TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE

Republicada por incorreção em 30/05/2014 págs. 02/04.

RESOLUÇÃO Nº 006, DE 28 DE ABRIL DE 2014.

Estabelece a Política de Segurança da Informação no âmbito da Justiça Eleitoral do Rio Grande do Norte.

O TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE, no exercício das atribuições que lhe são conferidas pelo art. 17, inciso II, do Regimento Interno (Resolução nº 9, de 24 de maio de 2012); e

Considerando que o TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE gera, absorve e mantém grande volume de informações essenciais ao exercício de suas competências e que essas informações devem permanecer íntegras, disponíveis e, quando for o caso, sob sigilo;

Considerando que o volume de informações mencionado, ressalvados os direitos autorais, integra o patrimônio da Justiça Eleitoral do Rio Grande do Norte e deve ser protegido;

Considerando que os diferentes meios de suporte, veiculação e armazenamento da informação são vulneráveis a incidentes como desastres naturais, acessos não autorizados, mau uso, falhas de equipamentos, extravio e furto, dentre outros;

Considerando que a gestão da informação precisa nortear todos os processos de trabalho das unidades do Tribunal Regional Eleitoral do Rio Grande do Norte e deve ser respaldada por uma política corporativa de segurança da informação,

RESOLVE:

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

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 do Rio Grande do Norte.

Art. 3º Compõe a Política de Segurança de Informação o documento constante do Anexo I desta Resolução.

Art. 4º 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 no Anexo I desta Resolução serão formalizadas por meio de portaria da Presidência deste Tribunal mediante proposta da Comissão Permanente de Segurança da Informação instituída pela Resolução TRE/RN nº 008/2009.

Art. 5º Todos os usuários de recursos de tecnologia da informação no âmbito do Tribunal deverão atestar ciência às normas da PSI mediante a assinatura do "Termo de Ciência da Política de Segurança de Informação" disponível na *Intranet*.

Art. 6º 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. 7º 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. 8º Casos omissos serão decididos pela Diretoria-Geral.

Art. 9º Esta Resolução entrará em vigor na data de sua publicação.

Natal, 28 de abril de 2014.

Desembargador Amílcar Maia
Presidente

Desembargador João Rebouças
Vice-Presidente e Corregedor Regional Eleitoral

Juiz Nilson Roberto Cavalcanti Melo

Juiz Artur Cortez Bonifácio

Juiz Verlano de Queiroz Medeiros

Juiz Carlo Virgilio Fernandes de Paiva

Doutor Gilberto Barroso de Carvalho Júnior
Procurador Regional Eleitoral

TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE (ANEXO I DA RESOLUÇÃO Nº 006, DE 28 DE ABRIL DE 2014)

SUMÁRIO

LISTA DE ACRÔNIMOS

ABNT – Associação Brasileira de Normas Técnicas
CFTV - Circuito Fechado de Televisão
CGTI - Comitê Gestor de Tecnologia da Informação
CNJ – Conselho Nacional de Justiça
PCN - Plano de Continuidade de Negócio
PSI - Política de Segurança da Informação
VPN - *Virtual Private Networks*
TCU – Tribunal de Contas da União
TIC - Tecnologia da Informação e Comunicação
TSE – Tribunal Superior Eleitoral

1 INTRODUÇÃO

Este documento dispõe sobre as Diretrizes Básicas da Política de Segurança da Informação, a serem cumpridas no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte (Secretaria, Zonas Eleitorais, Postos de Atendimento ao Eleitor e demais unidades) referentes ao conjunto de medidas de proteção, composto de normas e procedimentos que possam nortear quanto à garantia dos Príncípios de Segurança da Informação de Confiabilidade, Integridade, Disponibilidade, Autenticidade e Confidencialidade (quando necessário), tomando-se por base as orientações emanadas do Conselho Nacional de Justiça (CNJ), do Tribunal de Contas da União (TCU), bem como as elaboradas pela Comissão de Segurança da Informação do Tribunal Superior Eleitoral (TSE).

Tais diretrizes fundamentarão as ações a serem implementadas pelas/nas unidades, considerando as suas particularidades, de acordo com os objetivos a seguir.

2 OBJETIVOS

A Política de Segurança da Informação (PSI) do TRE/RN tem os seguintes objetivos específicos:

a) **Definir** o escopo da segurança das unidades;
b) **Orientar**, por meio de suas diretrizes, todas as ações de segurança das unidades, para reduzir riscos e garantir a integridade, sigilo e disponibilidade das informações dos sistemas de informação e recursos;
c) **Possibilitar** a adoção de soluções de segurança integradas;
d) **Servir** de referência para auditoria, apuração e avaliação de responsabilidades.

3 ABRANGÊNCIA

A PSI abrange os seguintes aspectos:

I) Estratégicos, Estruturais e Organizacionais, preparando a base para elaboração dos demais documentos normativos que os incorporarão;
II) Requisitos de Segurança Humana, conjunto de medidas e procedimentos de segurança, a serem observados por todos que atuam no âmbito da Justiça Eleitoral;
III) Requisitos de Segurança Física (ambiente físico), composto por todo ativo permanente da Justiça Eleitoral no Rio Grande do Norte;
IV) Requisitos de Segurança Lógica, composto por todo ativo de informações da Justiça Eleitoral.

4 TERMINOLOGIA

As regras e diretrizes de segurança devem ser interpretadas de forma que todas as suas determinações sejam obrigatórias e cogentes.

5 CONCEITOS E DEFINIÇÕES

Aplicam-se os conceitos abaixo no que se refere à PSI das unidades:

a) 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 e das Zonas Eleitorais;

b) Ativo de Informação – é o patrimônio composto por todos os dados e informações geradas e manipuladas durante a execução dos sistemas e processos das unidades;

c) Ativo de Processamento – é o patrimônio composto por todos os elementos de hardware e software necessários para a execução dos sistemas e processos das unidades, tanto os produzidos internamente quanto os adquiridos;

d) Autenticidade – propriedade que permite a validação de identidade de usuários e sistemas;

e) Comissão Permanente de Segurança da Informação – grupo de pessoas com a responsabilidade de promover a implementação das ações de segurança da informação;

f) Confidencialidade – a informação não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem autorização;

g) Controle de Acesso – são restrições ao acesso às informações de um sistema exercido pela gerência de Segurança da Informação das entidades;

h) Custódia – consiste na responsabilidade de se guardar um ativo para terceiros. Entretanto, a custódia não permite automaticamente o acesso ao ativo, nem o direito de conceder acesso a outros;

i) Disponibilidade – a informação será acessível e utilizável sob demanda da entidade autorizada;

j) Direito de Acesso – é o privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo;

k) Evento de Segurança da Informação – ocorrência identificada de um sistema, serviço ou rede que indica uma possível violação da PSI, ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação;

l) **Ferramentas** – é um conjunto de equipamentos, programas, procedimentos, normas e demais recursos através dos quais se aplica a PSI;

m) **Gestão de riscos** – atividades coordenadas para dirigir e controlar uma organização, no que se refere aos riscos. Inclui a avaliação, o tratamento, a aceitação e a comunicação do risco;

n) **Incidente de Segurança da Informação** – um evento ou uma série deles, referente à Segurança da Informação, indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações da Organização e ameaçar a segurança da informação;

o) **Integridade** – proteção à precisão e à perfeição de recursos;

p) **Manuseio** - fase na qual a informação é originada e manejada, seja na digitação, no folheamento de papéis, ou até mesmo na utilização de senhas.

q) **Política de Segurança** – é um conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos Sistemas de Informação das unidades;

r) **Proteção dos ativos** – é o processo pelo qual os ativos devem receber classificação quanto ao grau de sensibilidade. O meio de registro de um ativo de informação deve receber a mesma classificação de proteção dada ao ativo que o contém;

s) **Recurso** – além da própria informação, todo o meio direto ou indireto utilizado para seu tratamento, tráfego ou armazenamento;

t) **Responsabilidade** – é definida como as obrigações e os deveres da pessoa que ocupa determinada função em relação ao acervo de informações;

u) **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;

v) **Senha Fraca ou Óbvia** – é aquela onde se utilizam caracteres de fácil associação com o dono da senha, ou que seja muito simples ou pequena, tais como: datas de aniversário, de casamento, de nascimento, o próprio nome, o nome de familiares, seqüências numéricas simples, palavras e unidades léxicas que constem de dicionários de qualquer língua, dentre outras;

w) **Usuário** – quem utiliza, de forma autorizada, sistemas, serviços e/ou demais recursos inerentes às atividades precípuas da Justiça Eleitoral;

6. REGRAS GERAIS

6.1 Gestão de Segurança

A PSI do TRE/RN se aplica a todos os recursos humanos, administrativos e tecnológicos pertencentes às unidades que a compõem. A abrangência dos recursos citados refere-se tanto àqueles ligados às unidades em caráter permanente quanto às de caráter temporário.

Esta política deve ser comunicada para todo o pessoal envolvido e largamente divulgada em todas as unidades do tribunal, garantindo que todos dela tenham consciência e a pratiquem no Órgão.

Todo o pessoal deve receber as informações necessárias para cumprir o que está determinado na PSI.

Um programa de conscientização sobre segurança da informação deverá ser implementado para assegurar que todo o pessoal seja informado sobre os potenciais riscos de segurança e a exposição a que estão submetidos os sistemas e operações das entidades.

Os procedimentos deverão ser documentados e implementados para garantir a revogação dos privilégios de acesso aos sistemas, informações e recursos nos casos em que:

a) os servidores do quadro permanente, requisitados, cedidos, em exercício provisório ou removidos sejam aposentados, exonerados ou retornem aos seus Órgãos de origem;
b) os estagiários sejam desligados dos programas de estágio, quando do seu término ou interrupção;
c) os profissionais terceirizados tenham os seus contratos encerrados.

No que tange à previsão de mecanismo e repositório centralizado para ativação e manutenção de trilhas, *logs* e demais notificações de incidentes, estes deverão ser incluídos nas medidas a serem tomadas por um grupo encarregado de responder a este tipo de ataque, para prover uma defesa ativa e corretiva contra os mesmos.

Os processos de aquisição de bens e serviços, especialmente de Tecnologia da Informação e Comunicação – TIC, devem estar em conformidade com esta PSI.

6.2 Gerenciamento de Riscos

O processo de gerenciamento de riscos deve ser revisto, periodicamente, pela unidade competente, para prevenção contra riscos, inclusive aqueles advindos de novas tecnologias, visando à elaboração de planos de ação apropriados para proteção dos componentes ameaçados.

6.3 Inventário de ativos

Todos os ativos das unidades do TRE/RN devem ser inventariados, classificados, permanentemente atualizados pela unidade competente, e possuir gestor responsável formalmente designado.

6.4 Plano de Continuidade do Negócio

Um Plano de Continuidade do Negócio – PCN deve ser implementado e testado, pelo menos uma vez por ano, para garantir a continuidade dos serviços críticos ao negócio.

Todos os incidentes deverão ser reportados à Secretaria de Tecnologia da Informação do TRE/RN, a partir do momento em que for verificada a ocorrência. Esses incidentes devem ser reportados de modo sigiloso a pessoas especialmente designadas para isso.

7 REQUISITOS DE SEGURANÇA DE PESSOAL

7.1 Definição

Conjunto de medidas e procedimentos de segurança a serem observados pelos servidores, estagiários, prestadores de serviços, colaboradores e consultores externos, doravante nominados "usuários", no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte, necessários à proteção dos ativos de informação.

7.2 Objetivos

7.2.1 Reduzir os riscos de erros humanos, furto, roubo, apropriação indébita, fraude ou uso não apropriado dos ativos das unidades do TRE/RN.

7.2.2 Prevenir e neutralizar as ações sobre as pessoas que possam comprometer a segurança dessas unidades.

7.2.3 Orientar e capacitar todo o pessoal envolvido na realização dos trabalhos, assim como o pessoal em desempenho de funções de apoio, tal como manutenção das instalações físicas, para a compreensão de suas responsabilidades e adoção de medidas de proteção compatíveis com a natureza da função que desempenham.

7.2.4 Fomentar a conscientização, a capacitação e a educação em segurança da informação.

7.3 Diretrizes

7.3.1 O usuário externo que tiver acesso às informações da Justiça Eleitoral do Rio Grande do Norte fica sujeito às diretrizes, às normas e aos

procedimentos de segurança da informação concernentes à PSI deste Regional.

7.3.2 Todo acesso à informação deve ser controlado de acordo com a sua classificação, levando-se em conta as necessidades do usuário no desempenho de suas atividades.

7.3.3 Os usuários e administradores do sistema de controle de acesso devem ser formal e expressamente conscientizados de suas responsabilidades, mediante assinatura de termo de compromisso.

7.3.4 Os usuários assinarão termo de compromisso assumindo o dever de manter o devido sigilo, mesmo quando desligados da Justiça Eleitoral, se for o caso, sobre todos os ativos de informações e de processos das unidades.

7.3.5 A infração de dispositivos da PSI do TRE/RN poderá acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais.

7.3.6 Deve ser definido um processo pelo qual será apresentada aos usuários esta PSI, além de ser elaborada uma política de capacitação em segurança da informação para os usuários, com o objetivo de assegurar que estejam cientes das ameaças e preocupações e equipados para apoiar a política de segurança da instituição durante a execução normal do seu trabalho.

7.3.7 As falhas e incidentes de segurança da informação, o mau funcionamento e ouras fragilidades ou ameaças, ocorridas ou suspeitas, na segurança de sistemas ou serviços, devem ser registradas e imediatamente notificadas aos superiores, que acionarão a Comissão Permanente de Segurança da Informação do TRE/RN.

7.3.8 Os usuários não devem tentar remover uma fragilidade suspeita em um aplicativo ou equipamento, a menos que estejam autorizados. A investigação não autorizada de uma fragilidade pode ser interpretada como potencial uso impróprio do sistema.

7.3.9 Ao utilizar os recursos de informática, o usuário concorda com esta política e autoriza implicitamente as ações de auditoria, monitoração e inspeção eventualmente necessárias.

7.3.10 As permissões de acesso poderão ser bloqueadas, em caso de afastamento legal ou risco à segurança física e lógica, e revogadas, em caso de desligamento do usuário.

7.3.11 É obrigatório o uso de crachá nas dependências do TRE/RN.

7.4 Deveres e Responsabilidades

7.4.1 São deveres dos usuários:

a) preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento de informações;
b) cumprir a PSI, sob pena de incorrer nas sanções disciplinares e legais cabíveis;
c) utilizar os recursos e os sistemas informatizados somente no interesse da Justiça Eleitoral;
d) cumprir as regras específicas de proteção estabelecidas aos ativos de informação;
e) manter o caráter sigiloso das senhas de acessos aos recursos e sistemas informatizados;
f) não compartilhar, sob qualquer forma, informações confidenciais com outros que não tenham a devida autorização de acesso;
g) responder por todo e qualquer acesso aos recursos das unidades, bem como pelos efeitos desses acessos efetivados através do seu código de identificação ou outro atributo para esse fim utilizado;
h) respeitar a proibição de não usar, inspecionar, copiar ou armazenar programas de computador ou qualquer outro material, em violação da legislação de propriedade intelectual pertinente;
i) comunicar ao seu superior imediato o conhecimento de qualquer irregularidade ou desvio de material ativo ou falhas no acesso aos recursos e sistemas informatizados;e
j) obedecer às regras contidas nos regulamentos da Justiça Eleitoral que disciplinem o uso do correio eletrônico institucional e o acesso à internet, à intranet e à extranet.

7.4.2 São responsabilidades das chefias:

a) gerenciar o cumprimento da PSI;
b) identificar os desvios praticados, comunicando-os por escrito à Administração;
c) impedir o acesso de usuários desligados aos ativos de informações, utilizando-se dos mecanismos próprios elaborados pela unidade técnica competente;
d) proteger, em nível físico e lógico, os ativos de informação e de processamento das unidades relacionados com sua área de atuação;
e) garantir que o pessoal sob sua supervisão compreenda e desempenhe a obrigação de proteger a Informação das unidades:
f) comunicar formalmente à unidade que efetua a concessão de privilégios a usuários de TI, sob sua supervisão, que podem acessar as informações; e

g) observar as normas internas que disciplinem a concessão de privilégios e de acesso aos sistemas e ativos pelo pessoal sob sua supervisão.

7.4.3 São responsabilidades gerais:

a) cada área que detém os ativos de processamento e de informação é responsável por eles, devendo prover a sua proteção de acordo com a política de classificação da informação da unidade;
b) todos os ativos de informações deverão ter claramente definidos os responsáveis pelo seu uso;
c) todos os ativos de processamento das unidades devem estar relacionados no PCN.

7.4.4 São responsabilidades das unidades de TI:

a) estabelecer as regras de proteção dos ativos das unidades do TRE/RN;
b) decidir quanto às medidas a serem tomadas no caso de violação das regras estabelecidas;
c) revisar, periodicamente, as regras de proteção estabelecidas;
d) elaborar e manter atualizado o PCN; e
e) executar as regras de proteção estabelecidas pela PSI.

8 REQUISITOS DE SEGURANÇA DO AMBIENTE FÍSICO

8.1 Definição

Ambiente físico é aquele composto por todo o ativo permanente das unidades integrantes do Tribunal Regional Eleitoral do Rio Grande do Norte.

8.2 Diretrizes Gerais

8.2.1 As responsabilidades pela segurança física das unidades do TRE/RN deverão ser definidas e atribuídas a indivíduos claramente identificados na organização.

8.2.2 Recursos e instalações críticos ou sensíveis devem ser mantidos em áreas seguras, protegidos por um perímetro de segurança definido, com barreiras de segurança e controle de acesso. Eles devem ser fisicamente protegidos de acesso não autorizado, dano, ou interferência. A proteção fornecida deve ser proporcional aos riscos identificados.

8.2.4 O acesso aos componentes da infra-estrutura, atividade fundamental ao funcionamento dos sistemas das unidades, como painéis de controle de

energia, comunicações e cabeamento, deverá ser restrito ao pessoal autorizado.

8.2.5 O inventário de todo o conjunto de ativos de processamento deve ser registrado e mantido atualizado.

8.2.6 Quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar só devem ser utilizados nas áreas sensíveis (plenário, *datacenter,* galpão das urnas, etc) a partir de autorização formal e mediante supervisão.

8.2.7 Nas instalações das unidades do TRE/RN, todos deverão utilizar crachá e informar à segurança sobre a presença de qualquer pessoa não identificada ou de qualquer estranho não acompanhado.

8.2.8 Visitantes das áreas de segurança devem ser supervisionados. Suas horas de entrada e saída e o local de destino devem ser registrados. Essas pessoas devem obter acesso apenas às áreas específicas, com propósitos autorizados, e esses acessos devem seguir instruções baseadas nos requisitos de segurança da área visitada.

8.2.9 As áreas sensíveis deverão ser monitoradas, com as imagens registradas por meio de sistemas de Circuito Fechado de Televisão - CFTV.

8.2.10 Sistemas de detecção de intrusos devem ser instalados e testados regularmente de forma a cobrir os ambientes, as portas e janelas acessíveis, nos ambientes onde ocorrem processos críticos. As áreas não ocupadas devem possuir um sistema de alarme que permaneça sempre ativado.

9 REQUISITOS DE SEGURANÇA DO AMBIENTE LÓGICO

9.1 Definição

Ambiente lógico é composto por todo o ativo de informações das unidades.

9.2 Diretrizes gerais

9.2.1 A informação deve ser protegida de acordo com o seu valor, sensibilidade e criticidade. Para tanto, deve ser elaborado um plano de classificação da informação.

9.2.2 Os dados, as informações e os sistemas de informação das unidades e sob sua guarda devem ser protegidos contra ameaças e ações não

autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, o sigilo e a disponibilidade desses bens.

9.2.3 As violações de segurança devem ser registradas pela unidade competente e esses registros devem ser analisados para os propósitos de caráter corretivo, legal e de auditoria. Os registros devem ser protegidos e armazenados de acordo com a sua classificação.

9.2.4 Os sistemas e recursos que suportam funções críticas para operação das unidades devem assegurar a capacidade de recuperação nos prazos e condições definidas em situações de contingência.

9.2.5 O inventário sistematizado de toda a estrutura que serve como base para manipulação, armazenamento e transmissão dos ativos de processamento deve estar registrado e mantido atualizado em intervalos de tempo definidos pela unidade competente.

9.2.6 O acesso a *sites* externos (*Internet*) obedecerá à política de acesso definida pela unidade competente e autorizada pela Administração.

9.3 Diretrizes específicas

9.3.1 Sistemas

9.3.1.1 As necessidades de segurança devem ser identificadas para cada etapa do ciclo de vida dos sistemas disponíveis, caso sejam desenvolvidos por equipe interna. A documentação dos sistemas deve ser mantida atualizada. A cópia de segurança deve ser testada e mantida atualizada.

9.3.1.2 Os sistemas devem possuir controle de acesso de modo a assegurar o uso apenas a usuários ou processos autorizados. O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado.

9.3.1.3 Os arquivos de *logs* devem ser protegidos e armazenados durante o tempo definido em norma para permitir recuperação nas situações de falhas, auditoria nas situações de violações de segurança e contabilização do uso de recursos.

9.3.1.4 Os sistemas devem ser avaliados com relação aos aspectos de segurança (testes de vulnerabilidade) antes de serem disponibilizados para a produção. As vulnerabilidades do ambiente devem ser avaliadas periodicamente e as recomendações de segurança devem ser adotadas.

9.3.2. Máquinas servidoras

9.3.2.1 O acesso lógico, ao ambiente ou aos serviços disponíveis em servidores, deve ser controlado e protegido. As autorizações devem ser revistas, confirmadas e registradas continuadamente. O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado.

9.3.2.2 Os acessos lógicos devem ser registrados em *logs*. O tempo de retenção dos arquivos de *logs* e as medidas de proteção associadas devem estar definidos em norma.

9.3.2.3 Devem ser adotados procedimentos sistematizados para monitorar a segurança do ambiente operacional, principalmente no que diz respeito à integridade dos arquivos de configuração do Sistema Operacional e de outros arquivos críticos. Os eventos devem ser armazenados em relatórios de segurança (*logs*) de modo que sua análise permita a geração de trilhas de auditoria a partir destes registros.

9.3.2.4 Os relógios das máquinas devem estar sincronizados para garantir a consistência dos registros de *logs*.

9.3.2.5 Proteção lógica adicional (criptografia) deve ser adotada para evitar o acesso não autorizado às informações.

9.3.2.6 A versão do Sistema Operacional, assim como outros *softwares* básicos instalados em máquinas servidoras, devem ser mantidos atualizados, em conformidade com as recomendações dos fabricantes.

9.3.2.7 Devem ser utilizados somente *softwares* autorizados nos equipamentos. Deve ser realizado o controle da distribuição e instalação dos mesmos.

9.3.2.8 O acesso remoto a máquinas servidoras deve ser realizado adotando os mecanismos de segurança pré-definidos para evitar ameaças à integridade e ao sigilo do serviço.

9.3.2.9 Os procedimentos de cópia de segurança (*backup*) e de recuperação devem estar documentados, mantidos atualizados e regularmente testados, de modo a garantirem a disponibilidade das informações.

9.3.3 Redes

9.3.3.1 Componentes críticos da rede local devem ser mantidos em salas protegidas contra danos, furtos, roubos e intempéries e com acesso físico e lógico controlado.

9.3.3.2 A configuração de todos os ativos de processamento deve ser averiguada quando da sua instalação inicial, para que sejam detectadas e corrigidas as vulnerabilidades inerentes à configuração padrão que se encontra nesses ativos em sua primeira ativação.

9.3.3.3 Serviços vulneráveis devem receber nível de proteção adicional.

9.3.3.4 O uso de senhas deve estar submetido a uma política específica para sua gerência e utilização.

9.3.3.5 O acesso lógico aos recursos da rede local deve ser realizado por meio de sistema de controle de acesso. O acesso deve ser concedido e mantido pela administração da rede, baseado nas responsabilidades e tarefas de cada usuário.

9.3.3.6 A utilização de mecanismo capaz de realizar testes de qualquer natureza, como por exemplo, a monitoração sobre os dados e os sistemas e dispositivos que compõem a rede, só deve ocorrer a partir de autorização da unidade competente.

9.3.3.7 A conexão com outros ambientes de rede e as alterações internas na sua topologia e configuração devem ser formalmente documentadas e mantidas, de forma a permitir registro histórico, e devendo ser autorizada pela unidade competente. O diagrama topológico, a configuração e o inventário dos recursos devem ser mantidos atualizados.

9.3.3.8 Devem ser definidos relatórios de segurança (*logs*) de modo a auxiliar no tratamento de desvios, recuperação de falhas, contabilização e auditoria.

9.3.3.9. Devem ser adotadas proteções físicas adicionais para os recursos de rede considerados críticos.

9.3.3.10 Proteção lógica adicional deve ser adotada para evitar o acesso não autorizado às informações.

9.3.3.11 A infraestrutura de interligação lógica deve estar protegida contra danos mecânicos e conexão não autorizada.

9.3.3.12 A alimentação elétrica para a rede local deve seguir as recomendações dos fabricantes dos equipamentos utilizados, assim como as normas ABNT aplicáveis.

9.3.3.13 O tráfego de informações deve ser monitorado, a fim de verificar sua normalidade, assim como detectar situações anômalas do ponto de vista da segurança.

9.3.3.14 Devem ser observadas as questões envolvendo propriedade intelectual quando da cópia de *software* ou arquivos de outras localidades.

9.3.3.15 Informações sigilosas, corporativas ou que possam causar prejuízo às unidades devem estar protegidas e não devem ser enviadas para outras redes, sem proteção adequada.

9.3.3.16 Todo serviço de rede não explicitamente autorizado deve ser bloqueado ou desabilitado.

9.3.3.17 Mecanismos de segurança baseados em sistemas de proteção de acesso (*firewall*) devem ser utilizados para proteger as transações entre redes externas e a rede interna do TRE/RN.

9.3.3.18 Deve ser adotado um padrão de segurança para todos os tipos de equipamentos servidores, considerando aspectos físicos e lógicos.

9.3.3.19 Todos os recursos considerados críticos para o ambiente de rede, e que possuam mecanismos de controle de acesso, deverão fazer uso de tal controle.

9.3.3.20 Ambientes de rede considerados críticos devem ser isolados de outros ambientes de rede, de modo a garantir um nível adicional de segurança.

9.3.3.21 Ferramentas de detecção de intrusos devem ser implantadas para monitorar as redes críticas, alertando periodicamente os administradores das redes sobre as tentativas de intrusão.

9.3.3.22 Deve-se adotar recursos de VPN (*Virtual Private Networks* – redes privadas virtuais), baseadas em criptografia, para a troca de informações entre a rede pública (*Internet*) e a rede interna da Justiça Eleitoral.

9.3.4 Controle de acesso lógico (baseado em senhas)

9.3.4.1 Usuários e aplicações que necessitem ter acesso a recursos das unidades devem ser identificados e autenticados.

9.3.4.2 O sistema de controle de acesso deve manter as habilitações atualizadas e registros que permitam a contabilização do uso, a auditoria e a recuperação nas situações de falha.

9.3.4.3 Nenhum usuário deve ser capaz de obter os direitos de acesso de outro usuário.

9.3.4.4 A informação que especifica os direitos de acesso de cada usuário ou aplicação deve ser protegida contra modificações não autorizadas.

9.3.4.5 O arquivo de senhas deve ser criptografado e ter o acesso controlado.

9.3.4.6 As autorizações devem ser definidas de acordo com a necessidade de desempenho das funções (acesso motivado) e considerando o princípio dos privilégios mínimos (ter acesso apenas aos recursos ou sistemas necessários para a execução de tarefas).

9.3.4.7 As senhas devem ser individuais, secretas, intransferíveis e protegidas com grau de segurança compatível com a informação associada.

9.3.4.8 O sistema de controle de acesso deve possuir mecanismos que impeçam a geração de senhas fracas ou óbvias.

9.3.4.9 As seguintes características das senhas devem estar definidas de forma adequada:

- conjunto de caracteres permitidos, tamanho mínimo e máximo, prazo de validade máximo, forma de troca e restrições específicas.

9.3.4.10 A distribuição de senhas aos usuários (inicial ou não) deve ser feita de forma segura. A senha inicial, quando gerada pelo sistema, deve ser trocada, pelo usuário, no primeiro acesso.

9.3.4.11 O sistema de controle de acesso deve permitir ao usuário alterar sua senha sempre que desejar. A troca de uma senha bloqueada só deve ser executada após a identificação positiva do usuário. A senha digitada não deve ser exibida.

9.3.4.12 Devem ser adotados critérios para bloquear ou desativar usuários de acordo com período pré-definido sem acesso e tentativas sucessivas de acesso mal sucedidas.

9.3.4.13 O sistema de controle de acesso deve solicitar nova autenticação após certo tempo de inatividade da sessão (*time-out*).

9.3.4.14 O sistema de controle de acesso deve exibir, na tela inicial, mensagem informando que o serviço só pode ser utilizado por usuários autorizados. No momento de conexão, o sistema deve exibir para o usuário informações sobre o último acesso.

9.3.4.15 Os usuários e administradores do sistema de controle de acesso devem ser formal e expressamente conscientizados de suas responsabilidades.

9.3.5 Computação pessoal

9.3.5.1 As estações de trabalho, incluindo equipamentos portáteis ou *stand alone,* devem ser protegidas contra danos ou perdas, bem como acesso, uso ou exposição indevidos.

9.3.5.2 Devem ser adotadas medidas de segurança lógica referentes a: combate a vírus; *backup;* controle de acesso e uso de *software* não autorizado.

9.3.5.3 As informações armazenadas em meios eletrônicos devem ser protegidas contra danos, furtos ou roubos, devendo ser adotados procedimentos de *backup*.

9.3.5.4 Informações sigilosas, corporativas ou cuja divulgação possa causar prejuízo à Justiça Eleitoral, só devem ser utilizadas em equipamentos das unidades onde foram geradas ou naqueles por elas autorizadas, com controles adequados.

9.3.5.5 A unidade competente deverá estabelecer os aspectos de controle, distribuição e instalação de *softwares* utilizados.

9.3.5.6 O inventário dos recursos deve ser mantido atualizado.

9.3.5.7 Os sistemas em uso devem solicitar nova autenticação após certo tempo de inatividade da sessão (*time-out*).

9.3.5.8 As mídias devem ser eliminadas de forma segura, quando não forem mais necessárias.

9.3.5.9 É vedado aos usuários a utilização, nos computadores do TRE/RN, de quaisquer dispositivos que implementem conexão de dados, tais como: *modem*, celular, *wi-fi*, *bluetooth*, com exceção daqueles que tenham autorização superior prévia e obedeçam às diretrizes estabelecidas nesta PSI.

9.3.6 Combate a Vírus de Computador

Os procedimentos de combate a processos destrutivos (vírus, cavalo-de-tróia e *worms*) devem estar sistematizados e abranger máquinas servidoras, estações de trabalho, equipamentos portáteis e microcomputadores *stand alone*.

10 GERENCIAMENTO DE RISCOS

Diversas abordagens têm sido apresentadas para o tratamento de riscos, ou para averiguar de que maneira a prevenção de riscos pode influenciar a gestão da segurança da informação. De qualquer modo, é consensual que o risco deve ser adequadamente medido e avaliado, possibilitando a criação de normas preventivas voltadas à sua mitigação.

10.1 Definição de Gerenciamento de Riscos

Processo que visa à proteção dos serviços das unidades, por meio da eliminação, redução ou transferência dos riscos, conforme seja economicamente (e estrategicamente) mais viável. Os seguintes pontos principais devem ser abordados:

a) Identificar os riscos e as ameaças mais significantes tornando possível a determinação de ações apropriadas para reduzí-los;
b) Qualificar os riscos e as ameaças para que sejam priorizados em função de critérios de aceitação e dos objetivos relevantes para a organização;
c) Análise de riscos (contra quem ou contra o quê deve ser protegido);
d) Avaliação de riscos (análise da relação custo/benefício), com implementação de políticas apropriadas e controles relacionados, promovendo a conscientização das medidas, monitorando e avaliando políticas e controles efetivos.

10.2 Fases Principais

O gerenciamento de riscos consiste das seguintes fases principais:

a) **Identificação dos recursos a serem protegidos –** *hardware*, rede, *software*, dados, informações, documentação, suprimentos;

b) I**dentificação dos riscos** - as ameaças:

b.1) Naturais: tempestades, inundações;

b.2) Causadas por pessoas: ataques, furtos, vandalismos, erros ou negligências;

b.3) Acidentes não previstos: incêndios, curto-circuito, queda na comunicação;

c) **Análise dos riscos**: Identificar as vulnerabilidades e os impactos associados;

d) **Avaliação dos riscos**: Levantamento da probabilidade da ameaça vir a acontecer, estimando o valor do provável prejuízo. Esta avaliação pode ser feita com base nos históricos de ocorrências relatadas na Instituição;

e) **Tratamento dos riscos:** Medidas a serem adotadas para lidar com as ameaças de forma preventiva ou reativa. Principais alternativas a serem adotadas:

e.1) Eliminar os riscos – aplicar controles apropriados para reduzir ou eliminar definitivamente os riscos;

e.2) Prevenir o risco – não permitir ações que poderiam causar a ocorrência de riscos;

e.3) Limitar os riscos - transferir os riscos às empresas contratadas/conveniadas diminuindo a carga de responsabilidade;

e.4) Aceitar os riscos – conhecer e objetivamente saber que eles atendem claramente aos critérios de aceitação da política de segurança do Tribunal;

f) **Monitoração dos riscos**: Prover procedimentos eficazes de controle adotados para minimizar os riscos identificados, de forma a reduzí-los a um nível aceitável.

g) **Reavaliação dos riscos**: Avaliar periodicamente as situações e/ou recursos considerados de riscos ao Tribunal e aos seus ativos.

10.3 Riscos relacionados às unidades do TRE/RN

Os riscos a serem avaliados para as unidades compreendem, dentre outros, os seguintes:

Segmento	Riscos
Dados e Informação	Engenharia social, indisponibilidade, interrupção (perda), interceptação, modificação, fabricação e destruição;
Pessoas	Omissão, erro, negligência, imprudência, imperícia, desídia, sabotagem e perda de conhecimento;
Rede	*Hacker*, acesso desautorizado, interceptação, identidade forjada, reenvio de mensagem, violação de integridade e indisponibilidade ou recusa de serviço;
Hardware	Indisponibilidade, interceptação (furto ou roubo) e falha;
Software	Interrupção (apagamento), interceptação, modificação, desenvolvimento e falha;
Recursos criptográficos	Ciclo de vida dos certificados, gerenciamento das chaves criptográficas, *hardware* criptográfico, algoritmos (desenvolvimento e utilização) e material criptográfico.

10.4 Considerações Gerais

10.4.1 Os riscos que não puderem ser eliminados devem ter seus controles documentados e devem ser levados ao conhecimento da Comissão de Segurança da Informação para que sejam tomadas as providências cabíveis;

10.4.2 Um efetivo gerenciamento dos riscos permite decidir se o custo de prevenir um risco (medida de proteção) é mais alto que o custo das conseqüências do risco (impacto da perda).

10.4.3 São necessários a participação e o envolvimento da Alta Administração.

10.5 Implementação do Gerenciamento de Riscos

Os procedimentos de gerenciamento de riscos nas unidades administrativas do Tribunal devem obedecer à metodologia padrão adotada pela Comissão da Segurança da Informação.

11 PLANO DE CONTINUIDADE DO NEGÓCIO

11.1 Definição: Plano cujo objetivo é manter em funcionamento os serviços e processos críticos das unidades do Tribunal, na eventualidade da ocorrência de desastres, atentados, falhas e intempéries.

11.2 Diretrizes Gerais

11.2.1 A unidade responsável deve implantar dispositivos para proteger os processos críticos do negócio dos efeitos de falhas ou desastres, e para assegurar sua retomada em tempo hábil;

11.2.2 Os sistemas e dispositivos redundantes devem estar disponíveis para garantir a continuidade da operação dos serviços críticos de maneira oportuna;

11.2.3 Os processos de gerenciamento da continuidade do negócio devem ser adotados para minimizar o impacto nos desastres que poderão acontecer, adotando procedimentos de recuperação de perda da informação e ativos.

11.2.4 Os processos críticos para a Instituição deverão ser identificados e classificados, devendo sofrer o tratamento adequado na ocorrência dos seguintes eventos de segurança:
a) Comprometimento dos certificados digitais dos usuários;
b) Invasão do sistema e da rede interna da JE;
c) Incidentes de segurança física e lógica;
d) Indisponibilidade da Infraestrutura; e
e) Fraudes ocorridas no registro do usuário, na emissão, expedição, distribuição, revogação e no gerenciamento de certificados.

11.2.5 A análise de impacto no negócio será realizada para avaliar as consequências de desastres, falhas de segurança, perda ou indisponibilidade do serviço.

11.2.6 Todo pessoal envolvido com o PCN deve receber um treinamento específico para lidar com estes incidentes.

11.2.7 Um plano de ação de resposta a incidentes deverá ser estabelecido para todas as unidades do Tribunal. Este plano deve prever, no mínimo, o tratamento adequado dos seguintes eventos:

a) Comprometimento de controle de segurança em qualquer evento referenciado no PCN;

implantar trilhas de auditoria para gerências de acessos e concessões e

b) Divulgação de desastres ocorridos, com a notificação aos usuários, aumentando o compromisso de responsabilidade;
c) Revogação dos certificados afetados, se for o caso;
d) Procedimentos para interrupção ou suspensão de serviços e investigação;
e) Análise e monitoramento de trilhas de auditoria;
f) Relacionamento com o público e com meios de comunicação, se for o caso.

12 AUDITORIA E FISCALIZAÇÃO

12.1 As atividades das unidades do TRE/RN estão associadas ao conceito de confiança. Os processos de auditoria e fiscalização representam instrumentos que facilitam a percepção e a transmissão de confiança à comunidade de usuários, dado que o objetivo desses processos é verificar a capacidade das unidades em atender aos requisitos da PSI.

12.2 Deverão ser realizadas auditorias periódicas nas unidades do TRE/RN, conforme o disposto na Resolução TRE/RN nº 008/2009, **sendo facultada a divulgação do cronograma para conhecimento dos usuários e administradores**.

12.3 Por ocasião das auditorias dos requisitos de **segurança de pessoal** e dos **ambientes lógicos e físicos** deve-se utilizar, além dos métodos tradicionais pertinentes, a coleta de dados, as ferramentas especializadas na análise dos registros (*logs*) dos sistemas e dos bancos de dados, incluindo, no âmbito de planejamento de segurança, a análise dos logs de sistema operacional e do sistema de pagamento.

12.4 **Nos ambientes lógicos**, as unidades técnicas responsáveis, em conformidade com as recomendações contidas nas normas técnicas vigentes, zelarão por: i) manter ativado o "log" das operações de acesso direto ao banco de dados feitas pelos administradores e desenvolvedores; ii) implantar mecanismos de proteção dos "logs" de auditoria contra modificações e exclusões não autorizadas; iii) implantar trilhas de auditoria para gerências de acessos e concessões e revogações das contas de HOST e procedimentos que possibilitem o monitoramento proativo do uso dos recursos de infraestrutura de TI; e iv) implantar rotinas que mantenham o registro de eventos relevantes do sistema. Esses registros devem conter, no mínimo, o autor, a data e a descrição do evento.

13. DOCUMENTOS REFERENCIADOS

1. ASSOCIAÇÃO Brasileira de Normas Técnicas(abnt). NBR ISSO/IEC 27002:2005 – Segurança da Informação.
2. BRASIL. Constituição da República Federativa do Brasil. Brasília: Senado Federal, 1988.
3. BRASIL. Tribunal Superior Eleitoral. Resolução nº 20.882 de 2001.
4. BRASIL. Tribunal Superior Eleitoral. Resolução nº 22.780/2008.
5. BRASIL. Tribunal Superior Eleitoral. Resolução nº 22.833/2008.
6. BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.266/2010.
7. BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.387/2012.
8. BRASIL. Superior Tribunal de Justiça. Ato nº 138/2001.
9. SANTA CATARINA. Tribunal Regional Eleitoral. Resolução nº 7.776 de 2010.
10. SANTA CATARINA. Tribunal Regional Eleitoral. Diretoria Geral Portaria nº101/2011.
11. SANTA CATARINA. Tribunal Regional Eleitoral. Diretoria nº318/2009.
12. SANTA CATARINA. Tribunal Regional Eleitoral. Ordem de serviço nº 1/2011.
13. SANTA CATARINA. Tribunal Regional Eleitoral. Resolução nº 7.285/2002.
14. SANTA CATARINA. Tribunal Regional Eleitoral. Resolução nº 7.735/2008.
15. PARANÁ. Tribunal Regional Eleitoral. Ordem de Serviço nº 1/2007.
16. PARANÁ. Tribunal Regional Eleitoral. Ordem de Serviço nº 3/2010.
17. Padronização e Políticas de Segurança do Ambiente de Rede do TRE/MG/2007.
18. BRASIL. Tribunal de Contas da União. Resolução nº217 de2008.
19. BRASIL. Política de Segurança da ICP-Brasil (DOC-ICP-02) Versão 2.0