DISPOSIÇÕES FINAIS

Art. 8o 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. 9o 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. 10 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. 11 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. 12 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.

Claucio Cristiano Abreu Corrêa

Diretor-Geral

PORTARIA TRE-SP N. 216/2023

PORTARIA TRE-SP N. 216/2023

Dispõe sobre a instituição de Gestão de Identidade e Controle de Acesso Lógico 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 Gestão de Identidade e Controle de Acesso Lógico 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 de 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;
CONSIDERANDO que o acesso à informação, assim como aos recursos de processamento das informações e aos processos de negócios, deve ser controlado com base nos requisitos de negócio e da segurança da informação;
CONSIDERANDO a NC 07/IN01/DSIC/GSIPR, de 15 de julho de 2014, que estabeleceu diretrizes para implantação de controles de acesso relativos à segurança da informação e das comunicações na Administração Pública Federal;
CONSIDERANDO, ainda, as recomendações do Acórdão 1.603/2008-TCU, item 9.1.3, sobre a importância dos controles de acesso;
RESOLVE:
CAPÍTULO I
DAS DISPOSIÇÕES GERAIS
Art. 1º Fica instituída a Gestão de Identidade e Controle de Acesso Lógico, em consonância com a Política de Segurança da Informação (PSI) do Tribunal Regional Eleitoral de São Paulo.
Art. 2º Esta Portaria integra a Política de Segurança da Informação da Justiça Eleitoral de São Paulo, estabelecida pela Resolução TRE/SP 580/2022.
CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES
Art. 3º Para efeitos desta Portaria, consideram-se os termos e definições previstos na Portaria DG /TSE n. 444/2021, aplicando-se, de forma subsidiária, aqueles estabelecidos no Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República.
CAPÍTULO III
DOS PRINCÍPIOS
Art. 4º O controle de acesso lógico é regido pelos seguintes princípios:
I. necessidade de saber: as usuárias e os usuários deverão ter acesso somente às informações necessárias ao desempenho de suas tarefas;
II. necessidade de uso: as usuárias e os usuários deverão ter acesso apenas aos ativos (equipamentos de TI, sistemas, aplicações, procedimentos) necessários ao desempenho de suas atribuições;
III. privilégio mínimo: deverão ser conferidos apenas os privilégios necessários para que as usuárias e os usuários realizem suas atribuições;
IV. segregação de funções: consiste na separação das funções desempenhadas no controle de acesso, por exemplo, pedido de acesso, autorização de acesso e administração de acesso.
CAPÍTULO IV
DO ESCOPO E DO ÂMBITO DE APLICAÇÃO
Art. 5º O objetivo desta Portaria de Gestão de Identidade e Controle de Acesso Lógico relativos à segurança da informação e comunicação consiste em estabelecer diretrizes para implantação de controles de acesso lógico.
CAPÍTULO V
DO CONTROLE DE ACESSO FÍSICO À REDE
Art. 6º O cabeamento de energia elétrica e de telecomunicações que transporta dados ou fornece suporte aos serviços de informações deve ser protegido contra interceptação, interferência ou danos, conforme as seguintes diretrizes:
I. as linhas de energia elétrica e de telecomunicações que entram nas instalações de processamento da informação devem ser subterrâneas ou ficar abaixo do piso, sempre que possível, e devem atender aos requisitos mínimos de proteção;

II. os cabos de energia elétrica devem ser segregados dos cabos de comunicação, para evitar interferências;
III. os pontos de rede sem uso devem estar desabilitados nos patch panels.

CAPÍTULO VI

DO CONTROLE DE ACESSO LÓGICO

SEÇÃO I

DO GERENCIAMENTO DE ACESSO LÓGICO

Art. 7º O acesso aos sistemas de informação será assegurado, unicamente, à usuária e ao usuário devidamente identificado e autorizado.

§ 1º As gestoras e os gestores dos ativos devem determinar regras apropriadas de controle de acesso, direitos de acesso e restrições para papéis específicos das usuárias e dos usuários terem acesso aos ativos, com nível de detalhe e rigor de controle que reflitam os riscos de segurança da informação associados, observada a consistência entre os direitos de acesso e as políticas de classificação da informação.

§ 2º As regras de controle de acesso deverão ser baseadas na premissa de que "tudo é proibido a menos que expressamente permitido", em lugar da regra "tudo é permitido, a menos que expressamente proibido".

Art. 8º A concessão e a revogação de acesso serão implementadas por meio de um processo formal, preferencialmente automatizado, com estabelecimento de responsáveis pela solicitação, administração, concessão, bloqueio e revogação.

§ 1º Compete às proprietárias e aos proprietários de todos os tipos de ativos estabelecer regras de concessão, bloqueio e revogação de acesso aos ativos para as usuárias e os usuários, levando em conta as políticas, princípios e normas de controle de acesso aplicáveis.

§ 2º Os acessos deverão ser retirados imediatamente após a revogação dos direitos ou o encerramento das atividades, contratos ou acordos, ou ajustados após qualquer mudança de atribuições.

§ 3º As contas de acesso deverão ser desabilitadas/bloqueadas, em vez de excluídas, para preservação de trilhas de auditoria.

Art. 9º. A criação de nomes de usuária e usuário e de contas de e-mail seguirá critério padronizado.

Art. 10. O modelo de controle de acesso será, preferencialmente, fundamentado no controle de acesso baseado em papéis (RBAC).

Art. 11. Deverá ser estabelecido e mantido atualizado um inventário de todas as contas gerenciadas, contendo data de início e término, incluindo:

I. contas de usuária e usuário e de administradora e administrador;
II. contas de serviço e de departamento.

§ 1º O inventário das contas de usuária e usuário e de administradora e administrador deverá conter, no mínimo, o nome da pessoa, o nome de usuária ou usuário e a sua unidade de lotação, enquanto o das contas de serviço indicará ao menos a unidade gestora, as datas de revisão e o propósito.

§ 2º As contas deverão ser revisadas mensalmente, no último dia útil do mês, pela unidade responsável, para avaliar se as contas ativas permanecem autorizadas.

Art. 12. A Secretaria de Tecnologia da Informação deverá manter inventário dos sistemas de autenticação do Tribunal, abrangendo os internos e aqueles hospedados em provedores remotos.

SEÇÃO II

DO ACESSO ÀS REDES, SISTEMAS INTERNOS E SERVIÇOS DE REDE

Art. 13. A gestão de contas internas e o controle de acesso se darão de forma centralizada, por meio de serviço de diretório.

Art. 14. As operações de criação de usuárias e usuários da rede local serão solicitadas por meio de instrumento específico, observada a segregação de funções em todo o fluxo do gerenciamento de acesso, pelos seguintes agentes:

I. Secretaria de Gestão de Pessoas, chefia imediata da unidade de lotação da usuária ou do usuário ou ainda coordenadoria, secretaria ou assessoria a qual a unidade pertence, no caso de magistradas e magistrados, servidoras e servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo e estagiárias e estagiários;

II. Chefia imediata da unidade de lotação da usuária ou do usuário, no caso de colaboradoras e colaboradores e prestadoras e prestadores de serviços.

Parágrafo único. Nos demais casos, será necessária a aprovação da Comissão de Segurança da Informação.

Art. 15. A atribuição de permissões padronizadas da unidade de lotação da servidora ou do servidor se dará automaticamente após cadastro no SGRH, pela unidade responsável da Secretaria de Gestão de Pessoas.

§ 1º O perfil de acesso da usuária ou do usuário aos sistemas ou serviços de informação necessários à execução das atividades do departamento deverá ser providenciado pela chefia imediata por meio de sistema próprio e deverá ser mantido restrito ao desempenho de suas atividades.

§ 2º As gestoras ou os gestores do ativo de informação serão responsáveis pela autorização do direito de acesso, que poderá ser operacionalizado por equipe técnica designada.

§ 3º Na análise da solicitação de acesso, a gestora ou o gestor do ativo deverá considerar também a consistência entre a classificação da informação e os direitos de acesso, bem como as normas e legislação vigentes.

§ 4º Estas autorizações devem estar documentadas, para fins de auditoria e levantamento periódico, visando à detecção de usuárias e usuários com acesso indevido.

§ 5º Deverá ser estabelecido um perfil padrão para usuárias e usuários, ao qual todos retornarão em caso de mudança de lotação ou qualquer outro motivo que leve à suspensão de suas atividades, antes que sejam solicitados novos perfis de acesso pela nova chefia.

§ 6º A lotação de uma usuária ou um usuário em uma unidade permite acesso à área específica de armazenamento de arquivos da unidade, bem como o recebimento de mensagens para o e-mail da mesma.

§ 7º Caso existam mensagens ou arquivos para os quais nem todos tenham acesso, deve-se criar grupo de distribuição de mensagens ou de permissão de acesso distinto do padrão da unidade.

§ 8º O procedimento de atribuição de acesso não deve permitir que a permissão seja efetivada antes que a autorização formal seja finalizada.

§ 9º A chefia imediata da unidade de lotação anterior da usuária ou do usuário deverá solicitar a remoção de atribuição de direitos de acesso e perfis dos sistemas utilizados na lotação, por meio do sistema de service desk da Secretaria de Tecnologia da Informação, imediatamente após a alteração de lotação da usuária ou do usuário.

Art. 16. As usuárias e os usuários devem possuir identificação única e exclusiva para permitir relacioná-los às suas ações e responsabilidades.

Parágrafo único. O uso compartilhado de identificação de usuárias e usuários somente será permitido por razões operacionais, mediante procedimento de atribuição de responsabilidades compartilhado pelas chefias imediatas e autorização da Comissão de Segurança da Informação.

Art. 17. Compete à chefia imediata informar às gestoras e aos gestores do ativo a movimentação e o desligamento de qualquer usuária ou usuário alocado em sua unidade, dadas as implicações na manutenção de direitos de acesso aos ativos de informação, caso essa movimentação e desligamento não sejam realizados automaticamente via sistema.

§ 1º A retirada da usuária ou do usuário dos acessos citados no § 9º do art. 15 somente se dará após a mudança de lotação ou desligamento efetuado no sistema de gestão de recursos humanos.
§ 2º Periodicamente, a área de Tecnologia da Informação fará o bloqueio automático das credenciais de acesso das usuárias e dos usuários que não realizaram o acesso por mais de 45 (quarenta e cinco) dias consecutivos, incluídos as servidoras e os servidores aposentados, cedidos e licenciados.
Art. 18. Os direitos de acesso das usuárias e dos usuários devem ser revistos mensalmente, bem como após qualquer mudança de nível institucional que implique realocação de pessoas, unidades ou papéis.
Art. 19. As atividades de gerenciamento de identidades, acesso e autenticação devem ser registradas e arquivadas.
Parágrafo único. Deverão ser emitidos, com frequência mínima mensal, relatórios críticos com finalidade de identificar inconsistências nestas atividades, atentando-se às recomendações anteriores bem como para as seguintes:
I. identificação de usuárias e usuários redundantes;
II. identificação de solicitações de acesso sem segregação de funções.
Art. 20. Devem ser incluídas cláusulas nos contratos de prestadoras e prestadores de serviço elencando sanções nos casos de acessos não autorizados, ou mesmo tentativas, efetuados por pessoa ou agente, mediante ações diretas ou indiretas de suas colaboradoras e de seus colaboradores, mediante documento padrão apresentado pela STI, anexo ao contrato.
Art. 21. Compete à gestora ou ao gestor de ativo realizar a revisão de direitos de acesso ao ativo sob sua responsabilidade, podendo a Secretaria de Tecnologia da Informação automatizar o processo de retirada de acessos e alteração de perfil para usuárias e usuários, nos casos previstos nos arts. 22 e 23, conforme as regras estabelecidas formalmente.
SEÇÃO III
DO ACESSO PRIVILEGIADO
Art. 22. O acesso privilegiado aos sistemas e ativos de informação somente será concedido às usuárias e aos usuários que tenham como atribuição funcional o dever de administrá-los.
§ 1º O acesso privilegiado deve ser concedido à usuária e ao usuário por meio de credenciais de acesso exclusivas para este fim, distintas das credenciais de acesso concedidas a tal usuária ou usuário para a realização de suas atividades normais de negócio.
§ 2º O procedimento de concessão de acesso privilegiado deve manter arquivo de registro contendo informações sobre este pedido para posterior auditoria.
§ 3º As gestoras ou os gestores do ativo de informação devem definir prazos de expiração para as credenciais de acesso privilegiado, após os quais deve ser reavaliado o atendimento aos critérios para a atribuição de acesso privilegiado ao detentor das credenciais expiradas.
§ 4º A solicitação de acesso privilegiado para qualquer unidade que não seja gestora do ativo deverá ser encaminhada através de processo administrativo à gestora ou ao gestor do ativo para análise e, após, à Comissão de Segurança da Informação para deliberação.
Art. 23. As competências das usuárias e dos usuários com acesso privilegiado aos sistemas e ativos de informação deverão ser avaliadas em intervalos não superiores a um mês, para que estejam alinhadas às atividades e obedecendo as regras de segregação de funções.
Art. 24. O acesso privilegiado aos sistemas e ativos de informação através do uso de ID de usuária administradora ou usuário administrador genérico deve ser evitado, se o sistema assim permitir e, quando não houver esta possibilidade, deve ser concedido mediante procedimentos de troca periódica de senha e auditoria dos acessos, criados pela gestora ou pelo gestor do ativo.
§ 1º Após a saída ou mudança de lotação de usuária ou usuário com conhecimento de senha de usuária ou usuário administrador genérico, esta deve ser modificada imediatamente.

§ 2º A conta de administradora ou administrador genérico deve ser renomeada e ter sua função apagada, para que não possa ser facilmente identificada.

§ 3º A conta de administradora ou administrador genérico não deve ser usada para acesso à Internet, iniciar serviços de rede e acessar arquivos externos.

SEÇÃO IV

DA POLÍTICA DE SENHAS

Art. 25. Os sistemas ou serviços de informação, considerados passíveis de controle de acesso pela gestora ou pelo gestor de ativo, devem ter seu acesso restrito e controlado através do uso de senhas, token ou mecanismo de autenticação similar.

§ 1º Serão concedidas senhas temporárias, mediante concordância e assinatura de termo de confidencialidade de toda senha, ou outro mecanismo de autenticação que estiver em sua posse.

§ 2º O acesso remoto à rede, o acesso administrativo e o acesso a aplicações expostas externamente se darão por autenticação multifatorial (MFA).

§ 3º A Secretaria de Tecnologia da Informação, em conjunto com a gestora ou o gestor do ativo de informação, podem implantar a autenticação de multifatores para determinados tipos de acesso, em função de sua criticidade.

Art. 26. A senha de acesso da usuária ou do usuário, tokens, e outros fatores de autenticação devem ser de uso pessoal e intransferível.

Art. 27. As senhas devem ser secretas e definidas considerando as seguintes recomendações:

I. utilizar números, letras, alternando-as entre maiúsculas, minúsculas e caracteres especiais, como, por exemplo, $@#&%, com, no mínimo, 12 (doze) caracteres para contas com autenticação de multifatores e 14 (quatorze) para as demais;

II. não utilizar frases ou palavras que possam ser facilmente adivinhadas por terceiros, baseadas nas informações relativas à própria usuária ou ao próprio usuário, tais como nome de parentes, datas de aniversário e números de telefone. Evitar palavras contidas em dicionários de quaisquer idiomas;

III. não utilizar senhas formadas por sequência de caracteres, tais como 123456 ou abcde, ou senhas simples que repitam a identificação da usuária ou do usuário como, por exemplo, usuário joao.silva e senha joao.silva, ou ainda caracteres idênticos repetidos;

IV. modificar a senha temporária no primeiro logon;

V. não expor a senha em local visível para terceiras e terceiros, como anotações em papéis, sob pena de responsabilização pelos acessos indevidos.

Art. 28. Não utilizar as mesmas credenciais (nome de usuária ou usuário e senha) para fins pessoais (em serviços externos ao ambiente de TI da Justiça Eleitoral) e profissionais.

Art. 29. Sempre que houver indicação de possível comprometimento da senha, a usuária ou o usuário deve realizar sua alteração, bem como comunicar a ocorrência ou a suspeita de comprometimento ao service desk da Secretaria de Tecnologia da Informação.

Art. 30. O sistema de gerenciamento de senha deve:

I. permitir que as usuárias e os usuários selecionem e modifiquem suas próprias senhas, incluindo um procedimento de confirmação para evitar erros;

II. forçar as mudanças de senha a intervalos regulares de, no máximo, 3 (três) meses para contas comuns e mensal para contas administrativas;

III. manter um registro das últimas 5 senhas anteriores utilizadas e bloquear a reutilização;

IV. empregar criptografia no canal de comunicação utilizado para o tráfego de credenciais de acesso;

V. criptografar ou embaralhar (hash) com salt as credenciais de autenticação armazenadas;

VI. não mostrar as senhas na tela quando forem digitadas;

VII. garantir a alteração das senhas temporárias no primeiro acesso ao sistema ou serviço de informação;
VIII. manter, para fins de auditoria, registro dos acessos, das operações e dos respectivos períodos;
IX. desabilitar as contas que não possam ser associadas a uma usuária ou a um usuário ou processo de negócio;
X. monitorar tentativas de acesso a contas desativadas.
Art. 31. A senha temporária, para primeiro acesso ou no caso de a usuária ou o usuário esquecer a sua senha, deverá ser emitida através de procedimento instruído pela unidade técnica de Segurança da Informação e aprovado pela Comissão de Segurança da Informação, no qual deverá informar dados pessoais para comprovação de identidade.
Parágrafo único. Fica vedada a emissão de senha para ciência de terceiras e terceiros, ainda que chefes imediatos ou superiores da usuária ou do usuário, bem como o seu envio através de texto claro ou correio de terceiro.
SEÇÃO V
DOS PROCEDIMENTOS SEGUROS DE ENTRADA NO SISTEMA
Art. 32. O procedimento adequado de entrada no sistema (login) deve atender às seguintes recomendações:
I. não fornecer mensagens de ajuda ou informações do sistema durante o procedimento de entrada que possam auxiliar uma usuária ou um usuário não autorizado;
II. validar informações de entrada no sistema somente após todos os dados estarem completamente preenchidos;
III. no caso de erro, não indicar qual parte do dado de entrada está correta ou incorreta;
IV. bloquear o acesso da usuária ou do usuário ao sistema após, no máximo, 3 (três) tentativas de entrada no sistema;
V. registrar tentativas de acesso ao sistema, sem sucesso e bem-sucedidas;
VI. por ocasião da entrada no sistema, mostrar as seguintes informações:
a. data e hora da última entrada no sistema ou equipamento, com sucesso;
b. detalhes (data, hora e IP da máquina) de qualquer tentativa sem sucesso de entrada no sistema desde o último acesso com sucesso.
VII. encerrar sessões inativas após um período definido de inatividade de, no máximo, 10 (dez) minutos, sendo emitida mensagem de aviso à usuária e ao usuário antes do encerramento;
VIII. em caso de uso externo, deve restringir o tempo de conexão para reduzir oportunidade de acesso não autorizado.
SEÇÃO VI
DO ACESSO DOS EQUIPAMENTOS À REDE E AOS SERVIÇOS DE REDE
Art. 33. Os dispositivos e serviços de rede, bem como as demais aplicações do Tribunal devem ser configurados mediante regra "tudo é proibido a não ser que expressamente permitido".
Art. 34. O acesso de novo equipamento à rede é regulamentado pelo procedimento de autorização específico e deverá ser executado através da abertura de chamado de requisição de serviço em sistema de service desk.
Art. 35. São consideradas redes do Tribunal Regional Eleitoral de São Paulo, para efeito de controle, a rede cabeada da sede e seus anexos, todas as redes wifi em suas dependências e por ele provida, o acesso VPN, o perímetro para a Internet e as redes das zonas eleitorais, pontos e postos de atendimento.
Art. 36. É vedada a inclusão de equipamentos pessoais ou de terceiros em qualquer uma das redes internas do TRE, sem autorização da Comissão de Segurança da Informação.
Art. 37. A inclusão de equipamentos de terceiras ou de terceiros na rede será efetuada em sub rede segura, distinta das demais e por período definido.

Art. 38. O horário de funcionamento da VPN e do acesso à INTERNET será regulamentado em portaria interna e qualquer alteração excepcional deverá ser solicitada à Comissão de Segurança da Informação.
Art. 39. A inclusão de equipamentos e usuárias e usuários na VPN será solicitada através de sistema service desk, em formulário específico.
Art. 40. Os acessos à rede devem ser registrados, arquivados por um período mínimo de 6 meses, monitorados e mensalmente deve ser emitido relatório crítico com finalidade de identificar acessos indevidos.
Art. 41. Será exigido múltiplo fator de autenticação nas máquinas que acessarem a VPN do Tribunal Regional Eleitoral de São Paulo.
Art. 42. Os serviços de rede que não estejam em uso devem ser removidos e não apenas desabilitados.
Art. 43. As portas que não estiverem em uso nos equipamentos de rede deverão ser desativadas logicamente e desassociadas de qualquer VLAN.
Art. 44. Deverá ser implementado sistema de controle de acesso à rede que identifique a usuária e o usuário e estabeleça sua conexão e permissões conforme o perfil de acesso.
SEÇÃO VII
DO CONTROLE DE ACESSO AO CÓDIGO-FONTE DE PROGRAMAS
Art. 45. O código-fonte e itens associados (esquemas, especificações, planos de validação, etc) dos sistemas de informação desenvolvidos pelo Tribunal somente serão acessíveis pelas usuárias e pelos usuários que tenham como atribuição funcional seu desenvolvimento, manutenção ou outra atividade para a qual o acesso seja imprescindível.
§ 1º As bibliotecas de código-fonte e itens associados devem ser armazenadas em ferramentas apropriadas para este fim, em ambientes segregados dos sistemas operacionais onde os respectivos sistemas de informação sejam executados.
§ 2º Os eventos de acesso às bibliotecas de código-fonte e itens associados devem ser registrados, permitindo sua auditoria.
§ 3º Os códigos-fonte que sejam publicados para entidades externas devem contar com controles adicionais que garantam sua integridade.
§ 4º O disposto nesse artigo também se aplica à código-fonte armazenado em Sistemas de Gerenciamento de Bancos de Dados tais como códigos de Stored Procedures, Functions, Triggers, etc.
CAPÍTULO VII
DISPOSIÇÕES FINAIS
Art. 46. 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. 47. 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. 48. 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. 49. 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. 50. Esta Portaria entra em vigor na data de sua publicação, sua implementação iniciará imediatamente e deverá estar totalmente implantada no prazo de 12 (doze) meses a contar desta data.

Claucio Cristiano Abreu Corrêa

Diretor-Geral

PORTARIA TRE-SP N. 221/2023

PORTARIA TRE-SP N. 221/2023

Dispõe sobre a instituição da Gestão de Incidentes de Segurança da Informação 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 Gestão de Incidentes de Segurança da Informação 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 gestão de incidentes de segurança da informação previstas nas normas ABNT NBR ISO/IEC 27035;

CONSIDERANDO as boas práticas de resposta à incidentes previstas no guia NIST SP-800-61;

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 instituída Portaria para gestão de incidentes de segurança da informação, em consonância com a Política de Segurança da Informação (PSI) do Tribunal Regional Eleitoral de São Paulo.