RESOLUÇÃO TRE Nº 945, DE 17 DE DEZEMBRO DE 2013

Alterada pela Resolução TRE nº 1.091/2018

Regulamenta a Política de Segurança da Informação no âmbito do Tribunal Regional Eleitoral de Minas Gerais e dá outras providências.

O TRIBUNAL REGIONAL ELEITORAL DE MINAS GERAIS, no uso de suas atribuições legais e regimentais, e

CONSIDERANDO a necessidade de disciplinar a elaboração de normas e procedimentos visando à regulamentação e à operacionalização das diretrizes de segurança da informação no âmbito deste Tribunal, conforme o disposto na Resolução nº 22.780, de 24 de abril de 2008, do Tribunal Superior Eleitoral;

CONSIDERANDO a necessidade de preservar a integridade, a confidencialidade e a credibilidade dos ativos de informação deste Tribunal, por meio do combate a atos acidentais ou intencionais de destruição, modificação, apropriação ou divulgação indevida de informações,

RESOLVE:

~~Art. 1º Fica regulamentada, nos termos desta resolução, a Política de Segurança da Informação no âmbito do Tribunal Regional Eleitoral de Minas Gerais, em conformidade com a Resolução TSE nº 22.780, de 24 de abril de 2008.~~

Art. 1º Fica regulamentada, nos termos desta resolução, a Política de Segurança da Informação – PSI – no âmbito do Tribunal Regional Eleitoral de Minas Gerais.

§ 1º A PSI aplica-se a todos os Magistrados, servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo, estagiários, prestadores de serviço, colaboradores e usuários externos que fazem uso dos ativos de informação e de processamento no âmbito da Justiça Eleitoral.

§ 2º Os destinatários da PSI são corresponsáveis pela segurança da informação, observados os preceitos estabelecidos nesta resolução. (artigo com redação alterada pela Resolução TRE nº 1.091/2018)

~~Art. 2º São objetivos da Política de Segurança da Informação deste Tribunal:~~

~~I – a preservação da integridade, da confidencialidade e da credibilidade dos ativos de informação deste Regional;~~

~~II – o combate aos atos acidentais ou intencionais de destruição, modificação, apropriação ou divulgação indevida de informações.~~

~~Parágrafo único. Para os efeitos desta resolução, considera-se ativo de informação o patrimônio composto por todos os dados e informações geradas, adquiridas, utilizadas ou armazenadas pelo Tribunal Regional Eleitoral de Minas Gerais.~~

Art. 2º São objetivos da Política de Segurança da Informação do Tribunal:

I – instituir diretrizes estratégicas, responsabilidades e competências visando à estruturação da segurança da informação;

II – promover ações necessárias à implementação e à manutenção da segurança da informação;

III – combater atos acidentais ou intencionais de destruição, modificação, apropriação ou divulgação indevida de informações, de modo a preservar os ativos de informação e a imagem da instituição;

IV – promover a conscientização e a capacitação de recursos humanos em segurança da informação.
Parágrafo único. Para os efeitos desta resolução, considera-se ativo de informação o patrimônio composto por todos os dados e informações geradas, adquiridas, utilizadas ou armazenadas pelo Tribunal Regional Eleitoral de Minas Gerais. (artigo com redação alterada pela Resolução TRE nº 1.091/2018)

~~Art. 3º A operacionalização das diretrizes da Política de Segurança da Informação neste Tribunal se efetivará por meio das normas constantes dos anexos desta resolução, elaboradas com base em controles estabelecidos no conjunto de normas NBR ISO IEC 27000:2005, conforme dispõe a Resolução TSE nº 22.780/2008.~~
Art. 3º A operacionalização das diretrizes da Política de Segurança da Informação no Tribunal se efetivará por meio das normas constantes dos anexos desta resolução. (*caput* com redação alterada pela Resolução TRE nº 1.091/2018)
§ 1º Serão adotadas, para efeito desta resolução e das normas da Política de Segurança da Informação, as definições constantes do dicionário a que se refere o inciso X do art. 4º desta resolução.
§ 2º As normas deverão indicar o público-alvo a que se destinam e serão classificadas como gerais, quando tiverem ampla aplicação ou impacto, ou específicas, quando tiverem aplicação ou impacto restrito.

Art. 4º Compõem a Política de Segurança da Informação neste Tribunal os seguintes documentos e normas, constantes dos Anexos I a X desta resolução:
I – PSI-N001 – Norma geral de segurança para usuários;
II – PSI-N002 – Norma geral de segurança física de instalações;
III – PSI-N003 – Norma específica de segurança para profissionais de Tecnologia da Informação;
IV – PSI-N004 – Norma geral de segurança para controle dos acessos à rede de comunicação de dados;
V – PSI-N005 – Norma geral de segurança sobre códigos maliciosos;
VI – PSI-N006 – Norma específica de segurança para equipamentos servidores de rede de dados;
VII – PSI-N007 – Norma geral de segurança para tratamento de mídias e cópias de segurança;
VIII – PSI-N008 – Norma geral de segurança para sistemas administrativos e judiciais;
IX – PSI-N009 – Norma geral de segurança para sistemas eleitorais;
X – PSI-dicionário – Dicionário de termos e siglas.
§ 1º As normas que integram a Política de Segurança da Informação serão publicadas pela Secretaria de Tecnologia da Informação na intranet e no Portal deste Tribunal, em seção específica intitulada “Segurança da Informação”.
§ 2º Outras normas poderão ser acrescentadas às constantes dos incisos deste artigo, observados os procedimentos especificados no art. 5º desta resolução.

~~Art. 5º A revisão e a atualização das normas de segurança da informação ocorrerão a cada dois anos ou sempre que se fizer necessário ou conveniente para o Tribunal.~~
~~Parágrafo único. As alterações nos anexos desta resolução serão formalizadas por meio de portaria da Diretoria-Geral deste Tribunal mediante proposta do Comitê de Segurança da Informação, instituído pela Portaria nº 108, de 18 de fevereiro de 2013, da Diretoria-Geral.~~
Art. 5º A revisão e a atualização das normas de segurança da informação ocorrerão sempre que se fizer necessário ou conveniente ao Tribunal, por meio de portaria da Presidência do Tribunal. (artigo com redação alterada pela Resolução TRE nº 1.091/2018)

~~Art. 6º Todos os usuários de recursos de tecnologia da informação no âmbito do Tribunal deverão atestar ciência às normas que lhes dizem respeito mediante a assinatura do Termo de Ciência, constante do Anexo XI desta resolução e disponível na página da Secretaria de Tecnologia da Informação na intranet.~~
~~Parágrafo único. A chefia imediata do usuário ou o servidor por ele responsável deverá indicar as normas para as quais se deve atestar ciência.~~ (artigo revogado pela Resolução TRE nº 1.091/2018)

Art. 7º O Tribunal adotará as sanções legais e contratuais cabíveis contra qualquer usuário ou entidade que venha a praticar atos que violem a Política de Segurança da Informação regulamentada nos termos desta resolução.

Art. 8º Caberá aos setores competentes do Tribunal propor e implementar as ações necessárias à execução do disposto nesta resolução.
Parágrafo único. As normas da PSI cuja implementação depende de serviços ou aquisições ainda não disponíveis serão efetivadas gradativamente, tão logo sejam providenciados os recursos necessários.

Art. 9º Casos omissos serão decididos pela Diretoria-Geral.

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

Belo Horizonte, 17 de dezembro de 2013.

Desembargador ANTÔNIO CARLOS CRUVINEL – Presidente. Desembargador PAULO CÉZAR DIAS - Vice-Presidente. Juiz MAURÍCIO PINTO FERREIRA. Juíza ALICE DE SOUZA BIRCHAL. Juiz ALBERTO DINIZ JÚNIOR. Juíza MARIA EDNA FAGUNDES VELOSO.

Publicada no DJE/TRE-MG, de 19/12/2013.

TRIBUNAL REGIONAL ELEITORAL DE MINAS GERAIS

ANEXO I
(a que se referem os arts. 3º, 4º e 5º da Resolução nº 945, de 17 de dezembro de 2013)

PSI - N 001	NORMA GERAL DE SEGURANÇA PARA USUÁRIOS
Versão 2.5 21/06/2013	Política de Segurança da Informação da Justiça Eleitoral

SUMÁRIO

1 MATÉRIA DISCIPLINADA

1.1 Dispõe sobre as regras formais para controlar a distribuição de direitos de acesso aos recursos de tecnologia da informação do Tribunal Regional Eleitoral de Minas Gerais – TRE-MG.

1.2 Orienta os usuários sobre competências, usos e responsabilidades associados à segurança da informação no âmbito do TRE-MG.

1.3 Estabelece critérios gerais para disponibilização e manipulação dos recursos de tecnologia da informação considerando o envolvimento dos recursos humanos no âmbito das atividades precípuas da Justiça Eleitoral.

2 OBJETIVO GERAL

2.1 Orientar os usuários sobre o uso e as responsabilidades associadas à segurança da informação e estabelecer regras para criação, utilização e administração de contas e senhas de acesso aos recursos de tecnologia da informação, assim como orientar os usuários sobre a utilização segura desses recursos.

3 PÚBLICO ALVO

3.1 Aplica-se a todos os usuários de Tecnologia de Informação – TI –I, servidores e colaboradores do TRE-MG.

4 APLICAÇÃO

4.1 Norma de segurança de aplicação interna.

5 REFERÊNCIAS LEGAIS E NORMATIVAS

a) **Lei nº 9.609, de 19 de fevereiro de 1998 -** dispõe sobre a proteção de propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências;

b) **Lei nº 9.279, de 14 de maio de 1996 -** regula direitos e obrigações relativos à propriedade intelectual;

c) **Norma Técnica ABNT NBR ISO/IEC 27001:2006** - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação – Requisitos;

d) **Norma Técnica ABNT NBR ISO/IEC 27002:2005** - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação;

e) **Resolução nº 22.780/2008 - Política de Segurança da Informação da Justiça Eleitoral** - documento que registra as diretrizes da Alta Direção sobre o tema segurança da informação;

f) **Constituição Federal, art. 37, *caput* -** artigo em que se registra que a administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência;

g) **Instrução Normativa nº 1/2008, Gabinete de Segurança Institucional - Presidência da República, art. 5º, inciso VII -** disciplina a Gestão de Segurança da Informação e Comunicações na administração pública federal, direta e indireta, e dá outras providências;

h) **Norma Técnica - Gabinete de Segurança Institucional - Presidência da República - Norma Complementar nº 03/IN01/DSIC/GSIPR –** diretrizes para elaboração da Política de Segurança da Informação e Comunicações nos órgãos e entidades da administração pública Federal;

i) **Resolução nº 90/2009/CNJ, arts. 10 e 13 -** dispõe sobre a gestão da tecnologia da informação.

6 RELAÇÃO COM A NBR/ISO/IEC 27001:2005

SEÇÃO	CONTROLE
Anexo A	A.7 – Gestão dos ativos A.10.1.3 – Segregação de funções A.10.4.1 – Controle contra códigos maliciosos A.10.5 – Cópias de segurança A.10.6.2 – Segurança dos serviços de rede A.10.8 – Troca de informações A.11.2 – Gerenciamento de acesso do usuário A.11. 3 – Responsabilidades do usuário A.11.4 – Controle de acesso à rede A.11.5 – Controle de acesso ao sistema operacional A.11.6 – Controle de acesso à aplicação e à informação A.11.7 – computação móvel e trabalho remoto A.13 – Gestão de incidentes de segurança da informação A.15 – Conformidade

7 CONCEITOS E DEFINIÇÕES

7.1 Segurança da Informação [ABNT NBR ISO/IEC 27002]: preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confidencialidade, podem também estar envolvidas;

7.2 Outros termos: vide dicionário de termos e siglas.

NORMAS DE SEGURANÇA

8 DISPOSIÇÕES GERAIS

8.1 Os recursos de tecnologia da informação do Tribunal somente podem ser utilizados para execução de atividades pertinentes e de interesse da instituição.

8.2 O desenvolvimento de sistemas e as atividades especificas de TI deverão ser realizados exclusivamente por servidores da Secretaria de Tecnologia da Informação – STI –, que deverão estar aptos a prestar suporte e manutenção dos produtos por ela homologados.

8.3 Os usuários devem ter acesso unicamente aos recursos de tecnologia da informação que forem indispensáveis à realização de suas atividades.

8.4 Os acessos aos recursos de tecnologia da informação somente serão permitidos mediante identificação, autenticação e a respectiva autorização dos usuários.

8.5 Ao usuário devem ser disponibilizadas contas de acesso pessoal intransferíveis e únicas por ambiente ou sistema de informação.

8.5.1 Os visitantes poderão ter acesso aos recursos de tecnologia da informação do Tribunal (equipamentos, rede, internet, etc) desde que sob supervisão e responsabilidade de um servidor do Tribunal, que deverá providenciar à Secretaria de Tecnologia da Informação – STI – conta e senha de acesso especifico.

8.6 O usuário ficará responsável por todos os acessos realizados por meio de sua conta de identificação.

8.7 O usuário deve zelar pelo sigilo de sua(s) senha(s) de acesso, sendo responsável pelos possíveis danos que o seu uso vier a ocasionar.

8.8 É proibida a conexão de quaisquer recursos de tecnologia da informação à rede local, a estações de trabalho e a quaisquer outros ativos sem autorização da Secretaria de Tecnologia da Informação – STI –, após a devida análise técnica e de risco.

8.9 Os gestores das unidades do Tribunal devem estabelecer critérios que assegurem a segregação de funções, para que nenhum usuário detenha controle de um processo na sua totalidade, com vistas à redução de risco de mau uso acidental ou deliberado dos sistemas ou processos.

8.10 Os gestores das unidades do Tribunal, em seu âmbito, devem promover

a disseminação do conhecimento no uso dos recursos de tecnologia da informação e sistemas de informação, para garantir a continuidade das operações de seus processos.

9 COMPROMETIMENTO DOS USUÁRIOS

9.1 Os usuários devem ter ciência e assinar termo de responsabilidade e confidencialidade, disponibilizado eletronicamente, pela utilização dos recursos de tecnologia da informação e pela segurança das informações.

9.1.1 Os usuários que necessitarem de privilégios de administração de recursos de tecnologia da informação para uso restrito às necessidades dos serviços, previamente justificados e aprovados pela chefia imediata e pela STI, devem assinar termo de responsabilidade específico.

9.2 Os usuários devem preservar o sigilo das informações utilizadas, dentro e fora das dependências do Tribunal.

9.3 As práticas de segurança da informação do Tribunal devem ser seguidas e disseminadas por todos os seus usuários.

10 RESPEITO À PROPRIEDADE INTELECTUAL

10.1 A utilização de recursos de tecnologia da informação no ambiente do Tribunal deve respeitar a legislação vigente referente à proteção da propriedade intelectual (direitos autorais, *softwares*, e patentes).

10.2 Todo projeto desenvolvido no âmbito do Tribunal e com seus recursos é de exclusiva propriedade deste, não podendo os usuários participantes alegar propriedade de qualquer natureza.

11 CAPACITAÇÃO DOS USUÁRIOS

11.1 O conhecimento em segurança da informação deve ser constantemente difundido de forma a propiciar a conscientização de sua importância para as atividades do Tribunal.

11.2 Os usuários devem estar formalmente comunicados sobre a política de segurança da informação e suas normas aplicáveis, para minimizar os riscos à segurança da informação.

11.3 Todos usuários devem estar formalmente comunicados sobre as

responsabilidades administrativas, legais e sanções decorrentes da má utilização dos recursos colocados à sua disposição.

12 USO DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO

12.1 Os usuários são responsáveis pelos recursos de tecnologia da informação por eles utilizados, devendo contribuir para manter o seu bom funcionamento e, quando necessário, procurar sua manutenção na STI.

12.2 A disponibilização dos recursos de tecnologia da informação do Tribunal compete exclusivamente a STI.

12.3 Compete a STI a implementação de sistemas ou procedimentos que possam restringir o uso indevido de dispositivos de entrada e saída (USB, CD Rom, etc.) nas estações de trabalho e dispositivos móveis, quando entender necessário para segurança da informação e integridade de seu parque computacional.

12.4 A solicitação de empréstimo de recursos de tecnologia da informação do Tribunal deverá ser feita formalmente à STI.

12.4.1 O usuário que solicitar o empréstimo é responsável pela guarda e conservação do recurso de tecnologia da informação até sua devolução.

12.4.2 Na devolução dos recursos de tecnologia da informação, o usuário que os utilizou deve remover todos os arquivos de sua responsabilidade, além de todas as mídias removíveis, bem como realizar as respectivas copias de segurança (*backup*), quando necessário.

12.4.3 O Tribunal não se responsabiliza por dados, informações e dispositivos computacionais do usuário, que porventura venham a se perder em decorrência de empréstimos de seus recursos de tecnologia da informação.

12.5 As impressoras e multifuncionais são destinadas à manipulação e/ou impressão de documentos de interesse do TRE-MG, assim como outros recursos de TI.

12.6 Os documentos físicos impressos e escaneados devem ser retirados dos equipamentos o quanto antes, evitando assim que pessoas não autorizadas tenham acesso aos seus conteúdos.

12.7 A cópia de segurança (*backup*) dos arquivos de dados armazenados nas

estações de trabalho ou nos dispositivos móveis (*notebooks, tablets*, etc) é de responsabilidade do usuário, cabendo a ele garantir sua integridade e segurança.

12.7.1 Compete à STI fornecer orientações e recursos necessários à realização das cópias de segurança (*backup*).

12.8 A STI será responsável por manter cópias de segurança (*backup*) das bases de dados e informações contidas nos computadores servidores do ambiente computacional de produção, devendo criar os procedimentos para sua realização periódica, bem como procedimentos de restauração de informações, quando necessário.

12.9 O usuário que necessitar restaurar informações contidas nas cópias de segurança das bases de dados armazenadas nos computadores servidores do Tribunal deve solicitar formalmente à chefia imediata, informando o período e o motivo da restauração.

12.9.1 Após análise e aprovação da solicitação de restauração, a chefia imediata deve encaminhá-la à STI para análise e providências.

12.10 A restauração de cópia de segurança realizada nos computadores servidores do Tribunal somente poderá ser realizada pela STI.

12.11 Ficam reservados, preferencialmente, os finais de semana e feriados, para paralisações programadas para manutenções e atualizações dos serviços informatizados e da rede local.

12.11.1 Em casos excepcionais e urgentes poderão ser efetuadas manutenções em outros dias e horários previamente comunicados e autorizados pela administração.

12.11.2 A paralisação programada de quaisquer serviços disponibilizados pelo Tribunal deve ser comunicada com antecedência aos usuários, indicando os períodos de indisponibilidade.

13 SEGREGAÇÃO DE TAREFAS

13.1 A segregação de tarefas no tratamento da informação deve garantir que o controle das tarefas de um processo seja compartilhado. É vetado que apenas um único usuário possua controle de um processo por inteiro.

13.2 As atividades de controle e execução devem ser realizadas por usuários distintos, de forma a garantir a verificação da integridade do processo.

13.3 O controle das atividades realizadas pelo usuário deve ser executado pelo seu chefe imediato, a fim de garantir a rastreabilidade do processo e posterior auditoria.

14 INCLUSÃO, ALTERAÇÃO E EXCLUSÃO DE USUÁRIOS

14.1 A inclusão, alteração e exclusão dos usuários serão vinculadas automaticamente às bases de dados de pessoal mantidas pela Secretaria de Gestão de Pessoas – SGP.

14.1.1 Os usuários terceirizados deverão ter seus dados atualizados pelos fiscais dos respectivos contratos.

14.2 O titular das unidades é responsável por informar antecipadamente à SGP ou ao fiscal de contrato, no caso de terceirizados, a movimentação ou a saída de qualquer usuário alocado em suas respectivas unidades, dadas as implicações na manutenção de contas de acesso à rede local, sistemas eleitorais e administrativos e correio eletrônico.

14.2.1 Compete ao titular da unidade ou fiscal de contrato, quando for o caso, solicitar à STI e aos setores competentes a inclusão ou exclusão de usuários nos diversos sistemas informatizados utilizados pelo setor.

14.2.2 Será de responsabilidade do titular da unidade ou fiscal de contrato o acesso indevido ou a manipulação de dados realizada por usuário cujo bloqueio ou cancelamento não for solicitado tempestivamente.

14.3 Deve ser adotado como padrão para as contas dos usuários e para os endereços de correio eletrônico das caixas pessoais o formato nome.sobrenome@tre-mg.jus.br., para garantia de identificação clara e imediata do usuário.

14.3.1 A STI deve disponibilizar opções de endereço de *e-mail* para o usuário, conforme combinações possíveis entre seu nome e sobrenomes, devendo sua escolha recair sobre uma delas.

14.3.2 No caso da ocorrência de homônimo, não havendo mais opções disponíveis ou por estar devidamente justificado, o usuário poderá requerer à STI que seja criada uma conta no padrão nome1.nome2@tre-mg.jus.br, desde que haja coerência e clara associação entre o nome de *e-mail* proposto e a identificação do usuário.

14.4 Não é permitida a criação de *e-mail* fora dos padrões estabelecidos,

para que seja garantida a identificação do remetente.

14.5 Na liberação da conta de acesso do usuário à rede local, deve ser fornecida uma senha temporária que deve ser alterada obrigatoriamente no primeiro acesso realizado.

14.6 A chefia imediata é responsável por definir o perfil de acesso à rede local dos usuários lotados em sua área e por solicitar à STI os respectivos acessos.

14.7 Para o fim de manutenção do histórico do usuário, uma designação de conta de usuário nunca poderá ser utilizada por outro, mesmo que tenha sido inativada a qualquer tempo.

14.8 A STI é responsável por definir o padrão dos perfis básicos de acesso à rede local dos usuários lotados em cada área, cabendo à chefia imediata solicitar a alteração dos respectivos acessos, quando julgar necessário.

15 UTILIZAÇÃO DE SENHAS

15.1 Os meios de identificação, como senhas e certificados digitais, são únicos, pessoais e intransferíveis, não devendo ser compartilhados. Sua utilização ou consequências decorrentes do uso indevido são de responsabilidade exclusiva do usuário.

15.2 A senha da conta de acesso aos recursos de TI deve ser escolhida de acordo com os critérios definidos pela STI para garantir a máxima segurança.

15.3 As senhas de acesso aos recursos de TI terão seus prazos definidos em função do vinculo, da situação funcional, do tipo de sistema, do perfil de acesso, providenciado pelos gestores, que darão ampla divulgação aos usuários.

16 UTILIZAÇÃO DE ASSINATURA DIGITAL/ELETRÔNICA

16.1 Os documentos eletrônicos produzidos no Tribunal terão garantia de autoria, autenticidade e integridade asseguradas, mediante utilização de assinatura nas seguintes modalidades:

- assinatura digital: baseada em certificado digital;
- assinatura eletrônica: mediante uso de login e senha.

16.2 Os documentos eletrônicos produzidos no Tribunal deverão

obrigatoriamente ser assinados eletronicamente ou digitalmente, conforme exigência definida por tipo de documento ou de processo.

16.3 O certificado digital a ser utilizado no Tribunal deve ser do tipo A3 emitido por autoridade certificadora credenciada na Infraestrutura de Chaves Públicas Brasileira – ICP – Brasil.

16.4 Os documentos eletrônicos produzidos no Tribunal cuja modalidade de assinatura digital por certificado digital não for exigida poderão ser assinados mediante uso de assinatura eletrônica.

16.5 O Tribunal proverá os usuários internos de certificado digital e respectiva mídia de armazenamento na medida da necessidade e da implantação das funcionalidades tecnológicas que exijam o seu uso.

16.5.1 Caberá a STI as providências para o fornecimento dos certificados digitais, devendo formalizar sua entrega aos usuários e dar ciência de sua validade.

16.6 O detentor de certificado digital é responsável por sua utilização, guarda e conservação.

16.7 O certificado digital será inutilizado nas seguintes situações:

- digitação sucessiva de senha incorreta na tentativa de utilização do certificado;
- dano ou formatação da mídia que armazena o certificado;
- esquecimento da senha de utilização do certificado;
- perda ou extravio da mídia que contém o certificado;
- vencimento de sua data de validade.

16.8 Compete ao usuário detentor de certificado digital:

16.8.1 Apresentar tempestivamente, à autoridade certificadora, a documentação necessária à emissão do certificado digital;

16.8.2 Estar de posse do certificado digital para o desempenho de atividades profissionais que requeiram o uso deste;

16.8.3 Solicitar à autoridade certificadora, de acordo com procedimentos definidos para esse fim, a imediata revogação do certificado em caso de inutilização e comunicar à STI.

16.8.4 Observar as diretrizes definidas para criação e utilização de senhas de acesso ao certificado;

16.8.5 Manter a mídia de armazenamento dos certificados digitais em local seguro e com proteção física contra acesso indevido, descargas eletromagnéticas, calor excessivo e outras condições ambientais que representem risco à integridade dessas mídias;

16.8.6 Solicitar à STI o fornecimento de nova mídia ou certificado digital nos casos de inutilização;

16.8.7 Acompanhar a data de encerramento da validade do certificado e solicitar tempestivamente sua reposição.

17 UTILIZAÇÃO DE ESTAÇÕES DE TRABALHO

17.1 As estações de trabalho fornecidas devem possuir configurações de *hardware* e *software* homologadas pela STI.

17.2 Nas estações de trabalho somente devem ser instalados *softwares* e aplicativos padronizados e homologados pela STI e necessários à execução das atividades das respectivas unidades.

17.3 A posse e o gerenciamento da licença dos *softwares* credenciados pelo Tribunal são de responsabilidade da STI.

17.4 Não é permitida a abertura dos gabinetes das estações de trabalho, bem como a modificação por qualquer motivo da configuração do *hardware*.

17.5 Cabe somente a STI autorizar ou realizar modificações internas nas estações de trabalho.

17.6 O usuário deve informar à STI quando identificados danos ou violação da integridade física do equipamento por ele utilizado.

17.7 O usuário não deve alterar as configurações padronizadas pela STI dos *softwares* e aplicativos instalados nas estações de trabalho.

17.8 O usuário deve bloquear a estação de trabalho quando se ausentar, considerando que será o responsável por eventuais consequências advindas de manuseios indevidos realizados por meio de sua conta aberta.

17.9 Em caso de dúvidas para realização de procedimentos operacionais, como, por exemplo, o bloqueio das estações e as cópias de segurança de seus arquivos, o usuário deve sempre buscar orientação e suporte da

STI.

17.10 O usuário deve zelar pela sua estação de trabalho, sendo proibido:

- a colagem de adesivos;
- a mudança de local;
- o consumo de alimentos próximo às estações de trabalho.

18 UTILIZAÇÃO DE DISPOSITIVOS MÓVEIS DE TI

18.1 Os dispositivos móveis de TI devem ser utilizados para a execução de atividades de interesse do Tribunal.

18.2 Os dispositivos móveis de TI devem ser fornecidos pelo Tribunal, quando justificado e autorizado, não sendo permitido o uso de equipamentos particulares dos servidores para a execução de atividades de interesse do Tribunal, salvo em casos excepcionais e com autorização expressa da STI e da chefia imediata.

18.2.1 O Tribunal não se responsabilizará pela utilização de equipamentos particulares no desenvolvimento de atividades de seu interesse.

18.3 Os dispositivos móveis de TI devem possuir configurações de *hardware* e *software* homologadas pela STI.

18.3.1 É vedado ao usuário modificar as configurações do *hardware*.

18.3.2 O usuário não deve alterar as configurações dos *softwares* instalados nos dispositivos móveis.

18.3.3 Nestes dispositivos somente devem ser instalados *softwares* autorizados pela STI e necessários à execução das atividades de interesse das unidades.

18.4 A posse e o gerenciamento da licença dos *softwares* instalados nos dispositivos móveis de TI, credenciados pelo Tribunal, são de responsabilidade da STI.

18.5 O usuário deve sempre informar à STI quando identificados danos ou violação da integridade física dos dispositivos móveis de TI por ele utilizados.

18.6 Em caso de dúvidas para realização de procedimentos operacionais como, por exemplo, bloqueio das estações e cópias de segurança de seus arquivos, o usuário deve sempre buscar orientação e suporte na STI.

18.7 Os dispositivos móveis de TI devem ser adequadamente utilizados, armazenados, transportados e protegidos, a fim de manter sua conservação e segurança, em ambientes externos ou internos ao Tribunal, inclusive quando não utilizados.

18.7.1 Os usuários devem observar as boas práticas de segurança na utilização dos dispositivos móveis de TI em locais públicos.

18.8 Os dispositivos móveis de TI estão sujeitos a monitoramento e auditoria para o fim de identificação de quaisquer vulnerabilidades que representem ameaças à rede local.

18.9 A solicitação de empréstimo dos dispositivos móveis de TI deve ser feita formalmente à STI.

18.9.1 O usuário que solicitou o empréstimo é responsável pela guarda e conservação dos dispositivos móveis de TI até sua devolução.

18.9.2 Na devolução dos dispositivos móveis de TI, o usuário que o utilizou deve remover todos os arquivos pessoais armazenados no equipamento, realizando cópias de segurança das informações e arquivos, se for o caso.

19 COMPARTILHAMENTO E ARMAZENAMENTO DE INFORMAÇÕES

19.1 Os diretórios disponibilizados na rede local estão sujeitos a monitoramento a fim de preservar a integridade do ambiente.

19.2 As regras para compartilhamento e armazenamento de informações das unidades do Tribunal devem observar:

19.2.1 É de responsabilidade da STI disponibilizar diretórios nos servidores de rede conforme a estrutura organizacional.

19.2.2 São definidas:

- Área pública: área destinada à troca de arquivos de trabalho entre as unidades do Tribunal, liberada a todos os usuários previamente cadastrados.

- Área da unidade: área destinada ao armazenamento

de arquivos de trabalho das unidades do Tribunal, disponível apenas para os usuários da unidade.

19.2.3 Não será disponibilizada área para uso pessoal nos servidores de rede.

19.2.4 Todo o acesso e o conteúdo armazenado nos diretórios disponibilizados pela STI são de responsabilidade do titular da unidade ou da pessoa por ele formalmente designada.

19.2.5 Cabe ao titular ou pessoa por ele formalmente designada:

- Gerenciar o uso do espaço em disco, descartando as informações desnecessárias.
- Solicitar autorização especial para acesso aos diretórios e arquivos neles armazenados, caso a configuração de acesso padrão implementada pela STI não atenda aos seus requisitos.

20 ANTIVÍRUS

20.1 O antivírus instalado nas estações de trabalho deve estar atualizado e com a configuração de autoproteção ativa.

20.2 A rede local deverá ser protegida por antivírus com monitoramento constante para detecção e eliminação de vírus de computadores no servidor de correio e nas estações de trabalho.

20.3 O usuário deve utilizar o antivírus sempre que receber qualquer arquivo proveniente de fora da rede local.

20.4 O usuário não deve cancelar o processo de verificação de vírus quando este for iniciado automaticamente na sua estação de trabalho.

21 MANUTENÇÃO DOS RECURSOS DE TI

21.1 O usuário deve solicitar manutenção corretiva à STI quando identificar problemas no seu recurso de tecnologia da informação.

21.2 O usuário deve acompanhar o técnico durante a manutenção do recurso de tecnologia da informação quando ocorrer no seu local de trabalho ou quando o atendimento for realizado por meio de ferramenta de acesso remoto.

21.3 Caso seja necessária a retirada do equipamento para manutenção, deverá haver autorização formal do responsável pelo bem patrimonial.

22 ACESSO REMOTO À REDE

22.1 É proibido o acesso remoto à rede local do Tribunal através de computador que não esteja integrado à rede da Justiça Eleitoral.

22.1.1 Excluem-se os casos excepcionais, através de VPN (Virtual Private Network – Rede Privada Virtual) com usuário e senha pré-autorizados pela STI.

22.1.2 Exclui-se o acesso pela extranet.

22.1.3 Exclui-se o acesso externo ao *e-mail* corporativo, desde que solicitado formalmente pelo usuário e aprovado pela Diretoria-Geral.

22.2 O acesso remoto à rede local está sujeito ao monitoramento e à auditoria para o fim de identificação de quaisquer vulnerabilidades que representem ameaças à rede local.

22.3 Em nenhuma hipótese o acesso externo poderá configurar horas de trabalho com o fim de remuneração extraordinária, visto que tal acesso é realizado por exclusiva opção do usuário.

23 REGRAS E ÉTICA NO USO DE *E-MAIL*

23.1 Todo servidor do Tribunal, assim como profissionais terceirizados e estagiários, desde que de interesse deste Tribunal, receberão um único endereço de correio eletrônico nos padrões estabelecidos pelo TRE-MG, devendo responsabilizar-se por ele e por toda correspondência por ele gerada.

23.1.1 O servidor poderá escolher seu endereço eletrônico, de acordo com o padrão definido pelo TRE-MG.

23.1.2 O servidor que desejar alterar seu endereço eletrônico poderá fazê-lo de acordo com padrões definidos pelo Tribunal. As mensagens enviadas para seu *e-mail* antigo serão redirecionadas para o novo endereço durante tempo definido pela STI.

23.2 O correio eletrônico do TRE-MG será utilizado como ferramenta de comunicação institucional de uso obrigatório por seus servidores.

23.3 Toda mensagem de correio eletrônico deverá obrigatoriamente ter a identificação do remetente e inclusive dela constar seu vínculo com o Tribunal.

23.4 O correio eletrônico do TRE-MG possui recursos limitados de armazenamento e disponibilidade que deverão ser administrados pela STI.

23.4.1 A ampliação dos recursos de *e-mail* será de acordo com a disponibilidade dos recursos da infraestrutura de TI.

23.4.2 A STI poderá limitar a quantidade e o tamanho das mensagens de *e-mail*, os tipos de arquivos anexados, bem como o número de destinatários, de acordo com os recursos disponíveis.

23.4.3 A área de armazenamento de *e-mail* específica para cada usuário está sujeita a cotas que, quando alcançadas, impedirão o recebimento e envio de novas mensagens, retornando à sua normalidade assim que o usuário liberar espaço em suas caixas de correio.

23.5 O serviço de correio eletrônico disponibilizado aos usuários é considerado de propriedade do Tribunal com concessão de uso aos usuários no período em que estão prestando serviços ao Tribunal.

23.6 A inserção automática ou manual de endereço eletrônico do domínio tre-mg.jus.br em listas de mala direta, anúncios comerciais, entre outros, é de inteira responsabilidade do usuário, que responderá por eventuais danos causados à rede por uso indevido.

23.7 O recebimento de mensagens cujos conteúdos não expressam os interesses ou possam colocar em risco as informações do Tribunal deve ser recusado pelo serviço de correio eletrônico.

23.8 Todas as mensagens são passíveis de monitoramento e gravação quanto aos endereços de destino e origem (IP de origem, *e-mail* do remetente, IP de destino, *e-mail* do destinatário) e poderão ser usados para estabelecer critérios de recusa.

23.9 As caixas postais do domínio tre-mg.jus.br estão sujeitas a monitoramento e auditoria, respeitando-se os aspectos legais pertinentes.

23.10 O serviço de correio eletrônico disponibilizado pelo Tribunal se destina somente à transmissão de mensagens de seu interesse e relacionadas à execução de trabalhos pertinentes ao Tribunal, sendo vedado:

23.10.1 Transmissão de conteúdo potencialmente perigoso, tais como arquivos executáveis ou outros que possam conter vírus ou outras ameaças;

23.10.2 Divulgação de conteúdos pornográficos, eróticos, ofensivos ou que incentivem a violência, discriminação de raça ou credo e outros que não estejam relacionados às atribuições do Tribunal;

23.10.3 O envio simultâneo de grande quantidade de mensagens de *e-mail (junk mail* ou *spam*) que, de acordo com a capacidade técnica da rede, seja prejudicial ao seu desempenho. Neste contexto estão qualquer tipo de mala direta contendo publicidade, anúncios, informativos, textos de cunho pessoal, manifestações e criticas de qualquer natureza, propaganda política e outros.

23.10.4 O reenvio ou, de qualquer forma, propagar mensagens em cadeia ou "pirâmides", independentemente da vontade do destinatário de receber tais mensagens.

23.11 Compete à STI a definição de regras automatizadas de utilização do correio eletrônico.

23.12 Os *e-mails* e contas de acesso dos servidores em períodos de ausência prolongadas, por ocasião de cessão, transferência, licenças e afastamentos diversos do serviço, poderão ficar suspensos neste tempo, conforme análise de cada caso, devendo ser restabelecidas quando do retorno às atividades no Tribunal.

23.12.1 Caberá à Secretaria de Gestão de Pessoas – SGP – a atualização das informações relativas aos afastamentos para que seja possível a adoção da suspensão temporária dos acessos.

23.13 Listas de *e-mail* das unidades serão criadas automaticamente contendo os servidores lotados na unidade. Caberá à SGP informar eventuais criação e extinção de unidades para a manutenção destas listas.

23.14 Demais listas de *e-mail* devem ser formalmente solicitadas à STI contendo o motivo da sua criação, a sugestão do nome da lista, a indicação de um gestor, a relação dos *e-mails* dos participantes da lista, bem como o estabelecimento de um período de vigência.

23.14.1 Uma lista de e-mail tem que conter no mínimo dois usuários, sendo um deles, obrigatoriamente, o seu gestor.

23.14.2 O gestor da lista de *e-mail* é responsável pela sua manutenção,

devendo solicitar à STI a inclusão e exclusão de usuários sempre que necessário e o seu cancelamento quando não for mais necessária.

23.14.3 Nas listas de *e-mail* do TRE-MG é proibida a inclusão de endereços de correio eletrônico que não sejam da Justiça Eleitoral.

23.14.4 As listas serão excluídas automaticamente ao final de seu período de vigência, informado pelo Gestor, desde que não seja seu prazo de vigência prorrogado.

23.15 O envio de mensagens para muitos destinatários poderá ser realizado exclusivamente para o fim de interesse do Tribunal, devendo-se observar as boas práticas do procedimento, tais como: tamanho reduzido, sem anexação de imagens, sem anexação de arquivos grandes; de tal forma a evitar o impacto na rede de comunicação de dados. Em caso de necessidade ou dúvida, a STI deverá ser consultada.

23.16 O correio eletrônico do Tribunal é um meio de comunicação oficial e, por isso, não devem ser utilizadas em seu texto palavras ofensivas, frases pejorativas, ou termos indesejáveis que possam denegrir a qualidade das mensagens e a sua comunicação.

23.17 Mensagens recebidas por endereçamento incorreto serão retornadas imediatamente ao remetente.

23.18 O usuário deve administrar sua conta de *e-mai*l devendo manter somente mensagens importantes para o desenvolvimento de seu trabalho no momento, e sempre providenciar copias destas em outros meios (*backup*) para que possa ser possível a manutenção de área liberada para o continuo recebimento de novos *e-mails*.

23.19 A solicitação de criação de nova senha só poderá ser efetuada pelo titular da conta de correio eletrônico.

24 REGRAS E ÉTICA NO USO DA INTERNET/INTRANET

24.1 O acesso aos sistemas, serviços internos e à internet deve ocorrer exclusivamente para o fim de interesse da Justiça Eleitoral.

24.2 A STI deverá monitorar o tráfego individual de dados na rede, para garantir o compartilhamento e disponibilidade dos recursos de TI a todos os usuários:

24.2.1 Notificando os usuários que estejam prejudicando o uso dos

recursos de internet ou colocando em risco a segurança da rede.

24.2.2 Orientando e eventualmente bloqueando acesso para que se evite transferência de grande volume de dados e a navegação em sítios suspeitos ou que contenham conteúdo que não esteja em acordo com os interesses do Tribunal;

24.2.3 Viabilizando recursos para casos de necessidade de transferência de grandes volumes de informação, identificados e solicitados pelos titulares das unidades do Tribunal.

24.3 O acesso aos serviços da internet e da intranet deve ser realizado mediante autenticação do usuário.

24.4 Os usuários podem ter diferentes níveis de acesso de acordo com os perfis definidos pelos titulares das unidades.

24.5 Equipamentos do Tribunal ou a seu serviço somente podem acessar serviços de internet e intranet através de conexões providas pela STI.

24.6 A importação de arquivos oriundos da internet somente deve ocorrer quando utilizado para o cumprimento das atividades de interesse do Tribunal.

24.6.1 Sempre que for necessária e imprescindível a importação de grandes arquivos que possam impactar a rede, a STI deverá autorizar e orientar quanto ao correto procedimento para sua realização.

24.6.2 A importação de grandes arquivos, quando autorizada pela STI, deverá ser executado em horários fora do expediente.

24.6.3 A definição de parâmetros para viabilizar *download/upload* de arquivos deverá ser regulamentada pela STI.

24.7 A STI, a partir de análise de registro de acesso, pode limitar ou até mesmo bloquear o consumo de internet por usuário, quando entender que sua utilização extrapola os níveis médios de consumo aceitáveis e causa impactos na rede, sempre dando ciência aos usuários e às unidades interessadas.

24.8 A STI deverá monitorar e administrar o acesso dos *links* da rede, limitando ou liberando recursos, provisória ou permanentemente, no intuito de garantir disponibilidade de rede para as aplicações institucionais de relevância, conforme interesses do Tribunal.

24.9 Os problemas verificados pelos usuários, ocorridos durante o acesso

aos serviços da intranet ou extranet, devem ser comunicados à STI para que providencie manutenção adequada.

24.10 A utilização de recursos como compartilhadores de arquivos, comunicadores via internet e *software* de conversa *on-line* está restrita a ferramentas previamente autorizadas pela STI.

24.11 O acesso a *sites* de relacionamento do tipo redes sociais, *blogs* e *chats* deverá ser exclusivo aos serviços e interesses do TRE-MG.

24.12 Não é permitido acessar, armazenar ou transferir informações de conteúdo pornográfico, erótico, ofensivo ou que incitem a violência, discriminação de etnia ou credo, ou que violem as leis de direitos autorais.

24.13 Não é permitido o acesso à internet simultaneamente por meio da rede da Justiça Eleitoral e outro provido diretamente por operadora, colocando a rede do Tribunal em situação de grande risco à segurança da informação.

24.14 Não é permitido o uso de programas de envio de mensagens em massa ou mala direta nem de cooperação que possam sobrecarregar ou indisponibilizar a rede local ou o acesso à internet.

25 DISPOSIÇÕES FINAIS

25.1 Fica assegurado à STI, a qualquer tempo, tomar as medidas necessárias quando evidenciados os riscos à segurança da informação.

25.2 Os usuários e funcionários são responsáveis por suas contas, senhas e por qualquer ação que venha ferir a confidencialidade, a integridade e a disponibilidade da informação.

25.3 O uso indevido dos recursos de tecnologia da informação do Tribunal é passível de sanção disciplinar, de acordo com a legislação vigente e demais normas aplicadas à matéria.

26 COMPETÊNCIAS E RESPONSABILIDADES

26.1 As competências da Comissão de Segurança da Informação do Tribunal estão definidas na Política de Segurança da Informação (Resolução nº 22.780/2008/TSE).

26.2 Compete ainda à Comissão:

26.2.1 Manter contato permanente e estreito com a Comissão de Segurança da Informação do Tribunal Superior Eleitoral para o trato de assuntos relativos à segurança da informação.

26.2.2 Propor novas normas e procedimentos relativos à segurança da informação e comunicações no âmbito do Tribunal.

26.2.3 Revisar anualmente as normas da política de segurança da informação e, quando necessário, promover as alterações necessárias.

26.3 Compete à chefia imediata dos usuários:

26.3.1 Disseminar permanentemente a Política de Segurança da Informação, bem como assegurar que todos os servidores e colaboradores estejam cientes de suas responsabilidades no contexto da Justiça Eleitoral.

26.4 Compete aos Usuários:

26.4.1 Conhecer e cumprir as normas da Política de Segurança da Informação e suas atualizações.

26.4.2 Informar a chefia imediata sobre eventos e incidentes que comprometam ou possam comprometer os artigos das normas da Política de Segurança da Informação.

27 PENALIDADES

27.1 O Tribunal adotará as sanções legais cabíveis contra qualquer usuário ou entidade que venha a praticar atos que violem a Política de Segurança da Informação.

28 VIGÊNCIA E ATUALIZAÇÃO

28.1 Esta norma entra em vigor a partir da data de sua publicação, e sua atualização ocorrerá sempre que se fizer necessário através de proposição pela Comissão de Segurança da Informação, aprovação da Diretoria-Geral e publicação nos canais competentes para ciência aos usuários do Tribunal.

29 EXCEÇÕES

29.1 Devido à conveniência do negócio de, em alguns casos, comunicar registrando apenas o setor emitente, será admitido o compartilhamento de contas de *e-mail* setoriais, apenas aquelas expressamente aprovadas pela Direção-Geral do Tribunal.

29.1.1 Para as contas de *e-mail* setoriais compartilhadas a que se refere o *caput*, será considerado o responsável em todas as condições estabelecidas nas normas de segurança, incluindo esta, a chefia do respectivo setor.

29.1.2 O responsável pelas contas de *e-mail* compartilhadas deverá zelar especialmente pela segurança da senha compartilhada, trocando-a periodicamente e sempre que houver alteração de pessoal autorizado a utilizar o *e-mail* compartilhado.

29.1.3 Como requisitos específicos de segurança para as contas de *e-mail* compartilhadas, a STI estabelecerá os controles necessários, podendo restringir funcionalidades em caso de potencial vulnerabilidade.

29.1.4 À medida que sejam implementadas funcionalidades específicas em sistemas que substituam a necessidade de *e-mail* compartilhado, tais contas serão desativadas pela STI.

29.1.5 Esta exceção não altera o disposto a respeito de listas de distribuição constantes da norma, sendo a lista preferível ao *e-mail* compartilhado no que couber.

29.2 Demais dúvidas ou exceções a esta norma devem ser analisadas e aprovadas pela Comissão de Segurança da Informação, que emitirá parecer sobre o assunto, incluídos os casos não tratados nas políticas vigentes. A obtenção desta aprovação assegura que todas as alternativas razoáveis foram avaliadas e que os controles compensatórios são adequados para atenuar quaisquer riscos.

TRIBUNAL REGIONAL ELEITORAL DE MINAS GERAIS

ANEXO II

(a que se referem os arts. 3º, 4º e 5º da Resolução nº 945, de 17 de dezembro de 2013)

PSI - N 002	**NORMA GERAL DE SEGURANÇA FÍSICA DE INSTALAÇÕES TRE-MG**
Versão 2.5 21/06/2013	Política de Segurança da Informação da Justiça Eleitoral

SUMÁRIO

1. MATÉRIA DISCIPLINADA

1.1. Dispõe sobre os requisitos de proteção para as instalações físicas do Tribunal Regional Eleitoral de Minas Gerais – TRE-MG.

2. OBJETIVO GERAL

2.1. Estabelecer regras de segurança física para serem implementadas nas salas, portarias, corredores e outras instalações, visando à segurança das pessoas e das informações do TRE-MG.

3. PÚBLICO-ALVO

3.1. Aplica-se a todos os servidores e usuários do Tribunal Regional Eleitoral de Minas Gerais e visitantes.

4. APLICAÇÃO

4.1. Norma de segurança de aplicação interna.

5. REFERÊNCIAS LEGAIS E NORMATIVAS

a) **Lei nº 9.609, de 19 de fevereiro de 1998 -** dispõe sobre a proteção de propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências;

b) **Lei nº 9.279, de 14 de maio de 1996 -** regula os direitos e as obrigações relativas à propriedade intelectual;

c) **Norma Técnica ABNT NBR ISO/IEC 27001:2006** - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação – Requisitos;

d) **Norma Técnica ABNT NBR ISO/IEC 27002:2005** - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação;

e) **Resolução nº 22.780/2008 - Política de Segurança da Informação da Justiça Eleitoral** – documento que registra as diretrizes da Alta Direção sobre o tema segurança da informação;

f) **Constituição Federal, art. 37, *caput* –** artigo em que se registra que a administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência;

g) **Instrução Normativa nº 1/2008, Gabinete de Segurança Institucional - Presidência da República, art. 5º, inciso VII -** disciplina a Gestão de Segurança da Informação e Comunicações na administração pública federal, direta e indireta, e dá outras providências;

h) **Norma Técnica - Gabinete de Segurança Institucional - Presidência da República - Norma Complementar nº 03/IN01/DSIC/GSIPR –** diretrizes para elaboração da Política de Segurança da Informação e Comunicações nos órgãos e entidades da administração pública federal;

i) **Resolução nº 90/2009/CNJ, arts. 10 e 13 –** dispõe sobre a gestão da tecnologia da informação.

6. RELAÇÃO COM A NBR/ISO/IEC 27001:2005

SEÇÃO	CONTROLE
Anexo A	A.9 – Segurança física e do ambiente A.15 – Conformidade

7. CONCEITOS E DEFINIÇÕES

7.1. Segurança da Informação [ABNT NBR ISO/IEC 27002]: preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confidencialidade, podem também estar envolvidas.

7.2. Outros termos: vide dicionário de termos e siglas.

NORMAS DE SEGURANÇA

8. CONTROLE DE ACESSO FÍSICO

8.1. O acesso e a permanência de pessoas nas dependências do Tribunal serão precedidos de identificação, registro e autorização, conforme instituído por regulamentação específica.

9. SEGURANÇA DAS ÁREAS INTERNAS

9.1. Aplicam-se as regulamentações existentes contra ameaças de incêndio, explosões, manifestações civis, inundações e outras formas de desastres naturais ou causados pelo homem, nas áreas internas.

9.1.1. A proteção do ambiente de *datacenter* principal é feita através da sala-cofre.

9.2. É de responsabilidade dos usuários de cada setor o fechamento das portas de entrada e janelas após o encerramento das atividades das áreas.

9.2.1. Os usuários devem estar atentos particularmente às proteções extras das portas e janelas externas localizadas no andar térreo e subsolo.

9.3. É de responsabilidade dos usuários de cada setor o desligamento de todos os equipamentos eletroeletrônicos após o encerramento das atividades das áreas.

9.4. Sistemas de detecção de intrusos serão instalados por profissionais especializados e testados regularmente em prazo não superior a um ano, de forma a cobrir todas as portas e janelas acessíveis.

9.5. As áreas em que não existam pessoas trabalhando permanentemente, como depósitos, almoxarifados, devem possuir um sistema de alarme que permaneça sempre ativado.

9.6. Circuitos fechados de gravação de imagens (CFTV) serão instalados e monitorados nos acessos e dependências do TRE-MG.

9.6.1. As imagens gravadas devem ser periodicamente verificadas e arquivadas por um período, conforme criticidade do ambiente monitorado, para futuras investigações.

9.6.2. O tempo de retenção das imagens deverá ser definido pela tabela de temporalidade padrão e casos específicos, pelos setores competentes, conforme a criticidade de cada local .

9.7. Exercícios de simulação de incêndios devem ser realizados, periodicamente, incluindo pessoas de todos os ambientes, sob supervisão da área responsável.

9.8. Extintores portáteis, de tipos compatíveis com as classes de fogo a ser combatido, serão instalados no ambiente.

9.8.1. Deve ser observado o laudo de regularidade de extintores provido pelo órgão competente.

9.9. Saídas de emergência serão sinalizadas de modo a facilitar a evacuação do edifício.

9.9.1. As saídas de emergência devem estar desobstruídas, a fim de facilitar a evacuação.

9.10. Procedimentos de varreduras eletrônicas, por exemplo, identificação de "grampos" telefônicos, devem ser implementados, a fim de proteger as informações de interceptações ilegais.

9.11. Os veículos que entram e saem da garagem do edifício podem estar sujeitos a vistorias conforme critério da área de segurança.

9.12. As áreas que manipulam informações confidenciais devem ter dispositivo de destruição de documentos impressos, por exemplo, fragmentadoras de papel e mídias.

10. SEGURANÇA DAS ÁREAS DE ACESSO AO DATACENTER, À CENTRAL DE ENERGIA E À REDE DE DADOS

10.1. As áreas de acesso ao *datacenter* correspondem às dependências circunvizinhas ao ambiente deste.

10.2. As áreas de acesso ao *datacente*r serão localizadas de forma a evitar o acesso público, com indicações mínimas do seu propósito e sem sinalizações visuais.

10.3. O trabalho nas áreas de acesso ao *datacenter* deve ser supervisionado por razões de segurança. Os profissionais de serviços de suporte terceirizados devem ter acesso restrito a estas áreas. Este acesso deve ser autorizado e monitorado.

10.4. Materiais comburentes e inflamáveis devem ser guardados de forma segura a uma distância apropriada da área de segurança, em áreas destinadas a este fim.

10.5. As paredes externas dos locais devem possuir construção sólida e as portas externas devem ser protegidas de forma apropriada contra acessos não autorizados, como por exemplo, mecanismos de controle, travas, alarmes, grades, etc.

10.6. Uma área de recepção ou outro meio de controle de acesso físico à área de segurança deve ser usado. O acesso deve ser restrito ao pessoal autorizado.

10.7. Qualquer equipamento de gravação de imagem, vídeo ou som só deve ser utilizado com autorização da Diretoria-Geral.

10.8. Devem ser afixados avisos nas entradas, saídas e corredores de acesso, facilmente visíveis, contendo informações gerais sobre o controle de acesso para as pessoas e alertando sobre as restrições ao acesso público, de tal forma que desestimule as invasões. Exemplo de conteúdo dos avisos:

- É obrigatório o uso de identificação para qualquer pessoa nessas dependências. Os acessos aos recursos e áreas são controlados de acordo com as normas internas e de permissão de acesso. O descumprimento destas regras implicará responsabilidades civis.

10.9. Devem ser afixados em locais visíveis e de fácil acesso os números dos telefones de emergência, por exemplo, brigada de incêndio, segurança, entre outros.

10.10. O acesso físico aos *rack's* de comunicação que contenham equipamentos de conectividade deve ser controlado e, quando for necessária a intervenção de técnicos de fora dos quadros do Tribunal, estes deverão estar acompanhados de servidor designado e com registro de acesso documentado e arquivado.

10.11. O acesso aos quadros de distribuição de cabos de comunicação deve ser controlado e, quando for necessária a intervenção de técnicos de fora dos quadros do Tribunal, estes deverão estar acompanhados de servidor designado e com registro de acesso documentado e arquivado.

11. CONTROLE DA ENTRADA, SAÍDA E MOVIMENTAÇÃO INTERNA DE BENS

11.1. A entrada, a saída ou a movimentação interna de bens (materiais, máquinas, equipamentos e similares) depende de prévia e expressa autorização da área responsável.

11.2. A entrada, a saída e a movimentação interna de bens devem ser registradas por meio de sistema informatizado para posterior controle.

11.3. A saída de bens deve ser realizada mediante entrega da autorização nos pontos de entrada e saídas das instalações do TRE-MG.

11.4. No caso específico de bens de tecnologia da informação, as autorizações devem ter anuência prévia da STI.

12. DISPOSIÇÕES FINAIS

12.1. Fica assegurado à STI, a qualquer tempo, tomar as medidas necessárias quando evidenciados os riscos à segurança da informação.

12.2. Os usuários e funcionários são responsáveis por suas contas, senhas e por qualquer ação que venha ferir a confidencialidade, a integridade e a disponibilidade da informação.

12.3. O uso indevido dos recursos de tecnologia da informação do TRE-MG é passível de sanção disciplinar, de acordo com a legislação vigente e demais normas aplicadas à matéria.

13. PENALIDADES

13.1. O Tribunal adotará as sanções legais cabíveis contra qualquer usuário ou entidade que venha a praticar atos que violem a Política de Segurança da Informação.

14. VIGÊNCIA E ATUALIZAÇÃO

14.1. Esta norma entra em vigor a partir da data de sua publicação, e sua atualização ocorrerá sempre que se fizer necessário através de proposição pela Comissão de Segurança da Informação, aprovação da Diretoria-Geral e publicação nos canais competentes para ciência aos usuários do TRE-MG.

15. EXCEÇÕES

15.1. Qualquer exceção a esta norma deve ser aprovada pela Comissão de Segurança da Informação. A obtenção desta aprovação assegura que todas as alternativas razoáveis foram avaliadas e que os controles compensatórios são adequados para atenuar quaisquer riscos.

TRIBUNAL REGIONAL ELEITORAL DE MINAS GERAIS

ANEXO III

(a que se referem os arts. 3º, 4º e 5º da Resolução nº 945, de 17 de dezembro de 2013)

PSI - N 003	**NORMA ESPECÍFICA DE SEGURANÇA PARA PROFISSIONAIS DE TI – TRE-MG**
Versão 2.5 21/06/2013	Política de Segurança da Informação da Justiça Eleitoral

SUMÁRIO

1 MATÉRIA DISCIPLINADA

1.1 Dispõe sobre os aspectos de segurança para usuários com privilégios de administradores dos recursos de tecnologia da informação do Tribunal Regional Eleitoral de Minas Gerais – TRE-MG.

2 OBJETIVO GERAL

2.1 Apresentar e descrever as ações de segurança e definir critérios para a manipulação e a disponibilização dos recursos de tecnologia da informação para usuários com privilégios especiais de administradores do ambiente informatizado.

3 PÚBLICO-ALVO

3.1 Aplica-se aos administradores dos recursos de infraestrutura de TI do Tribunal Regional Eleitoral de Minas Gerais.

4 APLICAÇÃO

4.1 Norma de segurança de aplicação interna.

5 REFERÊNCIAS LEGAIS E NORMATIVAS

a) **Lei nº 9.609, de 19 de fevereiro de 1998 -** dispõe sobre a proteção de propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências;

b) **Lei nº 9.279, de 14 de maio de 1996 -** regula os direitos e as obrigações relativas à propriedade intelectual;

c) **Norma Técnica ABNT NBR ISO/IEC 27001:2006** - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação – Requisitos;

d) **Norma Técnica ABNT NBR ISO/IEC 27002:2005** - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação;

e) **Resolução nº 22.780/2008 - Política de Segurança da Informação da Justiça Eleitoral** – documento que registra as diretrizes da Alta Direção sobre

o tema segurança da informação;

f) **Constituição Federal, art. 37, *caput* –** artigo em que se registra que a administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência;

g) **Instrução Normativa nº 1/2008, Gabinete de Segurança Institucional - Presidência da República, art. 5º, inciso VII -** disciplina a Gestão de Segurança da Informação e Comunicações na administração pública federal, direta e indireta, e dá outras providências;

h) **Norma Técnica - Gabinete de Segurança Institucional - Presidência da República - Norma Complementar nº 03/IN01/DSIC/GSIPR –** diretrizes para elaboração da Política de Segurança da Informação e Comunicações nos órgãos e entidades da administração pública federal;

i) **Resolução nº 90/2009/CNJ, arts. 10 e 13 –** dispõe sobre a gestão da tecnologia da informação.

6 RELAÇÃO COM A NBR/ISO/IEC 27001:2005

SEÇÃO	CONTROLE
Anexo A	A.7 – Gestão dos ativos A.10.1.3 – Segregação de funções A.10.4.1 - Controle contra códigos maliciosos A.10.5 – Cópias de segurança A.10.6.2 – Segurança dos serviços de rede A.10.8 – Troca de informações A.11.2 – Gerenciamento de acesso do usuário A.11. 3 – Responsabilidades do usuário A.11.4 – Controle de acesso à rede A.11.5 – Controle de acesso ao sistema operacional A.11.6 – Controle de acesso à aplicação e à informação A.11.7 – computação móvel e trabalho remoto A.12 – Aquisição, desenvolvimento e manutenção de sistemas de informação A.13 – Gestão de incidentes de segurança da informação A.14 – Gestão da continuidade do negócio A.15 - Conformidade

7 CONCEITOS E DEFINIÇÕES

7.1 Segurança da Informação [ABNT NBR ISO/IEC 27002]: preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confidencialidade, podem também estar envolvidas.

7.2 Outros termos: vide dicionário de termos e siglas.

NORMAS DE SEGURANÇA

8 RESPONSABILIDADES DOS ADMINISTRADORES DOS RECURSOS DE TI

8.1 Os usuários que exercem função de administração dos recursos de infraestrutura de TI do Tribunal, para efeito desta norma, serão considerados administradores de recursos de TI, doravante denominados ARTI.

8.2 Os ARTI devem assinar um documento específico, responsabilizando-se pela confidencialidade, integridade e disponibilidade das informações a que tiverem acesso.

8.3 É vedado aos ARTI ler, apagar ou manipular informações de qualquer usuário, salvo nos casos em que haja previsão normativa ou devida autorização.

9 CONTROLE DE ACESSO

9.1 Os ARTI devem possuir contas de identificação, distintas e pessoais, de acesso à rede local, servidores e bancos de dados, sendo uma para a realização das tarefas não pertinentes à administração dos recursos e outra, ou outras, exclusivamente para atividades de administração.

9.2 As contas de acesso à rede local, servidores e bancos de dados, com privilégios de administração, devem:

- possuir nomenclatura de fácil associação com o administrador de rede;
- somente ser utilizadas para realização das atividades que necessitem de tais permissões;
- somente ser utilizadas em equipamentos e aplicativos previamente definidos para este fim.

9.3 A criação, o bloqueio ou o cancelamento da conta de acesso do administrador à rede local, aos sistemas e serviços devem ser executados somente com autorização superior.

9.4 A STI deve providenciar o bloqueio ou o cancelamento das contas de acesso à rede local, aos servidores e bancos de dados, dos administradores, nos casos de desligamento, deslocamento para outro setor, ou inatividade, por período a ser definido pela secretaria.

10 UTILIZAÇÃO DE SENHAS

10.1 Os meios de identificação, como senhas e certificados digitais, são únicos, pessoais e intransferíveis, não devendo ser compartilhados. Sua utilização ou as consequências decorrentes do seu uso indevido são de responsabilidade do usuário.

10.2 As senhas da identificação das contas de acesso à rede local, a servidores e bancos de dados devem seguir critérios de segurança, a serem definidos pela STI, que contemplem os seguintes preceitos:

- senha com determinado tamanho mínimo e diferentes tipos de caracteres;
- exigência de troca de senha em determinados intervalos;
- senha composta por letras do alfabeto, números e caracteres especiais que não tenham qualquer vínculo lógico com as informações do usuário.

10.3 A senha da identificação da conta de acesso à rede local do usuário deverá ter controles, estabelecidos pela STI, relativos a:

- bloqueio provisório para o caso de um certo número de tentativas consecutivas erradas;
- impossibilidade de sua alteração que coincida com uma das ultimas três utilizadas pelo usuário.

11 ADMINISTRAÇÃO DO AMBIENTE DE PRODUÇÃO

11.1 Os ARTI são responsáveis por manter a infraestrutura de TI em perfeitas condições de funcionamento, garantindo a qualidade e a disponibilidade dos serviços, bem como por informar às chefias superiores da STI, por meio de canal específico, todo e qualquer evento de segurança.

11.2 Os ambientes de produção devem ter seus recursos de tecnologia da informação constantemente avaliados e mantidos em perfeitas condições de funcionamento.

11.3 A documentação física e lógica dos ambientes de produção deve ser mantida atualizada e armazenada em local seguro.

11.4 A utilização de ferramentas para administração de sistemas deve ser realizada de forma controlada, não comprometendo a segurança das informações e dos ambientes.

11.5 As ferramentas para administração da rede local, dos sistemas e dos bancos de dados devem ser de uso exclusivo dos administradores dos respectivos serviços.

11.6 A manutenção e a atualização do ambiente de produção devem ser previamente agendadas, preferencialmente, fora do horário de funcionamento do Tribunal, levando-se em consideração o estabelecido na PSI-N001.

11.7 Para restringir o acesso físico ao ambiente de produção, os servidores de rede devem possuir consoles de gerência remota para sua administração.

11.8 O acesso físico aos servidores de rede em produção somente deve ser feito para a execução de tarefas que obrigatoriamente demandem interação com os equipamentos existentes, por exemplo, substituição de fitas de backup ou tarefas que possam ser prejudicadas pela perda de conectividade.

11.9 Os ARTI são responsáveis por comunicar, através do processo de gestão de mudança estabelecido pela STI, qualquer alteração de configuração identificada, que impacte no funcionamento dos recursos de tecnologia da informação implementados no Tribunal.

12 CONTROLE DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO

12.1 Os recursos de tecnologia da informação do Tribunal devem ser identificados, inventariados e receber proteção para seus componentes internos.

12.2 Os recursos de tecnologia da informação que não são de propriedade do Tribunal devem ser identificados de forma diferenciada.

12.3 O compartilhamento dos recursos de tecnologia da informação deve preservar a confidencialidade, a integridade e a disponibilidade das informações.

12.4 Todo sistema ou aplicação a ser disponibilizada em ambiente de produção deve ser devidamente homologado em ambiente próprio.

12.4.1 A STI deve prover os ambientes de desenvolvimento, testes, homologação e produção, independentes entre si.

12.5 Somente é permitida a utilização de *softwares* homologados e autorizados pela STI, respeitando-se os direitos autorais e contratuais.

12.6 Implementações, alterações e atualizações de recursos de tecnologia da informação devem ser homologadas antecipadamente pela STI.

12.7 Todo processo de homologação dos recursos de tecnologia da informação deve respeitar a política de segurança e ser documentado.

12.8 O processo de homologação dos recursos de tecnologia da informação deve, entre outras atividades, avaliar o impacto do uso do recurso na segurança das informações do Tribunal.

12.9 Os sistemas de informação devem, sempre que possível, ser mantidos atualizados com as versões mais recentes disponíveis.

12.10 A utilização de *softwares* deve respeitar a quantidade e o prazo das licenças disponíveis no âmbito do Tribunal.

12.11 Os recursos de tecnologia da informação devem possuir as informações de data e hora sincronizadas, obedecendo ao fuso horário de sua localização geográfica.

12.12 Os recursos de tecnologia da informação do Tribunal devem ser atualizados, após homologação, sempre que for detectada alguma vulnerabilidade.

13 MANUTENÇÃO DA INFRAESTRUTURA DE REDE LOCAL

13.1 Os pontos de rede devem ser controlados e documentados, identificando-se a existência de pontos ativos e os sem utilização.

13.2 As normas brasileiras devem ser seguidas na instalação, controle e manutenção do cabeamento elétrico e lógico.

13.3 Os recursos de tecnologia da informação que não suportem mais a demanda de serviço devem ser identificados e substituídos conforme sua obsolescência.

14 AUDITORIA DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO

14.1 Os ARTI e os gestores responsáveis (negócio e sistema) devem identificar necessidades de geração de logs e o seu nível de detalhamento.

14.2 Os arquivos de log devem fazer parte do processo de cópia de segurança (*backup*).

15 DISPOSIÇÕES FINAIS

15.1 Fica assegurado à STI, a qualquer tempo, tomar as medidas necessárias quando evidenciados os riscos à segurança da informação.

15.2 Os usuários e funcionários são responsáveis por suas contas, senhas e por qualquer ação que venha ferir a confidencialidade, a integridade e a disponibilidade da informação.

15.3 O uso indevido dos recursos de tecnologia da informação do TRE-MG é passível de sanção disciplinar, de acordo com a legislação vigente e demais normas aplicadas à matéria.

16 PENALIDADES

16.1 O Tribunal adotará as sanções legais cabíveis contra qualquer usuário ou entidade que venha a praticar atos que violem a Política de Segurança da Informação.

17 VIGÊNCIA E ATUALIZAÇÃO

17.1 Esta norma entra em vigor a partir da data de sua publicação, e sua atualização ocorrerá sempre que se fizer necessário através de proposição pela Comissão de Segurança da Informação, aprovação da Diretoria-Geral e publicação nos canais competentes para ciência aos usuários do TRE-MG.

18 EXCEÇÕES

18.1 Qualquer exceção a esta norma deve ser aprovada pela Comissão de Segurança da Informação. A obtenção desta aprovação assegura que todas as alternativas razoáveis foram avaliadas e que os controles compensatórios são adequados para atenuar quaisquer riscos.

TRIBUNAL REGIONAL ELEITORAL DE MINAS GERAIS

ANEXO IV

(a que se referem os arts. 3º, 4º e 5º da Resolução nº 945, de 17 de dezembro de 2013)

PSI - N 004	**NORMA GERAL DE SEGURANÇA PARA CONTROLE DE ACESSO INTERNO E EXTERNO À REDE TRE-MG**
Versão 2.5 21/06/2013	Política de Segurança da Informação da Justiça Eleitoral

SUMÁRIO

1 MATÉRIA DISCIPLINADA

1.1 Dispõe sobre os requisitos de segurança da informação referentes às regras de prevenção de acessos não autorizados aos serviços de rede do Tribunal Regional Eleitoral de Minas Gerais – TRE-MG.

2 OBJETIVO GERAL

2.1 Estabelecer regras de prevenção contra acessos não autorizados aos serviços de rede do TRE-MG.

3 PÚBLICO-ALVO

3.1 Aplica-se aos usuários com privilégios de administradores dos recursos de tecnologia da informação do TRE-MG.

4 APLICAÇÃO

4.1 Norma de segurança de aplicação interna.

5 REFERÊNCIAS LEGAIS E NORMATIVAS

a) Norma Técnica ABNT NBR ISO/IEC 27001:2006 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação – Requisitos;

b) Norma Técnica ABNT NBR ISO/IEC 27002:2005 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação;

c) Resolução nº 22.780/2008 - Política de Segurança da Informação da Justiça Eleitoral – documento que registra as diretrizes da Alta Direção sobre o tema segurança da informação;

d) Constituição Federal, art. 37, *caput* – artigo em que se registra que a administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência;

e) Instrução Normativa nº 1/2008, Gabinete de Segurança Institucional - Presidência da República, art. 5º, inciso VII - disciplina a Gestão de

Segurança da Informação e Comunicações na administração pública federal, direta e indireta, e dá outras providências;

f) Norma Técnica - Gabinete de Segurança Institucional - Presidência da República - Norma Complementar nº 03/IN01/DSIC/GSIPR – diretrizes para elaboração da Política de Segurança da Informação e Comunicações nos órgãos e entidades da administração pública federal;

g) Resolução nº 90/2009/CNJ, arts. 10 e 13 – dispõe sobre a gestão da tecnologia da informação.

6 RELAÇÃO COM A NBR/ISO/IEC 27001:2005

SEÇÃO	CONTROLE
Anexo A	A.10.10 – Monitoramento
	A.10.10.1 – Registros de auditoria
	A.10.10.2 – Monitoramento do uso do sistema
	A.11.2 – Gerenciamento de acesso do usuário
	A.11.2.1 – Registro de usuário
	A.11.2.2 – Gerenciamento de privilégios
	A.11.2.4 – Gerenciamento de senha do usuário
	A.11.4 – Controle de acesso à rede
	A.11.4.2 – Autenticação para conexão externa do usuário
	A.11.4.3 – Identificação de equipamento em redes
	A.11.4.4 – Proteção e configuração de portas de diagnóstico remotas
	A.11.4.5 – Segregação de redes
	A.11.4.6 – Controle de conexão de rede
	A.11.4.7 – Controle de roteamento de redes
	A.12.3 – Controles criptográficos

7 CONCEITOS E DEFINIÇÕES

7.1 Segurança da Informação [ABNT NBR ISO/IEC 27002]: preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confidencialidade, podem também estar envolvidas.

7.2 Outros termos: vide dicionário de termos e siglas.

NORMAS DE SEGURANÇA

8 DISPOSIÇÕES INICIAIS

8.1 Os usuários que exercem função de administração dos recursos de tecnologia da informação do TRE-MG são os que possuem privilégios de administração nos sistemas, aplicações e rede, e, para efeito desta norma, serão considerados administradores de recursos de TI, doravante denominados ARTI.

8.2 Os ARTI devem aplicar as regras gerais de acesso à rede do TRE-MG constantes nesta norma.

8.2.1 Para o acesso aos sistemas administrativos e judiciais, dever-se-ão seguir as definições da comissão ou do gestor do respectivo sistema, que assumem total responsabilidade pela segurança das aplicações e de seu relacionamento de forma segura com a rede de comunicação de dados.

8.2.2 Para o acesso aos sistemas eleitorais, dever-se-á seguir normatização específica.

9 CONTROLE DE ACESSO À REDE

9.1 Todo acesso interno e externo aos serviços de rede deve ser autorizado e controlado pela Secretaria de Tecnologia da Informação – STI.

9.2 Os usuários devem receber permissão de acesso aos serviços, respeitando-se o princípio do menor privilégio e tendo sido autorizados pela chefia imediata.

9.3 Portas de diagnóstico dos dispositivos de rede devem estar habilitadas somente a usuários com privilégios administrativos.

9.4 A rede de dados do TRE-MG deve ser segmentada em perímetros lógicos, atendendo às necessidades de fornecimento de serviços públicos e proteção da rede interna.

9.5 Controles de segurança devem ser implementados nos ativos de rede remota (roteadores) para controlar as conexões à rede da Justiça Eleitoral.

9.6 Mecanismos de autenticação apropriados para usuários e conexões devem ser implementados, a fim de aumentar o nível de segurança da rede do TRE-MG.

9.7 Arquivos de registros de eventos (logs) devem ser habilitados nos recursos de tecnologia da informação para armazenar informações de sucesso e insucesso de acessos, para efeito de eventuais auditorias futuras.

9.8 Pontos de acesso à rede do TRE-MG que não estejam em uso devem ser desabilitados.

9.9 O acesso físico aos *rack's* de comunicação que contenham equipamentos de conectividade deve ser controlado, e, quando for necessária a intervenção de técnicos de fora dos quadros do Tribunal, estes deverão estar acompanhados de servidor designado e com registro de acesso documentado e arquivado.

9.10 O acesso aos quadros de distribuição de cabos de comunicação deve ser controlado, e, quando for necessária a intervenção de técnicos de fora dos quadros do Tribunal, estes deverão estar acompanhados de servidor designado e com registro de acesso documentado e arquivado.

10 AUTENTICAÇÃO PARA CONEXÃO EXTERNA

10.1 Deverão ser criados mecanismos para buscar sempre o aumento da segurança das senhas.

10.2 Métodos apropriados de autenticação devem ser usados para controlar o acesso de usuários remotos.

10.3 Métodos apropriados de proteção das informações que trafegam entre a rede do TRE-MG e redes remotas, como por exemplo a criptografia, devem ser implementados.

10.4 Métodos apropriados de proteção para redes sem fio, por exemplo, *gateways* de autenticação ou registro de endereçamento *Mac Address*, devem ser implementados.

10.5 Todos os segmentos lógicos devem ser monitorados com ferramentas específicas que garantam a identificação de tentativas de ataques à rede, preventivamente.

11 IDENTIFICAÇÃO DE EQUIPAMENTOS EM REDES

11.1 Todos os recursos de tecnologia da informação que acessam a rede do TRE-MG devem ser identificados e autorizados.

11.2 Todos os acessos à rede do TRE-MG devem ser registrados, podendo

ser monitorados conforme necessidade.

12 DISPOSIÇÕES FINAIS

12.1 Fica assegurado à STI, a qualquer tempo, tomar as medidas necessárias quando evidenciados riscos à segurança da informação.

12.2 Os usuários e funcionários são responsáveis por suas contas, senhas e por qualquer ação que venha ferir a confidencialidade, a integridade e a disponibilidade da informação.

12.3 O uso indevido dos recursos de tecnologia da informação do TRE-MG é passível de sanção disciplinar, de acordo com a legislação vigente e demais normas aplicadas à matéria.

13 PENALIDADES

13.1 O Tribunal adotará as sanções legais cabíveis contra qualquer usuário ou entidade que venha a praticar atos que violem a Política de Segurança da Informação.

14 VIGÊNCIA E ATUALIZAÇÃO

14.1 Esta norma entra em vigor a partir da data de sua publicação, e sua atualização ocorrerá sempre que se fizer necessário através de proposição pela Comissão de Segurança da Informação, aprovação da Diretoria-Geral e publicação nos canais competentes para ciência aos usuários do TRE-MG.

15 EXCEÇÕES

15.1 Qualquer exceção a esta norma deve ser aprovada pela Comissão de Segurança da Informação do TRE-MG. A obtenção desta aprovação assegura que todas as alternativas razoáveis foram avaliadas e que os controles compensatórios são adequados para atenuar quaisquer riscos.

TRIBUNAL REGIONAL ELEITORAL DE MINAS GERAIS

ANEXO V

(a que se referem os arts. 3º, 4º e 5º da Resolução nº 945, de 17 de dezembro de 2013)

PSI - N 005	**NORMA GERAL DE SEGURANÇA SOBRE CÓDIGOS MALICIOSOS TRE-MG**
Versão 2.5 21/06/2013	Política de Segurança da Informação da Justiça Eleitoral

SUMÁRIO

1 MATÉRIA DISCIPLINADA

1.1 Dispõe sobre os requisitos de segurança da informação referentes aos cuidados contra a ação de códigos maliciosos em recursos de tecnologia da informação do Tribunal Regional Eleitoral de Minas Gerais – TRE-MG.

2 OBJETIVO GERAL

2.1 Estabelecer regras de prevenção contra códigos maliciosos em servidores, estações de trabalho e demais equipamentos do TRE-MG.

3 PÚBLICO-ALVO

3.1 Aplica-se aos usuários com privilégios de administradores dos recursos de tecnologia da informação do TRE-MG.

4 APLICAÇÃO

4.1 Norma de segurança de aplicação interna.

5 REFERÊNCIAS LEGAIS E NORMATIVAS

a) Norma Técnica ABNT NBR ISO/IEC 27001:2006 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação – Requisitos;

b) Norma Técnica ABNT NBR ISO/IEC 27002:2005 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação;

c) Resolução nº 22.780/2008 - Política de Segurança da Informação da Justiça Eleitoral – documento que registra as diretrizes da Alta Direção sobre o tema segurança da informação;

d) Constituição Federal, art. 37, *caput* – artigo em que se registra que a administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência;

e) Instrução Normativa nº 1/2008, Gabinete de Segurança Institucional -

Presidência da República, art. 5º, inciso VII - disciplina a Gestão de Segurança da Informação e Comunicações na administração pública federal, direta e indireta, e dá outras providências;

f) Norma Técnica - Gabinete de Segurança Institucional - Presidência da República - Norma Complementar nº 03/IN01/DSIC/GSIPR – diretrizes para elaboração da Política de Segurança da Informação e Comunicações nos órgãos e entidades da administração pública federal;

g) Resolução nº 90/2009/CNJ, arts. 10 e 13 – dispõe sobre a gestão da tecnologia da informação.

6 RELAÇÃO COM A NBR/ISO/IEC 27001:2005

SEÇÃO	CONTROLE
Anexo A	A.10.1 – Procedimentos e responsabilidades operacionais
	A.10.1.1 – Documentação dos procedimentos de operação
	A.10.1.2 – Gestão de mudanças
	A.10.1.4 – Separação dos recursos de desenvolvimento, teste e de produção
	A.10.4 – Proteção contra códigos maliciosos e códigos móveis
	A.10.4.1 – Controle contra códigos maliciosos
	A.13.1 – Notificação de fragilidades e eventos de segurança da informação
	A.13.1.1 – Notificação de eventos de segurança da informação
	A.13.1.2 – Notificando fragilidades de segurança da informação
	A.15.1 – Conformidade com requisitos legais
	A.15.1.2 – Direitos de propriedade intelectual

7 CONCEITOS E DEFINIÇÕES

7.1 Segurança da Informação [ABNT NBR ISO/IEC 27002]: preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confidencialidade, podem também estar envolvidas.

7.2 Código malicioso: programa ou *software* especificamente desenvolvido para executar ações danosas em um computador ou obter informações de forma ilícita.

7.3 Outros termos: vide dicionário de termos e siglas.

NORMAS DE SEGURANÇA

8 DISPOSIÇÕES INICIAIS

8.1 Os usuários que exercem função de administração dos recursos de tecnologia da informação do TRE-MG, a saber, os que possuem privilégios de administração nos sistemas, aplicações e rede, para efeito desta norma, serão considerados administradores de recursos de TI, doravante denominados ARTI.

8.2 Define-se como “solução para códigos maliciosos” a prevenção, detecção e bloqueio desses programas ou códigos.

9 ADMINISTRAÇÃO DA SOLUÇÃO CONTRA CÓDIGOS MALICIOSOS

9.1 Os recursos de tecnologia da informação existentes no TRE-MG devem estar providos de soluções de detecção e bloqueio de programas com códigos maliciosos, como *antispyware*, antivírus e filtros de análise de conteúdo de correio eletrônico e tráfego internet.

9.2 A Secretaria de Tecnologia da Informação – STI – deve especificar e homologar soluções para códigos maliciosos, considerando as seguintes características:

9.2.1 possuírem consoles de administração centralizada;

9.2.2 permitirem atualização automática e programável;

9.2.3 permitirem bloqueio de alteração das configurações por meio de senha de administração;

9.2.4 proverem serviço de atualização por parte do fabricante;

9.2.5 possuírem mecanismo de varredura em tempo real;

9.2.6 possuírem mecanismo de controle estatístico e emissão de relatórios;

9.2.7 possuírem mecanismo de controle centralizado com emissão de alertas de problemas;

9.2.8 possuírem bloqueio de execução de aplicações não homologadas pela STI;

9.2.9 possuírem bloqueio de conteúdos *web*;

9.2.10 possuírem *firewall* local.

9.3 A STI deve fazer verificação periódica com os fabricantes sobre a disponibilidade de atualizações da solução para códigos maliciosos.

9.4 Todas as atualizações e correções de versão das soluções para códigos maliciosos devem ser homologadas antes de serem aplicadas no ambiente de produção, com vistas a evitar impactos neste ambiente.

9.4.1 A STI deve elaborar e manter atualizada a documentação com a descrição dos procedimentos de instalação e configuração das soluções para códigos maliciosos.

9.4.2 A documentação deve ser guardada em local seguro, com acesso controlado e restrito a profissionais especialistas da STI.

9.5 A solução para códigos maliciosos deve colocar automaticamente os arquivos contaminados em uma área de acesso restrito, por tempo determinado pelo administrador de rede, para tratamento adequado.

10 INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO CONTRA CÓDIGOS MALICIOSOS

10.1 A instalação e a configuração da solução para códigos maliciosos somente devem ser realizadas pela STI.

10.2 A STI deve agendar e configurar o *software* antivírus para execução periódica de varredura completa nas estações de trabalho ou equipamentos portáteis do TRE-MG (como disco – HD – externo ou *pen drive*), para identificação de potenciais programas contendo códigos maliciosos.

10.3 A STI deve configurar as soluções para códigos maliciosos para verificação das mensagens recebidas por correio eletrônico e arquivos em anexo, quanto à contaminação por códigos maliciosos.

10.3.1 A solução para códigos maliciosos deve mover automaticamente mensagens de correio eletrônico e arquivos contaminados para uma área de acesso restrito, por tempo determinado pelo administrador de rede, para tratamento adequado.

11 USO E MANUTENÇÃO DA SOLUÇÃO CONTRA CÓDIGOS MALICIOSOS

11.1 É obrigatório o uso de *software* antivírus nos recursos de tecnologia da informação disponibilizados para os usuários pelo TRE-MG.

11.1.1 O *software* antivírus deve ser mantido sempre ativado e atualizado.

11.1.2 A solução para códigos maliciosos deve ser configurada para o envio de alertas aos administradores de rede, caso sejam identificados códigos maliciosos nos recursos de tecnologia da informação do TRE-MG sem tratamento conhecido.

11.2 A solução para códigos maliciosos deve enviar ao usuário uma notificação quando do recebimento de uma mensagem de correio eletrônico ou arquivo em anexo contaminado.

11.3 Os *softwares* que compõem a solução para códigos maliciosos devem estar configurados para operar de forma transparente para o usuário.

11.3.1 Esses *softwares* também devem ser configurados de forma a impedir que o usuário consiga desabilitar ou interromper o seu correto funcionamento.

11.3.2 Será passível de responsabilização pelos danos causados por códigos maliciosos o usuário que interromper a operação dos *softwares* aplicados para esta solução.

12 DISPOSIÇÕES FINAIS

12.1 Os usuários devem reportar os incidentes que afetam a segurança dos ativos ou o descumprimento da Política de Segurança da Informação à STI.

12.2 Em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação, a STI deverá ser imediatamente acionada para adotar as providências necessárias, podendo, inclusive, determinar a restrição temporária do acesso aos recursos de tecnologia da informação do TRE-MG.

13 PENALIDADES

13.1 O Tribunal adotará as sanções legais cabíveis contra qualquer usuário ou entidade que venha a praticar atos que violem a Política de Segurança da Informação.

14 VIGÊNCIA E ATUALIZAÇÃO

14.1 Esta norma entra em vigor a partir da data de sua publicação, e sua atualização ocorrerá sempre que se fizer necessário através de proposição pela Comissão de Segurança da Informação, aprovação da Diretoria Geral e publicação nos canais competentes para ciência aos usuários do TRE-MG.

15 EXCEÇÕES

15.1 Qualquer exceção a esta norma deve ser aprovada pela Comissão de Segurança da Informação. A obtenção desta aprovação assegura que todas as alternativas razoáveis foram avaliadas e que os controles compensatórios são adequados para atenuar quaisquer riscos.

TRIBUNAL REGIONAL ELEITORAL DE MINAS GERAIS

ANEXO VI

(a que se referem os arts. 3º, 4º e 5º da Resolução nº 945, de 17 de dezembro de 2013)

PSI - N 006	**NORMA ESPECÍFICA DE SEGURANÇA PARA INSTALAÇÃO E CONFIGURAÇÃO DE EQUIPAMENTOS SERVIDORES DE REDE TRE-MG**
Versão 2.5 21/06/2013	Política de Segurança da Informação da Justiça Eleitoral

SUMÁRIO

1 MATÉRIA DISCIPLINADA

1.1 Dispõe sobre os requisitos de segurança da informação para a correta instalação e configuração de sistemas operacionais utilizados nos equipamentos servidores de rede de comunicação de dados do Tribunal Regional Eleitoral de Minas Gerais – TRE-MG.

2 OBJETIVO GERAL

2.1 Estabelecer orientações de segurança para configuração dos sistemas operacionais nos equipamentos servidores de rede do TRE-MG.

3 PÚBLICO-ALVO

3.1 Aplica-se aos usuários com privilégios de administradores dos recursos de tecnologia da informação do TRE-MG.

4 APLICAÇÃO

4.1 Norma de segurança de aplicação interna.

5 REFERÊNCIAS LEGAIS E NORMATIVAS

a) Lei nº 9.609, de 19 de fevereiro de 1998 - dispõe sobre a proteção de propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências;

b) Lei nº 9.279, de 14 de maio de 1996 - regula direitos e obrigações relativos à propriedade intelectual;

c) Norma Técnica ABNT NBR ISO/IEC 27001:2006 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação – Requisitos;

d) Norma Técnica ABNT NBR ISO/IEC 27002:2005 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação;

e) Resolução nº 22.780/2008 - Política de Segurança da Informação da Justiça Eleitoral – documento que registra as diretrizes da Alta Direção sobre o tema segurança da informação;

f) Constituição Federal, art. 37, *caput* – artigo em que se registra que a administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência;

g) Instrução Normativa nº 1/2008, Gabinete de Segurança Institucional - Presidência da República, art. 5º, inciso VII - disciplina a Gestão de Segurança da Informação e Comunicações na administração pública federal, direta e indireta, e dá outras providências;

h) Norma Técnica - Gabinete de Segurança Institucional - Presidência da República - Norma Complementar nº 03/IN01/DSIC/GSIPR – diretrizes para elaboração da Política de Segurança da Informação e Comunicações nos órgãos e entidades da administração pública federal;

i) Resolução nº 90/2009/CNJ, arts. 10 e 13 – dispõe sobre a gestão da tecnologia da informação.

6 RELAÇÃO COM A NBR/ISO/IEC 27001:2005

SEÇÃO	CONTROLE
Anexo A	A.10 – Gerenciamento das operações e comunicações
	A.10.1 – Procedimentos e responsabilidades operacionais
	A.10.1.1 – Documentação dos procedimentos de operação
	A.10.1.2 – Gestão de mudanças
	A.10.1.3 – Segregação de funções
	A.10.10 – Monitoramento
	A.10.10.1 – Registro de auditoria
	A.10.10.2 – Monitoramento do uso do sistema
	A.11.5 – Controle de acesso ao sistema operacional
	A.11.5.1 – Procedimentos seguros de entrada no sistema (log-on)
	A.11.5.2 – Identificação e autenticação de usuário
	A.11.5.3 – Sistema de gerenciamento de senha
	A.11.5.4 – Uso de utilitários de sistema
	A.11.5.5 – Desconexão de terminal por inatividade
	A.11.5.6 – Limitação de horário de conexão
	A.15 – Conformidade
	A.15.1.2 – Direitos de propriedade intelectual

7 CONCEITOS E DEFINIÇÕES

7.1 Segurança da Informação [ABNT NBR ISO/IEC 27002]: preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confidencialidade, podem também estar envolvidas.

7.2 Outros termos: vide dicionário de termos e siglas.

NORMAS DE SEGURANÇA

8 DISPOSIÇÕES INICIAIS

8.1 Os usuários que exercem função de administração dos recursos de tecnologia da informação do TRE-MG, a saber, os que possuem privilégios de administração nos sistemas, aplicações e rede, para efeito desta norma, serão considerados administradores de recursos de TI, doravante denominados ARTI.

9 INSTALAÇÃO E CONFIGURAÇÃO DOS SISTEMAS OPERACIONAIS

9.1 Todos os sistemas operacionais utilizados nos recursos de tecnologia da informação do TRE-MG devem ser devidamente licenciados.

9.2 Os pacotes de atualização, disponibilizados pelos fabricantes dos sistemas operacionais, devem ser instalados nos recursos de tecnologia da informação, desde que previamente homologados em ambiente de teste pela Secretaria de Tecnologia da Informação – STI.

9.2.1 Para as atualizações, devem, preferencialmente, ser utilizadas soluções automáticas que permitam verificações de atualizações aplicáveis para os sistemas operacionais.

9.3 A STI deve ter documentação de todos os procedimentos de instalação e configuração dos sistemas operacionais.

9.3.1 Para as novas instalações, onde não exista documentação elaborada, devem ser seguidas as orientações fornecidas pelo fabricante.

9.4 A STI é a única responsável pela instalação e configuração dos sistemas operacionais nos computadores servidores do TRE-MG.

9.5 Deve ser configurado o serviço de sincronização de relógios (tempo) nos recursos de tecnologia da informação.

9.5.1 A STI deve observar anualmente as definições de horário de verão de forma a ajustar as configurações dos recursos de tecnologia da informação.

9.6 A instalação dos servidores de rede deve ser efetuada com um mínimo possível de pacotes e componentes, especialmente os que implementam serviços de rede.

9.7 Os protocolos de rede e os serviços desnecessários para o funcionamento e comunicação dos recursos de tecnologia da informação devem ser removidos ou desabilitados.

10 CONTAS E SENHAS

10.1 Os recursos de tecnologia da informação devem ser configurados de maneira que os usuários tenham permissão de alterar as suas próprias senhas de *login*, desde que atendam aos padrões estabelecidos pela STI.

10.2 A STI deve desabilitar as contas do tipo “Convidado” dos sistemas operacionais dos recursos de tecnologia da informação.

10.3 Os ARTI deverão acessar os servidores usando sua conta pessoal e a partir dela realizar suas tarefas, usando os privilégios mais elevados apenas quando estritamente necessário, observando a necessidade de registros destas nos arquivos de auditoria – *logs* – próprios.

10.4 O uso de contas com privilégio administrativo dos sistemas operacionais deve obedecer aos critérios definidos pela STI, com vistas à manutenção do padrão de segurança.

11 CONTROLE DE ACESSO

11.1 O controle de acesso lógico aos sistemas operacionais dos recursos de tecnologia da informação deve seguir as orientações definidas na PSI-N004 - Norma geral de segurança para controle dos acessos a rede.

12 DOCUMENTAÇÃO

12.1 A STI deve elaborar e atualizar os procedimentos de instalação e configuração dos recursos de tecnologia da informação.

12.1.1 A atualização dos procedimentos de instalação e configuração dos recursos de tecnologia da informação deve ser realizada sempre que houver alterações.

13 AUDITORIA E MONITORAMENTO

13.1 Devem ser definidos tamanhos máximos dos arquivos de auditoria – *logs* – dos sistemas operacionais.

13.2 Os registros de auditoria, gerados pelos sistemas operacionais, devem ser armazenados em local centralizado e protegidos contra acessos indevidos.

13.3 Os registros de auditoria, gerados pelos sistemas operacionais, devem ser verificados periodicamente.

13.4 O período de retenção dos arquivos de auditoria dos sistemas operacionais deve ser definido seguindo preferencialmente as orientações e melhores práticas do fabricante, alinhado às definições feitas pela STI.

13.5 Os sistemas operacionais devem ser configurados para:

13.5.1 Gravar um registro de auditoria sempre que ocorrer um erro fatal.

13.5.2 Registrar falhas de *logon*, indicando o número de tentativas realizadas.

13.5.3 Registrar a criação e a remoção dos usuários.

13.5.4 Não permitir que os registros de auditoria sejam removidos ou alterados.

13.5.5 Emitir alertas quando o limite de armazenamento dos registros de auditoria estiver próximo de sua capacidade máxima.

14 DISPOSIÇÕES FINAIS

14.1 Os ARTI devem reportar sempre os incidentes que afetam a segurança dos ativos ou o descumprimento da Política de Segurança da Informação à STI.

14.2 Em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação, a STI deverá ser imediatamente acionada para adotar as providências necessárias, podendo, inclusive, determinar a restrição temporária do acesso aos serviços do TRE-MG.

15 PENALIDADES

15.1 O Tribunal adotará as sanções legais cabíveis contra qualquer usuário ou entidade que venha a praticar atos que violem a Política de Segurança da Informação.

16 VIGÊNCIA E ATUALIZAÇÃO

16.1 Esta norma entra em vigor a partir da data de sua publicação, e sua atualização ocorrerá sempre que se fizer necessário através de proposição pela Comissão de Segurança da Informação, aprovação da Diretoria Geral e publicação nos canais competentes para ciência aos usuários do Tribunal Regional Eleitoral de Minas Gerais.

17 EXCEÇÕES

17.1 Qualquer exceção a esta norma operacional deve ser aprovada pela Comissão de Segurança da Informação. A obtenção desta aprovação assegura que todas as alternativas razoáveis foram avaliadas e que os controles compensatórios são adequados para atenuar quaisquer riscos.

TRIBUNAL REGIONAL ELEITORAL DE MINAS GERAIS

ANEXO VII

(a que se referem os arts. 3º, 4º e 5º da Resolução nº 945, de 17 de dezembro de 2013)

PSI - N 007	**NORMA GERAL DE SEGURANÇA PARA TRATAMENTO DE MÍDIAS E DE CÓPIAS DE SEGURANÇA (Backup) TRE-MG**
Versão 2.5 21/06/2013	Política de Segurança da Informação da Justiça Eleitoral

SUMÁRIO

1 MATÉRIA DISCIPLINADA

1.1 Dispõe sobre os requisitos de segurança relacionados ao manuseio das mídias de cópia de segurança (*backup*) dos recursos de tecnologia da informação do Tribunal Regional Eleitoral de Minas Gerais – TRE-MG.

2 OBJETIVO GERAL

2.1 Estabelecer regras de segurança da informação no que tange ao processo de *backup* de informações, desde a geração, o armazenamento até a restauração (*restore*).

3 PÚBLICO-ALVO

3.1 Aplica-se aos usuários com privilégios de administradores dos recursos de tecnologia da informação do TRE-MG envolvidos com as atividades de *backup*.

4 APLICAÇÃO

4.1 Norma de segurança de aplicação interna.

5 REFERÊNCIAS LEGAIS E NORMATIVAS

a) Norma Técnica ABNT NBR ISO/IEC 27001:2006 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação – Requisitos;

b) Norma Técnica ABNT NBR ISO/IEC 27002:2005 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação;

c) Res. 22780/2008 - Política de Segurança da Informação da Justiça Eleitoral – documento que registra as diretrizes da Alta Direção sobre o tema segurança da informação;

d) Constituição Federal de 1988, art. 37, *caput* – o artigo prevê que a administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência;

e) Instrução Normativa nº 1/2008, Gabinete de Segurança Institucional - Presidência da República, art. 5º, inciso VII - disciplina a Gestão de Segurança da Informação e Comunicações na administração pública federal, direta e indireta, e dá outras providências;

f) Norma Técnica - Gabinete de Segurança Institucional - Presidência da República - Norma Complementar nº 03/IN01/DSIC/GSIPR – diretrizes para elaboração da Política de Segurança da Informação e Comunicações nos órgãos e entidades da administração pública federal;

g) Resolução nº 90/2009/CNJ, arts. 10 e 13 – dispõe sobre a gestão da tecnologia da informação;

h) MoReq-JUS 2007, MODELO DE REQUISITOS para Sistemas Informatizados de Gestão de Projetos e Documentos da Justiça Federal; Item 6.1 – dispõe sobre cópias de segurança;

6 RELAÇÃO COM A NBR/ISO/IEC 27001:2005

SEÇÃO	CONTROLE
Anexo A	A.10 – Gerenciamento das operações e comunicações
	A.10.1 – Procedimentos e responsabilidades operacionais
	A.10.1.1 – Documentação dos procedimentos de operação
	A.10.1.2 – Gestão de mudanças
	A.10.1.3 – Segregação de funções
	A.10.10 – Monitoramento
	A.10.10.1 – Registro de auditoria
	A.10.10.2 – Monitoramento do uso do sistema
	A.11.5 – Controle de acesso ao sistema operacional
	A.11.5.1 – Procedimentos seguros de entrada no sistema (*log-on*)
	A.11.5.2 – Identificação e autenticação de usuário
	A.11.5.3 – Sistema de gerenciamento de senha
	A.11.5.4 – Uso de utilitários de sistema
	A.11.5.5 – Desconexão de terminal por inatividade
	A.11.5.6 – Limitação de horário de conexão
	A.15 – Conformidade
	A.15.1.2 – Direitos de propriedade intelectual

7 CONCEITOS E DEFINIÇÕES

7.1 Segurança da Informação [ABNT NBR ISO/IEC 27002]: preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confidencialidade, podem também estar envolvidas.

7.2 Documento eletrônico ou documento digital é todo registro (dados ou informações) gerado ou recebido, armazenado e disponibilizado por meio de Sistemas de Tecnologia da Informação. Esses registros compreendem os documentos digitais, metadados e informações de controle associados às camadas de *software*: sistema operacional, gerenciador de banco de dados, aplicativos e sistemas coorporativos e eleitorais.

7.2.1 Os documentos citados devem ser incluídos nos procedimentos das cópias de segurança (*backups*), que têm por objetivo prevenir a perda de dados e/ou informações em caso de sinistros ou falhas de sistema, bem como garantir a restauração (*restore*) de forma rápida e eficiente para prover o perfeito funcionamento dos sistemas de TI do TRE-MG.

7.3 Outros termos: vide dicionário de termos e siglas.

NORMAS DE SEGURANÇA

8 DISPOSIÇÕES INICIAIS

8.1 Os usuários que exercem função de administração das cópias de segurança – *backups* – dos recursos de tecnologia da informação do TRE-MG, para efeito desta norma serão considerados administradores de *backup*.

8.2 O mero procedimento de cópias de segurança não pode ser confundido ou utilizado como uma estratégia de temporalidade – guarda ou preservação de longo prazo – e sim para a recuperação de desastres – *Disaster Recovery* –, perda de dados originais por apagamentos acidentais ou corrupção de dados.

8.3 A temporalidade – guarda e preservação de longo prazo das informações e arquivos eletrônicos –, deve ser definida pelas áreas de negócio do TRE-MG gestoras da informação, juntamente à Comissão de Segurança da Informação, e informadas à Secretaria de Tecnologia da Informação – STI – para providências de implementação.

9 REALIZAÇÃO DE CÓPIA DE SEGURANÇA

9.1 A STI, juntamente à Comissão de Segurança da Informação, deve definir os prazos de realização, retenção e descarte das informações armazenadas nas mídias de *backup*, incluindo seu prazo de retenção máximo, o que deve ser formalizado na política de *backup*.

9.2 Os *backups* deverão ser programados e realizados através de demanda formal dos administradores dos servidores.

9.2.1 O procedimento para formalização da demanda de *backups* deverá constar da Política de *Backup* elaborada pela STI.

9.3 A STI deve documentar e manter atualizadas as rotinas de *backup* das informações do TRE-MG armazenadas nos servidores de rede.

9.4 O *backup* das informações armazenadas nos servidores de rede deve ser realizado em horário de baixa utilização da rede local, sendo executado, preferencialmente, fora do horário de expediente.

9.5 A STI deve definir um plano de realização de *backups*, envolvendo a rotina de rodízio das mídias utilizadas, respeitando as especificações de armazenamento e vida útil destas.

9.6 Após a realização dos *backups* das informações, a STI deve certificar-se da conclusão bem sucedida destes, analisando, se for o caso, os arquivos de auditoria – *logs* – gerados, para garantir o resultado da operação.

9.6.1 Em caso de insucesso ou problemas na operação do *backup*, as causas deverão ser analisadas e reparadas e, quando necessário, um novo *backup* deverá ser imediatamente realizado.

9.7 O *backup* e a restauração dos arquivos de dados armazenados nas estações de trabalho ou nos dispositivos móveis são de responsabilidade única e exclusiva do usuário.

9.7.1 Compete à STI fornecer aos usuários orientações e recursos necessários à realização dos *backups* de sua estação de trabalho.

10 IDENTIFICAÇÃO DAS MÍDIAS DE CÓPIA DE SEGURANÇA

10.1 As mídias utilizadas no processo de realização do *backup* das informações armazenadas nos recursos de tecnologia da informação do TRE-MG devem possuir identificação.

10.1.1 A identificação das mídias deve ser suficiente para permitir, direta ou indiretamente, a localização e extração das informações nelas armazenadas.

10.2 As mídias utilizadas na realização de *backups* solicitados fora da rotina normal devem conter identificação diferenciada.

11 ARMAZENAMENTO DAS MÍDIAS DE CÓPIA DE SEGURANÇA

11.1 As informações do TRE-MG devem ser providas de *backups*, a serem armazenados periodicamente em endereços distintos.

11.1.1 Os locais de armazenamento de *backups* devem possuir requisitos de segurança adequados e estar localizados fisicamente em endereços distintos, distante do parque central de servidores do TRE-MG.

11.1.2 A quantidade de cópias de *backup* e os locais de armazenamento devem ser definidos pela STI.

11.2 A STI deve manter as mídias de *backup* armazenadas de forma a

permitir sua rápida localização e recuperação.

11.3 As informações contidas nas mídias de backup devem conter mecanismos de segurança de forma a preservar sua integridade física e lógica.

11.4 A STI deve garantir a continuidade das cópias de segurança, incluindo os casos de vencimento da data de validade das mídias e nos casos de evolução da tecnologia (*hardware* e *software*).

11.5 O transporte das mídias de *backup*, quando necessário, deve ser realizado por servidor da STI, devidamente autorizado, ou acompanhado por ele.

12 RESTAURAÇÃO DAS INFORMAÇÕES CONTIDAS NAS MÍDIAS DE CÓPIA DE SEGURANÇA

12.1 A STI deve elaborar documentação referente à realização de restaurações de arquivos dos *backups*.

12.2 A STI deve executar procedimentos periódicos de restauração das informações contidas nas mídias de *backup*, com vistas à verificação da integridade das informações gravadas.

12.3 A restauração das informações contidas na mídia de *backup* deverá ser realizada mediante solicitação formal dos administradores dos servidores.

12.3.1 O procedimento para formalização da restauração deverá constar na Política de *Backup* elaborada pela STI.

12.4 A restauração das informações contidas na mídia de *backup* deve ser feita somente nas seguintes situações:

12.4.1 Para recompor o funcionamento e/ou integridade do servidor de rede afetado;

12.4.2 Para restauração de informações diversas, sendo obrigatória a solicitação formal do gestor do sistema, se for o caso, ou da unidade responsável pela informação;

12.4.3 É vedada a restauração de *backups* diretamente sobre os ambientes originais de produção, exceto em situações de recuperação de desastre ou plano de contingência;

12.4.3.1 Os *backups* devem ser restaurados em locais provisórios

cabendo ao setor solicitante a análise das informações, sua integridade e autorização de sua inserção no ambiente de produção.

12.4.3.2 Os *backups*, para serem restaurados no ambiente de produção, também serão objeto de análise técnica de impacto a ser realizada pela STI.

12.4.4 Para verificação da integridade dos *backups*;

12.4.5 Para testes necessários de manutenção da infraestrutura pelos administradores de infraestrutura de TI.

13 DESCARTE E SUBSTITUIÇÃO DAS MÍDIAS DE CÓPIA DE SEGURANÇA

13.1 A STI deverá observar os critérios de validade definidos pelos fabricantes das mídias utilizadas para a realização de *backups*.

13.1.1 Nos casos de substituição das soluções técnicas adotadas de *backup* (*hardware* e *software*), as informações contidas nas mídias da antiga solução devem ser transferidas em sua totalidade para as mídias compatíveis com a nova solução.

13.1.2 A solução técnica obsoleta somente poderá ser completamente desativada após a confirmação de que todas as informações anteriores foram transferidas para a nova solução implementada.

13.2 O descarte das mídias utilizadas para o fim de *backup* deve ser realizado de forma a impossibilitar sua recuperação total ou parcial.

13.3 A coleta e o encaminhamento das mídias para o descarte devem ser acompanhados por servidor autorizado pela STI.

13.3.1 O processo de descarte das mídias, quando realizado por empresa contratada, deve ser realizado por empresa especializada que utilize procedimentos seguros, tais como incineração, trituração ou desmagnetização.

14 DISPOSIÇÕES FINAIS

14.1 Os usuários devem reportar os incidentes que afetam a segurança dos ativos ou o descumprimento da Política de Segurança da Informação à STI.

14.2 Em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação, a STI deverá ser imediatamente acionada para adotar as providências necessárias, podendo, inclusive, determinar a restrição temporária do acesso aos serviços do TRE-MG.

15 PENALIDADES

15.1 O Tribunal adotará as sanções legais cabíveis contra qualquer usuário ou entidade que venha a praticar atos que violem a Política de Segurança da Informação.

16 VIGÊNCIA E ATUALIZAÇÃO

16.1 Esta norma entra em vigor a partir da data de sua publicação, e sua atualização ocorrerá sempre que se fizer necessário através de proposição pela Comissão de Segurança da Informação, aprovação da Diretoria-Geral e publicação nos canais competentes para ciência aos usuários do TRE-MG.

17 EXCEÇÕES

17.1 Qualquer exceção a esta norma operacional deve ser aprovada pela Comissão de Segurança da Informação. A obtenção desta aprovação assegura que todas as alternativas razoáveis foram avaliadas e que os controles compensatórios são adequados para atenuar quaisquer riscos.

TRIBUNAL REGIONAL ELEITORAL DE MINAS GERAIS

ANEXO VIII

(a que se referem os arts. 3º, 4º e 5º da Resolução nº 945, de 17 de dezembro de 2013)

PSI - N 008	**NORMA GERAL DE SEGURANÇA PARA SISTEMAS ADMINISTRATIVOS E JUDICIAIS – TRE-MG**
Versão 2.5 21/06/2013	Política de Segurança da Informação da Justiça Eleitoral

SUMÁRIO

1. MATÉRIA DISCIPLINADA

1.1 Dispõe sobre as regras formais para controlar a gestão dos sistemas administrativos e judiciais implantados no Tribunal Regional Eleitoral de Minas Gerais – TRE-MG.

1.2 Orienta os usuários sobre competências, usos e responsabilidades associados à segurança da informação relacionados aos sistemas administrativos e judiciais no âmbito do TRE-MG.

1.3 Estabelece critérios referentes à disponibilização, instalação, distribuição, concessão de permissão de acesso e utilização dos sistemas administrativos e judiciais considerando o envolvimento dos recursos humanos no âmbito das atividades precípuas da Justiça Eleitoral.

2. OBJETIVO GERAL

2.1 Orientar os usuários sobre o uso e responsabilidades associadas à segurança da informação e estabelecer regras para implantação, gestão e uso de sistemas administrativos e judiciais, assim como definições referentes ao controle de acesso às informações ali registradas.

3. PÚBLICO-ALVO

3.1 Aplica-se a todos os gestores e usuários dos sistemas administrativos e judiciais do TRE-MG.

4. APLICAÇÃO

4.1 Norma de segurança de aplicação interna.

5. REFERÊNCIAS LEGAIS E NORMATIVAS

a) **Lei nº 9.609, de 19 de fevereiro de 1998 -** dispõe sobre a proteção de propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências;

b) **Lei nº 9.279, de 14 de maio de 1996 -** regula direitos e obrigações relativos à propriedade intelectual;

c) **Norma Técnica ABNT NBR ISO/IEC 27001:2006** - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação – Requisitos;

d) **Norma Técnica ABNT NBR ISO/IEC 27002:2005** - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação;

e) **Resolução nº 22.780/2008 - Política de Segurança da Informação da Justiça Eleitoral** – documento que registra as diretrizes da Alta Direção sobre o tema segurança da informação;

f) **Constituição Federal, art. 37, *caput* –** artigo em que se registra que a administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência;

g) **Instrução Normativa nº 1/2008, Gabinete de Segurança Institucional - Presidência da República, art. 5º, inciso VII -** disciplina a Gestão de Segurança da Informação e Comunicações na administração pública federal, direta e indireta, e dá outras providências;

h) **Norma Técnica - Gabinete de Segurança Institucional - Presidência da República - Norma Complementar nº 03/IN01/DSIC/GSIPR –** diretrizes para elaboração da Política de Segurança da Informação e Comunicações nos órgãos e entidades da administração pública federal;

i) **Resolução nº 90/2009/CNJ, arts. 10 e 13 –** dispõe sobre a gestão da tecnologia da informação.

6. RELAÇÃO COM A NBR/ISO/IEC 27001:2005

SEÇÃO	CONTROLE
Anexo A	A.7.1 – Responsabilidade pelos ativos A.10.3.2 – Aceitação de sistemas A.10.8.5 – Sistemas de informações do negócio A.10.9.3 – Informações publicamente disponíveis A.11.2 – Gerenciamento de acesso do usuário A.11.6 – Controle de acesso à aplicação e à informação A.13 – Gestão de incidentes de segurança da informação A.15 – Conformidade

7. CONCEITOS E DEFINIÇÕES

7.1 Sistemas administrativos: conjunto de programas ou *software* de uso corporativo, não finalísticos e que são executados no ambiente produtivo de tecnologia da informação.

7.1.1 São considerados sistemas administrativos somente aqueles desenvolvidos, implantados e/ou homologados pela Secrertaria de Tecnologia da Informação – STI –, para os quais esta prestará suporte e cuidará de sua manutenção corretiva e evolutiva.

7.2 Sistemas eleitorais: conjunto de programas ou *software* de uso corporativo que são executados no ambiente produtivo de tecnologia da informação, utilizados diretamente no processo eleitoral.

7.2.1 São considerados sistemas eleitorais somente aqueles desenvolvidos, implantados e/ou homologados pela Secretaria de Tecnologia da Informação – STI –, para os quais esta prestará suporte e cuidará de sua manutenção corretiva e evolutiva.

7.2.2 A segurança da informação para os sistemas eleitorais está regulamentada na PSI-N009 – Norma geral de segurança para sistemas eleitorais.

7.3 Sistemas judiciais: conjunto de programas ou *software* de uso corporativo que são executados no ambiente produtivo de tecnologia da informação, utilizados nas atividades relacionadas à prestação jurisdicional

7.3.1 São considerados sistemas judiciais somente aqueles desenvolvidos, implantados e/ou homologados pela Secrertaria de Tecnologia da Informação – STI –, para os quais esta prestará suporte e cuidará de sua manutenção corretiva e evolutiva.

7.4 Outros termos: vide dicionário de termos e siglas.

NORMAS DE SEGURANÇA

8. DISPOSIÇÕES GERAIS

8.1 Os sistemas administrativos e judiciais do TRE-MG somente podem ser utilizados para execução de atividades pertinentes e de interesse da instituição.

8.2 Os sistemas administrativos e judiciais devem ter um gestor nomeado por meio de portaria da Diretoria-Geral do Tribunal, recaindo esta gestão sobre um servidor e um suplente, ou mesmo uma comissão quando se tratar de sistemas corporativos que envolvam mais de uma área.

8.2.1 Será responsabilidade do gestor do sistema todas as decisões referentes a ele, desde sua implantação, permissões de acessos, definições de níveis de acesso, definição das informações restritas, periodicidade necessária de cópias de segurança, autorização para restauração de cópias de segurança, solicitações de manutenção evolutiva e corretiva visando a integridade das informações processadas, realização e homologação de testes, acompanhamento e parecer periódico sobre a disponibilidade do sistema até sua desativação.

8.3 Os sistemas administrativos e judiciais podem atender às necessidades de toda a instituição com o compartilhamento de suas informações ou seu cruzamento com outras bases de dados, respeitando as restrições de acesso definidas pelos respectivos gestores.

8.4 Os chefes das unidades interessados deverão encaminhar solicitação de acesso para os respectivos gestores dos sistemas, indicando os nomes dos servidores, lotação e perfil de acesso para os quais deseja autorização para acesso ao sistema.

8.5 Os acessos aos sistemas administrativos e judiciais somente serão permitidos mediante identificação e autenticação dos usuários, com vistas a permitir auditoria das operações neles realizadas.

8.6 Ao usuário deve ser disponibilizado uma conta de acesso, pessoal e intransferível.

8.7 É proibido o acesso à qualquer sistema administrativo e judicial, assim como às informações registradas em seus respectivos bancos de dados, sem a devida autorização do respectivo gestor do sistema.

8.8 O controle de acesso aos sistemas administrativos e judiciais será, sempre que possível, automatizado. Para tanto, o acesso deverá ser categorizado por faixas de usuário a serem definidas pela STI conforme demanda do TRE-MG.

8.8.1 A STI definirá sistema oficial de cadastramento para cada categoria de usuário e especificará, para cada um deles, a unidade administrativa ou servidor responsável pela manutenção do respectivo cadastro, devendo este zelar para que esteja sempre atualizado.

8.8.2 A mudança de lotação ou de perfil do usuário poderá gerar, sempre que possível automaticamente, alteração ou exclusão de acesso aos sistemas.

9. RESPONSABILIDADES DO GESTOR DE SISTEMA OU COMISSÃO

9.1 Compete ao gestor do sistema definir os perfis de acesso a ele, inclusive perfis com acesso às consultas consideradas restritas.

9.2 Os gestores dos sistemas deverão informar à STI tabela de temporalidade, restrições de acesso aos dados e política de cópias de segurança (*backup*) necessárias para administração do sistema em produção.

9.3 Os gestores dos sistemas administrativos deverão zelar pela qualidade do cadastro das informações ali registradas e promover ações para capacitação dos servidores usuários de cada sistema sempre que necessário.

9.4 O acesso aos sistemas administrativos somente será concedido com autorização do respectivo gestor, que será responsabilizado pela autorização de acesso indevida.

9.5 O gestor do sistema deverá estabelecer, com auxílio da STI, políticas e procedimentos para proteger as informações geradas e manipuladas por cada aplicação, incluindo as associadas à interconexão de sistemas de informações do negócio.

9.6 Compete ao gestor do sistema solicitar manutenções evolutivas deste.

9.7 O gestor do sistema deve estabelecer critérios de aceitação para novas funcionalidades, atualizações e novas versões e acompanhar testes apropriados durante o desenvolvimento e antes da aceitação do sistema.

9.8 O gestor do sistema deve prestar suporte de negócio quanto ao seu uso

correto.

10. COMPROMETIMENTO DOS USUÁRIOS

10.1 O usuário é responsável por todos os acessos realizados por meio de sua conta de identificação.

10.2 O usuário deve zelar pelo sigilo de sua senha de acesso, sendo responsável pelos possíveis danos que o seu mau uso ocasione.

10.3 Os usuários devem assinar um termo de responsabilidade e confidencialidade pela utilização dos sistemas administrativos e judiciais e pela segurança das informações neles registradas.

10.3.1 Os usuários que necessitam de privilégios especiais de administração de recursos de tecnologia da informação para uso restrito às necessidades de serviços, previamente justificados e aprovados pela STI e chefia imediata, devem assinar termo de responsabilidade específico.

10.4 Os usuários devem preservar o sigilo das informações obtidas por meio dos sistemas administrativos e judiciais, dentro e fora das dependências do TRE-MG.

10.5 As práticas de segurança da informação do TRE-MG devem ser seguidas e disseminadas por todos os usuários que executam atividades laborais no TRE-MG.

11. RESPEITO À PROPRIEDADE INTELECTUAL

11.1 A utilização de recursos de tecnologia da informação no ambiente do TRE-MG deve respeitar a legislação vigente referente à proteção da propriedade intelectual (direitos autorais, inclusive do *software*, e patentes).

12. TREINAMENTO E SUPORTE AOS SISTEMAS ADMINISTRATIVOS E JUDICIAIS

12.1 Os treinamentos referentes aos sistemas administrativos e judiciais devem ser conduzidos pela área de negócio, gestora do sistema, em parceria com a STI.

12.2 O suporte técnico dos sistemas administrativos e judiciais deve ser prestado pela STI, e o suporte de negócio deve ser prestado pela área de negócio.

12.3 Quando se tratar de sistemas corporativos, que abranjam mais de uma área de negócio, devem-se definir comissões ou grupos de trabalho que serão responsáveis tanto pelo treinamento quanto pelo seu suporte.

12.4 Todos os usuários devem ser formalmente comunicados por suas respectivas chefias sobre as responsabilidades administrativas, legais e sanções decorrentes da má utilização dos sistemas administrativos e judiciais.

13. USO DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO

13.1 As atualizações de versão dos sistemas administrativos e judiciais serão programadas para ocorrer após o expediente ou aos finais de semana e feriados.

13.1.1 Em casos excepcionais poderão ser efetuadas atualizações em outros dias e horários previamente comunicados.

13.1.2 A paralisação programada de quaisquer sistemas administrativos e judiciais deve ser comunicada com antecedência aos usuários, indicando os períodos de indisponibilidade.

13.2 A cópia de segurança (*backup*) das bases de dados dos sistemas administrtivos e judiciais é de responsabilidade da STI, que iniciará o procedimento a partir da implantação dos sistemas, conforme especificado pelo gestor do sistema e definido na norma PSI-N007 – norma geral de segurança para tratamento de mídias e de cópias de segurança (*backup*).

13.3 Quando houver a necessidade de restauração de base de dados de sistema administrativo ou judicial, o respectivo gestor deverá fazer solicitação formal à STI, que somente executará o procedimento após análise técnica favorável.

14. INCLUSÃO, ALTERAÇÃO, EXCLUSÃO E BLOQUEIO DE USUÁRIOS

14.1 A inclusão, a alteração e a exclusão de usuários para acesso a sistemas administrativos e judiciais devem ser solicitadas pela chefia imediata ao gestor do sistema por meio de formulário específico.

14.1.1 Os usuários devem manter atualizados seus dados cadastrais nas unidades responsáveis.

14.2 A chefia imediata é responsável por definir o perfil de acesso a ser liberado para uso dos sistemas administrativos e judiciais para os

usuários lotados em sua área.

14.3 Os sistemas corporativos poderão ter regulamentação própria, definida de acordo com o processo de trabalho a que se refere e que deverá ser observada por todos seus usuários.

14.4 Sistemas sensíveis podem ter restrições de uso adicionais, tais como uso de criptografia ou certificados digitais, por exemplo, de acordo com sua criticidade.

15. REGRAS E ÉTICA NO USO DA INTERNET/INTRANET

15.1 A integridade das informações disponibilizadas em sistemas publicamente acessíveis deve ser protegida, para prevenir modificações não autorizadas.

15.2 É vedado o uso de recursos e informações de sistemas do TRE-MG para constranger, assediar, ofender, caluniar, ameaçar ou causar prejuízos a qualquer pessoa, física ou jurídica, bem como para veicular opiniões político-partidárias ou que possam expor a instituição e seus servidores.

15.3 É vedado valer-se do prestígio da Justiça Eleitoral, utilizando-se de sistemas ou outro meio de comunicação fornecido pelo TRE-MG, para lograr vantagens ou impor-se mediante qualquer situação.

16. DISPOSIÇÕES FINAIS

16.1 Fica assegurado à STI, a qualquer tempo, tomar as medidas necessárias quando evidenciados os riscos à segurança da informação.

16.2 O desenvolvimento de sistemas será feito somente pela STI que prestará suporte somente aos sistemas, aplicativos e *softwares* por ela desenvolvidos, implantados e/ou homologados.

16.3 Os usuários e funcionários são responsáveis por suas contas, senhas, e por qualquer ação que venha ferir a confidencialidade, a integridade e a disponibilidade da informação.

16.4 O uso indevido dos recursos de tecnologia da informação do Tribunal Regional Eleitoral de Minas Gerais é passível de sanção disciplinar, de acordo com a legislação vigente e demais normas aplicadas à matéria.

17. PENALIDADES

17.1 O Tribunal adotará as sanções legais cabíveis contra qualquer usuário ou entidade que venha a praticar atos que violem a Política de Segurança da Informação.

18. VIGÊNCIA E ATUALIZAÇÃO

18.1 Esta norma operacional entra em vigor a partir da data de sua publicação e sua atualização ocorrerá sempre que se fizer necessário através de proposição pela Comissão de Segurança da Informação, aprovação da Diretoria-Geral e publicação nos canais competentes para ciência aos usuários do Tribunal.

19. EXCEÇÕES

19.1 Qualquer exceção a esta norma deve ser aprovada pela Comissão de Segurança da Informação. A obtenção desta aprovação assegura que todas as alternativas razoáveis foram avaliadas e que os controles compensatórios são adequados para atenuar quaisquer riscos.

TRIBUNAL REGIONAL ELEITORAL DE MINAS GERAIS

ANEXO IX

(a que se referem os arts. 3º, 4º e 5º da Resolução nº 945, de 17 de dezembro de 2013)

PSI - N 009	**NORMA GERAL DE SEGURANÇA PARA SISTEMAS ELEITORAIS TRE-MG**
Versão 2.5 04/07/2013	Política de Segurança da Informação da Justiça Eleitoral

SUMÁRIO

1 MATÉRIA DISCIPLINADA

1.1 Dispõe sobre as regras formais para controlar a gestão dos sistemas eleitorais implantados no Tribunal Regional Eleitoral de Minas Gerais – TRE-MG.

1.2 Orienta os usuários sobre competências, usos e responsabilidades associados à segurança da informação relacionados aos sistemas eleitorais no âmbito do TRE-MG.

1.3 Estabelece critérios referentes à disponibilização, instalação, distribuição, concessão de permissão de acesso e utilização dos sistemas eleitorais considerando o envolvimento dos recursos humanos no âmbito das atividades precípuas da Justiça Eleitoral.

2 OBJETIVO GERAL

2.1 Orientar os usuários sobre o uso e responsabilidades associados à utilização dos sistemas eleitorais e estabelecer regras para criação, utilização e administração de contas e senhas de acesso aos referidos sistemas e às informações ali registradas.

3 PÚBLICO-ALVO

3.1 Aplica-se a todos os gestores e usuários dos sistemas eleitorais autorizados pelo TRE-MG.

4 APLICAÇÃO

4.1 Norma de segurança de aplicação interna.

5 REFERÊNCIAS LEGAIS E NORMATIVAS

a) **BRASIL. Lei nº 9.609, de 19 de fevereiro de 1998.** Dispõe sobre a proteção de propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências;

b) **BRASIL. Lei nº 9.279, de 14 de maio de 1996.** Regula direitos e obrigações relativos à propriedade intelectual;

c) **Norma Técnica ABNT NBR ISO/IEC 27001:2006. Dispõe sobre** Tecnologia

da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos;

d) **Norma Técnica ABNT NBR ISO/IEC 27002:2005. Dispõe sobre** Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação;

e) **Resolução nº 22.780/2008, que dispõe sobre Política de Segurança da Informação da Justiça Eleitoral** e registra as diretrizes da Alta Direção sobre o tema segurança da informação;

f) **BRASIL. Constituição Federal (1988), art. 37, *caput.*** Artigo que dispõe que a administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência;

g) **Instrução Normativa nº 1/2008, Gabinete de Segurança Institucional – Presidência da República, art. 5º, inciso VII. Artigo que** disciplina a Gestão de Segurança da Informação e Comunicações na administração pública federal, direta e indireta, e dá outras providências;

h) **Norma Técnica – Gabinete de Segurança Institucional – Presidência da República – Norma Complementar nº 03/IN01/DSIC/GSIPR, que dispõe sobre** diretrizes para elaboração da Política de Segurança da Informação e Comunicações nos órgãos e entidades da administração pública federal;

i) **Resolução nº 90/2009/CNJ, arts. 10 e 13. Artigos que** dispõem sobre a gestão da tecnologia da informação.

6 RELAÇÃO COM A NBR/ISO/IEC 27001:2005

SEÇÃO	CONTROLE
Anexo A	A.7.1 – Responsabilidade pelos ativos A.10.3.2 – Aceitação de sistemas A.10.8.5 – Sistemas de informações do negócio A.10.9.3 – Informações publicamente disponíveis A.11.2 – Gerenciamento de acesso do usuário A.11.6 – Controle de acesso à aplicação e à informação A.13 – Gestão de incidentes de segurança da informação A.15 – Conformidade

7 CONCEITOS E DEFINIÇÕES

7.1 Segurança da Informação [ABNT NBR ISO/IEC 27002] – preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confidencialidade, podem também estar envolvidas.

7.2 Cadastramento de usuários – a informação de todos os possíveis usuários dos sistemas eleitorais em sistema específico no Sub-sistema de Instalação Segura (SIS) quando for o caso.

7.3 Autorização de acesso – a delegação de acesso concedida em um sistema eleitoral a um usuário previamente cadastrado com permissão para execução de determinadas funcionalidades naquele sistema.

7.4 Gestor de autorização – o usuário do sistema previamente definido como responsável por efetuar as autorizações de acesso aos sistemas eleitorais em sistema específico no âmbito de sua competência.

7.5 ODIN – o sistema informatizado desenvolvido pelo TSE para cadastramento dos usuários, criação dos perfis de acesso, realização e controle das autorizações de acesso aos sistemas eleitorais.

7.6 Permissão – autorização de acesso concedida pelos SETORES aos usuários previamente cadastrados no SIS.

7.7 Gestor do sistema eleitoral – o setor, a coordenadoria ou a secretaria previamente definido como responsável pela administração dos sistemas, que ficará responsável por gerenciar as autorizações solicitadas e cadastradas no sistema específico.

7.8 Setores – os cartórios eleitorais, centrais de atendimento, regiões eleitorais e unidades da Secretaria do TRE-MG que utilizem sistema eleitoral.

7.9 Oficialização – procedimento necessário para que o sistema passe a operar na fase oficial.

7.10 Sistemas eleitorais – conjunto de programas ou *software* de uso corporativo que são executados no ambiente produtivo de tecnologia da informação, utilizados diretamente no processo eleitoral.

7.10.1. Sistema Eleitoral Stand Alone – sistema eleitoral que é executado

no computador cliente/estação de trabalho.

7.10.2. Sistema Eleitoral Remoto – sistema eleitoral que é executado no computador servidor.

7.10.3. São considerados sistemas eleitorais somente aqueles implantados e/ou homologados pela Secretaria de Tecnologia da Informação – STI/TRE-MG –, para os quais esta prestará suporte e cuidará de sua manutenção corretiva e evolutiva.

7.11 Atualização de *firmware* – atualização do conjunto de instruções programadas diretamente em um *hardware*.

7.12 Certificação – registro eletrônico que contém a chave pública do titular.

7.13 Autenticação – processo através do qual é validada a identidade de um utilizador, dispositivo ou processo.

7.14 Outros termos: vide dicionário de termos e siglas.

NORMAS DE SEGURANÇA

8 DISPOSIÇÕES GERAIS

8.1 Os sistemas eleitorais do TRE-MG somente podem ser utilizados para execução de atividades pertinentes e de interesse da instituição.

8.2 Os sistemas eleitorais devem ter um gestor nomeado, conforme Anexo I, recaindo esta gestão sobre um servidor e um suplente, ou mesmo uma comissão quando envolverem mais de uma área de negócio.

8.2.1. Será responsabilidade do gestor do sistema eleitoral todas as decisões referentes a ele, desde sua implantação, permissões de acessos, definição das informações restritas, autorização para restauração de cópias de segurança, realização e homologação de testes, acompanhamento e parecer periódico sobre a disponibilidade do sistema até sua desativação.

8.2.2. Para o desempenho de suas atribuições, o gestor do sistema eleitoral deverá observar a legislação pertinente e as instruções advindas da STI do TSE e do TRE-MG.

8.3 Os sistemas eleitorais podem atender às necessidades de toda a instituição com o compartilhamento de suas informações ou cruzamento delas com outras bases de dados, respeitando as restrições de acesso definidas pelos respectivos gestores.

8.4 O acesso aos sistemas eleitorais somente serão permitidos mediante identificação e autenticação dos usuários, com vistas a permitir auditoria das operações neles realizadas.

8.5 Ao usuário deve ser disponibilizada uma conta de acesso, pessoal e intransferível.

8.6 É proibido o acesso a qualquer sistema eleitoral, assim como às informações registradas em seus respectivos bancos de dados, sem a devida autorização do respectivo gestor.

8.7 O controle de acesso aos sistemas eleitorais será automatizado, sempre que possível.

8.7.1. A mudança de lotação ou de perfil do usuário poderá gerar, sempre que possível automaticamente, alteração ou exclusão de acesso aos sistemas.

9 ATRIBUIÇÕES DO GESTOR DO SISTEMA OU COMISSÃO

9.1 Compete ao gestor do sistema eleitoral zelar pela qualidade do cadastro das informações ali registradas.

9.2 O gestor do sistema eleitoral deve promover ações para capacitação dos servidores usuários do sistema sempre que necessário.

9.3 O gestor do sistema eleitoral deve conduzir os treinamentos referentes aos respectivos sistemas em parceria com a Secretaria de Tecnologia da Informação – STI/TRE-MG.

9.4 O gestor do sistema eleitoral deve prestar suporte de negócio quanto ao seu uso correto.

10 COMPROMETIMENTO DOS USUÁRIOS

10.1 O usuário é responsável por todos os acessos realizados por meio de sua conta de identificação.

10.2 O usuário deve zelar pelo sigilo de sua senha de acesso, sendo responsável pelos possíveis danos que o seu mau uso ocasione.

10.3 Os usuários devem assinar um termo de responsabilidade e confidencialidade pela utilização dos sistemas eleitorais e pela segurança das informações neles registradas.

10.3.1 Os usuários que necessitem de privilégios especiais de administração de recursos de tecnologia da informação para uso restrito às necessidades de serviços, previamente justificados e aprovados pela STI/TRE-MG e chefia imediata, devem assinar termo de responsabilidade específico.

10.4 Os usuários devem preservar o sigilo das informações obtidas por meio dos sistemas eleitorais, dentro e fora das dependências do TRE-MG.

10.5 As práticas de segurança da informação do TRE-MG devem ser seguidas e disseminadas por todos os usuários que executam atividades laborais no TRE-MG.

11 RESPEITO À PROPRIEDADE INTELECTUAL

11.1 A utilização de recursos de tecnologia da informação no ambiente do

TRE-MG deve respeitar a legislação vigente referente à proteção da propriedade intelectual (direitos autorais, inclusive do *software*, e patentes).

12 TREINAMENTO DOS USUÁRIOS

12.1 O treinamento referente aos sistemas eleitorais deve ser conduzido pelo gestor do sistema eleitoral em parceria com a STI/TRE-MG.

12.2 O suporte técnico aos sistemas eleitorais deve ser prestado pela STI/TRE-MG, e o suporte de negócio, pelo gestor do sistema eleitoral.

12.2.1. Quando se tratar de sistema destinado ao ambiente externo, as zonas eleitorais serão responsáveis pelo suporte, orientadas pelo gestor do sistema eleitoral e pela STI/TRE-MG.

12.3 Todos os usuários devem ser formalmente comunicados por suas respectivas chefias sobre as responsabilidades administrativas, legais e sanções decorrentes da má utilização dos sistemas eleitorais.

13 DISPONIBILIZAÇÃO, INSTALAÇÃO E VERIFICAÇÃO DOS SISTEMAS ELEITORAIS

13.1 Os sistemas eleitorais deverão ser homologados pelo TSE e TRE-MG.

13.2 Os arquivos de instalação segura dos sistemas eleitorais serão disponibilizados pela STI/TRE-MG.

13.3 Os sistemas eleitorais deverão ser instalados apenas em máquinas homologadas pelo TRE-MG.

13.4 Não será permitida instalação de sistema eleitoral do TSE, de outros Tribunais ou da internet sem a prévia autorização da STI/TRE-MG.

13.5 É de responsabilidade do usuário do sistema eleitoral manter atualizada a versão dos sistemas eleitorais, de acordo com as instruções da STI/TRE-MG.

14 CADASTRAMENTO, ALTERAÇÃO, EXCLUSÃO E BLOQUEIO DE USUÁRIOS

DO CADASTRAMENTO DOS USUÁRIOS

14.1 O cadastramento dos usuários dos sistemas eleitorais será realizado, de acordo com a relação de sistemas e responsáveis publicados pela STI/TRE-MG – Anexos I e II .

14.2 Para os sistemas eleitorais *Stand Alone*, o cadastramento dos usuários será realizado pela STI/TRE-MG no ambiente do TRE, e pelo chefe no ambiente da Zona Eleitoral, da central de atendimento e da região eleitoral.

14.3 Para os sistemas eleitorais remotos, o cadastramento dos usuários será realizado de forma centralizada pela STI/TRE-MG.

14.4 Para os sistemas eleitorais *Stand Alone*, as permissões de acesso para os usuários serão cadastradas pela STI/TRE-MG no ambiente do TRE e pelo chefe no ambiente da Zona Eleitoral, da central de atendimento e da região eleitoral.

DO CADASTRAMENTO DAS PUBLICAÇÕES DE ACESSO

14.5 O cadastramento de publicações de acesso para os sistemas eleitorais remotos será realizado de forma centralizada pela STI/TRE-MG no sistema ODIN.

14.6 Os chefes de cartório serão cadastrados como gestores de autorização de acesso aos sistemas eleitorais remotos em suas respectivas Zonas Eleitorais.

DA CONCESSÃO DE AUTORIZAÇÃO DE ACESSO

14.7 Ficará a cargo do gestor do sistema eleitoral a concessão das autorizações de acesso aos sistemas eleitorais pelos quais é responsável.

DA EFETIVAÇÃO DA AUTORIZAÇÃO DE ACESSO

14.8 Nas Zonas Eleitorais caberá ao chefe de cartório a efetivação das autorizações de acesso concedidas.

14.9 Na Secretaria caberá à STI/TRE-MG a efetivação das autorizações de acesso concedidas pelo gestor do sistema eleitoral.

14.9.1 Na secretaria, havendo possibilidade técnica e operacional, a STI/TRE-MG poderá delegar ao gestor do sistema eleitoral a efetivação das autorizações de acesso.

DA MANUTENÇÃO DAS AUTORIZAÇÕES DE ACESSO

14.10 Nas Zonas Eleitorais, centrais de atendimento e regiões eleitorais ficará a cargo do chefe o acompanhamento e a atualização regular das autorizações de acesso concedidas nos sistemas pelos quais é

responsável.

14.11 Na secretaria, ficará a cargo do gestor do sistema eleitoral o acompanhamento regular das autorizações de acesso concedidas nos sistemas pelos quais é responsável.

14.11.1 Em caso de constatação de inconsistência no cadastramento de usuário e/ou autorização de acesso concedida, caberá ao gestor do sistema eleitoral solicitar à STI/TRE-MG as devidas correções.

14.11.2 Caso a STI/TRE-MG tenha delegado a efetivação das autorizações de acesso ao gestor do sistema eleitoral, caberá a este a correção das inconsistências.

DOS SISTEMAS PARA AMBIENTE EXTERNO

14.12 Para os sistemas eleitorais instalados no ambiente externo, a instalação e a permissão serão de responsabilidade do usuário.

15 OFICIALIZAÇÃO DOS SISTEMAS ELEITORAIS

15.1 Para a oficialização dos sistemas eleitorais será necessária senha gerada pelo TSE específica para cada sistema e Zona Eleitoral.

15.1.1 As senhas de oficialização dos sistemas eleitorais são confidenciais e serão enviadas pelo Presidente do TRE-MG, por meio de ofício-circular em envelope lacrado, aos MMMM. Juízes das respectivas Zonas Eleitorais.

15.1.2 Na hipótese de extravio da senha de oficialização, caberá ao MM. Juiz Eleitoral solicitar nova senha ao Presidente do TRE-MG, que poderá ser encaminhada por meio digital em procedimento regulamentado pela STI/TRE-MG.

15.1.3 No caso dos sistemas eleitorais remotos, quando aplicável, antes da oficialização nas Zonas Eleitorais, é necessária a oficialização dos sistemas no ambiente do TRE.

16 UTILIZAÇÃO DE ESTAÇÕES DE TRABALHO

16.1 As estações de trabalho fornecidas devem possuir configurações de *hardware* e *software* homologadas pela STI/TRE-MG.

16.2 O usuário não deve alterar as configurações, padronizadas pela

STI/TRE-MG, dos *softwares* instalados nas estações de trabalho.

17 URNA ELETRÔNICA

17.1 Caberá às Zonas e regiões eleitorais efetuar os procedimentos de aceite das urnas eletrônicas executando o teste de funcionamento com aplicativo específico definido pela STI/TRE-MG nas urnas eletrônicas antes da carga oficial.

17.2 Caberá às Zonas e regiões eleitorais realizar a atualização de *firmware*, certificação e autenticação nas urnas eletrônicas, de acordo com instruções da STI/TRE-MG.

17.2.1 Havendo possibilidade técnica, o procedimento supra poderá ser realizado de forma centralizada no TRE-MG.

17.3 Caberá às Zonas Eleitorais efetuar a conferência do relógio e dados de carga das urnas eletrônicas, de acordo com o cronograma especificado pela STI/TRE-MG.

17.4 Caberá às Zonas Eleitorais o controle, a distribuição e a utilização do aplicativo de ajuste de data e hora.

17.4.1 Caberá ao TRE-MG a geração e o encaminhamento das mídias, bem como a distribuição da respectiva senha para ativação do aplicativo ao MM. Juiz(a) Eleitoral.

PROCEDIMENTOS PÓS-ELEIÇÃO

17.5 Após a totalização de resultado, caberá às Zonas Eleitorais a conferência do recebimento no TRE-MG dos arquivos de urna eletrônica, conforme orientação da STI/TRE-MG.

17.6 As urnas eletrônicas de seção em situação *sub judice* deverão permanecer lacradas com os respectivos *flashes* de votação, até a data prevista na resolução vigente ou decisão final, devendo ser observando o maior prazo.

17.7 As mídias de carga deverão permanecer nas Zonas Eleitorais até a data estipulada na resolução vigente, a partir da qual poderão ser devolvidas ao TRE-MG, conforme orientação da STI/TRE-MG.

17.8 As memórias de resultado de votação deverão ficar armazenadas no cartório para serem usadas nas próximas eleições.

18 *BACKUP*

18.1 Caberá às Zonas Eleitorais a realização de cópias de segurança do GEDAI-UE em todos os computadores que possuírem o sistema oficial instalado, conforme orientação da STI/TRE-MG.

18.2 Caberá à STI/TRE-MG a disponibilização de área compartilhada e o sistema específico para o armazenamento dos arquivos de *backup* de forma centralizada.

19 DISPOSIÇÕES FINAIS

19.1 Fica assegurado à STI/TRE-MG, a qualquer tempo, tomar as medidas necessárias quando evidenciados os riscos à segurança da informação nos sistemas eleitorais.

19.2 A STI/TRE-MG prestará suporte somente aos sistemas eleitorais implantados e/ou homologados por ela.

19.3 Os usuários e funcionários são responsáveis por suas contas, senhas, e por qualquer ação que venha ferir a confidencialidade, a integridade e a disponibilidade da informação.

19.4 O uso indevido dos sistemas eleitorais é passível de sanção disciplinar, de acordo com a legislação vigente e demais normas aplicadas à matéria.

20 PENALIDADES

20.1 O Tribunal adotará as sanções legais cabíveis contra qualquer usuário ou entidade que venha a praticar atos que violem a Política de Segurança da Informação.

21 VIGÊNCIA E ATUALIZAÇÃO

21.1 Esta norma operacional entra em vigor a partir da data de sua publicação, e sua atualização ocorrerá sempre que se fizer necessária através de proposição pela Comissão de Segurança da Informação, aprovação da Diretoria-Geral e publicação nos canais competentes para ciência aos usuários do TRE-MG.

22 EXCEÇÕES

22.1 Qualquer exceção a esta norma deve ser aprovada pela Comissão de Segurança da Informação. A obtenção desta aprovação assegura que todas as alternativas razoáveis foram avaliadas e que os controles compensatórios são adequados para atenuar quaisquer riscos.

23 ANEXO I

Relação de Sistemas e Responsáveis (Eleição Municipal)

Sistema	Tipo	Ambiente	Oficialização	Gestor
ELO	*Stand Alone*	Interno	Não se aplica	CRE
GEDAI-UE	*Stand Alone*	Interno	Manual	STI
TRANSPORTADOR	*Stand Alone*	Interno	Automática	STI
GERENCIAMENTO	Remoto	Interno	Manual	STI
CANDIDATURAS TRE	Remoto	Interno	Manual	SJU
CANDIDATURAS ZE	Remoto	Interno	Manual	ZE
CANDEX	*Stand Alone*	Externo	Não se aplica	SJU
HORÁRIO ELEITORAL TRE	Remoto	Interno	Manual	SJU
HORÁRIO ELEITORAL ZE	Remoto	Interno	Manual	SJU
SPCE CADASTRO	*Stand Alone*	Externo	Não se aplica	SCI
SPCE WEB	Remoto	Interno	Não se aplica	SCI
SPCE Envio	*Stand Alone*	Interno	Não se aplica	SCI
SRCF	*Stand Alone*	Externo	Não se aplica	SCI
RACE/RACEP	Remoto	Externo	Não se aplica	SCI
SIMULADOR DE ELEIÇÕES	*Stand Alone*	Interno	Não se aplica	STI
WEB ARQ URNA	Remoto	Interno	Não se aplica	STI
CONFIGURADOR DE ELEIÇÕES	Remoto	Interno	Não se aplica	STI
MONITOR DE FILAS DA TOTALIZAÇÃO	Remoto	Interno	Não se aplica	STI
ELO 6	*Stand Alone*	Interno	Não se aplica	CRE
FILIAWEB	Remoto	Externo	Não se aplica	CRE
PESQELE	Remoto	Externo	Não se aplica	SJU
SISTEMAS ELEITORAIS WEB	*Stand Alone*	Interno	Não se aplica	STI
SAVP	*Stand Alone*	Interno	Automática	Comissão

24 ANEXO II

Relação de Sistemas e Responsáveis (Eleição Geral)

Sistema	Tipo	Ambiente	Oficialização	Gestor
ELO	*Stand Alone*	Interno	Não se aplica	CRE
GEDAI-UE	*Stand Alone*	Interno	Manual	STI
TRANSPORTADOR	*Stand Alone*	Interno	Automática	STI
GERENCIAMENTO	Remoto	Interno	Manual	STI/Comissão
CANDIDATURAS TRE	Remoto	Interno	Manual	SJU
CANDEX	*Stand Alone*	Externo	Não se aplica	SJU
HORÁRIO ELEITORAL TRE	Remoto	Interno	Manual	SJU
SPCE CADASTRO	*Stand Alone*	Externo	Não se aplica	SCI
SPCE WEB	Remoto	Interno	Não se aplica	SCI
SPCE Envio	*Stand Alone*	Interno	Não se aplica	SCI
SRCF	*Stand Alone*	Externo	Não se aplica	SCI
RACE/RACEP	Remoto	Externo	Não se aplica	SCI
SIMULADOR DE ELEIÇÕES	*Stand Alone*	Interno	Não se aplica	STI
WEB ARQ URNA	Remoto	Interno	Não se aplica	STI
CONFIGURADOR DE ELEIÇÕES	Remoto	Interno	Não se aplica	STI
MONITOR DE FILAS DA TOTALIZAÇÃO	Remoto	Interno	Não se aplica	STI
ELO 6	*Stand Alone*	Interno	Não se aplica	CRE
FILIAWEB	Remoto	Externo	Não se aplica	CRE
PESQELE	Remoto	Externo	Não se aplica	SJU
SISTEMAS ELEITORAIS WEB	*Stand Alone*	Interno	Não se aplica	STI
SAVP	*Stand Alone*	Interno	Automática	Comissão

TRIBUNAL REGIONAL ELEITORAL DE MINAS GERAIS

ANEXO X

(a que se referem os arts. 3º, 4º e 5º da Resolução nº 945, de 17 de dezembro de 2013)

PSI - Dicionário	DICIONÁRIO DE TERMOS E SIGLAS TRE-MG
Versão 1.0 28/05/2013	Política de Segurança da Informação da Justiça Eleitoral

Siglas:

SGP: Secretaria de Gestão de Pessoas
STI: Secretaria de Tecnologia da Informação
TRE-MG: Tribunal Regional Eleitoral de Minas Gerais
TSE: Tribunal Superior Eleitoral
JE: Justiça Eleitoral
SGSI: sistema de gestão da segurança da informação
PSI: política de segurança da informação

Termos:

ativo
qualquer coisa que tenha valor para a organização
[ISO/IEC 13335-1:2004]

aceitação do risco
decisão de aceitar um risco
[ABNT ISO/IEC Guia 73:2005]

ameaça
causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização
[ISO/IEC 13335-1:2004]

análise de riscos
uso sistemático de informações para identificar fontes e estimar o risco
[ABNT ISO/IEC Guia 73:2005]

análise/avaliação de riscos
processo completo de análise e avaliação de riscos
[ABNT ISO/IEC Guia 73:2005]

avaliação de riscos
processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco
[ABNT ISO/IEC Guia 73:2005]

atividades críticas
conjunto de processos vinculados às atividades precípuas da Justiça Eleitoral, cuja interrupção ocasiona severos transtornos

[Resolução nº 22.780/2008/TSE]

atividades precípuas
conjunto de procedimentos e tarefas que utilizam recursos tecnológicos, humanos e materiais, inerentes à atividade fim da Justiça Eleitoral, contemplando todos os ambientes existentes, no âmbito do Tribunal Superior Eleitoral e Tribunais Regionais Eleitorais
[Resolução nº 22.780/2008/TSE]

backbone
infraestrutura central de interligação de equipamentos que compõem uma rede de comunicação

backup
cópias de segurança de arquivos
[ABNT NBR ISO/IEC 17799:2005]

código malicioso
programa ou *software* especificamente desenvolvido para executar ações danosas em um computador ou obter informações de forma ilícita

confidencialidade
propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados
[ISO/IEC 13335-1:2004]

criticidade
grau de importância da informação para a continuidade das atividades precípuas da Justiça Eleitoral
[Resolução nº 22.780/2008/TSE]

controle
forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal
NOTA Controle é também usado como um sinônimo para proteção ou contramedida.
[ABNT NBR ISO/IEC 17799:2005]

diretriz
descrição que orienta o que deve ser feito e como para se alcançarem os objetivos estabelecidos nas políticas
[ISO/IEC 13335-1:2004]

datacenter
ambiente composto pelos equipamentos centrais de processamento de dados (servidores e ativos de rede) que executam e armazenam a maioria dos sistemas e dados corporativos, compartilhando seus recursos para todos os usuários da organização (clientes internos e externos)

disponibilidade
propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada
[ISO/IEC 13335-1:2004]

declaração de aplicabilidade
declaração documentada que descreve os objetivos de controle e os controles que são pertinentes e aplicáveis ao SGSI da organização
NOTA Os objetivos de controle e os controles estão baseados nos resultados e conclusões dos processos de análise/avaliação de riscos e tratamento de risco, dos requisitos legais ou regulamentares, obrigações contratuais e os requisitos de negócio da organização para a segurança da informação.

[ABNT NBR ISO/IEC 27001:2006]

evento de segurança da informação
uma ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação
[ISO/IEC TR 18044:2004]

extranet
porção da rede de computadores de uma empresa que faz uso da internet para partilhar com segurança parte do seu sistema de informação

incidente de segurança da informação
um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação
[ISO/IEC TR 18044:2004]

internet
rede mundial de computadores baseada em padrões abertos

intranet
rede privada de computadores que segue os padrões da internet

integridade
propriedade de salvaguarda da exatidão e completeza de ativos
[ISO/IEC 13335-1:2004]

gestão de riscos
atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos
NOTA A gestão de riscos geralmente inclui a análise/avaliação de riscos, o tratamento de riscos, a aceitação de riscos e a comunicação de riscos.
[ABNT ISO/IEC Guia 73:2005]

hacker
pessoa que tenta acessar sistemas sem autorização, usando técnicas próprias ou não, no intuito de ter acesso a determinado ambiente para proveito próprio ou de terceiros. Dependendo dos objetivos da ação, podem ser chamados de *Cracker*, *Lammer* ou *BlackHat*.
[ABNT NBR ISO/IEC 17799:2005]

hardware
equipamentos de forma geral, em particular equipamentos de tecnologia da informação

firewall
sistema ou combinação de sistemas que protege a fronteira entre duas ou mais redes
[ABNT NBR ISO/IEC 17799:2005]

gateway
máquina que funciona como ponto de conexão entre duas redes
[ABNT NBR ISO/IEC 17799:2005]

logging
processo de estocagem de informações sobre eventos que ocorreram num *firewall* ou numa rede
[ABNT NBR ISO/IEC 17799:2005]

política
intenções e diretrizes globais formalmente expressas pela direção
[ABNT NBR ISO/IEC 17799:2005]

recursos de processamento da informação
qualquer sistema de processamento da informação, serviço ou infra-estrutura, ou as instalações físicas que os abriguem
[ABNT NBR ISO/IEC 17799:2005]

risco residual
risco remanescente após o tratamento de riscos
[ABNT ISO/IEC Guia 73:2005]

sala-cofre
ambiente modular estanque, testado e certificado, que protege o datacenter contra fogo, calor, umidade, gases corrosivos, fumaça, água, roubo, arrombamento, acesso indevido, sabotagem, impacto, pó, explosão, magnetismo e armas de fogo

***site* ou sítio**
primariamente, designa qualquer lugar ou local delimitado (sítio arquitetônico, sítio paisagístico, sítio histórico, entre outros), mas, quando referenciando um local numa rede de computadores (*website*), designa um sítio virtual, um conjunto de páginas virtualmente localizado em algum ponto da rede

segurança da informação
preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas
[ABNT NBR ISO/IEC 17799:2005]

sistema de gestão da segurança da informação
a parte do sistema de gestão global, baseado na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação
NOTA O sistema de gestão inclui estrutura organizacional, políticas, atividades de planejamento, responsabilidades, práticas, procedimentos, processos e recursos.
[ABNT NBR ISO/IEC 27001:2006]

sistemas administrativos
conjunto de programas ou *software* de uso corporativo, não finalísticos e que são executados no ambiente produtivo de tecnologia da informação

sistemas eleitorais
conjunto de programas ou *software* de uso corporativo que são executados no ambiente produtivo de tecnologia da informação, utilizados diretamente no processo eleitoral

sistemas judiciais
conjunto de programas ou *software* de uso corporativo que são executados no ambiente produtivo de tecnologia da informação, utilizados nas atividades relacionadas à prestação jurisdicional

software
conjunto de instruções e dados processado pelos computadores, também referenciado como programas, aplicativos ou sistemas

terceira parte
pessoa ou organismo reconhecido como independente das partes envolvidas, no que se refere a um dado

assunto
[ABNT ISO/IEC Guia 2:1998]

tratamento do risco
processo de seleção e implementação de medidas para modificar um risco
[ABNT ISO/IEC Guia 73:2005]
NOTA Em algumas normas o termo “controle” é usado como um sinônimo para “medida”.

usuário
quem utiliza, de forma autorizada, recursos inerentes às atividades precípuas da Justiça Eleitoral
[Resolução nº 22.780/2008/TSE]

vulnerabilidade
fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças
[ABNT NBR ISO/IEC 17799:2005]

wireless
sistema de comunicação que não requer fios para transportar sinais
[ABNT NBR ISO/IEC 17799:2005]

TRIBUNAL REGIONAL ELEITORAL DE MINAS GERAIS

~~ANEXO XI~~

~~(a que se refere o art. 6º da Resolução n º 945, de 17 de dezembro de 2013)~~

Anexo revogado pela Resolução TRE nº 1.091/2018

~~TERMO DE CIÊNCIA DE NORMAS DE SEGURANÇA DA INFORMAÇÃO~~

~~Nome:~~ _____

~~Cargo/Função:~~ _____

~~Matrícula:~~ _____

~~Lotação:~~ _____

~~□ PSI-N001 – Norma geral de segurança para usuários.~~
~~□ PSI-N002 – Norma geral de segurança física de instalações.~~
~~□ PSI-N003 – Norma específica de segurança para profissionais de TI.~~
~~□ PSI-N004 – Norma geral de segurança para controle dos acessos a rede de comunicação de dados.~~
~~□ PSI-N005 – Norma geral de segurança sobre códigos maliciosos.~~
~~□ PSI-N006 – Norma específica de segurança para equipamentos servidores de rede de dados.~~
~~□ PSI-N007 – Norma geral de segurança para tratamento de mídias e cópias de segurança.~~
~~□ PSI-N008 – Norma geral de segurança para sistemas administrativos e judiciais.~~
~~□ PSI-N009 – Norma geral de segurança para sistemas eleitorais.~~
~~□ ____~~

~~Declaro estar ciente das normas de segurança da informação e comprometo-me a cumpri-las, promovendo a Política de Segurança da Informação da Justiça Eleitoral. Comprometo-me também a comunicar imediatamente ao TRE-MG os casos de não observância de tais normas.~~

~~Estou ciente de que o Tribunal poderá adotar as sanções legais e contratuais cabíveis contra qualquer usuário ou entidade que venha a praticar atos que violem a Política de Segurança da Informação.~~

_____, _____ de _____de _____.
~~Local~~

_____
~~Assinatura do Juiz Membro ou servidor~~