organização. Tais instrumentos deverão ser revisados periodicamente.

VI - automação: incentivo à busca de soluções automatizadas de segurança cibernética para que o TRE-AP obtenha medições confiáveis, escaláveis e contínuas. Tal processo está correlacionado com os resultados almejados por meio dos instrumentos de controle e de métricas.

VII - resiliência: poder de recuperação ou capacidade de a organização resistir aos efeitos de um incidente, bem como impedir a reincidência secundária do incidente identificado.

CAPÍTULO III

DA GESTÃO DE INCIDENTES DE SEGURANÇA CIBERNÉTICA

Art. 5º A gestão de incidentes de segurança cibernética é realizada por meio de processo definido e constituído, conforme Portaria TRE-AP nº 226/2021, que estabelece o Processo de Gestão de Incidentes de Segurança da Informação no âmbito do Tribunal Regional do Amapá.

CAPÍTULO IV

DA COMPETÊNCIA DE ATUAÇÃO

Art. 6º A atuação operacional é de responsabilidade da ETIR (Equipe Técnica de Respostas a Incidentes de Redes Computacionais), nomeada em portaria específica.

CAPÍTULO V

DAS BOAS PRÁTICAS DE SEGURANÇA CIBERNÉTICAS

Art. 7º As dimensões e práticas da segurança cibernética são definidas em:

I - preparação: processo que envolve as equipes de tratamento a incidentes e respostas. Trata-se de resposta metódica, contemplando ferramentas forenses de análise e custódia, planejamento sobre como responder e notificar cada incidente de segurança, identificação de cadeia de comando em situação de crise, processos de educação e de formação.

II - identificação: capacidade de identificar que um ataque cibernético está em andamento, por meio da percepção de sinais de anomalias ou de comportamentos inesperados. Trata-se da aptidão dos entes para diferenciar as irregularidades em redes de dados e identificar o mau funcionamento dos sistemas críticos, em razão de ataques cibernéticos em curso. Para essa

atividade, podem ser elaboradas listas de verificação investigativas para apoiar o processo de diagnóstico, triagem e acionamento das equipes de resposta, permitindo a avaliação do impacto e a determinação dos próximos passos a serem tomados.
III - contenção: visa garantir que o incidente não cause mais danos. Nessa dimensão, a prioridade geral é isolar o que foi afetado, manter a produção e, acima de tudo, garantir que as ações não comprometam, ainda mais, a segurança ou as operações críticas. Tal atividade tende a ser complexa incluindo, dentre outros, a imediata comunicação prevista na Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSECPJ) e seus anexos, o isolamento da fonte do ataque, a aplicação de ferramentas forenses para remoção de malware das redes de produção, a limitação de transferências de dados desnecessárias e a adoção dos mecanismos de comunicação previstos no Protocolo de Gerenciamento de Crises Cibernéticas.
IV - erradicação: remoção da ameaça, garantindo que as operações essenciais sejam apoiadas, caso surjam desafios no processo de restauração. Os métodos possíveis para essa função podem variar desde patches ou reconstruções do sistema até redesenho completo da arquitetura, devendo, sempre que possível, preservar evidências que apoiarão o processo de investigação do crime cibernético.
V - recuperação: promulgação de plano de recuperação em fases para restauração de operações, com foco prioritário nos sistemas críticos ou na execução da operação em modo analógico até que haja confiança no desempenho do sistema. Nessa atividade, são necessárias verificações ambientais e de segurança paralelas ao controle dos impactos de desempenho não intencionais da restauração.
VI - lições aprendidas: atividade contínua que não só deve capturar os impactos imediatos de um incidente, mas também as melhorias em longo prazo da segurança cibernética do órgão. Tal função pode variar de um sistema de controle de processos melhor projetado até a evolução e preparação de centros de identificação e resposta a ataques cibernéticos do Poder Judiciário.
Art. 8º. Esta Portaria entra em vigor na data da sua publicação.

Documento assinado eletronicamente por GILBERTO DE PAULA PINHEIRO, Presidente, em 17/09/2022, às 18:27, conforme art. 1º, III, "b", da Lei 11.419/2006.

PORTARIA PRESIDÊNCIA Nº 227/2022 TRE-AP/PRES/DG/SGP/COPES/SRFD

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO AMAPÁ, no uso de suas atribuições legais e regimentais, e tendo em vista o contido no P.A nº 0003643-63.2022.6.03.8000.
RESOLVE:
Artigo 1º Designar o servidor ANTONIO JAMERSON MENDES DA ROCHA CORTES, Analista Judiciário - Área Administrativa, do quadro de pessoal efetivo deste Tribunal Regional Eleitoral, para ocupar a função comissionada de Assistente II, do Gabinete da Diretoria-Geral.
Art. 2º Esta Portaria entra em vigor na data de sua publicação.

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.

ATOS DA CORREGEDORIA REGIONAL ELEITORAL

INTIMAÇÕES

AÇÃO DE INVESTIGAÇÃO JUDICIAL ELEITORAL(11527) Nº 0600892-95.2022.6.03.0000

: 0600892-95.2022.6.03.0000 AÇÃO DE INVESTIGAÇÃO JUDICIAL