

CONSIDERANDO a necessidade de verificação da regularidade dos serviços cartorários na 153ª Zona Eleitoral - Mirandópolis e a sua eventual correção;

RESOLVE:

Art. 1º Instaurar procedimento de Inspeção de Ciclo da 153ª Zona Eleitoral - Mirandópolis, na modalidade presencial, a ser realizado na sede do Cartório Eleitoral, das 11 às 18 horas do dia 24 de agosto de 2023, sem prejuízo do expediente e do atendimento ao público, nos termos do artigo 9º do Provimento CGE nº 02/2023.

Art. 2º Convocar o(a) Excelentíssimo(a) Juiz(Juíza) Eleitoral da 153ª ZE - Mirandópolis, para estar presente na data da realização dos trabalhos da Inspeção presencial a ser realizada na Zona Eleitoral em epígrafe, por esta Corregedoria Regional.

Art. 3º Designar as servidoras e os servidores abaixo elencados para compor a equipe que inspecionará o Juízo da 153ª Zona Eleitoral - Mirandópolis, ao lado da Excelentíssima Senhora Juíza Assessora da Corregedoria, Doutora Fernanda Mendes Simões Colombini:

Elizete Yoshie Kato - SEIC

Fabiana Reis Pacheco - COAJU

Geraldo Oliveira Reis Rabello Sampaio - COAJU

Honor Barbosa Cabral - SEUE

João Roberto dos Santos - SEIC

Joaquim Honório Filho - SEIC

Johnny Andrei Luig - SEDIPO

Juliana Lages da Silva Yokoyama - SEIC

Luana Leite de Araújo Feitosa - SEIC

Lucas Luís da Silva - SEFAC

Lúcia Muniz Aslan Ribeiro - SEIC

Maria Fernanda Amado de Andrade - SEIC

Ramon Pontes da Costa Souza - SEIC

Rosângela Emilia Binato Rodrigues - COAS

Wagner Pajor - SEUE

Art. 4º Determinar a publicação do presente ato normativo na imprensa oficial, bem como o seu encaminhamento à zona eleitoral a ser inspecionada, para afixação em local visível.

Esta Portaria entrará em vigor na data de sua publicação.

SILMAR FERNANDES

Corregedor Regional Eleitoral

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

PORTARIAS

PORTARIA TRE-SP N. 226/2023

PORTARIA TRE-SP N. 226/2023

Dispõe sobre a instituição do Uso de Recursos Criptográficos relativa à Política de Segurança da Informação do Tribunal Regional Eleitoral do Estado de São Paulo, TRE-SP.

O DIRETOR-GERAL DA SECRETARIA DO TRIBUNAL REGIONAL ELEITORAL DO ESTADO DE SÃO PAULO, no uso de suas atribuições legais e regulamentares, conforme delegação de competência estabelecida no artigo 2º, inciso I, da Portaria TRE-SP n. 1/2022;

CONSIDERANDO a necessidade de definir processos de Uso de Recursos Criptográficos no âmbito do Tribunal Regional Eleitoral de São Paulo;

CONSIDERANDO a necessidade de apoiar os processos de continuidade de serviços de TI, em caso de eventos de causas naturais, acidentais, tecnológicas ou humanas;

CONSIDERANDO a necessidade de apoiar a gestão do processo de tratamento e resposta a incidentes em redes computacionais no Tribunal Regional Eleitoral de São Paulo;

CONSIDERANDO a Res. CNJ 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

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

CONSIDERANDO a Portaria DG/TSE 444/2021, que dispõe sobre a instituição da norma de termos e definições relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral;

CONSIDERANDO a Res. TRE/SP 580/2022, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral de São Paulo;

CONSIDERANDO as boas práticas em segurança da informação e privacidade previstas nas normas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002, complementadas pela norma ABNT NBR ISO/IEC 27701;

CONSIDERANDO as boas práticas na gestão da continuidade de negócios previstas nas normas ABNT NBR ISO/IEC 22301 e 22313;

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

CONSIDERANDO a necessidade de implementar controles para o tratamento de dados pessoais, de acordo com a Lei 13.709/2018 (LGPD);

CONSIDERANDO que a segurança da informação e a proteção de dados pessoais são condições essenciais para a prestação dos serviços jurisdicionais e administrativos do Tribunal Regional Eleitoral de São Paulo;

RESOLVE:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituído o uso de recursos criptográficos, em consonância com a Política de Segurança da Informação (PSI) do Tribunal Regional Eleitoral de São Paulo.

Art. 2º Para os efeitos da Política de Segurança da Informação do Tribunal Regional Eleitoral de São Paulo, aplicam-se os termos e definições conceituados na Portaria DG/TSE 444/2021.

CAPÍTULO II

DAS DEFINIÇÕES

Art. 3º Para efeitos desta Portaria consideram-se os termos e definições previstos na Portaria DG/TSE 444/2021.

Art. 4º O uso de recursos criptográficos visa proteger a confidencialidade, a integridade, a autenticidade e a irretratabilidade dos dados transmitidos pelas redes de computadores, assim como dos dados em repouso, armazenados em servidores, microcomputadores, dispositivos móveis e bancos de dados.

CAPÍTULO III

DA CRIPTOGRAFIA DOS DADOS EM TRÂNSITO

Art. 5º É obrigatório o uso de protocolo seguro, como HTTPS, em todos os sistemas e portais web, independentemente de serem acessados pela rede interna ou pela Internet.

Art. 6º Toda comunicação cliente/servidor pela qual trafeguem dados pessoais ou logins e senhas, deve utilizar protocolos de comunicação segura.

CAPÍTULO IV

DA CRIPTOGRAFIA DOS DADOS ARMAZENADOS

Art. 7º Os dados pessoais sensíveis armazenados em servidores e bancos de dados devem adotar técnicas de criptografia ou anonimização, visando diminuir o risco em caso de vazamento de dados.

Art. 8º As cópias de segurança (backups) que contenham dados pessoais sensíveis devem adotar técnicas de criptografia, visando diminuir o risco em caso de vazamento de dados.

Art. 9º Os computadores, notebooks e dispositivos móveis, de propriedade da Justiça Eleitoral, utilizados em trabalho remoto, devem ter seus discos rígidos protegidos por criptografia, visando diminuir o risco de vazamento de dados em caso de furto.

CAPÍTULO V

DA ASSINATURA DIGITAL

Art. 10 A STI deverá distribuir e gerenciar certificados para assinatura digital, sejam do tipo A1 (arquivo digital com senha) ou A3 (token), de acordo com as necessidades da usuária ou do usuário internos e com os procedimentos técnicos adotados.

Art. 11 Os certificados digitais poderão ser utilizados como segundo fator de autenticação (2FA) em computadores ou sistemas, de acordo com a sua criticidade e disponibilidade da tecnologia.

CAPÍTULO VI

DA AUTORIDADE CERTIFICADORA

Art. 12 O TRE/SP poderá manter Infraestrutura de Chaves Públicas (ICP) própria para uso em sistemas e computadores de uso interno, sendo permitido o modelo de AC (autoridade certificadora) autoassinada.

Parágrafo único. O servidor utilizado para geração de certificados deverá ser mantido sob condições seguras, contemplando configurações, aplicação de patches e controles de acesso.

Art. 13 Os certificados digitais instalados em servidores e sistemas Web com acesso pela Internet deverão utilizar certificados digitais fornecidos por AC (autoridade certificadora) comercial, visando a compatibilidade com os computadores e dispositivos móveis das usuárias e dos usuários externos.

CAPÍTULO VII

DAS RESPONSABILIDADES

Art. 14 Cabe à STI, por meio de suas áreas técnicas:

- I - implementar o nível adequado de criptografia nos sistemas e dispositivos;
- II - adquirir e gerenciar os certificados digitais para usuárias e usuários;
- III - implementar e manter infraestrutura de chaves públicas interna;
- IV - adquirir e gerenciar os certificados digitais para servidores e aplicações;
- V - informar à Comissão de Segurança da Informação (CSI) eventuais não-conformidades.

Art. 15 Cabe à usuária e ao usuário:

- I - zelar pela segurança do certificado digital recebido, não compartilhando o seu uso e a sua senha com terceiros;
- II - assinar termo de compromisso no ato do recebimento de certificado digital;
- III - informar imediatamente à STI em caso de extravio ou comprometimento do certificado digital para adoção das providências de revogação;
- IV - a usuária e o usuário devem estar cientes de que a assinatura ou login feitos por meio de certificado digital são irrevogáveis, não podendo alegar a não realização de uma ação.

CAPÍTULO VIII

DISPOSIÇÕES FINAIS

Art. 16 No caso de algum equipamento, aplicação, aplicativo, sistema ou banco de dados não permitir a adoção de protocolos seguros, a informação deverá constar em documento de análise de riscos de segurança da informação, sendo imediatamente submetido para apreciação da Comissão de Segurança da Informação (CSI).

Art. 17 Os casos omissos e eventuais dúvidas quanto à aplicação desta Portaria serão dirimidos pela Comissão de Segurança da Informação do Tribunal Regional Eleitoral de São Paulo.

Art. 18 A STI elaborará, em até 120 dias, os procedimentos operacionais para aplicação desta Portaria que levem em conta as boas práticas de cibersegurança e os recursos tecnológicos disponíveis.

Art. 19 A STI deverá informar à Gestora ou ao Gestor de Segurança da Informação, no prazo de 120 dias, quais ativos de informação não puderam se adequar a esta Portaria.

Art. 20 Esta Portaria deverá ser revisada a cada 12 meses pela Gestora ou pelo Gestor de Segurança da Informação e encaminhada para nova apreciação da Comissão de Segurança da Informação (CSI).

Art. 21 O descumprimento não fundamentado desta Portaria deve ser comunicado e registrado como incidente de segurança da informação pela Gestora ou pelo Gestor de Segurança da Informação e será objeto de apuração pela unidade competente do Tribunal com consequente aplicação das penalidades cabíveis a cada caso.

Art. 22 Esta Portaria entra em vigor na data de sua publicação e sua implementação iniciará imediatamente e deverá estar totalmente implantada no prazo de 12 (doze) meses a contar desta data.

Claudio Cristiano Abreu Corrêa
Diretor-Geral

PORTARIA TRE-SP N. 229/2023

PORTARIA TRE-SP N. 229/2023

Dispõe sobre a instituição de Segurança de TIC para serviços em nuvem, relativa à Política de Segurança da Informação do Tribunal Regional Eleitoral do Estado de São Paulo, TRE-SP.

O DIRETOR-GERAL DA SECRETARIA DO TRIBUNAL REGIONAL ELEITORAL DO ESTADO DE SÃO PAULO, no uso de suas atribuições legais e regulamentares, conforme delegação de competência estabelecida no artigo 2º, inciso I, da Portaria TRE-SP n. 1/2022;

CONSIDERANDO a necessidade de definir processos de Segurança de TIC para serviços em nuvem no âmbito do Tribunal Regional Eleitoral de São Paulo;

CONSIDERANDO a necessidade de apoiar os processos de continuidade de serviços de TI, em caso de eventos de causas naturais, acidentais, tecnológicas ou humanas;

CONSIDERANDO a necessidade de apoiar a gestão do processo de tratamento e resposta a incidentes em redes computacionais no Tribunal Regional Eleitoral de São Paulo;

CONSIDERANDO a Res. CNJ 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

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

CONSIDERANDO a Portaria DG/TSE 444/2021, que dispõe sobre a instituição da norma de termos e definições relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral;

CONSIDERANDO a Res. TRE/SP 580/2022, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral de São Paulo;

CONSIDERANDO as boas práticas em segurança da informação e privacidade previstas nas normas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002, complementadas pela norma ABNT NBR ISO/IEC 27701;

CONSIDERANDO as boas práticas na gestão da continuidade de negócios previstas nas normas ABNT NBR ISO/IEC 22301 e 22313;

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