INSTRUÇÃO NORMATIVA Nº 62, DE 26 DE NOVEMBRO DE 2021

Estabelece normas gerais para garantir o gerenciamento das operações e comunicações dos recursos de processamento da informação e a proteção de dados pessoais na 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 a Portaria nº 682, de 23 de setembro de 2021, deste Tribunal, que define as Unidades Gestoras de Sistema e de Solução de Tecnologia da Informação e Comunicação,

RESOLVE:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Instrução Normativa estabelece normas gerais para garantir o gerenciamento das operações e comunicações dos recursos de processamento da informação e a proteção de dados pessoais da Justiça Eleitoral de Pernambuco.

Art. 2º As diretrizes estabelecidas nesta Instrução Normativa visam a:

I - garantir a operação segura e correta dos recursos de processamento da informação;

II - implementar e manter o nível apropriado de segurança da informação e de entrega de serviços;

III - minimizar o risco de falhas nos sistemas de informação;

IV - proteger a integridade do software e da informação;

V - manter a integridade e disponibilidade da informação e dos recursos de processamento de informação;

VI - garantir a proteção das informações em redes e da infraestrutura de suporte;

VII - prevenir contra a divulgação não autorizada, a modificação, a remoção ou a destruição dos ativos, e contra as interrupções das atividades do negócio;

VIII - manter a segurança na troca de informações e softwares internamente, entre as unidades do Tribunal, e com quaisquer entidades externas;

IX - garantir a segurança de serviços oferecidos via internet e intranet, e a sua utilização segura; e

X - detectar atividades de processamento da informação não autorizadas.

Art. 3º Quando a operação envolver tratamento de dados pessoais, deve ser observado o conceito de "privacidade desde a concepção", de acordo com os seguintes princípios:

I - abordagem proativa, visando a antecipar e evitar eventos invasivos de privacidade;

II - privacidade por padrão, ou seja, garantia de que os dados pessoais serão protegidos automaticamente;

III - privacidade incorporada ao projeto e arquitetura do sistema, considerado componente essencial e parte indissociável da solução desenvolvida;

IV - funcionalidade total, que representa o compromisso com a privacidade sem perda de funcionalidade do projeto;

V - segurança e proteção de ponta a ponta durante o ciclo de vida de tratamento dos dados;

VI - visibilidade e transparência para demonstrar o alinhamento do tratamento às premissas e aos objetivos declarados; e

VII - pela privacidade do(a) titular dos dados pessoais.

CAPÍTULO II

DOS PROCEDIMENTOS E RESPONSABILIDADES OPERACIONAIS

Art. 4º Os procedimentos de operação dos recursos de processamento da informação devem ser documentados e mantidos atualizados e disponíveis a todos(as) que deles necessitem.

Art. 5º A documentação dos procedimentos de operação deve conter, sempre que aplicável:

I - inicialização e desligamento de computadores;

II - geração de cópias de segurança (backup);

III - manutenção de equipamentos; e

IV - tratamento de mídias.

Art. 6º Os procedimentos de operação devem especificar as instruções para execução detalhada de cada tarefa, incluindo, sempre que aplicável:

I - processamento e tratamento da informação;

II - backup;

III - requisitos de agendamento, incluindo interdependência com outros sistemas;

IV - instruções para tratamento de erros ou outras condições excepcionais;

V - dados para contatos de suporte, no caso de eventos operacionais inesperados ou dificuldades técnicas;

VI - instruções especiais quanto ao manuseio e saída de mídias, com uso de formulários específicos;

VII - procedimentos para o reinício e recuperação do recurso de processamento da informação, em caso de falha; e

VIII - gerenciamento de trilhas de auditoria e informações de registros (logs) de sistemas.

Art. 7º As funções e áreas de responsabilidade devem ser segregadas para reduzir as oportunidades de modificação e uso indevido, não autorizado ou não intencional, dos ativos do Tribunal.

Art. 8º Os ambientes de desenvolvimento, teste e produção dos recursos de processamento da informação devem ser separados, para reduzir o risco de acessos ou modificações não autorizados aos sistemas operacionais.

Art. 9º Para a separação dos ambientes de desenvolvimento, teste e produção, devem ser considerados:

I - regras definidas e documentadas para a transferência de software da situação de desenvolvimento para a de produção;

II - compiladores, editores e outras ferramentas de desenvolvimento ou utilitários de sistemas não acessíveis a partir de sistemas operacionais;

III - ambientes de testes que simulem o ambiente de produção o mais próximo possível, resguardando a privacidade dos dados;

IV - usuários(as) com diferentes perfis para sistemas em testes e em produção, com a adequada informação, em cada sistema, sobre o ambiente ao qual o(a) usuário(a) está conectado(a);

V - sistemas com exibição de mensagens apropriadas de identificação para reduzir riscos de erro; e

VI - anonimização dos dados sensíveis do ambiente de produção, copiados para os ambientes de teste, exceto nos casos onde haja autorização expressa e justificada do representante da unidade gestora ou da comissão gestora do sistema ou da solução de tecnologia da informação e comunicação (TIC) para o seu uso na íntegra.

CAPÍTULO III

DA GESTÃO DE MUDANÇAS

Art. 10. As modificações nos recursos de processamento da informação e sistemas devem observar o disposto no processo de gestão de mudanças de tecnologia da informação e comunicação.

Art. 11. O processo de gestão de mudanças de TIC deve considerar, no mínimo:

I - a identificação e o registro das mudanças significativas;

II - o planejamento e os testes das mudanças;

III - a avaliação de impactos potenciais, incluindo impactos de segurança;

IV - o procedimento formal de aprovação das mudanças propostas;

V - a comunicação dos detalhes das mudanças para todas as pessoas envolvidas; e

VI - os procedimentos de recuperação dos recursos de processamento da informação, incluindo procedimentos e responsabilidades pela interrupção e recuperação de mudanças, em caso de insucesso ou na ocorrência de eventos inesperados.

Art. 12. O controle de gestão de cada mudança de TIC deve ser conduzido pela área solicitante da mudança.

CAPÍTULO IV

DO GERENCIAMENTO DE SERVIÇOS TERCEIRIZADOS

Art. 13. A contratação de serviços terceirizados relacionados às operações e comunicações dos recursos de processamento da informação deve prever e manter um nível apropriado de segurança da informação e de entrega de serviços em consonância com os acordos estabelecidos.

Art. 14. Para a entrega dos serviços terceirizados, referidos no caput deste artigo, devem ser previstos:

I - os controles de segurança, as definições de serviço e os níveis de entrega; e

II - os mecanismos de manutenção da capacidade da entrega, descritos nos planos de operação, que visem a garantir a continuidade dos níveis de serviço acordados.

Art. 15. Devem ser estabelecidos procedimentos de monitoramento e análise crítica dos serviços entregues.

Art. 16. As mudanças relacionadas a serviços terceirizados devem observar o disposto no processo de gestão de mudanças de TIC, a criticidade dos sistemas e processos de negócio envolvidos e a avaliação de riscos.

CAPÍTULO V

DO PLANEJAMENTO E ACEITAÇÃO DOS SISTEMAS

Art. 17. Para reduzir os riscos de falhas na execução dos sistemas informatizados, a STIC deve adotar os seguintes procedimentos:

I - monitoramento e ajuste da utilização dos recursos, com projeções para garantir a disponibilidade adequada e a capacidade de desempenho futura dos sistemas;

II - identificação de requisitos de capacidade para cada funcionalidade, nova ou em andamento;

III - monitoramento do desempenho e aplicação de ajustes para melhorar a disponibilidade e a eficiência dos sistemas;

IV - implantação de controles de detecção antecipada de problemas, sempre que possível; e

V - identificação e prevenção contra potenciais gargalos de desempenho e a dependência de pessoas-chave que possam representar ameaças à segurança dos sistemas ou aos serviços, bem como orientação para o planejamento da ação corretiva apropriada.

Art. 18. Para a aceitação de novos sistemas, inclusive os sistemas operacionais, suas atualizações e novas versões, devem ser preenchidos os seguintes requisitos, quando aplicáveis:

I - a realização de testes, inclusive na fase de desenvolvimento;

II - a definição de requisitos de:

a) desempenho e de capacidade computacional; e

b) continuidade do negócio;
III - a recuperação de erros, procedimentos de reinicialização e planos de contingência;
IV - a preparação e o teste de procedimentos operacionais de rotina;
V - a concordância do(a) titular(a) da unidade de negócio acerca do conjunto de controles de segurança utilizados;
VI - a definição de procedimentos manuais eficazes;
VII - a análise e o registro de que a instalação de novo sistema não afetará de forma adversa os sistemas existentes, particularmente, nos períodos de pico de processamento;
VIII - a evidência de que tenha sido considerado o impacto do novo sistema na segurança da informação;
IX - o treinamento na operação ou no uso de novos sistemas; e
X - a facilidade de uso, uma vez que afeta o desempenho do(a) usuário(a) e evita falhas humanas.

CAPÍTULO VI

DA PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS E CÓDIGOS MÓVEIS

Art. 19. Devem ser implantados controles de detecção, prevenção e recuperação de recursos de processamento da informação para protegê-los contra códigos maliciosos, assim como procedimentos para a devida conscientização dos(as) usuários(as), que contemplem, no mínimo:
I - a proibição de uso de softwares não autorizados pela área de TIC;
II - as análises críticas regulares dos softwares e dados dos sistemas que suportem processos críticos (essenciais) de negócio;
III - a investigação formal quando identificada a presença de quaisquer arquivos não aprovados ou de atualização não autorizada;
IV - a instalação e a atualização regulares de softwares de detecção e remoção de códigos maliciosos para o exame de computadores e mídias digitais, de forma preventiva e rotineira; e
V - a coleta de dados sobre segurança da informação, utilizando recursos tais como assinaturas de listas de discussão, participação em grupos de whatsapp, telegram ou outra rede social utilizada pela Justiça Eleitoral, bem como consultas a sítios e fóruns informativos sobre novos códigos maliciosos.

Art. 20. Onde o uso de códigos móveis for autorizado, a sua configuração deve garantir que ele opere de acordo com a política de segurança da informação do Tribunal e com observância dos requisitos a seguir:
I - a execução em ambientes isolados logicamente;
II - a ativação de medidas técnicas para garantir que o código móvel esteja sendo administrado;
III - o controle dos recursos disponíveis para acesso ao código móvel; e
IV - os controles criptográficos de autenticação exclusiva do código móvel, quando possível.

Art. 21. O uso de códigos móveis não autorizados deve ter a sua execução impedida.

CAPÍTULO VII

DAS CÓPIAS DE SEGURANÇA

Art. 22. Devem ser realizadas cópias de segurança, visando a manter a integridade e disponibilidade da informação e dos recursos de processamento de informação.

Art. 23. As cópias de segurança das informações e dos softwares devem ser efetuadas e testadas regularmente, conforme a política de geração de cópias de segurança definida pelo Tribunal.

Art. 24. Para a realização das cópias de segurança, devem ser considerados:
I - a produção de registros completos e exatos das cópias de segurança;
II - a documentação apropriada dos procedimentos de restauração;
III - a definição do nível necessário das cópias de segurança das informações;
IV - a extensão e frequência da geração das cópias de segurança em sintonia com os requisitos de negócio e a criticidade da informação, para a continuidade da operação do Tribunal;

V - o armazenamento das cópias de segurança em local distante o suficiente do local principal, para escapar dos danos de um eventual desastre que venha a ocorrer nas instalações principais;
VI - o nível apropriado de proteção física e ambiental das informações das cópias de segurança, conforme as regras aplicadas no local principal;
VII - a realização de testes regulares das mídias de cópias de segurança para garantir que são suficientemente confiáveis para seu uso em caso de emergência;
VIII - os controles aplicados às mídias no local principal devem ser também aplicados no local das cópias de segurança;
IX - a verificação e o teste regulares dos procedimentos de recuperação; e
X - a proteção das cópias de segurança por encriptação, quando tecnicamente possível, em situações de confidencialidade e quando solicitado formalmente à unidade responsável.

CAPÍTULO VIII

DO GERENCIAMENTO DA SEGURANÇA EM REDES

Art. 25. Redes computacionais devem ser adequadamente gerenciadas e controladas, de forma a serem protegidas contra ameaças e a ser mantida a segurança de sistemas e aplicações que as utilizem e da informação em trânsito.
Art. 26. Devem ser definidos níveis de serviço e requisitos de gerenciamento das operações e comunicações dos recursos de processamento da informação, tanto para serviços de rede providos internamente ou terceirizados.
Art. 27. Os serviços de rede incluem o fornecimento de conexões, serviços de rede privados, redes de valor agregado e soluções de segurança de rede, gerenciadas como firewalls e sistemas de detecção de intrusos, entre outros.

CAPÍTULO IX

DO MANUSEIO DE MÍDIAS REMOVÍVEIS

Art. 28. Devem ser definidos e implementados procedimentos para o gerenciamento de mídias removíveis.
Parágrafo único. São consideradas mídias removíveis fitas, discos, flash disks, discos removíveis, cartões de memória, CD, DVD e mídia impressa.
Art. 29. Para prevenir contra a divulgação não autorizada, modificação, remoção ou destruição de mídia removível, devem ser adotadas as seguintes diretrizes:
I - o conteúdo de qualquer meio digital reutilizável deve ser destruído, caso a mídia venha a ser descartada pelo Tribunal;
II - a remoção de qualquer mídia do Tribunal deve ser requerida formalmente à chefia imediata;
III - as mídias devem ser guardadas de forma segura, em um ambiente protegido, de acordo com as especificações do fabricante;
IV - as informações armazenadas em mídias removíveis que precisem estar disponíveis por muito tempo, devem ser armazenadas, de forma redundante, em outro local, para evitar a sua perda;
V - as unidades de mídias removíveis devem ser habilitadas somente se houver uma necessidade do negócio;
VI - as mídias removíveis, quando não forem mais necessárias, devem ser descartadas de forma segura e por meio de procedimentos formais; e
VII - o descarte seguro de mídias removíveis, que contenham informações sensíveis, deve ser realizado de forma a impossibilitar o acesso aos dados nelas contidos.

CAPÍTULO X

DA TROCA DE INFORMAÇÕES

Art. 30. Políticas, procedimentos e controles devem ser estabelecidos e formalizados para proteger a troca de informações em todos os tipos de recursos de comunicação, de acordo com as seguintes diretrizes:

I - a adoção de procedimentos para proteger:
a) a informação em trânsito contra interceptação, cópia, modificação, desvio e destruição;
b) as informações eletrônicas sensíveis que sejam transmitidas na forma de anexos;
II - a adoção de precauções para evitar que:
a) informações críticas ou sensíveis sejam deixadas em equipamentos de impressão;
b) conversas telefônicas confidenciais sejam escutadas ou interceptadas;
III - o uso de:
a) procedimentos para detecção e proteção contra código malicioso que possa ser transmitido através do uso eletrônico de comunicação;
b) técnicas de criptografia para proteger a confidencialidade, a integridade e a autenticidade das informações;
c) dispositivos móveis funcionais, exclusivamente para atendimento às necessidades do trabalho;
d) redes sociais em dispositivos ou de linhas telefônicas funcionais, exclusivamente para atendimento às necessidades do negócio; e
IV - a exclusão de mensagens, contendo informações sensíveis, veiculadas através de dispositivos móveis e redes sociais.
Art. 31. A troca de informações e softwares entre o Tribunal e entidades externas deve estar prevista em acordo específico e em conformidade com a legislação vigente.
Art. 32. As informações que trafeguem através de mensagens eletrônicas devem ser adequadamente protegidas contra acesso não autorizado, modificação ou negação do serviço.
§ 1º O(A) usuário(a) deve adotar todos os cuidados para o correto endereçamento da mensagem eletrônica.
§ 2º O serviço de mensagem eletrônica deve observar os princípios da confidencialidade, integridade e disponibilidade.
Art. 33. A troca de informações por meio da interconexão de sistemas de informações deve ser protegida por procedimentos e mecanismos de segurança.
CAPÍTULO XI
DAS TRANSAÇÕES VIA INTERNET/INTRANET
Art. 34. As informações envolvidas em transações on-line institucionais devem ser protegidas para prevenir:
I - transmissões incompletas;
II - erros de roteamento;
III - alterações e divulgação não autorizadas de mensagem; e
IV - duplicação ou reapresentação de mensagem não autorizada.
Art. 35. Para a realização de transações on-line, devem ser considerados, sempre que possível e /ou exigido:
I - o uso de assinaturas eletrônicas para transações on-line críticas; e
II - a garantia, para todos os aspectos da transação, de:
a) credenciais válidas e verificáveis;
b) confidencialidade;
c) integridade;
d) protocolos de comunicação seguros; e
e) armazenamento dos detalhes da transação em local não publicamente acessível.
Art. 36. A integridade das informações disponibilizadas em sistemas publicamente acessíveis deve ser protegida para prevenir modificações não autorizadas.
Art. 37. Os sistemas de publicação eletrônica, especialmente os que permitam realimentação e entrada direta de informação, devem ser cuidadosamente controlados, de forma que:

I - as informações sejam obtidas em conformidade com a legislação de proteção de dados pessoais;
II - as informações de entrada sejam processadas completa e corretamente em um tempo adequado;
III - as informações sensíveis sejam protegidas durante todo o ciclo do tratamento; e
IV - não haja acesso, intencional ou não, as redes às quais o sistema esteja conectado.

CAPÍTULO XII

DO MONITORAMENTO DO PROCESSAMENTO DA INFORMAÇÃO

Art. 38. Para detectar atividades não autorizadas de processamento da informação, deve haver registros (logs) de auditoria, contendo as atividades dos(as) usuários(as), as exceções e outros eventos de segurança da informação, produzidos e mantidos por um período de tempo acordado, para auxiliar em futuras investigações e monitoramento de controle de acesso.
Art. 39. Os registros (logs) de auditoria devem incluir, no mínimo:
I - a identificação do(a) usuário(a);
II - as datas, os horários e os detalhes de eventos-chave, tais como horário de entrada (log-on) e saída (log-off) no sistema;
III - a identidade do terminal ou, quando possível, a sua localização;
IV - os registros das tentativas de acesso ao sistema aceitas e rejeitadas;
V - os registros das tentativas de acesso a outros recursos e os dados aceitos e rejeitados;
VI - as alterações na configuração do sistema;
VII - o uso de privilégios;
VIII - o uso de aplicações e utilitários do sistema;
IX - os arquivos acessados e tipo de acesso;
X - os endereços e protocolos de rede;
XI - os alarmes provocados pelo sistema de controle de acesso; e
XII - a ativação e a desativação dos sistemas de proteção, tais como sistemas antivírus e sistemas de detecção de intrusos.
Parágrafo único. Quando o registro dos eventos listados neste artigo não puder ser realizado, deverá haver o mapeamento e a documentação quanto ao tipo e ao formato de registro de auditoria possíveis e armazenados.
Art. 40. Devem ser estabelecidos procedimentos para o monitoramento dos sistemas e redes de comunicação de dados, registrando-se, minimamente, os seguintes eventos de segurança:
I - a utilização de usuários(as), perfis e grupos privilegiados;
II - a inicialização, a suspensão e a reinicialização de serviços;
III - o acoplamento e o desacoplamento de dispositivos de hardware, com especial atenção para mídias removíveis;
IV - as modificações da lista de membros de grupos privilegiados;
V - as modificações de política de senhas, como tamanho, expiração, bloqueio automático, histórico, etc.; e
VI - o acesso ou a modificação de arquivos ou sistemas considerados críticos.
Parágrafo único. Os resultados das atividades de monitoramento devem ser analisados criticamente, de forma regular, a fim de identificar as oportunidades de melhoria.
Art. 41. Os recursos e informações de registros (logs) de auditoria devem ser protegidos contra falsificação e acesso não autorizado.
Art. 42. Os registros (logs) de falhas ocorridas devem ser armazenados e analisados para adoção de ações apropriadas.

Art. 43. Os relógios de todos os sistemas de processamento de informações relevantes, dentro do Tribunal ou do domínio de segurança, devem ser sincronizados de acordo com a hora oficial estabelecida pelos órgãos de controle.

CAPÍTULO XIII

DISPOSIÇÕES FINAIS

Art. 44. Os casos omissos e a avaliação de exceções a esta Instrução Normativa serão decididos pelo(a) Presidente.

Art. 45. Fica revogada a Instrução Normativa nº 15, de 30 de março de 2017.

Art. 46. Esta Instrução Normativa entra em vigor na data de sua publicação.

Recife, 26 de novembro de 2021.

CARLOS FREDERICO GONÇALVES DE MORAES

Presidente

PORTARIAS

PORTARIA Nº 843/2021

O DESEMBARGADOR PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DE PERNAMBUCO, no uso de suas atribuições legais e tendo em vista o contido nos autos do SEI nº 0033433-78.2017.6.17.8000

R E S O L V E

Art. 1º. Definir os Cartórios Eleitorais em que serão lotados provisoriamente os candidatos nomeados para provimento dos cargos de Analista Judiciário e Técnico Judiciário, por meio das Portarias nºs 809, 810, 811, 812, 813 e 814, todas, de 16 de novembro de 2021, publicadas no DJE em 23 de novembro de 2021:

a) ANALISTA JUDICIÁRIO:

136ª ZE - Saloá

b) TÉCNICO JUDICIÁRIO

48ª ZE - Altinho;

55ª ZE - Pesqueira;

58ª ZE - Pedra;

62ª ZE - Sertânia;

64ª ZE - Águas Belas;

72ª ZE - Floresta;

74ª ZE - São José do Belmonte;

80ª ZE - Bodocó;

89ª ZE - Tacaratu.

Art. 2º. Convocar os referidos candidatos para comparecerem à Audiência Pública a ser realizada no dia 30 de novembro de 2021, às 14h, na Sala de Sessões do Tribunal Regional Eleitoral de Pernambuco, a fim de optarem pela lotação provisória em uma das unidades definidas no art. 1º, para o Analista Judiciário e, a seguir, para os Técnicos Judiciários, a qual será presidida pelo Secretário de Gestão de Pessoas do Tribunal Regional Eleitoral de Pernambuco.

Art. 3º. Determinar que a escolha da lotação será feita mediante a ordem de nota obtida no concurso público.

Art. 4º. Em caso de ausência ou de não manifestação de escolha pelos servidores, a Administração indicará a lotação atribuída ao candidato, anunciando-a em audiência.

Art. 5º. Tornar sem efeito a Portaria TRE-PE nº 828 de 19 de novembro de 2021.

Recife, 25 de novembro de 2021.

CARLOS FREDERICO GONCALVES DE MORAES