TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE

PORTARIA N.º 75/2020 - GP

Dispõe sobre a política de atualização dos sistemas operacionais dos servidores de rede físicos e virtuais, 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 n.º 09/2012 – TRE/RN, e

CONSIDERANDO a necessidade de garantir a disponibilidade, a confidencialidade e a integridade dos dados e dos sistemas de informação;

CONSIDERANDO os controles previstos na norma ABNT/ISO/IEC 27001:2013;

CONSIDERANDO a necessidade de definir as políticas de atualizações dos sistemas operacionais dos servidores de rede físicos e virtuais, no âmbito da Justiça Eleitoral do Rio Grande do Norte no TRE/RN;

CONSIDERANDO que a segurança da informação é condição essencial para a prestação dos serviços jurisdicionais e administrativos da Justiça Eleitoral do Rio Grande do Norte;

CONSIDERANDO o contido no expediente administrativo PAE n.º 4084/2020;

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Ficam estabelecidas as diretrizes para a atualização de servidores de rede, físicos e virtuais no TRE-RN, nos termos desta Portaria.

Art. 2º Esta norma complementa a Política de Segurança de Informação do Tribunal Regional Eleitoral do RN, estabelecida pela Resolução n.º 20, de 11 de setembro de 2019, artigos 9º e 10.

CAPÍTULO II

DAS DEFINIÇÕES

Art. 3º Para efeitos desta norma consideram-se as seguintes definições:

I - Ameaça - causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização;

Documento assinado digitalmente por:
Glauber Antonio Nunes Rego 25/06/2020 16:24:29

II - Ativo de informação - patrimônio composto por todos os dados e informações gerados, adquiridos, utilizados ou armazenados pela Justiça Eleitoral;

III - Risco - potencial associado à exploração de vulnerabilidades de um ativo de informação por ameaças, com impacto negativo no negócio da organização;

IV - Vulnerabilidade - fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

CAPÍTULO III

DAS AÇÕES PREVENTIVAS

Art. 4º Devem ser implementadas ações preventivas de acordo com as melhores práticas, para, no mínimo:

I - Atualizar e manter atualizados os sistemas operacionais de servidores de rede, sejam estes físicos ou virtuais;

II - Atualizar e manter atualizados os SGBDs (Sistemas de Gestão de Bancos de Dados) usados em ambientes de produção, homologação e desenvolvimento, condicionado à análise técnica e de viabilidade;

III - Atualizar e manter atualizados os equipamentos utilizados na infraestrutura de virtualização;

Parágrafo único. Toda atualização deve, sempre que possível, ser precedida de análise de compatibilidade e, se aplicável, testes em ambiente de homologação com o intuito de garantir a disponibilidade e integridade dos sistemas e minimizar o risco de incompatibilidades que possam produzir incidentes e perturbações indesejáveis no ambiente de TI.

CAPÍTULO IV

DAS RESPONSABILIDADES

Art. 5º. Cabe ao titular da Seção de Suporte e Segurança da Informação:

I - Monitorar as atualizações dos sistemas operacionais de servidores de rede realizadas pelas unidades técnicas nos períodos estabelecidos nesta norma;

II - Atuar junto às unidades técnicas para garantir que as informações sobre as atualizações dos sistemas operacionais dos servidores de rede sejam registradas em área específica do site intranet.

Art. 6º. Cabe às unidades técnicas responsáveis pelos ativos de informação:

I - Realizar, mensalmente ou sempre que surgir uma nova atualização crítica de segurança, os procedimentos de que trata o artigo 4º;
II - Implementar medidas para mitigar o risco referente às vulnerabilidades que não puderem ser corrigidas tempestivamente.

Art. 7º. As unidades técnicas a que se referem os artigos 5º e 6º são:

I - Seção de Redes e Infraestrutura/COINF;

II - Seção de Novas Tecnologias/COSIS;

III - Seção de Banco de Dados e Sistemas/COSIS;

IV - Seção de Desenvolvimento de Sistemas/COSIS.

Art. 8º. Os responsáveis pelos procedimentos de atualização constantes do artigo 4º devem observar:

I - As atualizações regulares dos servidores de rede devem ser realizadas, preferencialmente, na última sexta-feira de cada mês, após às 16:00h, e em esquema de revezamento de servidores nos setores envolvidos, de modo a se evitar a prestação de serviço extraordinário.

II - Na segunda-feira seguinte, todos os setores envolvidos nas atualizações devem funcionar pela manhã e realizar testes de funcionamento visando sanar alguma pendência não detectada anteriormente.

III - Em período eleitoral, as atualizações serão agendadas levando-se em consideração o calendário de atividades das unidades e acontecerá em horário diverso ao expediente.

IV - Sempre que for detectada alguma vulnerabilidade crítica que comprometa a segurança, serão realizadas atualizações extraordinárias em horário diverso ao expediente.

V - Sempre que possível, o comunicado de indisponibilidade dos sistemas afetados pelas atualizações deve ser emitido com, no mínimo, três dias de antecedência.

CAPÍTULO V

DAS DISPOSIÇÕES FINAIS

Art. 9º. Os casos omissos e eventuais dúvidas quanto à aplicação desta norma serão dirimidos pela Comissão Permanente de Segurança da Informação deste Tribunal.

Art. 10. Esta Portaria entra em vigor na data de sua publicação.

Natal, 22 de junho de 2020.

Desembargador **Glauber Antonio Nunes Rêgo**

Presidente

Documento assinado digitalmente por:
Glauber Antonio Nunes Rego 25/06/2020 16:24:29