TRIBUNAL REGIONAL ELEITORAL DO PIAUI

Portaria Presidência Nº 387/2024 TRE/PRESI/DG/ASSDG, de 17 de julho de 2024

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 CNJ nº 140/2024 que determina a implementação do método de autenticação do tipo Múltiplo Fator de Autenticação (MFA) como requisito funcional para acesso a sistemas judiciais sensíveis.

CONSIDERANDO a Portaria TRE-PI nº 330/2023 que estabelece a Política de Gestão de Identidade e Controle de Acessos Físico e Lógico;

CONSIDERANDO a Portaria TRE-PI nº 51/2024 que estabelece o 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 Gestão de Identidade e Controle de Acesso Físico e Lógico, estabelecida pela Portaria TRE-PI nº 330/2023.

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 - Autenticidade: 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

DAS DISPOSIÇÕES INICIAIS

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

§ 1º O uso de MFA é obrigatório para usuários internos e externos.

§ 2º A habilitação do MFA é mandatória, não cabendo aos usuários optarem por sua utilização.

§ 3º A implementação do MFA não exclui ou limita a aplicação de outras medidas de segurança ou práticas que contribuam para o fortalecimento da segurança da informação e proteção dedados, devendo ser associada a uma cadeia de credenciais confiáveis adequadamente protegidas.

Art. 4º Consideram-se sistemas judiciais sensíveis:

a) sistemas de processo judicial eletrônico;

b) sistemas ou serviços que permitam acesso a dados sensíveis ou confidenciais;

c) sistemas ou serviços que permitam a emissão de mandados de prisão e alvarás de soltura;

d) sistemas ou serviços que permitam a pesquisa de ativos financeiros, sua constrição e movimentação;

e) sistemas de tramitação de processos administrativos;

f) ferramentas de acessos a redes privadas virtuais (VPNs);

g) sistemas ou serviços que permitam acesso remoto ao ambiente interno de rede (VPN, datacenter, equipamentos servidores, firewall etc);

h) sistemas ou serviços de e-mail funcional ou corporativo;

i) quaisquer outros sistemas ou serviços considerados críticos na avaliação interna do Tribunal, incluindo quaisquer sistemas expostos ao acesso remoto via internet.

j) o serviço ou sistema de informação que estiver disponível na internet e intranet; e

§ 1º Sistemas de processo judicial eletrônico e módulos da Plataforma Digital do Poder Judiciário Brasileiro (PDPJ-Br) deverão utilizar o Serviço de Autenticação Única (*Single Sign-On - SSO*) disponibilizado na PDPJ-Br.

§ 2º Ficam excluídos da obrigatoriedade de implementação do MFA os serviços públicos cuja utilização não depende de autenticação.

§ 3º O uso do MFA também deve ser considerado quando for necessário garantir a identidade da credencial.

Art. 5º Esta norma aplica-se a todos os magistrados, promotores, servidores, colaboradores em geral e usuários externos que utilizam recursos ou serviços de TI que se enquadrem nos requisitos do Art. 4º.

CAPÍTULO IV
DA GESTÃO DO MÚLTIPLO FATOR DE AUTENTICAÇÃO

Seção I
Dos Critérios de Seleção

Art. 6º A solução de MFA adotada pelo TRE-PI deverá considerar os seguintes critérios na seleção dos métodos de MFA:

I - Compatibilidade: escolha de métodos de MFA que se integrem de maneira eficiente com a infraestrutura tecnológica existente;

II - Usabilidade: priorização de soluções que ofereçam facilidade de uso para promover ampla adoção pelos usuários; e

III - Segurança: avaliação rigorosa do nível de segurança fornecido por cada método de MFA, visando proteção efetiva contra ameaças cibernéticas.

Seção II
Mecanismos de Revisão e Atualização do Múltiplo Fator de Autenticação (MFA)

Art. 7º A STI deverá avaliar, de forma contínua, a eficácia das medidas de MFA adotadas. Este monitoramento deverá incluir a análise de tentativas de acesso, a taxa de sucesso de autenticações MFA e a detecção de padrões anormais que possam indicar tentativas de violação.

Parágrafo único. Caso o método de MFA implementado seja considerado insuficiente em termos de eficácia, eficiência, segurança ou usabilidade, a STI deverá tomar as medidas necessárias para sua revisão ou substituição, podendo incluir a avaliação de novas tecnologias de autenticação e a implementação de soluções mais robustas e adaptáveis às necessidades atuais e futuras.

Art. 8º Para fins de revisão regular da solução de MFA adotada devem ser observados:

a) a necessidade de aprimoramento tecnológico;

b) a necessidade de ajustes nas políticas de MFA.

c) ameaças de segurança cibernética; e

d) adoção de práticas de segurança recomendadas por entidades nacionais e internacionais de segurança da informação.

Parágrafo único. Todas as revisões, atualizações e substituições de soluções MFA deverão ser devidamente documentadas, incluindo justificativa para as mudanças, impactos esperados e orientações para implementação. As atualizações serão comunicadas a todos os usuários afetados de forma clara e acessível, garantindo a compreensão e a adoção das novas medidas.

Seção III
Capacitação e Compartilhamento

Art. 9º O TRE-PI deverá desenvolver ações periódicas de capacitação e conscientização de seus usuários, internos e externos, destinadas a garantir uso seguro e eficaz do MFA.

Parágrafo único. A periodicidade das ações de que trata o *caput* deste artigo será definida pelo órgão e informado anualmente ao Conselho Nacional de Justiça.

CAPÍTULO V

DAS RESPONSABILIDADES

Art. 10. Caberá à Secretaria de Tecnologia da Informação (STI) viabilizar soluções para uso do múltiplo fator de autenticação (MFA) nos casos definidos no Art. 4º. 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. 11. O usuário deverá seguir as orientações estabelecidas para o uso do MFA e responsabilizar-se pela guarda e sigilo dos fatores de autenticação.

Art. 12. A usuária ou o usuário deverá assinar o Termo de Responsabilidade - Recebimento do *Token*, no qual consta, dentre outras determinações, que o extravio, furto ou roubo do token deverá ser comunicada(o) imediatamente à Secretaria de Tecnologia da Informação e registrado o boletim de ocorrência.

Art. 13. 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. 14. 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 VI

DA INDISPONIBILIDADE

Art. 15 A indisponibilidade de um *token* físico ou do dispositivo *smartphone* no qual esteja instalado o *token* virtual, fornecido pelo Tribunal, deve ser comunicada imediatamente à STI por meio de chamado registrado na Central de Serviços de TI.

§ 1º A STI disponibilizará uma solução temporária visando garantir o desenvolvimento das atividades jurisdicionais ou administrativas, durante o expediente do dia.

§ 2º A STI deverá bloquear o uso do *token* físico aos serviços de TI imediatamente, podendo desbloqueá-lo mediante nova informação pelo usuário que o dispositivo foi localizado.

§ 3º A usuária ou o usuário deve comprovar por meio do registro de boletim de ocorrência, registrado em órgão competente, o extravio, furto ou roubo.

§ 4º A usuária ou o usuário arcará com os custos de novo *token* físico, em caso de extravio.

§ 5º Em caso de indisponibilidade do dispositivo físico *smartphone* no qual esteja instalado um *token* virtual, não haverá custos para o fornecimento de novo *token* virtual.

CAPÍTULO VII

DAS DISPOSIÇÕES FINAIS

Art. 16. Os casos omissos serão resolvidos pela Presidência.

Art. 17. É responsabilidade da Comissão de Segurança da Informação realizar o

monitoramento da implementação do múltiplo fator de autenticação no TRE-PI, propondo os ajustes necessários quando for o caso.

Art. 18. A STI deverá implementar a solução de múltiplo fator de autenticação (MFA) em 90 (noventa) dias, nos termos da Portaria CNJ nº 140/2024..

Art. 19. A revisão deste normativo poderá ser realizada anualmente 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. 20. Fica revogada a Portaria Presidência nº 269/2023, de 06 de julho de 2023.

Art. 21. Esta Portaria entra em vigor na data de sua publicação.

Desembargador SEBASTIÃO RIBEIRO MARTINS

Presidente do TRE-PI

Documento assinado eletronicamente por **Sebastião Ribeiro Martins**, **Presidente**, em 18/07/2024, às 09:12, 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 **0002153647** e o código CRC **AAE3FABB**.