Art. 2º Os servidores lotados nos locais constantes do §1º poderão ser autorizados pelo seu respectivo juízo a auxiliar em outra unidade zonal integrante do seu município, sempre imprescindível a comunicação à Secretaria de Gestão de Pessoas para os devidos registros.
Art. 3º Autorizar a prestação do serviço extraordinário, nos dias úteis e sábados, no limite de 44 (quarenta e quatro) horas, no período de 7 a 30 de janeiro de 2021 e 1º a 27 de fevereiro de 2021, em cada intervalo, a serem restituídas mediante anotação em banco de horas, aos servidores que compõem as comissões designadas para atuarem na análise das prestações de contas dos benefícios-alimentação e dos suprimentos de fundos, por meio, respectivamente, das Portarias da Presidência nº 416/2020 e nº 419/2020.
Art. 4º A realização do serviço extraordinário, no período autorizado, não excederá a 02 (duas) horas em dias úteis e 10 (dez) horas aos sábados, ficando resguardado o intervalo de, no mínimo, 01 (uma) hora para repouso e/ou alimentação, bem como um período de repouso de, no mínimo, 08 (oito) horas ininterruptas entre cada jornada diária de trabalho e o repouso semanal remunerado aos domingos.
Art. 5º Fica vedada a prestação de serviço extraordinário no período entre 22 (vinte e duas) horas de um dia e 5 (cinco) horas do dia seguinte.
Art. 6º É vedado, durante a execução do serviço extraordinário autorizado nesta Portaria, o registro de ponto eletrônico lançado pela chefia imediata ou aquele condicionado a homologação.
Parágrafo único. Compete à Secretaria de Gestão de Pessoas e à Secretaria de Tecnologia da Informação, no âmbito de suas respectivas atribuições, a adoção das medidas necessárias ao fiel cumprimento do constante do caput.
Art. 7º A convocação, o acompanhamento e o controle da prestação do serviço extraordinário de cada servidor são de responsabilidade da sua chefia imediata, observando, inclusive, as demais normas de regência.
Art. 8º As dúvidas porventura suscitadas serão dirimidas pelo Presidente do Tribunal.
Art. 9º Esta Portaria entrará em vigor na data da sua publicação, produzindo efeitos retroativos ao dia 7 de janeiro de 2021.
Salvador, 8 de janeiro de 2021.
Des. Jatahy Júnior Presidente do Tribunal Regional Eleitoral da Bahia

PORTARIA Nº 497, DE 30 DE DEZEMBRO DE 2020

Aprova a Norma de Segurança da Informação nº 11 (NSI 011).
O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DA BAHIA, no uso de suas atribuições regimentais,
CONSIDERANDO a necessidade contínua de estabelecer e revisar processos de segurança e privacidade da informação no âmbito da Justiça Eleitoral da Bahia;
CONSIDERANDO o que estabelece a Portaria nº 356, de 4 de julho de 2018,
RESOLVE:
Art. 1º Aprovar a Norma de Segurança da Informação nº 11 (NSI 011) constante do Anexo desta Portaria.
Art. 2º Esta Portaria entra em vigor na data de sua publicação.
Salvador, 30 de dezembro de 2020
Desembargador JATAHY JÚNIOR
Presidente do Tribunal Regional Eleitoral da Bahia
ANEXO
A que se refere o art. 1º da Portaria nº 497, de 30 de dezembro de 2020
NSI 011 - PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS
1. OBJETIVO

Dispor sobre as regras de segurança que nortearão a definição e a implantação de medidas para a proteção contra a ação de códigos maliciosos no ambiente de rede do Tribunal Regional Eleitoral da Bahia.

2. CONCEITOS E DEFINIÇÕES

Para os efeitos desta norma são estabelecidos os seguintes conceitos e definições:

1. Antivírus: ferramenta desenvolvida para detectar, anular e eliminar vírus e outros tipos de códigos maliciosos de um computador. Pode incluir também a funcionalidade de *firewall* pessoal;

2. Código malicioso: termo genérico que se refere a todos os tipos de programas especificamente desenvolvidos para executar ações danosas em recursos de tecnologia da informação;

3. *Firewall*: dispositivo de segurança usado para dividir e controlar o acesso entre redes de computadores;

4. *Firewall* pessoal: tipo específico de *firewall*. Programa usado para proteger um computador contra acessos não autorizados; e

5. *Log*: registro de atividades gerado por programas e serviços de um computador. Termo técnico que se refere ao registro de atividades de diversos tipos como, por exemplo: de conexão (informações sobre a conexão de um computador à Internet) e de acesso a aplicações (informações de acesso de um computador a uma aplicação de Internet).

3. CONSIDERAÇÕES INICIAIS

1. Conforme estabelecido na NSI-002 - Uso de Recursos de Tecnologia da Informação e Controle de Acesso, os usuários são responsáveis pelos recursos de tecnologia da informação por eles utilizados, devendo contribuir para seu funcionamento e segurança.

2. Códigos maliciosos são agentes potencialmente graves à segurança da informação, pois possibilitam o roubo de informações sigilosas e a paralisação dos serviços.

3. Convém que os recursos de tecnologia da informação estejam protegidos por sistemas de detecção e bloqueio de códigos maliciosos, prevenção e detecção de acesso não autorizado, tais como programas antivírus, programas de análise de conteúdo de correio eletrônico e *firewall*.

4. Padrões e procedimentos para instalação, configuração, utilização e atualização de sistemas de detecção e bloqueio de códigos maliciosos devem ser estabelecidos pela Secretaria de Tecnologia da Informação.

4. CONTROLES

1. É vedada qualquer atividade, por parte dos usuários, que vise à criação ou distribuição de códigos maliciosos.

2. É vedada ao usuário a desativação ou a alteração de configuração de quaisquer de seus componentes de proteção contra códigos maliciosos (por ex.: antivírus, *firewall* pessoal etc.). Caso julgue necessário alguma modificação, o setor responsável deverá ser informado.

3. Antes de sua utilização, é conveniente que toda e qualquer mídia de armazenamento que tenha origem externa ao Tribunal seja verificada quanto à existência de códigos maliciosos.

4. Convém que todo e qualquer arquivo recebido por correio eletrônico ou Internet seja verificado de forma automática quanto à existência de códigos maliciosos.

5. Convém que todos os dispositivos de processamento do Tribunal devam estar configurados de acordo com os padrões de segurança mais adequados aos serviços previstos, de maneira que prestem apenas os serviços previstos.

6. Convém que todos os dispositivos de processamento do Tribunal estejam atualizados conforme as recomendações dos respectivos fabricantes e fornecedores.

7. Os dispositivos de processamento portáteis, sempre que tecnicamente possível, devem possuir *firewall* pessoal instalado e configurado de forma a possibilitar que o dispositivo seja utilizado somente para os fins previstos.

8. Os sistemas de detecção e bloqueio de códigos maliciosos devem prover monitoramento, em tempo de execução, dos arquivos e programas, quanto à contaminação por código malicioso.
9. Os arquivos contaminados por código malicioso devem ser imediatamente descontaminados, isolados ou removidos do sistema pelo programa antivírus. Em caso de persistência do problema, o equipamento deve ser isolado até que seja sanado o problema para não afetar o desempenho das atividades do Tribunal.
5. COMPETÊNCIAS E RESPONSABILIDADES
Ficam definidas as seguintes competências e responsabilidades:
1. À Secretaria de Tecnologia da Informação:
1. auxiliar a Comissão de Segurança da Informação no processo de conscientização dos usuários quanto às melhores práticas de prevenção contra códigos maliciosos;
2. proceder com a instalação dos sistemas de detecção e bloqueio de códigos maliciosos nos equipamentos computacionais, mantendo-os atualizados conforme disponibilização do fabricante; e
3. monitorar os *logs* dos sistemas de detecção e bloqueio de códigos maliciosos, prevenção e detecção de acesso não autorizado, com objetivo de atuar de forma proativa na identificação de ameaças.
2. Ao usuário:
1. utilizar somente programas homologados pela Secretaria de Tecnologia da Informação;
2. observar se o programa de antivírus está instalado, atualizado e ativo no equipamento computacional;
3. utilizar mídia de armazenamento que tenha origem externa à organização conforme disposto no item 4.3; e
4. notificar imediatamente à Comissão de Segurança da Informação e/ou Secretaria de Tecnologia da Informação qualquer suspeita de ataque por código malicioso à dispositivo de processamento sob sua custódia, ou mesmo a sua rede local.
6. DISPOSIÇÕES FINAIS
1. As atualizações e as correções para os sistemas de detecção e bloqueio de códigos maliciosos devem ser homologadas pela Secretaria de Tecnologia da Informação antes de aplicadas ao ambiente de produção.
2. As correções ou atualizações para os sistemas de detecção e bloqueio de códigos maliciosos, depois de homologadas, devem ser implementadas, a fim de se evitar que estes sistemas fiquem vulneráveis a códigos maliciosos ou a qualquer tentativa de acesso não autorizado.
3. Os casos omissos e as dúvidas surgidas na aplicação desta norma serão dirimidos pelo Comitê Gestor de Segurança da Informação.
7. VIGÊNCIA E ATUALIZAÇÃO
A atualização desta norma ocorrerá de forma periódica ou sempre que se fizer necessário, não excedendo o período máximo de 02 (dois) anos.

PORTARIA Nº 489, DE 28 DE DEZEMBRO DE 2020

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DA BAHIA, no uso das suas atribuições legais e regimentais, e considerando o contido no processo SEI n.º 0136789-20.2020.6.05.8000
RESOLVE:
Art. 1° Prorrogar o prazo previsto no art. 3º da Portaria nº 443/2020, por mais 15 (quinze) dias, a contar de 20 de janeiro de 2020.
Art. 2º Esta portaria entrará em vigor na data da sua publicação.
Salvador, 28 de dezembro de 2020.
Desembargador JATHAY JUNIOR
Presidente do Tribunal Regional Eleitoral da Bahia