§ 1º Para o desenvolvimento das competências devem ser considerados os requisitos técnicos e gerenciais necessários, inclusive aqueles identificados quando da execução dos testes e/ou aplicação do Plano de Continuidade de Negócios.

§ 2º Os treinamentos identificados como necessários devem constar no Plano Anual de Capacitação (PAC) deste Tribunal.

CAPÍTULO VI

DISPOSIÇÕES FINAIS

Art. 19. Fica revogada a Instrução Normativa nº 18, de 17 de maio de 2017.

Art. 20. Esta Instrução Normativa entra em vigor na data de sua publicação.

Recife, 24 de setembro de 2021.

CARLOS FREDERICO GONÇALVES DE MORAES

Presidente

INSTRUÇÃO NORMATIVA Nº 51, DE 23 DE SETEMBRO DE 2021

Estabelece regras para o uso de recurso de criptografia para a segurança e proteção de informações, no âmbito da Justiça Eleitoral de Pernambuco.

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

CONSIDERANDO a Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD);

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

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

CONSIDERANDO o disposto no Relatório de Atividades (documento SEI nº 1348732) para atendimento à Recomendação nº 73, de 20 de agosto de 2020, do CNJ, que recomenda aos órgãos do Poder Judiciário brasileiro a adoção de medidas preparatórias e ações iniciais para adequação às disposições contidas na Lei Geral de Proteção de Dados (LGPD),

RESOLVE:

CAPÍTULO I

DO OBJETIVO E DAS DEFINIÇÕES

Art. 1° As regras para o uso de recurso de criptografia para a segurança e proteção de informações no âmbito da Justiça Eleitoral de Pernambuco, ficam estabelecidas nos termos desta instrução normativa.

Art. 2° Para os efeitos desta norma, são estabelecidos os seguintes conceitos e definições:

I - algoritmo: função matemática utilizada na cifração e na decifração de informações;

II - algoritmo assimétrico: função matemática que utiliza chaves criptográficas distintas para cifração e decifração de informações;

III - algoritmo simétrico: função matemática que utiliza a mesma chave criptográfica tanto para cifração quanto para a decifração de informações;

IV - autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

V - Autoridade Certificadora: entidade, pública ou privada, subordinada à hierarquia da ICP-Brasil, responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais;

VI - backup*:* cópia de segurança de dados;

VII - certificado digital: certificado, emitido por uma Autoridade Certificadora, que permite a identificação segura e inequívoca do(a) autor(a) de uma mensagem ou transação feita em meios eletrônicos;
VIII - cifração: ato de cifrar uma linguagem mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para substituir sinais de linguagem em claro, por outros ininteligíveis para pessoas não autorizadas a conhecê-la;
IX - chave ou chave criptográfica: valor que trabalha com um algoritmo criptográfico para cifração ou decifração;
X - confidencialidade: garantia de que o acesso a determinados dados e informações é concedido apenas a quem tem autorização para isso;
XI - controle criptográfico: sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração;
XII - credencial: permissão que habilita determinada pessoa, sistema ou organização ao acesso, que pode ser física, como crachá, ou lógica, como usuário e senha;
XIII - decifração: ato de decifrar uma linguagem, mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter o processo de cifração;
XIV - disponibilidade: garantia de que o dado esteja disponível sempre que necessário;
XV - HTTPS (Hyper Text Transfer Protocol Secure): Protocolo de Transferência de Hipertexto Seguro, que implementa o protocolo HTTP com a utilização do protocolo SSL/TLS para criar uma camada adicional de segurança, permitindo que os dados da comunicação sejam transmitidos por meio de uma conexão criptografada e que se verifique a autenticidade do servidor e do(a) cliente por meio de certificados digitais, nos sítios onde se utiliza essa proteção extraordinária na transmissão dos dados;
XVI - ICP-Brasil: Infraestrutura de Chaves Públicas Brasileira;
XVII - integridade: garantia de que os dados estão íntegros, sem qualquer modificação indevida;
XVIII - SSL (Secure Sockets Layer): ferramenta de segurança digital que permite a comunicação criptografada entre um sítio e um navegador;
XIX - TLS (Transport Layer Security): protocolo projetado para fornecer segurança nas comunicações sobre uma rede de computadores; e
XX - VPN (Virtual Private Network): rede privada construída sobre uma infraestrutura de rede pública.

CAPÍTULO II

DO USO DE CRIPTOGRAFIA

Art. 3º O recurso de criptografia será utilizado para assegurar:
I - a confidencialidade, a integridade, a autenticidade e a disponibilidade de informações pessoais, sensíveis ou críticas que se encontrem armazenadas no Centro de Processamento de Dados (CPD);
II - a proteção dos arquivos de backup referente às informações armazenadas no CPD;
III - a proteção do tráfego de login/senha de rede, quando da autenticação de usuários; e
IV - a proteção contra interceptações e capturas dos dados transmitidos por meio de VPN.
§ 1º As informações pessoais e/ou sensíveis referem-se àquelas definidas na Lei nº 13.709, de 2018 (Lei Geral de Proteção de Dados Pessoais).
§ 2º As informações críticas são aquelas relacionadas aos serviços essenciais definidos pelo Comitê de Gestão Estratégica (COGEST).
§ 3º Outras informações poderão ser alvo de criptografia, desde que seja deliberado pelo COGEST e haja recurso tecnológico disponível.

Art. 4º A escolha do tipo, da qualidade e da força do algoritmo apropriado para cada propósito, sempre que possível, terá como referencial a matriz de riscos elaborada pela Comissão de Segurança da Informação (CSI).

Parágrafo único. O recurso criptográfico indicado pela(s) unidade(s) técnica(s) para uso no TRE, deverá ser submetido à análise do Comitê Executivo de Tecnologia da Informação e Comunicação (CETIC).

Art. 5º O tráfego de autenticação de usuários(as) e o tráfego de informações pessoais, sensíveis ou críticas, entre as camadas envolvidas nos sistemas ou serviços disponibilizados pelo TRE, deverão ser protegidos com o uso de mecanismos de criptografia como HTTPS, SSL, TLS e VPN.

Parágrafo único. Poderá ser utilizado recurso diverso de criptografia, desde que previamente aprovado pelo CETIC e demonstrada a segurança no tratamento do dado.

Art. 6º Quando autorizado pelo COGEST e havendo recurso tecnológico disponível, informações pessoais, sensíveis ou críticas armazenadas em dispositivos móveis (notebook, tablet, smartphone, etc.) ou em mídias removíveis (pendrive, DVD, HD externo, etc.) poderão ser criptografadas para evitar sua divulgação indevida em caso de perda ou furto do equipamento ou da mídia.

Art. 7º Certificados digitais poderão ser utilizados para identificação de servidor/aplicação (hardware ou software) de uso interno ou para substituir credenciais de autenticação de usuários (as) utilizados em sistemas do TRE.

Parágrafo único. A concessão de certificado digital dar-se-á mediante autorização do COGEST ou quando configurar um requisito estabelecido em norma.

Art. 8º A unidade e/ou usuário(a) que utilizar recurso de criptografia ou certificado digital será responsável pela guarda da chave criptográfica sob sua responsabilidade.

Parágrafo único. A chefia da unidade e/ou o(a) usuário(a) de recurso criptográfico deverá assinar o Termo de Uso de Recursos Criptográficos, de acordo com modelo constante no Anexo I.

Art. 9º No caso de perda ou dano à chave criptográfica, a Secretaria de Tecnologia da Informação e Comunicação (STIC) deverá ser imediatamente comunicada, por meio da Central de Serviços de TIC.

§ 1º A unidade técnica da STIC adotará procedimentos de recuperação da chave e/ou das informações cifradas, caso seja possível.

§ 2º A concessão de novo recurso criptográfico e/ou certificado digital, na hipótese prevista no caput deste artigo, deverá ser autorizada pelo COGEST.

CAPÍTULO III

DA AQUISIÇÃO DE RECURSOS DE CRIPTOGRAFIA

Art. 10. A STIC ficará responsável por prever, quando da elaboração da Proposta Orçamentária do TRE, a aquisição dos recursos de criptografia aprovados pelo CETIC.

Art. 11. A distribuição dos recursos criptográficos adquiridos deverá seguir o estabelecido nesta instrução normativa.

CAPÍTULO IV

DISPOSIÇÕES FINAIS

Art. 12. A unidade responsável por distribuir/entregar o recurso criptográfico e/ou certificado digital deverá adotar procedimentos de controle que registre, no mínimo:

I - unidade/usuário(a) contemplado(a);

II - data de início de uso do recurso;

III - data de finalização do uso do recurso; e

IV - identificação do documento em que consta a autorização de uso do recurso criptográfico.

Art. 13. O comprometimento do sigilo de qualquer recurso criptográfico deverá ser comunicado, imediatamente, à CSI.

Art. 14. Na hipótese de alteração na estrutura orgânica deste Tribunal, com a constituição de novos organismos em substituição ao COGEST, ao CETIC e/ou à CSI, as decisões destes permanecerão válidas, desde que os novos organismos tenham as mesmas atribuições.
Art. 15. Esta instrução normativa entrará em vigor na data de sua publicação.
Recife, ____ de setembro de 2021.
CARLOS FREDERICO GONÇALVES DE MORAES
Presidente
ANEXO DA INSTRUÇÃO NORMATIVA Nº 51/2021
TERMO DE USO DE RECURSO CRIPTOGRÁFICO
Pelo presente instrumento, eu, (nome), (lotado(a) na unidade), DECLARO, sob pena das sanções cabíveis e nos termos da Instrução Normativa - TRE-PE nº ____/2021, que tenho conhecimento sobre o uso do recurso criptográfico sob minha responsabilidade, sendo vedado seu uso:
a) para fins diversos dos funcionais ou institucionais;
b) para interceptar ou tentar interceptar transmissão de dados ou informações não destinados ao seu próprio acesso por quaisquer meios;
c) para tentar ou efetuar a interferência em serviços de outros(as) usuários(as) ou o seu bloqueio por quaisquer meios;
d) para violar ou tentar violar os recursos de segurança dos equipamentos que utilizem recursos criptográficos;
e) para cifração ou decifração de informações ilícitas, entre as quais, materiais obscenos, ofensivos, ilegais, não éticos, ameaças, difamação, injúria, racismo ou quaisquer outras que venham a causar molestamento, tormento ou danos a terceiros(as);
f) de forma inadequada, expondo-o a choques elétricos ou magnéticos, líquidos ou outros fatores que possam vir a causar-lhe danos, incluindo testes de invasão/intrusão, de quebra de senhas, de quebra de cifração e de técnicas de invasão e defesa.
Recife, ___ de _____de 2021.
Assinatura
Nome do(a) usuário(a) / Unidade

INSTRUÇÃO NORMATIVA Nº 52, DE 23 DE SETEMBRO DE 2021

Institui a realização de perícia por junta oficial com a utilização do recurso de videoconferência, no âmbito do Tribunal Regional Eleitoral de Pernambuco (TRE-PE).
O) PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DE PERNAMBUCO, no uso de suas atribuições legais e regimentais,
CONSIDERANDO que a Resolução nº 207, de 15 de outubro de 2015, do Conselho Nacional de Justiça (CNJ), ao dispor sobre a política de atenção à saúde de magistrados(as) e servidores(as), faculta aos tribunais a realização de perícias oficiais administrativas em saúde mediante videoconferência e, se necessário, com a colaboração de profissionais de outros órgãos do Poder Judiciário e de instituições públicas;
CONSIDERANDO o disposto na Portaria nº 190, de 5 de setembro de 2019, do Ministério da Economia, que institui a avaliação por junta oficial com a utilização do recurso de videoconferência e estabelece os procedimentos a serem observados pelas Unidades do Subsistema Integrado de Atenção à Saúde do Servidor (SIASS) na execução das avaliações, por junta oficial, previstas na Lei nº 8.112, de 11 de dezembro de 1990, e no Decreto nº 7.003, de 9 de novembro de 2009, com a utilização desse recurso;
CONSIDERANDO o reduzido número de profissionais de saúde para atendimento da demanda de perícias a serem realizadas pela junta oficial deste Tribunal Regional Eleitoral de Pernambuco (TRE-PE); e