PORTARIA 188/2023

Institui o Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ) no Tribunal Regional Eleitoral de Sergipe.

A PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DE SERGIPE, no uso das atribuições que lhe são conferidas pelo art. 28, inciso X, do Regimento Interno;

CONSIDERANDO os termos da Resolução 370, de 28 de janeiro de 2021, do Conselho Nacional de Justiça, que estabeleceu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), as diretrizes para sua governança, gestão e colaboração tecnológica;

CONSIDERANDO os termos da Resolução 396, de 7 de junho de 2021, do Conselho Nacional de Justiça, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) e, em seu art. 26, determina a adoção do Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ) constante do Anexo III da Portaria 162, de 2021, do CNJ;

CONSIDERANDO a Norma Complementar 21/IN01/DSIC/GSIPR, do Gabinete de Segurança Institucional da Presidência da República, de 10 de outubro de 2014, 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;

CONSIDERANDO que é imprescindível garantir a segurança cibernética do ecossistema digital da instituição;

CONSIDERANDO a importância de estabelecer objetivos, princípios e diretrizes de Segurança da Informação alinhados às recomendações constantes da norma NBR ISO/IEC 27001:2013, que trata da segurança da informação;

CONSIDERANDO o número crescente de incidentes cibernéticos no ambiente da rede mundial de computadores e a necessidade de processos de trabalho orientados para a boa gestão da segurança da informação;

CONSIDERANDO que os ataques cibernéticos têm se tornado cada vez mais avançados e com alto potencial de prejuízo, cujo alcance e complexidade não têm precedentes, que os impactos financeiros, operacionais e de reputação podem ser imediatos e significativos, e que é fundamental aprimorar a capacidade da instituição de estabelecer 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,

RESOLVE:

Art. 1º Fica instituído o Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ), constante do Anexo III da Portaria 162, de 10 de junho de 2021, do Conselho Nacional de Justiça (CNJ), no Tribunal Regional Eleitoral de Sergipe.

Art. 2º Para os efeitos deste normativo, consideram-se os seguintes conceitos e definições:

I - ativo: qualquer coisa que represente valor para uma instituição, tal como a informação;

II - ativos de informação: meios de armazenamento, transmissão e processamento de informação, sistemas de informação e locais onde se encontram esses meios e as pessoas que a eles têm acesso;

III - atividades críticas: atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão, de maneira que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo;

IV - crise: um evento ou série de eventos graves que apresentam propriedades emergentes capazes de exceder as habilidades de uma organização em lidar com as demandas de tarefas que eles geram, e que apresentam implicações que afetam uma proporção considerável da organização, bem como de seus constituintes;

V - crise cibernética: crise que ocorre em decorrência de incidente em dispositivos, serviços e redes de computadores, que causam dano material ou de imagem, atraem a atenção do público e da mídia e fogem ao controle direto da organização;
VI - evento: qualquer ocorrência observável em um sistema ou rede de uma organização;
VII - gestão de riscos de segurança da informação: processo que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação e para equilibrá-los com os custos operacionais e financeiros envolvidos;
VIII - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
IX - incidente de segurança da informação: evento que viola ou representa uma ameaça iminente de violação de uma política de segurança, de uma política de uso aceitável ou de uma prática de segurança padrão;
X - processo de gestão de incidentes de segurança da informação: atividades que devem ser executadas para prevenir e tratar a ocorrência de evento adverso de segurança da informação, avaliar o impacto, determinar a resposta inicial e restabelecer a normalidade;
XI - procedimento: conjunto de ações sequenciadas e ordenadas para o atingimento de determinado fim;
XII - evidência digital: informação ou dado, armazenado ou transmitido eletronicamente, em modo binário, que pode ser reconhecida como parte de um evento;
XIII - coleta de evidências de segurança em redes computacionais: processo de obtenção de itens físicos que contém potencial evidência, mediante a utilização de metodologia e ferramentas adequadas e inclui a aquisição, ou seja, a geração das cópias das mídias ou a coleção de dados que contenham evidências do incidente;
XIV - preservação de evidência de incidentes em redes computacionais: é o processo que compreende a salvaguarda das evidências e dos dispositivos para garantir que os dados ou metadados não sofram alteração, preservando-se a integridade e a confidencialidade das informações.
Art. 3º A Secretaria de Tecnologia da Informação e Comunicação (STI) deve incluir no Plano Diretor de TIC (PDTIC) as ações necessárias para adequação dos ativos de tecnologia da informação que suportam as atividades essenciais aos requisitos elencados no Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário.
§ 1º A lista dos projetos com a inclusão das ações mencionadas no *caput* deste artigo deve ser encaminhada ao Comitê Gestor de Segurança da Informação e integrada ao Sistema de Gestão de Segurança da Informação do TRE-SE.
§ 2º O mesmo tratamento previsto no *caput* deste artigo deve ser aplicado aos ativos considerados relevantes, mesmo que não estejam diretamente relacionados à sustentação dos serviços críticos que poderiam ser ponto de entrada para a exploração de falhas.
§ 3º As atividades de Tecnologia da Informação e Comunicação (TIC) essenciais a que se refere o *caput* deste artigo são as mesmas definidas para o processo vigente de gestão de riscos de tecnologia da informação.
Art. 4º A Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR), durante o processo de tratamento do incidente, deve, sem prejuízo de outras ações:
I - conduzir o tratamento do incidente, observando os procedimentos para coleta e preservação das evidências definidos no Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário, quando constatado ser penalmente relevante;
II - comunicar o fato ao Comitê Gestor de Segurança da Informação e à Presidência;

III - comunicar ao encarregado(a) pelo tratamento de dados pessoais do TRE-SE, quando o incidente envolver dados pessoais.

§ 1º Cabe ao encarregado(a) pelo tratamento de dados pessoais do TRE-SE comunicar o incidente aos titulares de dados pessoais e, se entender necessário, à Agência Nacional de Proteção de Dados Pessoais (ANPD).

§ 2º O Comitê de Crise Cibernética deve ser acionado, nos termos do Protocolo de Gerenciamento de Crises Cibernéticas, considerando o incidente uma Crise Cibernética.

Art. 5º Recebida a comunicação de Incidente de Segurança em Redes Computacionais penalmente relevante, a Presidência deve encaminhá-la ao Ministério Público e ao órgão de polícia judiciária com atribuição para o início da persecução penal, em conjunto com as evidências coletadas.

Art. 6º As ações de coleta e preservação de evidências devem observar o Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ), constante do Anexo III da Portaria n. 162, de 2021, do CNJ.

Art. 7º. Este protocolo deverá ser revisado e atualizado pelo menos a cada dois anos, mediante provocação da Secretaria de Tecnologia da Informação e Comunicação (STI).

Art. 8º A presente Portaria entra em vigor a partir da data de sua publicação.

Documento assinado eletronicamente por ELVIRA MARIA DE ALMEIDA SILVA, Presidente, em 14 /03/2023, às 13:24, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site
https://sei.tre-se.jus.br/sei/controlador_externo.php?
acao=documento_conferir&id_orgao_acesso_externo=0
informando o código verificador 1337606 e o código CRC C76D885C.

PORTARIA 189/2023

Institui o Protocolo de Prevenção a Incidentes Cibernéticos do Poder Judiciário no âmbito do Tribunal Regional Eleitoral de Sergipe.

A PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DE SERGIPE, no uso das atribuições que lhe são conferidas pelo art. 28, inciso X, do Regimento Interno;

CONSIDERANDO a Lei Federal 13.709/2018, com a redação dada pela Lei Federal 13.853/2019, que dispõe sobre a proteção de dados pessoais;

CONSIDERANDO a Resolução nº 396, de 07 de junho de 2021, do Conselho Nacional de Justiça, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO o anexo I da Portaria nº 162, de 10 de junho de 2021, do Conselho Nacional de Justiça, que constitui o Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ);

CONSIDERANDO os anexos IV, V e VI da Portaria nº 162, de 10 de junho de 2021, do Conselho Nacional de Justiça, que contêm os manuais referentes à Proteção de Infraestruturas Críticas de TIC, Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital, e, ainda, Gestão de Identidades;

CONSIDERANDO a Resolução nº 23.644, de 1 de julho de 2021 do TRIBUNAL SUPERIOR ELEITORAL, que institui a Política de Segurança da Informação (PSI) no âmbito Da Justiça Eleitoral;

CONSIDERANDO o Decreto nº 9.637, de 26 de dezembro de 2018, que "Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação";