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";

CONSIDERANDO a Norma Complementar 05/IN01/DSIC/GSIPR, do Gabinete de Segurança Institucional da Presidência da República, de 14 de agosto de 2009, que disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais (ETIR) nos órgãos e entidades da Administração Pública Federal;
CONSIDERANDO a Norma Complementar 08/IN01/DSIC/GSIPR, do Gabinete de Segurança Institucional da Presidência da República, de 24 de agosto de 2010, que estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal;
CONSIDERANDO a Norma ABNT NBR ISO/IEC 27001:2005, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro da organização;
CONSIDERANDO a Norma ABNT NBR ISO/IEC 27002:2005, que trata de código de prática para a Gestão da Segurança da Informação.
RESOLVE:
CAPÍTULO I
DISPOSIÇÕES PRELIMINARES
Art. 1º Adotar o Protocolo de Prevenção a Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ), no âmbito do TRE-SE, com os seguintes objetivos:
I - disciplinar a criação e funcionamento da Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores (ETIR) no âmbito do Tribunal Regional Eleitoral de Sergipe (TRE-SE);
II - promover alinhamento às normas, regulamentações e às melhores práticas, relacionadas à Gestão de Incidentes de Segurança da Informação;
III - promover ações que contribuam para a resiliência dos serviços de Tecnologia da Informação e Comunicação (TIC) aos ataques cibernéticos.
Art. 2º O Protocolo de Investigação para Ilícitos Cibernéticos e o Protocolo de Gerenciamento de Crises Cibernéticas são complementares e harmonizam-se com este Protocolo de Prevenção a Incidentes Cibernéticos.
Parágrafo único. Para os efeitos deste normativo, são estabelecidas as seguintes definições:
I - Incidente cibernético ou Incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores, tais como: divulgação não autorizada de dados ou de informação sigilosa contida em sistema, arquivo ou base de dados do TRE-SE; invasão de dispositivo informático; interrupção de serviço essencial ao desempenho das atividades; inserção ou facilitação de inserção de dados falsos, alteração ou exclusão de dados corretos nos sistemas informatizados ou bancos de dados do TRE-SE e/ou prática de ato definido como crime ou infração administrativa;
II - Equipe de Tratamento e Resposta a Incidentes 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.
Art. 3º Para implementação desta norma, deverão ser observados pelas áreas envolvidas os princípios críticos definidos no PPINC-PJ, que são:
I - uso de base de conhecimento de defesa;
II - priorização da segurança da informação;
III - definição e estabelecimento de métricas;
IV - diagnóstico contínuo;
V - formação e capacitação;
VI - busca de soluções automatizadas de segurança cibernética;
VII - resiliência.

Art. 4º A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) do TRE-SE, para as finalidades deste protocolo, foi instituída pela Portaria TRE/SE nº 700/2021.

Art. 5º Cabe ao Comitê Gestor de Segurança da Informação:

I - deliberar sobre as principais diretrizes e temas relacionados à Gestão de Incidentes de Segurança da Informação;

II - monitorar e avaliar periodicamente a estrutura de Gestão de Incidentes de Segurança da Informação e o sistema de controles internos, assim como propor melhorias consideradas necessárias;

III - aprovar formalmente o processo de Gestão de Incidentes de Segurança da Informação e suas futuras revisões;

IV - deliberar sobre ações de contenção ou prevenção de incidentes de segurança da informação.

Art. 6º Cabe à Presidência:

I - analisar as deliberações do Comitê Gestor de Segurança da Informação sobre Gestão de Incidentes de Segurança da Informação e decidir sobre possíveis providências;

II - formalizar a aceitação da execução das ações propostas para conter ou prevenir incidentes de segurança da informação;

III - comunicar ao órgão de polícia judiciária com atribuição para apurar os fatos, na ocorrência de incidentes penalmente relevantes;

IV - acionar o Comitê de Crises Cibernéticas, nos termos do Protocolo de Gerenciamento de Crises Cibernéticas, quando necessário.

Art. 7º Cabe às unidades vinculadas à Secretaria de Tecnologia da Informação e Comunicação (STI):

I - monitorar e comunicar à ETIR os Incidentes de segurança da informação dos ativos sob sua responsabilidade;

II - assegurar a implementação das ações e dos controles definidos para prevenção e contenção de incidentes de segurança da informação dos ativos sob sua responsabilidade.

Art. 8º Cabe à Assessoria Técnica de Segurança Cibernética/STI (ASSEC):

I - desenvolver, testar e implementar o processo de Gestão de Incidentes de Segurança Cibernética e garantir sua efetividade;

II - coordenar a instituição, capacitação, implementação e manutenção da infraestrutura necessária à ETIR;

III - gerenciar as atividades e distribuir tarefas para a ETIR;

IV - garantir que os incidentes de segurança na Rede de Computadores do TRE-SE sejam devidamente tratados;

V - 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;

VI - disseminar cultura voltada para comunicação de incidentes de segurança cibernética;

VII - subsidiar o Comitê Gestor de Segurança da Informação com informações pertinentes à estrutura de gestão de incidentes de segurança cibernética.

Parágrafo único. Cabe ao responsável pela Assessoria Técnica de Segurança Cibernética/STI o papel de Agente Responsável pela ETIR, além de ser a interface com o Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR GOV).

CAPÍTULO II

DAS FUNÇÕES DO PROTOCOLO DE PREVENÇÃO A INCIDENTES CIBERNÉTICOS

Art. 9º São funções básicas do Protocolo de Prevenção a Incidentes Cibernéticos, conforme definição do PPINC-PJ, identificar, detectar, responder o incidente, proteger e recuperar a informação.

Seção I

Da Função Identificar

Art. 10. A função "Identificar" consiste na análise dos riscos a que os recursos de TIC estão expostos, incluindo a elaboração e a execução do plano de tratamento dos riscos.

§ 1º A função identificar é executada dentro do escopo do processo de Gestão de Riscos de Segurança da Informação de TI, instituído em ato próprio, e está limitada aos ativos incluídos no respectivo ciclo de análise de riscos no âmbito do TRE-SE.

§ 2º O mesmo tratamento previsto no parágrafo § 1º deste artigo deve ser dispensado a 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 O rol de atividades de TIC consideradas essenciais, para fins deste normativo, é o mesmo constante no ciclo de análise de riscos vigente.

Seção II

Da Função Proteger

Art. 11. A função "Proteger" consiste no desenvolvimento e na implementação de salvaguardas que assegurem a proteção de dados, inclusive pessoais, ativos de informação e a prestação de serviços.

§ 1º A função "Proteger" deve ser implementada pelo conjunto mínimo de ações elencadas a seguir:

I - aprimoramento contínuo do Sistema de Gestão de Segurança da Informação (SGSI) do TRE-SE;

II - controle de acesso e de utilização de recursos de TIC;

III - cópia de segurança e de restauração de sistemas, aplicativos, dados e de documentos;

IV - plano de contingência dos serviços essenciais;

V - gestão de capacidade e disponibilidade de TIC dos serviços essenciais;

VI - processo de gerenciamento de mudanças para todos os ativos de TIC;

VII - gestão de vulnerabilidades técnicas dos serviços essenciais;

VIII - utilização de ferramenta de segurança para estações de trabalho, contendo, no mínimo, as funções de antivírus, automação de políticas de segurança de endpoint, proteção contra criptografia (ransomware), controle de aplicativos e de dispositivos removíveis;

IX - controle de acesso a conteúdo na internet (filtragem web);

X - utilização de ferramentas de segurança de rede (firewall), para filtragem e bloqueio de tráfego de rede, prevenção de ameaças e implementação de redes privadas virtuais (VPN);

XI - integridade da rede protegida por meio da segmentação e segregação de ambientes, de maneira a estabelecer barreiras de contenção de danos em caso de comprometimento (sub-redes distintas por serviços) e para garantia de recursos para serviços prioritários (missão crítica, em detrimento de ambientes de laboratório/desenvolvimento/homologação);

XII - anualmente promover campanha e/ou treinamento sobre segurança da informação para magistrados e servidores;

XIII - atualização tecnológica constante;

XIV - implementação gradual dos controles de segurança da informação presentes na Norma NBR 27002;

XV - implementação gradual dos controles mínimos recomendados no Manual de Referência para Proteção de Infraestruturas Críticas de TIC, editado pelo Conselho Nacional de Justiça, considerando a escala de aplicabilidade de cada controle em relação ao porte e maturidade do TRE-SE em segurança da informação;

XVI - implementação gradual dos requisitos de resiliência cibernética recomendados no Manual de Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital, editado pelo Conselho Nacional de Justiça, considerando a aplicabilidade dos requisitos em relação ao porte e maturidade do TRE-SE em segurança da informação.

§ 2º As salvaguardas elencadas no § 1º deste artigo devem ser implementadas para todos os ativos de TIC, no que couber, considerados essenciais ou não ao negócio, permitindo variar quanto ao nível de implementação, de acordo com a natureza e criticidade do ativo.

§ 3º As atualizações dos ativos de TIC (pacotes de segurança, firmware, entre outros) devem ser aplicadas, sempre que possível, tão logo liberadas, mas considerando:

I - os riscos decorrentes da atualização;

II - os riscos decorrentes da não aplicação (ou postergação);

III - a criticidade do ativo;

IV - a estabilidade dos serviços.

Seção III

Das Funções Detectar, Responder e Recuperar

Art. 12. As atividades decorrentes das funções "Detectar", "Responder" e "Recuperar" do PPINC-PJ devem estar cobertas pelo Processo de Gestão de Incidentes de Segurança Cibernética.

Art. 13. Quando houver indícios de ilícitos criminais durante o gerenciamento dos incidentes de segurança, deverá, ainda, ser seguido o Protocolo de Investigação para Ilícitos Cibernéticos (PIILC-PJ).

Parágrafo único. Na ocorrência da hipótese prevista no caput deste artigo, o Comitê Gestor de Segurança da Informação e a Presidência do TRE-SE deverão ser comunicados.

Art. 14. Quando o incidente de segurança da informação decorrer de suspeita de descumprimento da Política de Segurança da Informação, será observado o sigilo durante todo o processo, ficando as evidências, informações e demais registros restritos aos envolvidos na investigação.

Art. 15. 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. 16. Esta portaria entra em vigor na data de sua publicação.

Documento assinado eletronicamente por ELVIRA MARIA DE ALMEIDA SILVA, Presidente, em 14/03/2023, às 13:25, 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 1337699 e o código CRC 22E75E01.

ATOS DA SECRETARIA JUDICIÁRIA

INTIMAÇÃO

PROCESSO ADMINISTRATIVO(1298) Nº 0600017-79.2023.6.25.0000

PROCESSO	: 0600017-79.2023.6.25.0000 PROCESSO ADMINISTRATIVO (Estância - SE)
RELATOR	**: DESEMBARGADORA PRESIDENTE ELVIRA MARIA DE ALMEIDA SILVA**
Destinatário	: TRIBUNAL REGIONAL ELEITORAL DE SERGIPE
FISCAL DA LEI	: PROCURADORIA REGIONAL ELEITORAL EM SERGIPE
REQUERENTE	: JUÍZO DA 06ª ZONA ELEITORAL DE SERGIPE
SERVIDOR(ES)	: PAULO CESAR GOMES DE ANDRADE