

2. Ao usuário:

1. utilizar somente programas homologados pela Secretaria de Tecnologia da Informação;
2. observar se o programa de antivírus está instalado 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.

Anexo XIII

• *Anexo XIII acrescentado pela Portaria 654/21.*

(NSI 013 - Gerenciamento de Contas de Usuários Terceirizados, Estagiários, Requisitados, Juízes e Servidores Aposentados)

1 OBJETIVO

Estabelecer diretrizes para o gerenciamento das contas de rede, usuários de sistemas e e-mail institucional de terceirizados, estagiários, requisitados, magistrados e servidores aposentados no âmbito do Tribunal Regional Eleitoral da Bahia.

2 CONCEITOS E DEFINIÇÕES

Bloquear contas de acesso - Ação de impedir que a conta seja utilizada para acesso aos recursos computacionais correspondentes (rede, e-mail ou banco de dados). Uma conta bloqueada não poderá ser usada, mas permanece consumindo cotas e espaço de armazenamento.

Excluir contas de acesso - Ação de remover definitivamente uma conta, de modo que os recursos por

ela consumidos passam a estar liberados para uso por outros usuários.

Princípio do "privilégio mínimo" - estratégia de segurança, aplicável a diferentes áreas, que se baseia na ideia de conceder autorizações apenas quando estritamente necessárias para o desempenho de uma atividade específica.

3 DIRETRIZES

3.1 Cabe à unidade responsável pelos contratos do TRE-BA o cadastramento dos contratos de terceirização firmados por este Regional em sistema apropriado.

3.2 As unidades gestoras dos contratos dos colaboradores terceirizados deverão manter os dados dos contratados atualizados em sistema destinado a esse fim, inclusive quanto à data de desligamento.

3.2.1 Ocorrido o desligamento do colaborador contratado, as unidades da STI (Secretaria de Tecnologia da Informação e Comunicação), de acordo com a sua área de competência, promoverão o bloqueio imediato das contas de acesso à rede de dados, e-mail institucional e sistemas. Transcorridos 10 (dez) dias do fim do desligamento do colaborador contratado, a STI promoverá a exclusão das contas de acesso à rede, e-mail institucional e sistemas.

3.3 A unidade gestora dos contratos de estágio deverá manter os dados atualizados em sistema de informática destinado ao cadastramento de estagiários, inclusive quanto à data fim do contrato.

3.3.1 Na data posterior ao fim do contrato de estágio, unidades da STI, de acordo com a sua área de competência, promoverão o bloqueio imediato das contas de acesso à rede de dados, e-mail institucional e sistemas dos referidos estagiários. Transcorridos 10 (dez) dias do fim do contrato de estágio, a STI promoverá a exclusão das contas de acesso à rede, e-mail institucional e sistemas.

3.4 Cabe à unidade gestora de informações de servidores requisitados registrar no Sistema de Gestão de Recursos Humanos a data de retorno de servidores requisitados ao órgão de origem, após comunicação formal da unidade requisitante

3.4.1 Transcorrido 1 (um) dia útil do registro da data de retorno, a STI providenciará o bloqueio ou exclusão das contas de acesso à rede, e-mail institucional e sistemas.

3.5 A unidade gestora de dados de magistrados deverá informar em sistema de informática utilizado para cadastramento de juízes e desembargadores a data fim do biênio dos mesmos neste Regional, ao final do efetivo exercício.

3.5. Após o fim do biênio dos desembargadores eleitorais e juízes eleitorais, a STI providenciará o bloqueio imediato das contas de acesso à rede de dados, e-mail institucional e sistemas. A STI promoverá a exclusão definitiva desses acessos atendendo às seguintes regras:

I - imediatamente, para os Desembargadores Eleitorais titulares e substitutos, pertencentes à Classe dos Advogados, para os juízes das zonas eleitorais da capital e para os juízes indicados para substituir por tempo determinado em uma unidade zonal;

II - após 4 (quatro) meses, para os Desembargadores Eleitorais titulares e substitutos, pertencentes às Classes de Desembargador, Juiz de Direito e Juiz Federal, bem como para os juízes eleitorais das zonas eleitorais do interior.

3.6 A unidade responsável pela gestão dos dados dos servidores aposentados deverá manter atualizadas as informações de e-mail pessoal e telefone no Sistema de Gestão de Recursos Humanos adotado pela Justiça Eleitoral.

3.6.1 Quando do registro da data de aposentadoria de um servidor no Sistema de Gestão de Recursos

Humanos, a STI providenciará o bloqueio imediato das contas de acesso à rede de dados, e-mail institucional e sistemas. Transcorridos 10 (dez) dias do registro da data de aposentadoria de um servidor, a STI promoverá a exclusão definitiva desses acessos.

3.6.2A unidade responsável pela gestão dos dados dos servidores aposentados deverá atualizar o endereço de e-mail pessoal de servidor inativo e proceder à devida comunicação no prazo de 180 dias. Após esse período, as contas de e-mail institucional de servidores aposentados que se encontrarem ativas serão excluídas.

3.7 As ações para bloqueio imediato, bem como para a exclusão definitiva de contas de rede, e-mail e sistemas se darão através de procedimentos automatizados a serem desenvolvidos pela STI, num prazo de 180 dias.

3.8 As contas de acesso à rede, e-mail e sistemas atualmente ativas que se encontrem sem uso pelo período de um ano no momento em que esta norma entrar em vigor deverão ser imediatamente bloqueadas. A STI promoverá a sua exclusão definitiva após novo prazo de 3 (três) meses contatos a partir do bloqueio, caso não ocorra solicitação explícita para sua reativação.

3.9 No caso da exclusão definitiva das contas de acesso a sistemas, deve haver mecanismo automático de auditoria, armazenando dados identificadores da exclusão (conta excluída, titular da conta, responsável pela exclusão, data e hora da exclusão, permissões a objetos de banco de dados) para fins de posterior necessidade de recuperação.

3.10 No caso de exclusão definitiva das contas de e-mail, em atenção ao disposto na Política de Segurança da Informação da Justiça Eleitoral, deve-se manter cópias de segurança desses dados pelo prazo de 240 dias, para eventual necessidade de análise e investigação de incidentes.

3.11 A STI dará conhecimento às unidades competentes de quais dados são pré-requisito para a possível criação de recursos (contas de rede, e-mail e sistemas) para colaboradores. Dessa forma, caso o indivíduo não esteja cadastrado adequadamente em seu sistema correspondente, não haverá a criação das contas.

3.12 O(A) servidor(a) removido(a) ou cedido(a) a outro órgão terá seu acesso à rede bloqueado, a contar da data do seu afastamento. **(Incluído pela Portaria 647/22)**

4 PAPÉIS E RESPONSABILIDADES

4.1 Constitui incumbência dos fiscais de contratos de terceiros comunicar à STI, no prazo de 30 dias contados a partir da entrada em vigor dessa NSI, a relação nominal de colaboradores terceirizados que necessitem de recursos de TIC fornecidos pelo TRE/BA, com justificativa fundamentada, em atenção ao princípio do "privilegio mínimo".

4.1.1 A comunicação deverá abranger tanto os acessos já existentes quanto os novos, que vierem a ser concedidos.

4.1.2 Enquanto não disponibilizada pela STI a solução técnica citada no item 3.7, essa comunicação se dará, preferencialmente, através de abertura de chamados na Central de Serviços de TIC.

4.1.2.1 O mesmo se aplica com relação ao desligamento dos terceiros, ao término do contrato. Nessa hipótese, a comunicação deve ser imediata.

4.1.3 Transcorrido o prazo de 10 (dez) dias sem manifestação dos fiscais de contratos, os acessos serão revogados e as contas excluídas, até o advento de nova solicitação com as informações requeridas.

5 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.