

Art. 9º O registro das regras de uso relacionadas aos sistemas informatizados e bens permanentes de TIC constam da Ficha Técnica dos serviços de TIC, descrita na Instrução Normativa nº 7, de 2015.

Art. 10. O CGSI, deve contemplar nas ações de conscientização as orientações concernentes ao adequado uso dos ativos de TIC, visando o aprimoramento da segurança da informação e a proteção de dados.

Parágrafo único. A conscientização referida no *caput* deverá contemplar servidores, fornecedores e terceiros e contar com o apoio e atuação direta dos gestores do TRE.

## CAPÍTULO V

### DISPOSIÇÕES GERAIS

Art. 11. O CGSI deverá atualizar o processo de Gestão de Ativos de TIC, no prazo de trinta dias a partir da revisão dos serviços essenciais de TIC pelo COGEST.

Art. 12. Fica revogada a Instrução Normativa nº 11, de 18 de fevereiro de 2016.

Art. 13. Esta instrução normativa entra em vigor na data de sua publicação.

Recife, 18 de novembro de 2021.

CARLOS FREDERICO GONÇALVES DE MORAES

Presidente

## **INSTRUÇÃO NORMATIVA Nº 60, DE 18 DE NOVEMBRO DE 2021**

Estabelece a Política de Gestão de Incidentes de Segurança da Informação da Justiça Eleitoral de Pernambuco.

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

CONSIDERANDO a Resolução nº 370, de 28 de janeiro de 2021, do Conselho Nacional de Justiça (CNJ), que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD); e

CONSIDERANDO a Resolução nº 396, de 7 de junho de 2021, do CNJ, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ),

RESOLVE:

## CAPÍTULO I

### DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Instrução Normativa estabelece a Política de Gestão de Incidentes de Segurança da Informação da Justiça Eleitoral de Pernambuco.

Parágrafo único. Os critérios gerais para a notificação de fragilidades e eventos de segurança da informação de que trata o *caput* deste artigo obedecerão às regras estabelecidas nesta Instrução Normativa.

Art. 2º O Comitê de Governança de Segurança da Informação (CGSI) deve manter iniciativas de conscientização em segurança da informação, visando à disseminação do conhecimento e à internalização de atitudes proativas e cautelosas por parte dos(as) usuários(as).

## CAPÍTULO II

### DA NOTIFICAÇÃO DE EVENTOS DE SEGURANÇA DA INFORMAÇÃO

Art. 3º Os eventos de segurança da informação devem ser notificados ao CGSI assim que forem identificados.

Parágrafo único. A notificação deve conter relatos importantes, tais como o tipo de não conformidade, violação ou mau funcionamento, mensagem apresentada na tela ou comportamento considerado estranho.

Art. 4º São exemplos de evento ou incidente de segurança da informação:

I - perda de serviço, equipamento ou recursos;

II - mau funcionamento ou sobrecarga de sistema;

III - erros humanos;

IV - não conformidade com as políticas e diretrizes estabelecidas;

V - violações de procedimentos de segurança física;

VI - mudanças descontroladas de sistemas, tais como realizadas sem monitoramento ou sem decorrência de invasão;

VII - mau funcionamento de software ou hardware; e

VIII - violação de acesso a um sistema.

Art. 5º O(a) usuário(a) não deve realizar nenhuma ação por iniciativa própria nem, sob nenhuma circunstância, tentar averiguar uma fragilidade, para evitar o risco de causar danos ao sistema ou serviço de informação.

Parágrafo único. O descumprimento da orientação contida no caput deste artigo poderá resultar em responsabilização legal.

Art. 6º O CGSI deve realizar ações de orientação aos(às) usuários(as), visando a instruí-los como registrar e notificar a ocorrência de qualquer evento ou suspeita de fragilidade em sistemas ou serviços.

Parágrafo único. A notificação deve ser realizada, preferencialmente, por meio de mensagem de correio eletrônico.

### CAPÍTULO III

#### DOS PROCEDIMENTOS

Art. 7º O CGSI deve realizar, de forma prioritária, a análise das notificações de evento ou incidente de segurança da informação recebidas.

Art. 8º Constatado que a notificação configura um incidente de segurança cibernética, ela deve ser enviada de imediato à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR).

§ 1º Quando não se tratar de um incidente de segurança da informação, o CGSI deve prestar os devidos esclarecimentos ao(à) usuário(a) que apresentou a notificação.

§ 2º O(a) gestor(a) do ativo envolvido na notificação deve ser comunicado(a) em ambos os casos.

Art. 9º A gestão de incidentes em segurança cibernética deve observar o Protocolo de Prevenção de Incidentes Cibernéticos no âmbito do Poder Judiciário (PPINC-PJ), o Protocolo de Gerenciamento de Crises Cibernéticas no âmbito do Poder Judiciário (PGCRC-PJ) e o Protocolo de Investigação para Ilícitos Cibernéticos no âmbito do Poder Judiciário (PIILC-PJ), todos integrantes da Política de Segurança Cibernética do Poder Judiciário (PSEC-PJ), instituída pelo Conselho Nacional de Justiça (CNJ).

Art. 10. Quando o incidente de segurança caracterizar-se como uma crise cibernética, deve ser observado o Plano de Gestão de Incidentes Cibernéticos, sem prejuízo de outras ações que possam ser identificadas pelo Comitê de Crises Cibernéticas e/ou pela ETIR.

Art. 11. Ações preventivas e de controle devem ser adotadas visando a minimizar os riscos relacionados à segurança da informação, especialmente aquelas indicadas no Manual de Referência - Proteção de Infraestruturas Críticas de TIC, Manual de Referência - Gestão de Identidade e Controle de Acessos, ambos aprovados pelo CNJ.

### CAPÍTULO IV

#### DISPOSIÇÕES FINAIS

Art. 12. Os casos omissos e a avaliação de exceções a esta Instrução Normativa serão objeto de decisão do Diretor(a)-Geral.

Art. 13. O fluxo do processo de gestão de incidentes de segurança da informação deve ser revisto em até 60 (sessenta) dias após a publicação desta Instrução Normativa.

Art. 14. Fica revogada a Instrução Normativa nº 16, de 30 de março de 2017.

Art. 15. Esta Instrução Normativa entra em vigor na data de sua publicação.

Recife, 18 de novembro de 2021.

CARLOS FREDERICO GONÇALVES DE MORAES

Presidente

## **INSTRUÇÃO NORMATIVA Nº 58, DE 18 DE NOVEMBRO DE 2021**

Estabelece normas gerais para garantir a segurança da informação, mediante o controle do acesso, circulação e permanência de pessoas nas instalações da Justiça Eleitoral de Pernambuco.

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DE PERNAMBUCO, no uso de suas atribuições legais e

CONSIDERANDO a Lei nº 9.609, de 19 de fevereiro de 1998, que dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no país, e dá outras providências, e a Lei nº 9.279, de 14 de maio de 1996, que regula direitos e obrigações relativos à propriedade industrial;

CONSIDERANDO a Resolução nº 370, de 15 de dezembro de 2015, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), com a alteração promovida pela Resolução nº 396, de 7 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), ambas do Conselho Nacional de Justiça (CNJ);

CONSIDERANDO a Resolução nº 23.644, de 1º de julho de 2021, do Tribunal Superior Eleitoral (TSE), e a Resolução nº 164, de 10 de julho de 2012, deste Tribunal que dispõem sobre a Política de Segurança da Informação (PSI);

CONSIDERANDO a Resolução nº 305, de 18 de dezembro de 2017, deste Tribunal, que dispõe sobre o controle do acesso e da circulação de pessoas, materiais e veículos, a utilização de cartões de acesso, catracas, detectores de metais e escâneres de raios-X e o monitoramento de imagens nas dependências de prédios da Justiça Eleitoral de Pernambuco, e a Resolução nº 334, de 7 de novembro de 2018, que institui o Plano de Segurança Institucional (PLANSEG) do Tribunal Regional Eleitoral de Pernambuco (TRE-PE);

CONSIDERANDO a Norma Técnica ABNT NBR ISO/IEC 27001, de 8 de novembro de 2013, que especifica requisitos para um Sistema de Gestão de Segurança da Informação, e a Norma Técnica ABNT NBR ISO/IEC 27002, de 8 de novembro de 2013, que fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações; e CONSIDERANDO, ainda, a Instrução Normativa nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências, e a Norma Complementar nº 03, de 30 de junho de 2009, que estabelece diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações (POSIC) nos órgãos e entidades da Administração Pública Federal, ambas do Gabinete de Segurança Institucional da Presidência da República,

RESOLVE:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 1º Esta Instrução Normativa estabelece normas gerais para garantir o controle de acesso de pessoas e a segurança da informação nas instalações da Justiça Eleitoral de Pernambuco.

CAPÍTULO II

DO CONTROLE DE ACESSO, CIRCULAÇÃO E PERMANÊNCIA DE PESSOAS

Art. 2º O acesso, a circulação e a permanência de pessoas nas dependências dos imóveis onde são desenvolvidas as atividades da Justiça Eleitoral em Pernambuco devem obedecer ao disposto