NSI-003 – Controle de Acesso à Internet

1. Objetivos

1.1. Estabelecer diretrizes e padrões para o acesso à Internet no âmbito do Tribunal Regional Eleitoral da Bahia (TRE-BA).

2. Motivações

2.1. Alinhamento às normas, regulamentações e melhores práticas, relacionadas à matéria.

2.2. Proteção do ambiente tecnológico do Tribunal.

2.3. Correto direcionamento e dimensionamento de recursos tecnológicos para prover o serviço de acesso à Internet.

3. Referências normativas

3.1. Norma Complementar 01/IN01/DSIC/GSIPR, de 15 de outubro de 2008, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre a Gestão de Segurança da Informação e Comunicações, no âmbito da Administração Pública Federal, direta e indireta.

3.2. Norma Complementar nº 07/IN01/DSIC/GSIPR (Revisão 01), de 15 de julho de 2014, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece diretrizes para a implementação de controles de acesso à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

3.3. Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.

3.4. Norma Técnica ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação.

4. Conceitos e definições

4.1. Arquivo de registro de mensagens (*logs*): registro de eventos relevantes, utilizados para restaurar um sistema, diagnosticar problemas ou realizar auditorias.

4.2. Código malicioso: termo comumente utilizado para genericamente se referir a programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel. Tipos específicos de códigos maliciosos são: vírus, worm, bot, spyware, backdoor, cavalo de troia e rootkit.

4.3. Intranet: rede de computadores circunscrita aos limites internos de uma instituição, na qual são utilizados os mesmos programas e protocolos de comunicação empregados na Internet.

4.4. *Proxy*: também conhecido por filtro de conteúdo, é o servidor responsável por intermediar o acesso à Internet, aplicando regras de controle de acesso e mecanismos de proteção contra códigos maliciosos, previamente configurados, e por controlar a alocação de recursos de rede.

4.5. *Proxy* externo: são servidores, não administrados pelo TRE-BA, responsáveis por intermediar o acesso à Internet, mas que não aplicam as regras de controle de acesso e mecanismos de proteção da mesma forma que o *proxy* administrado pelo Tribunal.

4.6. Sítio: conjunto de páginas *web* organizadas e acessíveis a partir de um URL da rede interna (Intranet) ou da Internet.

4.7. Situação de contingência: estado ou condição na qual exista a ocorrência de falha/problema, em um ou mais recursos tecnológicos, que reduzam a capacidade dos sistemas e serviços que suportam a atividade da organização.

4.8. URL: sigla correspondente às palavras inglesas "*Uniform Resource Locator*", traduzidas para o português como “Localizador Uniforme de Recursos”. Trata-se da indicação do endereço de um recurso de informática disponível em uma rede, seja ela a Internet ou a intranet de uma organização.

5. Diretrizes

5.1. O acesso à Internet dar-se-á, exclusivamente, pelos meios autorizados, configurados e disponibilizados pela Secretaria de Tecnologia da Informação.

5.1.1. É expressamente proibido o uso de *proxies* externos ou similares.

5.2. O acesso à Internet é disponibilizado para uso nas atividades relacionadas ao trabalho, observado o disposto nesta Norma.

5.3. Constitui acesso indevido à Internet qualquer das seguintes ações:

5.3.1. Acessar páginas de conteúdo considerado ofensivo, ilegal, impróprio ou incompatível com as atividades funcionais ou com a Política de Segurança da Informação, tais como pornografia, pedofilia, racismo, jogos e páginas de distribuição e de compartilhamento de *software*.

5.3.2. Utilizar programas de troca de mensagens em tempo real (bate-papo) ou programas para troca de conteúdo via rede ponto-a-ponto (*peer- to-peer*), exceto os autorizados pelo Comitê de Segurança da Informação.

5.3.3. Utilizar programas e/ou acessar páginas de áudio e vídeo em tempo real, ou sob demanda, exceto os autorizados pelo Comitê de Segurança da Informação.

5.3.4. Acessar sítios que representem ameaça de segurança ou que possam comprometer de alguma forma a integridade da rede de computadores do TRE-BA.

5.3.5. Acessar ou fazer *download* de arquivos não relacionados ao trabalho, em especial músicas, imagens, vídeos, jogos e programas de qualquer tipo.

5.4. Todo tráfego de Internet será controlado e inspecionado, de forma automática, pela ferramenta de *proxy* (filtro de conteúdo), configurada de acordo com os limites estabelecidos por esta Norma ou definidos pela Administração do Tribunal.

5.4.1. A liberação de acesso a sítios e serviços bloqueados, mas necessários ao desempenho das atribuições funcionais do usuário, dependerá de solicitação, devidamente justificada, à Secretaria de Tecnologia da Informação, por meio da Central de Serviços de TIC, que a submeterá, quando for o caso, ao Comitê de Segurança da Informação, para deliberação.

5.5. Cabe ao gestor da unidade orientar os usuários sob sua responsabilidade a respeito do uso adequado do recurso de Internet, conforme as regras estabelecidas nesta Norma, bem como reportar ao Comitê de Segurança da Informação o seu descumprimento.

5.6. A critério da Administração, poderão ser adotadas medidas visando a manutenção da disponibilidade e da qualidade do acesso à Internet, seja em situações normais de funcionamento, seja em situações de contingência, tais como:

5.6.1. Bloqueios totais ou parciais e/ou priorização de acessos a determinados sítios e serviços; e

5.6.2. Limitação de banda de tráfego de dados.

5.7. As medidas identificadas no item anterior, quando implementadas, serão comunicadas à Central de Serviços de TIC, a fim de possibilitar o repasse de informações aos usuários interessados.

6. Monitoramento e auditorias

6.1. Por motivos de segurança, todo acesso à Internet será monitorado e os registros serão mantidos pela Secretaria de Tecnologia da Informação.

6.2. Em caso de indícios de descumprimento das diretrizes previstas nesta Norma, a chefia imediata ou superior deverá solicitar, justificadamente, ao Comitê de Segurança da Informação, a realização de auditoria extraordinária.

6.2.1. Em caso de deferimento da solicitação, o Comitê de Segurança da Informação demandará à Secretaria de Tecnologia da Informação a execução da auditoria e a elaboração do respectivo relatório.

6.2.2. Os relatórios decorrentes das auditorias ordinárias e extraordinárias deverão ser encaminhados ao Comitê de Segurança da Informação para os devidos fins.