Art. 32. Esta portaria deverá ser revisada a cada 12 meses.
Art. 33. Os casos omissos e eventuais dúvidas quanto à aplicação desta norma serão dirimidos pela Comissão Permanente de Segurança da Informação deste Tribunal.
Art. 34. Revogam-se as disposições em contrário, em especial, a Portaria GP n.º 130, de 24 de abril de 2017.
Art. 35. Esta Portaria entra em vigor na data de sua publicação e sua implementação iniciará imediatamente e deverá estar totalmente implantada no prazo de 24 (vinte e quatro) meses a contar desta data.
Natal/RN, 12 de dezembro de 2023.
Desembargador Cornélio Alves
Presidente

PORTARIA N.° 235/2023 - GP

Dispõe sobre a Continuidade de Serviços Essenciais de Tecnologia da Informação e Comunicação, no âmbito da Justiça Eleitoral do Rio Grande do Norte.
O DESEMBARGADOR-PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE, no uso das atribuições que lhe são conferidas pelo artigo 20, inciso XIX, da Resolução nº 09/2012 - TRE/RN, e
CONSIDERANDO a necessidade de definir processos continuidade de serviços de TI, em caso de eventos de causas naturais, acidentais, tecnológicas ou humanas;
CONSIDERANDO a Resolução CNJ n.º 396/2021, que dispõe sobre a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
CONSIDERANDO a Resolução TSE n.º 23.644/2021, que dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;
CONSIDERANDO a Resolução TRE-RN nº 110/2023, que institui a Política de Segurança da Informação (PSI) no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte;
CONSIDERANDO a Portaria DG/TSE n.º 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 as boas práticas em segurança da informação previstas nas normas ABNT ISO /IEC 27001 e ABNT NBR ISO/IEC 27002;
CONSIDERANDO as boas práticas em segurança da informação previstas no modelo CIS Controls V.8;
CONSIDERANDO a necessidade de implementar controles para o tratamento de dados pessoais, de acordo com a Lei nº 13.709/2018 (LGPD);
CONSIDERANDO as boas práticas na gestão da continuidade de negócios previstas nas normas ABNT ISO/IEC 22303 e 22313; e
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 do Rio Grande do Norte, e tendo em vista o que consta no Processo PAE nº 10.487/2023;
RESOLVE:
CAPÍTULO I
DISPOSIÇÕES PRELIMINARES
Art. 1º Os procedimentos para Continuidade de Serviços Essenciais de TI, no âmbito do Tribunal, observarão as disposições contidas nesta portaria.
Art. 2º Esta norma integra a Política de Segurança de Informação da Justiça Eleitoral, estabelecida pela Resolução TSE nº 23.644/2021.

Art. 3ª Considere-se, no que couber, a Política de Gestão de Serviços Essenciais de Tecnologia da Informação do TRE/RN, instituída pela Portaria GP n.º 177/2019, que dispõe sobre o Sistema de Gestão de Continuidade de Negócios, da qual esta norma também será integrante.

Art. 4ª Será elaborado um plano operacional de continuidade de serviços de TI, considerando os processos e ativos críticos, no prazo máximo de 90 dias.

CAPÍTULO II

DAS DEFINIÇÕES

Art. 5º Para efeitos desta norma, consideram-se os termos e definições previstos na Portaria DG /TSE nº 444/2021, além das seguintes:

I - PCNSTI - Plano de continuidade de serviços de TI - Plano de nível operacional que contém os detalhes para manter ou recuperar as atividades da organização frente a incidentes que causem uma disrupção.

II - Objetivo de Tempo de Recuperação (OTR/RTO) - Período de tempo gasto pela organização para recuperar uma atividade ou processo crítico após sua interrupção.

III - O Objetivo de Ponto de Recuperação (OPR/RPO) - Posição (no tempo) na qual deverão estar disponíveis os dados das aplicações recuperadas após a ocorrência de uma disrupção.

IV - O Período Máximo de Interrupção Tolerável (PMIT/MTO) - Tempo necessário para que os impactos adversos tornem-se inaceitáveis, que pode surgir como resultado de não fornecer um produto/serviço ou realizar uma atividade.

V - Análise de Impacto no Negócio (AIN/BIA) - Documento que registra a análise de uma disrupção na organização ao longo do tempo.

VI - Disrupção - Incidente, seja previsto ou imprevisto, que causa um desvio não planejado e negativo da expectativa de entrega de produtos e serviços de acordo com os objetivos da organização.

CAPÍTULO III

DO ESTABELECIMENTO DO CONTEXTO

Art. 6ª Para estabelecimento do contexto para criação do PCNSTI deverão ser analisados:

I - O documento de Análise de Impacto no Negócio (AIN/BIA), que será elaborado pelo Gestor de Continuidade de Negócios.

II - Os sistemas e aplicativos descritos como essenciais ou críticos para o negócio, conforme definidos em portaria específica.

III - Os macroprocessos de trabalho e sua importância para a organização.

IV - A infraestrutura tecnológica em uso ou em implantação.

Art. 7º O contexto estabelecido deve ser apresentado ao Comitê Gestor de Segurança da Informação e ao Comitê Gestor de Continuidade de Negócios para validação.

CAPÍTULO IV

DO PLANEJAMENTO

Art. 8º A Análise de Impacto no Negócio (AIN/BIA) é documento oficial de avaliação e planejamento da continuidade de negócio, nela devendo constar, no mínimo:

I - Os objetivos institucionais;

II - Os macroprocessos de trabalho afetados;

III - As pessoas impactadas;

IV - Os ativos de informação impactados;

V - A avaliação dos riscos; e

VI - A definição dos tempos de possíveis perdas e interrupções.

CAPÍTULO V

DAS PERDAS E INTERRUPÇÕES

Art. 9º O Objetivo de Tempo de Recuperação (OTR/RTO) fica definido em:

I - Sistemas críticos: 24h.
II - Sistemas não-críticos: 72h.
III - Infraestrutura de rede, incluindo equipamentos de comunicação, infraestrutura de virtualização, servidores de DNS e DHCP, serviços de autenticação (Active Directory e Single-Sign-On): 12h.
IV - Sistemas de homologação e testes: Sem tempo definido.
Art. 10. O Objetivo de Ponto de Recuperação (OPR/RPO) fica definido em:
I - Sistemas críticos: 12h.
II - Sistemas não-críticos: 72h.
III - Infraestrutura de rede, incluindo equipamentos de comunicação, infraestrutura de virtualização, servidores de DNS e DHCP, serviços de autenticação (Active Directory e Single-Sign-On): 6h.
Art. 11. O Período Máximo de Interrupção Tolerável (PMIT/MTO) fica definido em:
I - Sistemas críticos: 72h.
II - Sistemas não-críticos: 168h.
III - Infraestrutura de rede, incluindo equipamentos de comunicação, infraestrutura de virtualização, servidores de DNS e DHCP, serviços de autenticação (Active Directory e Single-Sign-On): 48h.
IV - Sistemas de homologação e testes: Sem tempo definido.
CAPÍTULO VI
DO PLANO DE CONTINUIDADE DE SERVIÇOS DE TIC
Art. 12. O Gestor de Continuidade de Negócios elaborará Plano para Continuidade dos Serviços Essenciais de TI, em conjunto com as áreas técnicas, conforme níveis de serviço previstos no capítulo V e em consonância com a Política de Gestão de Continuidade de Negócios, estabelecida pela Portaria GP n.º 177/2019.
Art. 13. O plano de continuidade de serviços de TI será aprovado pelo Comitê Gestor de Segurança da Informação e mantido com acesso restrito, evitando exposição desnecessária de informações relativas à segurança do ambiente computacional.
Art. 14. O Gestor de Continuidade de Negócios é o responsável por elaborar e manter a documentação sobre o plano de continuidade de serviços de TIC.
Art. 15. O plano será testado anualmente, na mesma data, por completo ou em partes, de acordo com a maturidade e com a disponibilidade das equipes técnicas.
Art. 16. O resultado dos testes será documentado e posteriormente avaliado pelo Comitê Gestor de Segurança da Informação, que poderá solicitar ajustes ou outras providências.
Art. 17. O plano de continuidade de serviços de TIC deverá ter cópias físicas impressas em locais de fácil acesso aos gestores das equipes técnicas responsáveis pela sua execução.
Art. 18. A política de cópias de segurança (backup) deve suportar os níveis de serviço previstos no capítulo V.
CAPÍTULO VII
DISPOSIÇÕES FINAIS
Art. 19. Os casos omissos serão resolvidos pelo Comitê Gestor de Segurança da Informação ou pelo Comitê Gestor de Continuidade de Negócios.
Art. 20. Qualquer descumprimento desta normativa deve ser imediatamente comunicado e registrado pelo Gestor de Segurança da Informação, com consequente adoção das providências cabíveis.
Art. 21. Esta norma complementar deve ser revisada a cada 12 (doze) meses pelo Gestor de Segurança da Informação e encaminhada para nova apreciação do Comitê Gestor de Segurança da Informação.
Art. 22. Esta Portaria entra em vigor na data de sua publicação e sua implementação inicia-se imediatamente.
Natal/RN, 12 de dezembro de 2023.

Desembargador Cornélio Alves
Presidente

PORTARIA N° 236/2023 - GP

Dispõe sobre a gestão de incidentes de segurança da informação do Tribunal Regional Eleitoral do Rio Grande do Norte.

O DESEMBARGADOR-PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE, no uso das atribuições que lhe são conferidas pelo artigo 20, inciso XIX, da Resolução nº 09/2012 - TRE/RN, e

CONSIDERANDO a necessidade de apoiar a gestão de incidentes de segurança da informação do Tribunal Regional Eleitoral do Rio Grande do Norte;

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 dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

CONSIDERANDO a Portaria DG/TSE nº 444/2021, que dispõe sobre a instituição da norma de termos e definições relativas à Política de Segurança da Informação do Tribunal Superior Eleitoral;

CONSIDERANDO a Resolução TRE/RN nº 110/2023, que institui a Política de Segurança da Informação (PSI) no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte;

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

CONSIDERANDO as boas práticas em gestão de incidentes de segurança da informação previstas nas normas ABNT ISO/IEC 27035 (1,2 e 3);

CONSIDERANDO as boas práticas de resposta à incidentes previstas no guia NIST SP-800-61 rev. 2;

CONSIDERANDO a necessidade de gerenciar os incidentes de segurança da informação que envolvam dados pessoais, de acordo com a Lei nº 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 do Rio Grande do Norte, e tendo em vista o que consta no Processo PAE nº 10.487/2023;

RESOLVE:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º A gestão de incidentes de segurança da informação, no âmbito do Tribunal, observará as disposições contidas nesta portaria.

Art. 2º Esta norma integra a Política de Segurança de Informação da Justiça Eleitoral, estabelecida pela Resolução TSE 23.644/2021.

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 3º Para efeitos desta norma, consideram-se os termos e definições previstos na Portaria DG /TSE nº 444/2021, além dos seguintes:

I - ANPD: Agência Nacional de Proteção de Dados Pessoais.

II - CTIR GOV: Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo.

III - ETIR (Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética): Equipe de tecnologia da informação, de constituição multidisciplinar, coordenada por um Agente Responsável.