TRIBUNAL REGIONAL ELEITORAL DO PIAUI

Portaria Presidência Nº 269/2023 TRE/PRESI/DG/ASSDG, de 06 de julho de 2023

Dispõe sobre as regras e os procedimentos para uso do Múltiplo Fator de Autenticação (MFA) no âmbito do Tribunal Regional Eleitoral do Piauí.

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

CONSIDERANDO a necessidade de definir normativo para estabelecer diretrizes para o uso do Múltiplo Fator de Autenticação (MFA) no âmbito do TRE-PI;

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

CONSIDERANDO a Resolução TSE nº 23.644/2021, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

CONSIDERANDO a Resolução TRE-PI nº 448/2022 que adota a PSI da Justiça Eleitoral estabelecida pela Resolução TSE nº 23.644/2021;

CONSIDERANDO a Portaria CNJ nº 162/2021 que disciplina os protocolos e manuais criados pela Resolução CNJ nº 396/2021;

CONSIDERANDO a Portaria TRE-PI nº 440/2021 que estabelece a Política de Controle de Acessos e Uso Aceitável dos Recursos de Tecnologia da Informação do TRE-PI;

CONSIDERANDO as boas práticas em segurança da informação previstas nas normas ABNT ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013;

CONSIDERANDO as boas práticas em segurança da informação previstas no modelo CIS Controls V.8;

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Esta norma é complementar à Política de Controle de Acessos e Uso Aceitável dos Recursos de Tecnologia da Informação do TRE-PI, estabelecida pela Resolução TRE-PI nº 440/2021.

CAPÍTULO II

DAS DEFINIÇÕES

Art. 2º Para efeitos desta norma, consideram-se os termos e definições a seguir:

I - Atividades precípuas: conjunto de procedimentos e tarefas que utilizam recursos tecnológicos, humanos e materiais, inerentes à atividade-fim da Justiça Eleitoral;

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

III - Confidencialidade: propriedade da informação que garante que ela não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem a devida autorização;

IV - Disponibilidade: propriedade da informação que garante que ela será acessível e utilizável sempre que demandada;

V - Informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

VI - Integridade: propriedade que garante que a informação mantém todas as características originais estabelecidas pelo proprietário;

VII - Irretratabilidade (ou não repúdio): garantia de que a pessoa se responsabilize por ter assinado ou criado a informação;

VIII - Recurso: além da própria informação, é todo o meio direto ou indireto utilizado para o seu tratamento, tráfego e armazenamento;

IX - Recursos de Tecnologia da Informação: são o conjunto de bens e serviços de tecnologia da informação que constituem a infraestrutura tecnológica de suporte automatizado ao ciclo da informação, que envolve as atividades de produção, coleta, tratamento, armazenamento, transmissão, recepção, comunicação e disseminação;

X - Segurança da informação: abrange aspectos físicos, tecnológicos e humanos da organização e orienta-se pelos princípios da autenticidade, da confidencialidade, da integridade, da disponibilidade e da irretratabilidade da informação, entre outras propriedades;

XI - Tecnologia da Informação e Comunicação (TIC): ativo estratégico que suporta processos institucionais, por meio da conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, fazer uso e disseminar informações;

XII – Usuária(o): pessoa que utiliza, de forma autorizada, recursos inerentes às atividades precípuas da Justiça Eleitoral.

CAPÍTULO III

DO ESCOPO

Art. 3º O Múltiplo Fator de Autenticação (MFA) será utilizado nas atividades precípuas do TRE-PI para garantir a segurança da informação e a integridade dos recursos de Tecnologia da Informação.

§ 1º Para efeito deste normativo o MFA será utilizado no âmbito do TRE-PI para:

I - acesso remoto aos recursos de TI críticos ou essenciais ao Tribunal (VPN, datacenter, equipamentos servidores, firewall etc);

II - o serviço ou sistema de informação que estiver disponível na internet e intranet; e

III - garantir a identidade da credencial.

Art. 4º Esta norma aplica-se a todos os magistrados, promotores, servidores e colaboradores em geral que utilizam recursos ou serviços de TI que se enquadrem nos requisitos do Art. 3º.

CAPÍTULO IV

DAS RESPONSABILIDADES

Art. 5º Caberá à Secretaria de Tecnologia da Informação (STI) viabilizar soluções para uso do múltiplo fator de autenticação (MFA) nos casos definidos no Art. 3º. Para tanto, poderão ser utilizados:

I - tokens virtuais ou físicos;

II - Aplicativo instalado em smartphone;

III - SMS; ou

IV - ligação telefônica.

§ 1º A definição acerca do tipo de solução a ser adotada dependerá do serviço ou recurso de TI que esteja sendo utilizado.

§ 2º A solução poderá utilizar equipamentos ou dispositivos particulares, mediante permissão do usuário e orientação da STI, ficando neste caso o acesso condicionado ao atendimento de requisitos de segurança estabelecidos em procedimentos definidos pela STI.

Art. 6º O usuário deverá seguir as orientações estabelecidas para o uso do MFA e responsabilizar-se pela guarda e sigilo dos fatores de autenticação.

Art. 7º A usuária ou o usuário deverá assinar o Termo de Responsabilidade - Recebimento do Token, no qual consta, dentre outras determinações, que a perda ou o extravio do token deverá ser comunicada(o) imediatamente à Secretaria de Tecnologia da Informação.

Art. 8º Caberá à usuária ou ao usuário zelar pelo cumprimento das atividades jurisdicionais ou administrativas mediante o uso da solução de múltiplo fator de autenticação adotada pelo Tribunal.

Art. 9º É vedado o uso de token físico não fornecido ou contratado pelo Tribunal para o atendimento dos requisitos deste normativo, salvo em situações gerenciadas pela STI.

CAPÍTULO V

DA INDISPONIBILIDADE

Art. 10. Em caso de indisponibilidade temporária de um token físico ou virtual, fornecido pelo Tribunal, deve ser comunicado imediatamente à STI por meio de chamado registrado na Central de Serviços de TI.

Parágrafo único - A STI disponibilizará uma solução temporária visando garantir o desenvolvimento das atividades jurisdicionais ou administrativas, durante o expediente do dia.

Art. 11. Em caso de indisponibilidade permanente de token físico ou do dispositivo (smartphone) no qual esteja instalado um token virtual, devido a roubo ou furto, a usuária ou o usuário devem comprovar por meio do registro de boletim de ocorrência registrado em órgão competente.

CAPÍTULO VI

DAS DISPOSIÇÕES FINAIS

Art. 12. Os casos omissos serão resolvidos pela Diretoria-Geral.

Art. 13. A revisão deste normativo poderá ser realizada bianualmente ou sempre que se fizer necessário, visando garantir as condições de segurança cibernéticas necessárias ao uso de recursos ou serviços de TI do Tribunal.

Art. 14. Esta Portaria entra em vigor na data de sua publicação.

Desembargador ERIVAN LOPES

Presidente do TRE-PI

Documento assinado eletronicamente por **Erivan José da Silva Lopes**, **Presidente**, em 07/07/2023, às 09:20, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-pi.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0001869102** e o código CRC **E88BC236**.