



TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE  
COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

**ATA DE REUNIÃO N. 05/2020**

**I . Identificação da Reunião**

| Data       | Horário |         | Local   | Coordenador                   |
|------------|---------|---------|---------|-------------------------------|
|            | Início  | Término |         |                               |
| 03.03.2020 | 13h30   | 15h30   | CGESTIC | Marcos Flávio Nascimento Maia |

**II. Objetivo**

Reunião do CGESTIC para tratar do seguinte assunto:

- Apresentar a minuta de norma contendo a Política de Atualização dos Servidores de Rede.

**III. Participantes**

| Nome  | Lotação                 | Assinatura |
|---|-------------------------|------------|
| Marcos Flávio Nascimento Maia                 | STIC                    |            |
| Osmar Fernandes de Oliveira Júnior            | COSIS                   |            |
| Tyronne Dantas de Medeiros                    | COTEL                   |            |
| Daniel César Gurgel Coelho Ponte              | COINF (em substituição) |            |
| Dina Márcia de Vasconcelos Maranhão da Câmara | GAPSTIC                 |            |
| Jussara de Gois Borba Melo Diniz              | GAPSTIC                 |            |



TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE  
COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

**IV. Discussão da Pauta**

| Nº | Descrição/Decisão   | Responsável            |
|----|---|------------------------|
| 01 | <b>Apresentação da minuta de norma contendo a Política de Atualização dos Servidores de Rede</b><br><br>Foi apresentada a minuta da norma de "Dispõe sobre a política de atualização dos sistemas operacionais dos servidores físicos e virtuais no âmbito da Justiça Eleitoral do Rio Grande do Norte" por Daniel (COINF, em substituição) e diante disso, foi destacado por Marcos a importância de submeter a minuta à apreciação da CPSI. Ato contínuo, a minuta foi apreciada, pelos presentes, sendo realizados ajustes nas considerações, bem como, nos textos dos artigos, sendo debatidos por todos os presentes e aprovada a minuta conforme o Anexo I desta ata. | Todos os participantes |
| Nº | Descrição/Decisão   | Responsável            |
| 02 | <b>Lei Geral de Proteção de Dados - Lei nº 13.709/2018</b><br><br>Em decorrência das discussões em torno da minuta posta em discussão, objeto do item 1 desta ata, e considerando que em agosto/2020 entrará em vigor a norma Lei Geral de Proteção de Dados - Lei nº 13.709/2018, foi sugerido por Osmar que a STIC agende momento oportuno para discussão sobre o tema, após as estudos de cada coordenadoria da STIC.<br><br>Prazo: 1º CGesTIC de abril/2020.  | Todos os participantes |

**V. Pendências Identificadas**

| Nº | Pendências  | Responsável   | Data limite               |
|----|---|---------------|---------------------------|
| 01 | Estudo da Lei Geral de Proteção de Dados - Lei nº 13.709/2018 | Coordenadores | 1º CGesTIC de abril/2020. |

**VI. Fechamento da Ata**

| Data       | Nome do relator                               | Assinatura |
|------------|---|------------|
| 14.02.2020 | Dina Márcia de Vasconcelos Maranhão da Câmara |            |



**TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE**

**COMITÊ DE GESTÃO DE TIC - RESOLUÇÃO Nº 029/2019**

**REUNIÃO CGesTIC N.º 05/2020**

**ANEXO I**



## TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE

PORTARIA Nº XX/2020 - DG

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 DIRETOR-GERAL DO TRIBUNAL REGIONAL ELEITORAL, no uso de suas atribuições legais e regimentais,

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 nº PAE XXX/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.

Art. 2º Esta norma complementa a Política de Segurança de Informação do Tribunal Regional Eleitoral do RN, estabelecida pela Resolução nº 20 de 11 de setembro de 2019.

### 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;

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

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

IV - Ativo de informação - todo dado ou informação gerado, adquirido, utilizado ou custodiado pela Justiça Eleitoral, assim como qualquer equipamento, software ou recurso utilizado para seu processamento ou armazenamento.

### 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 Gestor 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 devem ser emitidos 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, XX de XXXXX de 2020

Simone Maria de Oliveira Soares Mello  
Diretora Geral