DIÁRIO DA JUSTIÇA ELETRÔNICO

DO TRIBUNAL REGIONAL ELEITORAL DO AMAPÁ

Ano: 2022, nº 168

Disponibilização: terça-feira, 20 de setembro de 2022
Publicação: quarta-feira, 21 de setembro de 2022

Tribunal Regional Eleitoral do Amapá

Desembargador Gilberto de Paula Pinheiro
Presidente

Desembargador João Guilherme Lages Mendes
Vice-Presidente e Corregedor

Dr. Francisco Valentim Maia
Diretor-Geral

Avenida Mendonça Júnior, 1502 - Centro
Macapá/AP
CEP: 68900-914

Contato
(96) 3198 - 7541
sejud@tre-ap.jus.br

SUMÁRIO

ATOS DA PRESIDÊNCIA

PORTARIAS

PORTARIA PRESIDÊNCIA Nº 230/2022 TRE-AP/PRES/ASPRES

Institui o Protocolo de Investigação para Ilícitos Cibernéticos no âmbito do Tribunal Regional Eleitoral 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 Investigação para Ilícitos Cibernéticos do Poder Judiciário - Anexo III da Portaria CNJ n.º 162 de 10/6/2021 -, que aprovou os Protocolos e Manuais criados pela Resolução CNJ nº 396/2021;

RESOLVE:

Artigo 1º Instituir o Protocolo de Investigação para Ilícitos Cibernéticos no Tribunal Regional Eleitoral do Amapá (PIILC/TRE-AP), cuja finalidade é estabelecer os procedimentos básicos para coleta e preservação de evidências e para comunicação obrigatória dos fatos penalmente relevantes ao Ministério Público e ao órgão de polícia judiciária com atribuição para o início da persecução penal..

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.

CAPÍTULO I

DOS REQUISITOS PARA ADEQUAÇÃO DOS ATIVOS DE TECNOLOGIA DA INFORMAÇÃO

Art. 2º O horário dos ativos de tecnologia da informação deve ser ajustado por meio de mecanismos de sincronização de tempo, de forma a garantir que as configurações de data, hora e fuso horário do relógio interno estejam sincronizados com a Hora Legal Brasileira (HLB), de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON).

Art. 3º Os ativos de tecnologia da informação devem ser configurados de forma a registrar todos os eventos relevantes de Segurança da Informação e Comunicações (SIC), tais como:

I - autenticação, tanto as bem-sucedidas quanto as malsucedidas;

II - acesso a recursos e dados privilegiados; e

III - acesso e alteração nos registros de auditoria.

Art. 4º Os registros dos eventos previstos no artigo anterior devem incluir as seguintes informações:

I - identificação inequívoca do usuário que acessou o recurso;

II - natureza do evento, como, por exemplo, sucesso ou falha de autenticação, tentativa de troca de senha etc.;

III - data, hora e fuso horário, observando-se a HLB; e

IV - endereço IP (Internet Protocol), porta de origem da conexão, identificador do ativo de informação, coordenadas geográficas, se disponíveis, e outras informações que possam identificar a possível origem do evento;

Art. 5º Os ativos de informação que não propiciem os registros dos eventos listados nos artigos 3 e 4 devem ser mapeados e documentados quanto ao tipo e formato de registros de auditoria permitidos e armazenados.

Art. 6º Os sistemas e as redes de comunicação de dados devem ser monitorados, registrando-se, minimamente, os seguintes eventos de segurança, sem prejuízo de outros considerados relevantes:

I - utilização de usuários, perfis e grupos privilegiados;

II - inicialização, suspensão e reinicialização de serviços;

III - acoplamento e desacoplamento de dispositivos de hardware, com especial atenção para mídias removíveis;

IV - modificações da lista de membros de grupos privilegiados;
V - modificações de política de senhas, como, por exemplo, tamanho, expiração, bloqueio automático após exceder determinado número de tentativas de autenticação, histórico etc.;
VI - acesso ou modificação de arquivos ou sistemas considerados críticos; e
VII - eventos obtidos por meio de quaisquer mecanismos de segurança existentes.
Art. 7º Os servidores de hospedagem de página eletrônica, bem como todo e qualquer outro ativo de informação que assim o permita, devem ser configurados para armazenar registros históricos de eventos (logs) em formato que possibilite a completa identificação dos fluxos de dados.
Art. 8º Os registros devem ser armazenados pelo período mínimo de 6 (seis) meses, sem prejuízo de outros prazos previstos em normativos específicos.
Art. 9º Recomenda-se que os ativos de informação sejam configurados de forma a armazenar seus registros de auditoria não apenas localmente, mas também remotamente, por meio do uso de tecnologia aplicável.
CAPÍTULO II
DO PROCEDIMENTO PARA COLETA E PRESERVAÇÃO DAS EVIDÊNCIAS
Art. 10º A ETIR/TRE-AP, sob a supervisão de seu responsável, durante o processo de tratamento do incidente penalmente relevante, deverá, sem prejuízo de outras ações, coletar e preservar:
I - as mídias de armazenamento dos dispositivos afetados ou as suas respectivas imagens forenses;
II - os dados voláteis armazenados nos dispositivos computacionais, como a memória principal (memória RAM); e
III - todos os registros de eventos citados neste documento.
Art. 11º Nos casos de inviabilidade de preservação das mídias de armazenamento dos dispositivos afetados ou das suas respectivas imagens forenses, em razão da necessidade de pronto restabelecimento do serviço afetado, a ETIR/TRE-AP, sob a supervisão do seu responsável, deverá coletar e armazenar 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.
Art. 12º O coordenador da ETIR/TRE-AP deverá fazer constar em relatório a eventual impossibilidade de preservação das mídias afetadas e listar todos os procedimentos adotados.
Art. 13º As ações de restabelecimento do serviço não devem comprometer a coleta e a preservação da integridade das evidências.
Art. 14º Para a preservação dos arquivos coletados, deve-se:
I - gerar arquivo que contenha a lista dos resumos criptográficos de todos os arquivos coletados;
II - gravar os arquivos coletados, acompanhados do arquivo com a lista dos resumos criptográficos descritos na alínea a deste subitem; e
III - gerar resumo criptográfico do arquivo a que se refere a deste subitem.
Art. 15º Todo material coletado deverá ser lacrado e custodiado pelo coordenador pela ETIR/TRE-AP, o qual deverá preencher Termo de Custódia dos Ativos de Informação relacionados ao incidente de segurança penalmente relevante.
Art. 16º O material coletado ficará à disposição da autoridade responsável pelo órgão do Poder Judiciário competente.
CAPÍTULO III
DA COMUNICAÇÃO DO INCIDENTE DE SEGURANÇA

Art. 17º Assim que tomar conhecimento de Incidente de Segurança Cibernética penalmente relevante, deverá o responsável do Tribunal Regional Eleitoral do Amapá (TRE-AP) afetado comunicá-lo de imediato ao órgão de polícia judiciária com atribuição para apurar os fatos e ao Ministério Público.

Art. 18º Considerado o incidente Crise Cibernética, o Comitê de Crise deverá ser acionado, nos termos do Protocolo de Gerenciamento de Crises Cibernéticas da Portaria TRE-AP 281/2021.

Art. 19º Após a conclusão do processo de coleta e preservação das evidências do incidente penalmente relevante, o responsável pela ETIR/TRE-AP deverá elaborar Relatório de Comunicação de Incidente de Segurança Cibernética, descrevendo detalhadamente os eventos verificados.

Art. 20º O Relatório de Comunicação de Incidente de Segurança Cibernética deverá conter as seguintes informações, sem prejuízo de outras julgadas relevantes:

I - nome do responsável pela preservação dos dados do incidente, com informações de contato;

II - nome do coordenador da ETIR/TRE-AP e informações de contato;

III - órgão comunicante com sua localização e informações de contato;

IV - número de controle da ocorrência;

V - relato sobre o incidente que descreva o que ocorreu, como foi detectado e quais dados foram coletados e preservados;

VI - descrição das atividades de tratamento e resposta ao incidente e todas as providências tomadas pela ETIR/TRE-AP, incluindo as ações de preservação e coleta, a metodologia e as ferramentas utilizadas e o local de armazenamento das informações preservadas;

VII - resumo criptográfico dos arquivos coletados;

VIII - Termo de Custódia dos Ativos de Informação Relacionados ao Incidente de Segurança;

IX - número de lacre de material físico preservado, se houver; e

X - justificativa sobre a eventual inviabilidade de preservação das mídias de armazenamento dos dispositivos afetados, diante da impossibilidade de mantê-las.

Art. 21º O Relatório de Comunicação de Incidente de Segurança em Redes Computacionais deverá ser assinado pelo coordenador da ETIR/TRE-AP e encaminhado formalmente em processo restrito à autoridade responsável do TRE-AP.

Art. 22º Deverá constar no documento formal de encaminhamento a que se refere o artigo anterior apenas a informação de que se trata de comunicação de evento relacionado à segurança da informação, sem a descrição dos fatos.

Art. 23º Recebida a Comunicação de Incidente de Segurança em Redes Computacionais, a Diretoria Geral deverá encaminhá-la formalmente ao Ministério Público e ao órgão de polícia judiciária com atribuição para apurar os fatos, juntamente com o todo o material previsto neste protocolo, para fins de instrução da notícia crime.

Documento assinado eletronicamente por GILBERTO DE PAULA PINHEIRO, Presidente, em 17/09/2022, às 18:30, conforme art. 1º, III, "b", da Lei 11.419/2006.

PORTARIA PRESIDÊNCIA Nº 232/2022 TRE-AP/PRES/DG/SGP/COPES/SRFD

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO AMAPÁ, no uso das atribuições legais que lhe são conferidas pelo Regimento Interno desta Corte, e tendo em vista o contido no P. A. nº 0000242-56.2022.6.03.8000,

RESOLVE:

Artigo 1º Incluir na Comissão de Fiscalização da Propaganda Eleitoral constituída pela Portaria Presidência n.º 152/2022, de 12.07.2022, publicada no DJE nº 125, em 13 de julho de 2022, o servidor GEMARQUES VIEIRA MARQUES JÚNIOR (Membro).