

**RESOLUÇÃO N. 197/2015/TCE-RO**

*Altera o anexo da Resolução n. 90/TCE-RO/2012.*

**O PRESIDENTE DO TRIBUNAL DE CONTAS DO ESTADO DE RONDÔNIA**, no uso das atribuições legais que lhe são conferidas pelo art. 3º da Lei Complementar Estadual n. 154, de 26 de julho de 1996, c/c art. 263 do Regimento Interno desta Corte de Contas;

**CONSIDERANDO** a necessidade de estabelecer princípios diretores de Segurança Institucional voltados para a prevenção e obstrução de ações adversas de qualquer natureza contra pessoal, áreas, instalações, documentos, materiais e sistemas de informações do Tribunal de Contas do Estado de Rondônia;

**CONSIDERANDO** que tais alterações regulamentares têm como objeto definir as ações de Segurança Institucional a serem implementadas, concorrem para o aperfeiçoamento do funcionamento deste Tribunal e suas Secretarias Regionais de Controle Externo.

**RESOLVE:**

**Art. 1º** Alterar o anexo da Resolução n. 90/TCE/RO-2012 (Plano de Segurança Institucional do Tribunal de Contas do Estado de Rondônia e os Procedimentos Gerais de Segurança);

**Art. 2º** Esta Resolução entra em vigor na data de sua publicação, revogando-se as disposições em contrário.

Porto Velho, 14 de dezembro de 2015.

**JOSÉ EULER POTYGUARA PEREIRA DE MELLO**  
Conselheiro Presidente

**ANEXO DA RESOLUÇÃO N. 90/TCE/RO-2012**

**RESERVADO**

**PLANO DE SEGURANÇA INSTITUCIONAL - PSI**



**TRIBUNAL DE CONTAS DO ESTADO DE RONDÔNIA**

**2015**

**ESTADO DE RONDÔNIA**  
**TRIBUNAL DE CONTAS DO ESTADO DE RONDÔNIA**  
**GABINETE DA PRESIDÊNCIA**  
**ASSESSORIA DE SEGURANÇA INSTITUCIONAL**

**PLANO DE SEGURANÇA INSTITUCIONAL**

**1.FINALIDADE**

Estabelecer princípios diretores de Segurança Institucional que visem à prevenção e à obstrução de ações adversas de qualquer natureza contra pessoal, áreas, instalações, documentos, materiais e sistemas de informações do Tribunal de Contas do Estado de Rondônia.

**2.OBJETO**

Definir as ações de Segurança Institucional a serem implementadas no âmbito do Tribunal de Contas do Estado de Rondônia e suas Secretarias Regionais de Controle Externo, fundamentadas nos conceitos, finalidades, medidas e procedimentos **gerais de segurança expressos no presente plano(anexo)**.

**3. COMPETÊNCIAS**

- 3.1.** Compete à Assessoria de Segurança Institucional - ASI do Gabinete da Presidência do Tribunal de Contas do Estado de Rondônia o planejamento e estratégia de segurança do TCE e ainda:
- 3.1.1.** Elaborar as proposições de Normas e os Planos acessórios aos procedimentos de segurança física das instalações e contra incêndios previstos neste plano e no Plano de Emergência de Combate a Incêndio e Atuação em Sinistros (tramitando no TCE);
  - 3.1.2.** Planejar e coordenar a execução das atividades de segurança ostensiva e velada do Presidente do TCE-RO e demais Membros da Corte de Contas, Ministério Público de Contas, Conselheiros Substitutos e servidores em geral, quando necessário;
  - 3.1.3.** Executar os serviços do cerimonial militar, em harmonia com o Gabinete da Presidência;
  - 3.1.4.** Acompanhar os atos e visitas do Presidente do Tribunal de Contas ou de outras autoridades da Administração do TCE, em situações especiais que requeiram maior segurança ou outros cuidados;
  - 3.1.5.** Transmitir ordens e instruções do Conselheiro Presidente do Tribunal de Contas, bem como controlar sua execução no âmbito das respectivas esferas de atribuições da Assessoria de Segurança Institucional;
  - 3.1.6.** Propor cursos, estágios, seminários e palestras para aperfeiçoamento dos integrantes

da Assessoria de Segurança Institucional, bem como educação de segurança aos demais funcionários do Tribunal em parceria com a Escola Superior de Contas - ESCon;

- 3.1.7.** Participar, através da Presidência, das relações institucionais do TCE-RO com as Corporações Militares do Estado, com as Forças Armadas e Órgãos Cíveis de Segurança Pública, da União e do Estado;
- 3.1.8.** Colaborar no planejamento e elaboração dos programas e planos de viagens e visitas do Presidente, quando for determinado;
- 3.1.9.** Supervisionar e sugerir medidas envolvendo normas gerais de operação e segurança que regulam o funcionamento do prédio do Tribunal;
- 3.1.10.** Sugerir medidas visando um efetivo controle geral de entrada e saída de pessoas, veículos e materiais, de acordo com as normas em vigor, bem como do fluxo de pessoas nas áreas de livre circulação, incluindo os acessos principais, corredores, escadas, elevadores e garagens, dos bens materiais e dos estacionamentos internos e externos do Tribunal de Contas;
- 3.1.11.** Sugerir medidas objetivando o aperfeiçoamento do controle e a segurança dos pontos críticos como: caixas eletrônicos, depósitos, caixas, motores, centrais telefônicas e de distribuição de energia elétrica e hidráulica, equipamentos de combate a incêndios, entre outros;
- 3.1.12.** Comunicar aos órgãos competentes do Tribunal as ocorrências suspeitas ou anormais de que tiver conhecimento, sem prejuízo da adoção das providências cabíveis na esfera de suas atribuições;
- 3.1.13.** Participar de comissões ou grupos de trabalho constituídos com a finalidade de discutir e propor soluções para questões internas de segurança, disciplina, normas gerais de funcionamento e outros temas, quando designado pelo Conselheiro Presidente;
- 3.1.14.** Acompanhar atos e visitas oficiais do Conselheiro Presidente do Tribunal de Contas ou de outras autoridades da Corte de Contas ou ainda autoridades nacionais e estrangeiras, quando em visita oficial ao TCE-RO, assim como em Sessões Plenárias e das Câmaras, em situações especiais que requeiram maior segurança ou outros cuidados, quando solicitado;
- 3.1.15.** Receber autoridades que visitarem ao TCE-RO e encaminhá-las aos gabinetes competentes, zelando pela segurança destas;
- 3.1.16.** Supervisionar a segurança das telecomunicações no âmbito dos Gabinetes da Presidência e dos órgãos da Administração Superior do TCE-RO;
- 3.1.17.** Elaborar relatórios de atividades da Assessoria de Segurança Institucional, bem como outros relatórios de atividades correlatas eventualmente solicitados pela Presidência;
- 3.1.18.** Elaborar estudos, pesquisas e pareceres sobre assuntos compreendidos na esfera de atribuições da Assessoria de Segurança Institucional;
- 3.1.19.** Elaborar manuais de procedimentos para apuração de ocorrências internas relacionadas

às questões de segurança, bem como colaborar, quando devidamente designado, nos procedimentos administrativos que vierem a ser instaurados pelo Tribunal;

**3.1.20.** Programar e desenvolver campanhas educativas que visem à melhoria das condições gerais de segurança no âmbito do Tribunal;

**3.1.21.** Coordenar e controlar a utilização das armas e munições pelo pessoal de segurança e mantê-las em perfeitas condições de uso;

**3.1.22.** Organizar, em ocasiões especiais, sempre que lhe for determinado pela Presidência, recepções formais ou informais a autoridades em visita ao Tribunal de Contas;

**3.1.23.** Providenciar guarda e escoltas de honra para as autoridades, em solenidades e ocasiões especiais realizadas no Tribunal de Contas;

**3.1.24.** Manter articulação com o cerimonial do Governo do Estado e com as Assessorias Militares dos Poderes Legislativo e Judiciário e do Ministério Público;

**3.1.25.** Exercer outras atribuições que lhe sejam cometidas pelo Conselheiro Presidente.

**3.2.** Compete ao **Assessor de Segurança Institucional** (art. 19 da Lei [Complementar n. 799/2014](#)):

**3.2.1.** Planejar, coordenar e executar a estratégia de segurança do Tribunal de Contas do Estado, atendendo às recomendações e políticas estratégicas pré-estabelecidas nas respectivas normas e pelo Presidente do Tribunal de Contas do Estado;

**3.2.2.** Dirigir a Assessoria de Segurança Institucional;

**3.2.3.** Propor normas e planos acessórios aos procedimentos de segurança física das instalações, dos membros e servidores do Tribunal de Contas do Estado e Membros do Ministério Público de Contas;

**3.2.4.** Propor normas e planos acessórios aos procedimentos de segurança contra incêndios das instalações físicas do Tribunal de Contas do Estado;

**3.2.5.** Realizar, assegurado o poder de polícia, a segurança ostensiva e velada dos membros do Tribunal de Contas do Estado e de outras autoridades ou personalidades, quando determinado pelo Presidente do Tribunal, podendo contar com os servidores terceirizados de vigilância e o apoio institucional dos órgãos de Segurança Pública do Estado;

**3.2.6.** Exercer a representação militar do Tribunal de Contas do Estado;

**3.2.7.** Zelar pela segurança dos membros do Tribunal de Contas do Estado, podendo contar com os serviços terceirizados de vigilância e o apoio institucional dos órgãos de Segurança Pública do Estado; e

**3.2.8** Realizar outras atividades ou tarefas de sua atribuição legal, a serem definidas por ato do Tribunal de Contas do Estado.

**Obs:** Para cumprimento das atribuições definidas neste artigo (art. 19 [da LC 799/2014](#)) o Tribunal de Contas do Estado disponibilizará serviço de segurança em suas instalações e a

seus Membros, podendo contar com o apoio institucional dos órgãos da Segurança Pública do Estado.(NR)

**3.3. Compete ao Assistente de Segurança Institucional** (art. 20 da Lei Complementar n. [799/2014](#)):

**3.3.1** Auxiliar na organização, coordenação, controle e execução das atividades de segurança institucional;

**3.3.2** Organizar os trabalhos afetos à sua área de atuação, de acordo com as diretrizes definidas pela chefia imediata e normas de regência;

**3.3.3** Realizar cálculos, análises e interpretação de dados necessários às suas atividades, além de exercer as atribuições inerentes ao cargo;

**3.3.4** Acompanhar, quando requisitado, os membros do Tribunal de Contas do Estado e do Ministério Público ou servidores nas missões de apoio e em situações que requeiram maior segurança e cuidados;

**3.3.5** Executar as ordens do Assessor de Segurança Institucional;

**3.3.6** Realizar outras atividades ou tarefas de sua atribuição legal, a serem definidas por ato do Tribunal de Contas do Estado. (NR)

**3.4. Compete ao Chefe de Equipe de Segurança** (art. 21 da Lei Complementar n. [799/2014](#)):

**3.4.1** Coordenar a execução da atuação da equipe de acordo com as diretrizes definidas pela Assessoria de Segurança Institucional e respectivas normas do Tribunal de Contas do Estado, quanto à execução das estratégias e planos, elaboração e cumprimento de escalas de serviço;

**3.4.2** Fiscalizar a utilização do fardamento;

**3.4.3** Registrar ocorrências; e

**3.4.4** Realizar outras atividades ou tarefas de sua atribuição legal, a serem definidas por ato do Tribunal de Contas do Estado. (NR).

**3.5 Compete à Secretaria de Gestão de Pessoas - SEGESP:**

**3.5.1** Elaborar as proposições de Normas e os Planos acessórios aos procedimentos de segurança relativa aos dados e informações sobre recursos humanos e a vida funcional dos servidores integrantes do Tribunal de Contas do Estado de Rondônia, em observância às diretrizes e princípios definidos na política de gestão de pessoas do TCE-RO;

**3.6 Compete à Secretaria Estratégica de Tecnologia da Informação e Comunicação - SETIC:**

**3.6.1** Elaborar as proposições de Normas e os Planos acessórios aos procedimentos de segurança de tecnologia da informação previstos neste plano;

**3.6.2** Orientar os setores sobre os procedimentos de segurança de tecnologia da informação do Tribunal de Contas do Estado de Rondônia relacionados às suas respectivas esferas de responsabilidade;

#### **4 REFERÊNCIAS:**

**4.1** Constituição da República Federativa do Brasil, 1988;

**4.2** Lei n. 8.159, de 08 de janeiro de 1991 (Política Nacional de Arquivos Públicos);

**4.3** Decreto n. 7.845, de 14 de novembro de 2012 (Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento);

**4.4** [Lei n. 12.527, de 18 de novembro de 2011](#) (Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei n. 8.112, de 11 de dezembro de 1990; revoga a Lei n. 11.111, de 5 de maio de 2005, e dispositivos da Lei n. 8.159, de 8 de janeiro de 1991; e dá outras providências);

**4.5** [Decreto n. 7.724, de 16 de maio de 2012](#) (Regulamenta a [Lei n. 12.527, de 18 de novembro de 2011](#), que dispõe sobre o acesso a informações previsto no inciso XXXIII do **caput** do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição);

**4.6** Plano de Segurança Institucional do Ministério Público e Tribunal de Contas do Estado do Rio Grande do Sul;

**4.7** IP 30-3 – Ramo Contra-Inteligência do Ministério do Exército;

**4.8** Resolução n. [041/TCE-RO-2006](#) (Dispõe sobre a política de segurança de informações do Tribunal de Contas – PSI/TCE-RO e dá outras providências);

**4.9** Resolução n. [157/2014/TCE-RO](#) (Institui o Comitê de Segurança Institucional no âmbito do Tribunal de Contas do Estado de Rondônia);

**4.10** [Resolução n. 104, de 06 de abril de 2010, do Conselho Nacional de Justiça](#) (Dispõe sobre medidas administrativas para a segurança e a criação de Fundo Nacional de Segurança, e dá outras providências);



- 4.11** Resolução n. 116, de 06 de outubro de 2014, do Conselho Nacional do Ministério Público (Estabelece regras gerais para proteção pessoal de Membros do Ministério Público e de seus familiares diante de situação de risco decorrente do exercício da função).

## **5. CONCEITOS BÁSICOS, FINALIDADES, MEDIDAS E PROCEDIMENTOS DE SEGURANÇA ORGÂNICA:**

A Segurança Institucional engloba um conjunto de medidas voltadas para a prevenção e para a obstrução de ações adversas de qualquer natureza. Tais medidas estão agrupadas nos segmentos de Segurança de Pessoal, Segurança da Documentação e Material, Segurança dos Sistemas de Informação e Informática e Segurança das Áreas e Instalações, conforme segue:

### **5.1 SEGURANÇA DE PESSOAL:**

Define medidas e procedimentos de segurança na seleção e no ingresso de servidores com o propósito de evitar a admissão de pessoas com características e/ou antecedentes que possam causar algum tipo de comprometimento da Instituição. Define, ainda, procedimentos de lotação de pessoal observando os cuidados necessários à salvaguarda de dados e/ou de conhecimentos sigilosos.

Visa ainda prevenir e obstruir as ações adversas de infiltração, de recrutamento e de entrevista, que possam ser utilizadas em decorrência de falhas no processo seletivo e no acompanhamento funcional dos servidores. Estabelece um conjunto de medidas destinadas a assegurar comportamentos adequados à proteção do conhecimento sensível.

#### **5.1.1 Segurança no Processo Seletivo**

Define medidas e procedimentos a serem adotados durante o processo seletivo de candidatos, com o propósito de evitar a admissão de pessoas com características e/ou antecedentes que possam causar algum tipo de comprometimento da Instituição.

Tendo em vista que o TCE-RO tem como missão **“fiscalizar a administração pública estadual e municipal zelando pela legalidade, moralidade, eficiência e garantindo a correta aplicação dos recursos públicos”**, os procedimentos para provimento dos cargos efetivos e comissionados obedecerá à normatização própria.

Vale ressaltar que os procedimentos de seleção e desenvolvimento de pessoal seguirão critérios estabelecidos na Resolução n. 69/TCE-RO-2010, que dispõe sobre a política de gestão de pessoas desta Corte de Contas.

Salienta-se ainda que os seguintes procedimentos serão adotados no processo de recrutamento e seleção:

- Estabelecer o perfil profissional de cada candidato em consonância com a Política de Gestão de Pessoas do TCE-RO;



- Pesquisa dos antecedentes de todos os candidatos (etapa de pesquisa social, se normatizada antes do concurso), ficha de informações confidenciais – FIC, certidões circunstanciadas de antecedentes criminais da localidade onde reside ou residiu nos últimos cinco anos, conforme item 5.1.3 do levantamento de dados pessoais.
- Somente serão aceitas certidões expedidas, no máximo, nos 90 (noventa) dias anteriores à data de entrega fixada em edital e dentro do prazo de validade específico constante da mesma.
- Serão desconsiderados documentos rasurados.
- Comunicar a Assessoria de Segurança Institucional as nomeações e exonerações para fins de controle de acesso.

### **5.1.2 Determinação da sensibilidade e desempenho das funções**

Os diversos setores do TCE-RO deverão elaborar o “Relatório de Sensibilidade de Função”, definindo o nível de informações e arquivos sigilosos que manuseiam para a determinação das áreas sensíveis existentes no âmbito deste Tribunal de Contas, em consonância com as [Resoluções n. 69 e 70/2010](#).

- 5.1.2.1** Acompanhar o desempenho das funções exercidas pelo servidor da admissão ao desligamento;
- 5.1.2.2** Verificar indícios e investigar procedimentos ou comportamentos inadequados do servidor, havendo qualquer suspeita de comprometimento;
- 5.1.2.3** Proceder à educação de segurança de forma contínua, buscando a mentalidade de segurança;
- 5.1.2.4** Aplicar medidas corretivas, se necessário, após investigação.

### **5.1.3 Levantamento de dados pessoais**

O candidato a cargo no Tribunal de Contas do Estado de Rondônia, durante fase do concurso ou no ato de posse, deverá apresentar os seguintes documentos, os quais subsidiarão o procedimento de investigação social:

- 5.1.3.1** Ficha Cadastral;
- 5.1.3.2** Declaração de Bens;
- 5.1.3.3** Certidão Circunstanciada Negativa da Justiça Estadual (Cível e Criminal);

**5.1.3.4** Certidão Negativa da Justiça Federal (Cível e Criminal);

**5.1.3.5** Certidão Negativa da Justiça Militar Federal;

**5.1.3.6** Certidão Negativa da Justiça Militar Estadual;

**5.1.3.7** Certidão Negativa da Justiça Eleitoral.

#### **5.1.4 Análise dos dados pessoais e entrevista**

A Secretaria de Gestão de Pessoas analisará a Ficha Cadastral e os documentos apresentados pelos futuros servidores e, ocorrendo algum registro de ocorrência nos Órgãos civis, militares e criminais da Justiça Federal, Estadual ou Militar, solicitará à Assessoria de Segurança Institucional averiguação, diligências e elucidação das dúvidas, e após parecer, encaminhará à comissão de concurso ou autoridade determinada para as medidas cabíveis.

#### **5.1.5 Segurança no desempenho da função**

Os servidores serão habilitados, mediante credenciamento, para acesso a assuntos sigilosos, através de treinamento sobre medidas e procedimentos de segurança para o desempenho da atividade.

Caberá à chefia imediata o acompanhamento do desempenho funcional do servidor, em relação às normas de segurança.

#### **5.1.6 Concessão de credenciais de segurança**

As credenciais de segurança habilitam o servidor a ter acesso a assunto sigiloso até o grau de sigilo compatível com o cargo e/ou função a desempenhar, bem como a serviços de tecnologia da informação e comunicação.

Serão concedidas pelo Conselheiro Presidente do TCE-RO, ou outra autoridade do Tribunal por delegação do Conselheiro Presidente, assessorado pela Assessoria de Segurança Institucional.

As credenciais de segurança devem ser entendidas como todos os dispositivos físicos ou eletrônicos que permitam acesso a locais ou serviços próprios da estrutura organizacional do TCE-RO e serão concedidas mediante a necessidade de acesso às informações para o desempenho das funções.

#### **5.1.7 Educação de Segurança**

Processo pelo qual são apresentados aos servidores às normas e os procedimentos de segurança orgânica, sobre os cuidados quanto a documentos e assuntos sigilosos, segurança de pessoal, áreas, instalações, equipamentos e nas comunicações, com o objetivo de desenvolver e manter uma

efetiva mentalidade de segurança, assim como de instruir o público interno para o seu fiel cumprimento.

A Educação de Segurança é efetivada através da:

**5.1.7.1 Orientação Inicial** – A Assessoria de Segurança Institucional será responsável, na Sede do Tribunal de Contas do Estado de Rondônia e e nas Secretarias Regionais, pela capacitação sobre normas de segurança dirigidas aos novos servidores em exercício de cargo e/ou função. É ministrada a todos os novos servidores antes do início efetivo do desempenho de sua função, oportunidade em que se faz uma apresentação das medidas de segurança orgânica adotadas no âmbito do TCE-RO. Ao final da respectiva apresentação, o servidor assinará um **Termo de Compromisso e/ou Termo de confidencialidade e sigilo**, por intermédio do qual se declarará ciente da necessária manutenção do sigilo dos assuntos sigilosos e dos procedimentos de segurança prescritos neste plano e nas Normas, devendo cumpri-los, fielmente, no exercício de suas funções.

**5.1.7.2 Orientação Específica** - Fica a cargo das chefias imediatas, que devem apresentar aos servidores os procedimentos de segurança orgânica inerentes às funções que irão desempenhar. Para isso, as chefias devem, ao receber novos servidores, orientá-los quanto aos procedimentos de segurança orgânica a serem observados no exercício da função, assegurando a salvaguarda dos assuntos sigilosos.

**5.1.7.3 Orientação Periódica** – A Escola Superior de Contas (ESCon), em conjunto com a Assessoria de Segurança Institucional, deverá realizar orientações periódicas, no mínimo anuais, nas quais devem abordar e discutir com os servidores as medidas de segurança orgânica vigentes, a importância de seu cumprimento, as possibilidades de vulnerabilidades da organização e o comportamento esperado dos servidores no sentido de preveni-las.

**5.1.7.4 Orientação para familiares** – Serão realizadas através de palestras de sensibilização, organizada pela Escola Superior de Contas (ESCon), por meio das quais são ministradas noções básicas de segurança, incluindo aspectos da segurança residencial, para os dependentes dos servidores, principalmente para as famílias daqueles que ocupam cargos com maior grau de sensibilidade. A principal finalidade desta medida é aumentar o grau de motivação dos servidores e gerar um efeito multiplicador do entendimento geral da importância de adotar uma cultura de segurança.

**5.1.7.5 Recursos Informativos** - a Assessoria de Segurança Institucional e Assessoria de Comunicação Social desenvolverão as atividades utilizando cartazes, pôsteres, panfletos, adesivos e outros, com a finalidade de inculcar e manter nos servidores uma mentalidade voltada para o cumprimento das normas e dos procedimentos de segurança.

#### **5.1.8 Acompanhamento no desempenho da função**

O acompanhamento no desempenho da função resulta de um processo que deve ser desenvolvido,

diariamente, por meio da observação, por parte da chefia imediata, do comportamento pessoal e funcional do servidor. Atos e atitudes positivos e negativos relevantes, verificados durante o exercício profissional do servidor, devem merecer registro e encaminhamento para Corregedoria e Assessoria de Segurança Institucional, para que constem na pasta de controle de expedição de credenciais de segurança e possam orientar o processo de educação de segurança.

Para a execução desse acompanhamento, é fundamental que haja contato permanente entre as chefias dos servidores e a Assessoria de Segurança Institucional. Os comportamentos contrários às normas devem ser motivo de orientação, inicialmente por parte da chefia imediata, com vistas à prevenção de situações que possam causar comprometimento. Caso necessário, a ASI deverá ser informada, para a revisão do credenciamento concedido e encaminhamento do assunto à Administração Superior.

As chefias imediatas devem assegurar-se de que todos os seus servidores tenham conhecimento e compreensão das medidas e dos procedimentos de segurança prescritos nas normas em vigor. O acompanhamento do desempenho das funções dos Conselheiros será realizado pela Corregedoria Geral do Tribunal de Contas.

### **5.1.9 Segurança no desligamento**

Procedimentos que visam assegurar a salvaguarda dos assuntos sigilosos após o afastamento do servidor da função que dava acesso a informações privilegiadas.

Para assegurar a efetivação dessa medida, devem-se observar os seguintes procedimentos:

#### **5.1.10 Restrição de acesso**

É restrito o acesso de servidores ativos e inativos às instalações onde sejam produzidos, manuseados, tratados ou armazenados documentos e/ou materiais sigilosos, salvo aqueles com credenciamento de acesso.

Aos servidores que não mais ocupem função com credenciamento de acesso a esses documentos e materiais, aplica-se a mesma regra. O servidor, ao ser destituído de uma função com credencial de segurança, deve ter seu caso comunicado a Assessoria de Segurança Institucional pelo seu chefe imediato, para que seja atualizada a pasta de controle de expedição de credenciais de segurança.

#### **5.1.11 Controle para liberação**

Deve ser obtido pelo servidor, antes de seu desligamento, um **“nada consta”** das diversas seções que compõem a sua unidade de lotação. Este item é regulamentado em Norma.

**5.1.11.1** Informar de imediato o desligamento do servidor a Assessoria de Segurança Institucional para controle de acesso ao TCE-RO;

- 5.1.11.2** Realizar uma entrevista final;
- 5.1.11.3** Cientificar o ex-servidor da responsabilidade da manutenção do sigilo do conhecimento e dados sigilosos;
- 5.1.11.4** Orientar o ex-servidor do TCE-RO sobre seu comportamento fora da Instituição;
- 5.1.11.5** Controlar o ex-servidor após o desligamento da Instituição, dando atenção especial àqueles que ocuparam funções mais sensíveis.

## **5.2 SEGURANÇA DA DOCUMENTAÇÃO E DO MATERIAL**

Define medidas e procedimentos destinados à proteção de documentos e materiais que contenham conhecimentos e dados sigilosos nos termos do Decreto n. 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.

As ameaças quanto aos documentos e materiais compreendem: a **espionagem**, objetivando a obtenção de conhecimentos e/ou dados sigilosos ou não, e a **sabotagem**, produzindo danos que possam provocar a perda da documentação ou material.

Normas definem os procedimentos complementares e subsidiários aos prescritos no decreto mencionado, especialmente no que se refere à produção, a classificação, a expedição, o recebimento, o registro, o manuseio, a guarda, o arquivamento, a reprodução de documentos classificados, bem com a destruição e tratamento dado ao lixo classificado, situações que requerem permanente atuação da Assessoria de Segurança Institucional.

Os equipamentos de reprodução de documentos sigilosos serão operados por servidores devidamente credenciados e deverão estar localizados em áreas cujo acesso possa ser efetivamente controlado.

Deverá ser instituída na Comissão Permanente de Gestão de Documentos uma subcomissão para tratar dos documentos sigilosos.

As medidas a seguir descritas estão relacionadas objetivamente aos documentos sigilosos, devendo sofrer as necessárias adaptações quando da sua aplicação aos materiais e aos documentos não sigilosos.

### **5.2.1.SEGURANÇA NA PRODUÇÃO:**

**a. Objetivo:** Atribuir um grau de sigilo, controlar recursos utilizados e marcar documentos produzidos no TCE-RO com sinais de segurança, caso necessário.

**b. Procedimentos:**

- b.1** Atribuir um grau de sigilo preliminar considerando a natureza dos assuntos, a finalidade, os usuários e aspectos sensíveis;
- b.2** Manter o grau de sigilo pré-determinado pela Chefia em todos os estágios da missão imposta;
- b.3** Atentar para possíveis comprometimentos através de acessos a conhecimentos ou dados sigilosos;
- b.4** Controlar os recursos utilizados de acordo com o grau de sigilo de cada um, tais como rascunhos, notas, carbonos, desenhos etc, os quais devem ser objeto de controle de segurança por parte de seus responsáveis. Entre estes recursos, alguns devem ser destruídos após a sua utilização e outros devem ser objeto de cuidados especiais relativos a sua segurança;
- b.5** Destruir diariamente os documentos classificados que não servirão mais;
- b.6** Arquivar em pastas os documentos classificados que serão reutilizados com o mesmo grau de sigilo do documento;
- b.7** Utilizar depósitos de lixo distintos para documentos classificados e não classificados;
- b.8** Numerar os documentos produzidos, que será um sinal de segurança contra extravio e a subtração;
- b.9** Classificar e marcar o grau de sigilo dos documentos produzidos no TCE-RO, conforme legislação pertinente da salvaguarda de assuntos sigilosos e o princípio da segurança;
- b.10** Revisar os documentos produzidos com o objetivo de reclassificação ou desclassificação;
- b.11** Estabelecer os procedimentos de segurança de acordo com o grau de sigilo durante a difusão, recepção, manuseio, arquivamento e destruição;
- b.12** Autenticar o documento de forma a confirmar a fidelidade da origem;
- b.13** Estabelecer sinais convencionais, inclusive, eletrônicos se disponíveis.

**5.2.2.SEGURANÇA NA DIFUSÃO E RECEPÇÃO:**

**5.2.2.1 Objetivo:** estabelecer controles de segurança nas rotinas de tramitação dos documentos entre emissor e o usuário.

**5.2.2.2 Procedimentos:**

- 5.2.2.2.1** Acondicionar os documentos produzidos, verificando possíveis violações ou indícios de comprometimento;
- 5.2.2.2.2** Registrar a saída de documentos;
- 5.2.2.2.3** Atribuir responsabilidades individuais pela expedição e tráfego dos documentos sigilosos;
- 5.2.2.2.4** Atentar sempre para o endereçamento dos documentos expedidos;
- 5.2.2.2.5** Estabelecer normas para controlar a recepção e a tramitação interna dos documentos;
- 5.2.2.2.6** Verificar possíveis violações dos documentos sigilosos, e caso positivo, retornar à origem para apurar responsabilidades;
- 5.2.2.2.7** Estabelecer os servidores conforme grau de sigilo do documento, quem poderá abri-los e assinar recibos.

### **5.2.3. SEGURANÇA NO MANUSEIO:**

**5.2.3.1 Objetivo:** estabelecer procedimentos para reprodução, custódia e revisão de classificação sigilosa dos documentos, bem como implementar controles durante a utilização.

#### **5.2.3.2 Procedimentos:**

**5.2.3.2.1** Reproduzir documentos só com autorização;

**5.2.3.2.2** Estabelecer o controle centralizado de reprodução;

**5.2.3.2.3** Elaborar extratos de documentos sigilosos quando necessário;

**5.2.3.2.4** Estabelecer cuidados especiais em caso de destruição;

**5.2.3.2.5** Reclassificar e desclassificar, de acordo com cada caso, através de reavaliações periódicas considerando a legislação vigente;

**5.2.3.2.6** Estabelecer critérios específicos para custódia e guarda;

**5.2.3.2.7** Reduzir ao máximo os acessos a documentos classificados a serem arquivados;

**5.2.3.2.8** Estabelecer critérios para seleção de documentos classificados a serem arquivados ou destruídos;

**5.2.3.2.9** Nos termos de destruição e nos arquivos, referenciar o conteúdo dos documentos;

**5.2.3.2.10** Verificar oportunamente a possibilidade de reutilização dos documentos produzidos;

**5.2.3.2.11** Consulta aos terminais de acordo com a credencial de segurança.

### **5.2.4. SEGURANÇA NO ARQUIVAMENTO:**

**5.2.4.1. Objetivo:** definir locais e processos adequados ao arquivamento e recuperação de documentos sigilosos, bem como, estabelecer rotinas para situações de emergência.

#### **5.2.4.2. Procedimentos:**

**5.2.4.2.1.** Estabelecer local seguro, com pouca circulação de pessoas e definir seu grau de sigilo;

**5.2.4.2.2.** Prever procedimentos em caso de emergência no deslocamento dos documentos;

**5.2.4.2.3.** Escolher arquivos e cofres de acordo com o grau de sigilo dos documentos e grau de segurança dos mesmos;

**5.2.4.2.4.** Estabelecer credenciais do servidor conforme o grau de sigilo dos documentos a serem arquivados;

**5.2.4.2.5.** Estabelecer rotinas de controle para arquivamento e recuperação;

**5.2.4.2.6.** Definir responsáveis pelo manuseio e controle dos documentos;

**5.2.4.2.7.** Estabelecer prioridade na evacuação dos documentos em caso de emergência;

**5.2.4.2.8.** Definir responsabilidades individuais durante a evacuação dos documentos salvos em caso de emergência;

**5.2.4.2.9.** Estabelecer local alternativo para arquivo temporário dos documentos salvos em caso de emergência.

### **5.2.5. SEGURANÇA NA DESTRUIÇÃO:**



**5.2.5.1. Objetivo:** Definir meios e locais de destruição, determinando formas de controle, e estabelecer rotinas em situações de emergência.

**5.2.5.2. Procedimentos:**

**5.2.5.2.1.** Escolher os meios de destruição;

**5.2.5.2.2.** Escolher o local restrito para destruição, considerando a circulação de pessoas e proteção contra intempéries;

**5.2.5.2.3.** Estabelecer um grau de sigilo para o local;

**5.2.5.2.4.** Confeccionar termo de destruição, juntando as autorizações necessárias;

**5.2.5.2.5.** Centralizar o trabalho para evitar extravios ou comprometimentos;

**5.2.5.2.6.** Estabelecer rotinas criteriosas durante a destruição;

**5.2.5.2.7.** Obedecer fielmente à legislação pertinente;

**5.2.5.2.8.** Estabelecer rotinas para destruição em situações de emergência, entre elas, plano de evacuação, responsabilidades específicas e forma de destruição.

### **5.3. SEGURANÇA DA INFORMAÇÃO E INFORMÁTICA**

#### **5.3.1. Segurança da Informação**

Define-se Segurança da Informação como a 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 27001:2006]

Define-se Sistema de Gestão da Segurança da Informação como 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. O sistema de gestão inclui estrutura organizacional, políticas, atividades de planejamento, responsabilidades, práticas, procedimentos, processos e recursos. [ABNT NBR ISO/IEC 27001:2006]

O TCE-RO lida diariamente com informações consideradas estratégicas e de apoio à tomada de decisão que necessitam de gerenciamento e garantia de confidencialidade, integridade e disponibilidade. Sendo assim, faz-se necessário o cumprimento do **Plano de Segurança da Informação**, conforme [Resolução nº 041/TCE-RO-2006](#), que dispõe sobre a Política de Segurança de Informações do Tribunal de Contas - PSI/TCE-RO e dá outras providências, e ainda, que seja integrado com as formas de tratamento das informações concebidas pela Ciência da Informação e pelas Técnicas de Gestão utilizadas no Planejamento Estratégico, no caso, no **Plano de Gestão de Segurança da Informação (PGSI)** a ser desenvolvido pela SETIC.

O objetivo é criar um Plano Corporativo de Gestão da Segurança da Informação, que siga as recomendações da [NBR ISO/IEC 27001 de 2006](#), e seja composto por um Plano Diretor de Segurança da Informação e um Modelo de Gestão para a Área de Segurança da Informação.

#### **5.3.1.1. Plano Diretor de Segurança da Informação (a ser desenvolvido pela SETIC).**

Deve identificar de forma concreta e embasada os reais riscos da Instituição e definir um Plano de Ação, levando em consideração as prioridades, de acordo com a realidade da Instituição, e suas principais necessidades em termos de Segurança da Informação. Essas necessidades deverão ser traduzidas em medidas e procedimentos divididos em três grupos: controle de acesso, controle dos serviços e mecanismo de proteção dos canais de comunicação.

##### **5.3.1.1.1. Controle de Acesso**

Apenas os servidores devidamente credenciados podem ter acesso às informações. O controle de acesso deve alertar sobre qualquer falha no sistema e identificar os responsáveis por acessos indevidos. O controle de acesso deve ainda:

1. Identificar os usuários com necessidade de acesso;
2. Conceder acesso apenas àqueles devidamente credenciados e negá-la aos não-autorizados;
3. Registrar os horários de entrada e saída, bem como as ações das pessoas com autorização de acesso;
4. Registrar os acessos de violação ou suspeitos de violação das regras estabelecidas.

- **Controle de acesso físico**

Limita o acesso às áreas em que se encontram os equipamentos do Sistema de Informação. Deve funcionar como uma primeira barreira de segurança, minimizando a possibilidade de danos causados intencionalmente ou não aos equipamentos.

- **Controle de acesso aos equipamentos**

Limita quem pode usar os equipamentos. Esta medida decorre da incapacidade de colocar todos os equipamentos do Sistema de Informação em áreas restritas.

O controle de acesso deve estender-se também ao uso de equipamentos compartilhados por mais de um usuário, auxiliando, dessa forma, na segurança do controle de acesso aos recursos do sistema. Na implementação desta medida, pode-se usar controles por meio de hardware, software ou uma combinação dos dois.

O sistema de controle de acesso de equipamentos deve identificar e discriminar os usuários,

registrar as ações e alertar os responsáveis pela segurança a respeito de todas as tentativas de violação das instruções em vigor.

- **Controle de acesso aos recursos do sistema**

Limita os recursos (arquivos, diretórios, filas de impressão ou sistemas de comunicação) que o sistema oferece e discrimina os usuários credenciados, autorizados a utilizá-los. O controle de acesso deve ser feito de tal forma que alguns recursos do sistema estejam disponíveis apenas para alguns usuários, impedindo o acesso a pessoas não autorizadas ou sem necessidade de acesso.

O controle de acesso aos recursos do sistema deve permitir discriminá-los por usuários, e registrar o uso desses recursos de acordo com a identificação do usuário. Os casos de tentativa de violar a compartimentação dos recursos devem gerar avisos de alerta.

#### **5.3.1.1.2. Controle dos serviços e mecanismos de proteção**

Devem-se adotar medidas e procedimentos para a proteção contra ameaças oriundas de fatores não controlados pelo homem, tais como interrupções do fornecimento de energia elétrica, incêndios, inundações e outros tipos de sinistro, bem como para a prevenção contra ameaças humanas, como erros e omissões, acidentes, sabotagens e programação com objetivos escusos.

##### **5.3.1.1.2.1. Controle de fornecimento de energia elétrica**

Devem-se adotar medidas com o propósito de garantir o fornecimento constante de energia elétrica, dentro dos parâmetros aceitáveis. Deve-se prever também o uso de geradores, retificadores, transformadores, estabilizadores e *no break*, conforme as necessidades do local de instalação dos equipamentos.

##### **5.3.1.1.2.2. Controle das cópias de segurança (backup)**

Devem-se adotar medidas para garantir que todas as informações possuam cópias de segurança e estejam atualizadas e em condições de serem restauradas em curto período de tempo. Deve-se atentar para a segurança dos meios utilizados para armazenar essas informações (DVD, CD-ROM ou outros), tanto em relação ao tempo de vida útil, quanto em relação à proteção física.

##### **5.3.1.1.2.3. Controle de ameaças**

Devem-se adotar medidas e procedimentos de prevenção contra as ameaças oriundas de códigos de programação escusos (vírus eletrônicos, cavalos-de-troia e outros), contra a instalação de programas não-autorizados e contra as tentativas de invasão, internas ou externas, realizadas por exploração de vulnerabilidades do sistema. Devem-se definir políticas claras de aquisição e atualização de software e hardware, para garantir a implementação rápida de medidas contra novas ameaças, conforme a mais recente tecnologia de segurança da informação disponível no mercado.

### **5.3.1.2. Modelo de Gestão para a Área de Segurança da Informação:**

O Modelo de Gestão deve ser feito com base nas necessidades levantadas no Plano Diretor de Segurança da Informação a ser desenvolvido pela Secretaria Estratégica de Tecnologia da Informação e Comunicação - SETIC.

### **5.3.6. Segurança da Informática:**

Tem como objetivo prover proteção ao sistema de informática, estabelecendo padrões de garantia à integridade dos equipamentos e bancos de dados.

#### **5.3.6.1. Proteção de dados e de software**

Tem como objetivo evitar e reduzir os riscos criados ou mantidos no sistema, através dos seguintes procedimentos:

**5.3.6.1.1** Controlar mudanças de programas entre os ambientes;

**5.3.6.1.2** Implantar “Back-up” de sistemas e arquivos;

**5.3.6.1.3** Implantar controle de “password”;

**5.3.6.1.4** Implantar “time-out”;

**5.3.6.1.5** Estabelecer mecanismos de identificação de usuários;

**5.3.6.1.6** Estabelecer mecanismos de registro de ocorrências e auditorias;

**5.3.6.1.7** Estabelecer diretriz para implantação de redes;

**5.3.6.1.8** Empregar técnicas criptográficas;

**5.3.6.1.9** Elaborar plano de contingência para situações de emergência;

**5.3.6.1.10** Criar programa de controle de acesso do público em geral ao TCE-RO, interligado às Secretarias Regionais.

### **5.4. SEGURANÇA DAS COMUNICAÇÕES:**

Tem como objetivo proporcionar ações para salvaguarda dos conhecimentos e/ou dados sigilosos durante os atos de transmissão e de recepção. Essas ações serão divididas em segurança na transmissão e segurança no conteúdo.

#### **5.4.1. Segurança na transmissão:**

Objetiva dificultar a interceptação e a conseqüente análise do fluxo de mensagens, através dos seguintes procedimentos:

**5.4.1.1** Escolher os meios de comunicação;

**5.4.1.2** Escolher os locais para instalação dos equipamentos de rede nacional;

**5.4.1.3** Normatizar o uso dos meios de comunicação;

**5.4.1.4** Escolher os locais para instalação de rede privada;

**5.4.1.5** Estabelecer códigos de chamada;

**5.4.1.6** Estabelecer canais de comunicações que confundam o interceptador.

#### **5.4.2. Segurança do conteúdo:**

Objetiva dificultar o entendimento dos textos transmitidos por elementos adversos, adotando os seguintes procedimentos:

**5.4.2.1** Preparar as mensagens;

**5.4.2.2** Escolher os recursos criptológicos;

**5.4.2.3** Estabelecer códigos de autenticação;

**5.4.2.4** Estabelecer códigos de assinantes.

#### **5.4.3. Proteção dos canais de comunicação**

Uma das vantagens do uso de um sistema de informação é a possibilidade de receber e enviar as informações armazenadas por meio de canais apropriados de comunicação, como, por exemplo: cabeamentos de rede, sistemas de telefonia pública e privada, sinais de rádio e outros. Dessa forma, devem-se adotar medidas que visem à proteção desses canais, no que se refere à preservação do sigilo e à disponibilidade e integridade das informações que trafegam por um sistema de informação ou entre vários sistemas diferentes.

#### **5.4.4. Proteção física dos canais de comunicação**

Devem-se adotar medidas para garantir a integridade e a confiabilidade dos canais de comunicação, tais como cabeamentos, roteadores, concentradores e outros, além da proteção contra o monitoramento e a interceptação do tráfego de dados.

#### **5.4.5. Verificação dos canais de comunicação**

Devem-se adotar medidas para o monitoramento das comunicações efetuadas através dos canais disponíveis. Nesse contexto, deve-se prever a utilização de procedimentos capazes de garantir o sigilo e a integridade das informações trafegadas, tais como a criptografia, a assinatura digital e a autenticação eletrônica.

### **5.5 SEGURANÇA DAS ÁREAS E DAS INSTALAÇÕES**

Define medidas de proteção voltadas para áreas e instalações em que são elaborados tratados, manuseados ou guardados documentos e/ou conhecimentos sigilosos, bem como materiais sigilosos e equipamentos sensíveis, com a finalidade de salvaguardá-los, tendo por base o controle de acesso.

A ocorrência de acidentes de qualquer natureza também desencadeia o comprometimento desses documentos, conhecimentos e materiais. Em consequência, devem-se considerar acidentes involuntários e fenômenos naturais na elaboração do Plano de Segurança Orgânica.

A segurança das áreas e instalações é realizada pela Assessoria de Segurança Institucional, por intermédio de convênio de execução de serviços de policiamento de guarda firmado junto à Polícia Militar e também por serviços de vigilância privada contratados através de procedimentos licitatórios.

### **5.5.1. Demarcação das Áreas**

Estabelece ações para identificação das áreas de acordo com os tipos (livre, restrita ou sigilosa), a classificação conforme o grau de sigilo dos assuntos nelas tratados, guardados ou manuseados e a delimitação segundo os tipos e a classificação.

### **5.5.2. Implantação de barreiras**

Visa dificultar o ingresso de pessoas não autorizadas nas áreas sigilosas ou restritas, bem como permitir um efetivo controle da circulação das pessoas que tenham autorização para isso. Devem-se estabelecer prioridades na definição e implementação dos diversos tipos de barreiras, levando-se em consideração a área a ser protegida e os recursos disponíveis. Procedimentos importantes:

- Estabelecer sistema de alarmes eletrônicos e visuais;
- Estabelecer guaritas de segurança se necessário.

#### **5.5.2.1. Classificação dos dispositivos de segurança**

Discrimina os dispositivos de proteção e vigilância das áreas definidas como prioritárias:

**5.5.2.1.1.** Proteção tipo 1 - elementos arquitetônicos existentes em todas as sedes do Tribunal de Contas do Estado de Rondônia, como muros, grades, portões de estacionamento, grades de janela, portas-de-ferro, portas pantográficas e fechaduras de segurança.

**5.5.2.1.2.** Proteção tipo 2 – sistemas de alarme patrimonial nas edificações, com sensores localizados em pontos vulneráveis do prédio, capazes de detectar qualquer movimentação não autorizada, acionando um conjunto de sirenes no local e/ou remotamente, por meio de discador telefônico.

**5.5.2.1.3.** Proteção tipo 3 – sistemas de cerca eletrônica instalados sobre muros e grades, nas divisas dos terrenos onde se situam os prédios da Instituição. Previnem a ocorrência de invasões do perímetro, mediante o acionamento de um conjunto de sirenes no local.

**5.5.2.1.4.** Proteção tipo 4 – dispositivos de detecção de metais, fixos ou manuais, que previnem o ingresso de pessoas portando armas. Os níveis de sensibilidade podem ser ajustados de modo a evitar constrangimentos desnecessários.

**5.5.2.1.5.** Proteção tipo 5 – sistemas de CFTV, com câmeras de vídeo e equipamentos de gravação digital de imagens, que permitem o monitoramento de áreas internas e externas em tempo

real ou mediante a recuperação de quadros, no local ou remotamente, via web. Também podem ser utilizados como sensor de movimento.

**5.5.2.1.6.** Proteção tipo 6 – barreiras físicas de controle de acesso, como catracas, cancelas e portas com fechaduras magnéticas, acionadas por cartões de identificação, crachás ou biometria, que restringem a entrada e a circulação de pessoas na edificação, conforme os níveis de acesso estabelecidos.

Os equipamentos acima relacionados devem possuir alimentação alternativa por bateria ou *no break*, evitando o desligamento quando houver interrupção no fornecimento de energia elétrica.

A operação dos diversos sistemas de segurança pode ser integrada em uma central de monitoramento, com acesso remoto aos dispositivos definidos como prioritários. A centralização da vigilância possibilita a otimização dos recursos humanos disponíveis. Contudo, requer grandes investimentos em tecnologia da informação.

### **5.5.3 Prevenção e combate contra incêndios e prevenção de acidentes**

Devem-se adotar medidas e procedimentos preventivos para evitar sinistros, de qualquer espécie, capazes de colocar em risco não só os servidores, como também os documentos/conhecimentos sigilosos, materiais e equipamentos do Tribunal e as medidas e os procedimentos corretivos para os casos de emergência. Ainda, avaliação pontual da necessidade de contratação de seguro predial onde envolvam coberturas específicas para eventuais sinistros.

No planejamento, devem-se considerar todas as medidas e os procedimentos para a proteção de documentos e materiais sigilosos, assim como as rotinas para evacuação.

A Brigada de Combate a Incêndio foi criada através da [Resolução n. 158/2014/TCE-RO](#), onde prevê o treinamento dos servidores quanto aos procedimentos a serem adotados em situações de emergência, em caso de sinistros e de acidentes pessoais com exercícios simulados anuais.

Todas as sedes do Tribunal de Contas do Estado de Rondônia deverão possuir **Alvará de Prevenção Contra Incêndio**, integrante do conjunto de projetos complementares, e o **PECIAS – Plano de Emergência de Combate a Incêndios e Atuação em Sinistros**, em fase de análise pelo Conselho Superior de Administração, o qual foi desenvolvido obedecendo às exigências das normas e legislação específicas. O Plano tem por objetivo reduzir a possibilidade de incêndio, proteger a vida dos ocupantes, minimizar a propagação do fogo e reduzir os danos materiais, entre outros.

Já na elaboração do projeto arquitetônico da reforma do edifício sede, deverão ser previstas as medidas de proteção passiva a serem adotadas, como pontos de acessibilidade, implantação de rotas de fuga, dimensionamento dos elementos estruturais, compartimentação, definição de materiais de acabamento e revestimentos, instalação de sistemas de alarme, entre outros. Posteriormente, será realizado o estudo das proteções ativas, as quais comportam uma variedade de sistemas, do mais simples ao mais complexo, como a extinção automática por meio de gás, utilizada para proteção de equipamentos do datacenter, por exemplo.

**Dessa forma, toda edificação construída, ampliada ou reformada deverá ter os sistemas de prevenção contra incêndios instalados. Nenhum termo de recebimento definitivo de obra será**



**emitido sem a apresentação do Alvará de Prevenção Contra Incêndio.**

- **MEDIDAS ADMINISTRATIVAS:**

A Assessoria de Segurança Institucional – ASI, junto com as Secretarias, divisões e demais assessorias responsáveis farão os levantamentos dos recursos humanos, materiais e financeiros necessários à implantação do Plano de Segurança Institucional e Plano de Emergência de Combate a Incêndios e Atuação em Sinistros do TCE-RO.

- **PRESCRIÇÕES DIVERSAS**

- a. Responsabilidade:**

- A **Resolução n. 157/2014/TCE-RO** institui o Comitê de Segurança Institucional no âmbito do Tribunal de Contas do Estado de Rondônia, o qual passará a coordenar, organizar, especializar e sistematizar as atividades de segurança Institucional do TCE-RO;

- Caberá a Assessoria de Segurança Institucional – ASI, o planejamento, a elaboração e a execução do Plano de Segurança Institucional (PSI) e Plano de Emergência de Combate a Incêndios e atuação em Sinistros após aprovadas às mudanças pelo CSI/TCE-RO, no âmbito do Tribunal de Contas do Estado de Rondônia, devendo receber tratamento prioritário para suprir a deficiência advinda da inexistência de normas subsidiárias que atendam às características de cada setor.

- A Assessoria de Segurança Institucional atuará de forma coordenada para evitar a dispersão de esforços e meios e garantir a plenitude do cumprimento dos procedimentos para proteção de dignitários, de instalações e de pessoal, salvaguarda dos documentos, materiais e/ou equipamentos orgânicos do Tribunal de Contas ou sob sua responsabilidade.

- Todo o servidor, no limite de suas atribuições, deve observar as medidas de segurança orgânica, sendo em consequência, responsável por atos ou atitudes que venham a comprometê-la.

- b. Inspeções:**

- A fim de acompanhar a observância das medidas de segurança preconizadas no presente plano, bem como avaliar a adequabilidade das mesmas, deverão ser realizadas as seguintes inspeções de segurança:

- a) Programada:** é uma inspeção de rotina através da qual o Conselheiro Presidente do TCE-RO, CSI/TCE-RO e Secretários baixam, em documento, a data e os aspectos inerentes aos diversos tipos de segurança que serão avaliados.

**b) Inopinada:** é uma inspeção conduzida pelo Conselheiro Presidente do TCE-RO, do CSI/TCE-RO ou, em seu nome, pelos Secretários, Assessorias e Chefes, através da qual, sem um alerta prévio, é verificada a execução das medidas de segurança de forma a evitar que a rotina venha a comprometê-la.

**c) Situacional:** Será procedida sempre que qualquer fato anormal venha a ocorrer, comprometendo a segurança do Tribunal. Deverá ser conduzida pela Assessoria de Segurança Institucional, buscando apurar causas. Se o fato justificar, poderá, em consequência, ser determinada uma investigação de lealdade.

**c. Relatórios:**

Qualquer uma das inspeções anteriormente apresentadas deverá produzir, como resultado, um relatório, o qual apontará, se for o caso, as falhas encontradas e as medidas para corrigi-las e, ainda, sugestões para alterações ao presente plano, quando for constatado que uma medida de segurança tenha se tornado ineficaz.

**d. Investigação:**

Quando da ocorrência de situações que, de forma direta ou indireta, possam causar o comprometimento de conhecimento e/ou dados sigilosos, deverá ser feita uma investigação no sentido de identificar suas causas, os agentes causadores e a extensão do comprometimento.

• **DISPOSIÇÕES FINAIS:**

Este plano de segurança será objeto de análise e revisão a cada 3 (três) anos contados da data de sua aprovação pelo Conselheiro Superior de Administração do Tribunal de Contas do Estado de Rondônia ou a qualquer tempo em caso de mudanças na legislação em vigor.

Os casos omissos ao Plano de Segurança Institucional serão decididos pela Presidência do TCE-RO.

Porto Velho-RO, 13 de novembro de 2015.

**JOSÉ ITAMIR DE ABREU – TEN CEL PM**

Assessor de Segurança Institucional

**JOSÉ EULER POTYGUARA PEREIRA DE MELLO**

Conselheiro Presidente do TCE-RO

**ANEXO**

**PROCEDIMENTOS GERAIS DE SEGURANÇA**

## **I. PROCEDIMENTOS QUANTO À UTILIZAÇÃO E ACESSO ÀS EDIFICAÇÕES**

### **1. ACESSO DE SERVIDORES:**

- O acesso às instalações do TCE-RO será realizado sempre a partir da entrada principal da edificação, pela Avenida Presidente Dutra, salvo situações extraordinárias devidamente autorizadas;
- O controle de acesso às dependências do TCE-RO será realizado pela Recepção, sob a supervisão do Departamento de Serviços Gerais - DESG da Secretaria Geral de Administração e Planejamento - SGAP e da ASI, por meio de uso de crachá ou outro instrumento de identificação;
- O acesso principal será dotado de portal com detector de metais, devendo todos obedecerem à passagem obrigatória pelos mesmos;
- Não estão sujeitas à regra do item anterior, desde que devidamente identificadas, pessoas que, em decorrência de necessidades especiais, utilizem equipamentos auxiliares para locomoção, e pessoas portadoras de aparelhos marca-passo;
- Na hipótese do item anterior, será efetuada revista para verificação de posse ou não de arma de fogo e de outros objetos que representem ameaça à segurança, e essas pessoas terão acesso através da porta secundária, localizada ao lado da porta principal;
- Para o acesso às instalações físicas do TCE-RO cada usuário deverá obrigatoriamente utilizar seu crachá de identificação funcional, em lugar de fácil visualização, para fins de identificação e manutenção da segurança nas dependências do TCE-RO;
- Entende-se por servidores, os servidores do Tribunal de Contas efetivos, comissionados e estagiários;
- Nos casos de perda ou indisponibilidade do crachá, o usuário deverá identificar-se junto ao balcão de atendimento localizado no acesso principal, comunicando a situação e solicitando crachá de acesso provisório, o qual deverá ser restituído quando do encerramento do expediente administrativo pelo usuário da edificação;
- Em casos de perda, furto e roubo do crachá de identificação funcional, o usuário deverá registrar ocorrência policial no Distrito Policial e entregar cópia na SEGESP, solicitando, via requerimento, novo crachá;

- O acesso ou a permanência de servidor fora do seu horário de trabalho e nos finais de semana, feriados e recessos somente será permitido mediante prévia comunicação por escrita da Chefia imediata à SGAP e deverá ser restrita à respectiva unidade de lotação;
- Em casos excepcionais, caracterizados por situações imprevisíveis que não permitam o comunicado prévio, a SGAP autorizará a entrada e notificará a Chefia imediata do servidor;
- É vedado ao servidor fazer adentrar nas dependências do Tribunal acompanhante sem a identificação da recepção;
- É vedado ao servidor agendar compromisso de caráter particular com terceiros nas dependências do Tribunal;
- Os servidores inativos, para ingressar no TCE-RO, deverão identificar-se junto ao serviço de recepção respectivo, a fim de obter o crachá de “SERVIDOR APOSENTADO – Trânsito Livre”;
- Os funcionários terceirizados de serviços continuados ou não deverão portar crachá de identificação, expedidos pelas respectivas empresas;
- Entende-se por funcionários terceirizados, os prestadores de serviços, contínuos ou não;
- Fica vedado o acesso de servidores, visitantes e funcionários terceirizados pelo portão de acesso à garagem do Tribunal;
- Os portões de acesso às garagens são destinados à entrada e saída e ao estacionamento de veículos oficiais do Tribunal, de veículos de autoridades visitantes e de veículos devidamente autorizados;
- Os veículos oficiais e/ou de empresas prestadoras de serviços terceirizados, por fundadas suspeitas e/ou irregularidades, quando do ingresso ou saída das garagens do Tribunal, poderão ser vistoriados a critério do SGAP ou ASI;
- Caberá à SGAP, através da Secretaria de Gestão de Pessoas, o fornecimento de crachá provisório dos funcionários terceirizados que realizarem serviços de curta duração, desde que a empresa contratada não disponha de identificação própria;
- Determinar a todo servidor e àqueles que por força de lei, contrato ou qualquer outro ato jurídico, prestam serviços de natureza permanente, temporária ou excepcional, desde que vinculados direta ou indiretamente ao Tribunal de Contas, que ao se apresentarem para o trabalho, o façam com vestimentas adequadas ao exercício do cargo ou da função, atentando para o decoro e zelo, preservando a tradição dos serviços públicos e a conduta ética, visando ao atendimento do princípio da moralidade da Administração Pública (art. 2º da Portaria n. 549, de 06 de julho de 2015);

- Determinar aos servidores, estagiários e terceirizados do sexo masculino que se apresentem, durante o expediente normal de trabalho, com vestimentas adequadas ao exercício do cargo e da função, observando-se (art 3º da Portaria n. 549, de 06 de julho de 2015):

I) O uso de camisa social, camisa de manga curta ou camisa polo, calça comprida de brim ou jeans, sapato social, tênis ou similar.

a) Ao usarem jeans para o trabalho, prefiram os modelos tradicionais, sem bolsos extras e/ou rasgados.

b) Evitem o uso de acessórios e objetos incompatíveis ou extravagantes.

II) Vedação ao uso de camisetas regatas, camisetas justas, camisetas com logotipos ou marcas de equipes desportivas, bermudas, shorts, chinelos, sandálias, bonés e chapéus.

III) Nas solenidades e sessões Plenárias deste Tribunal, o uso de terno e gravata pelos ocupantes de cargos de Secretário, Assessor de Conselheiro e Diretor de Departamento.

- Determinar às servidoras, estagiárias e terceirizadas que se abstenham de comparecer ao local de trabalho usando bermuda, shorts, calça comprida e vestidos confeccionados em tecidos de lycra ou similares, minissaia, miniblusa, blusas com decote exagerado, transparência, blusas e vestidos sem alças, roupas íntimas aparentes, calças jeans de cós baixo ou rasgadas, bem como o uso de sandálias estilo rasteiras, ressalvado nesse caso, a necessidade, por motivo de saúde, desde que devidamente comprovada (art 4º da Portaria n. 549, de 06 de julho de 2015).

## **2. ACESSO DO PÚBLICO EM GERAL:**

- O acesso às instalações do TCE-RO será realizado sempre a partir da entrada principal da edificação, pela Avenida Presidente Dutra, salvo situações extraordinárias devidamente autorizadas pela administração;

- O acesso principal será dotado de portal com detector de metais, devendo todos obedecerem à passagem obrigatória pelos mesmos e seus pertences serem submetidos a averiguações;

- Não estão sujeitas à regra do item anterior, desde que devidamente identificadas, pessoas que, em decorrência de necessidades especiais, utilizem equipamentos auxiliares para locomoção, e pessoas portadoras de aparelhos marca-passo;

- Na hipótese do item anterior, será efetuada revista para verificação de posse ou não de arma de fogo e de outros objetos que representem ameaça à segurança, e essas pessoas terão acesso através da porta secundária, localizada ao lado da porta principal;

- Todos os indivíduos que acorrerem às instalações físicas do TCE-RO deverão ser identificados junto ao balcão de atendimento da edificação e, após prévia autorização por parte da unidade ou Gabinete de destino, receberão crachá de identificação próprio;

- Para os fins previstos no item anterior, serão considerados “visitantes” os representantes de jurisdicionados, os prestadores de serviços, os servidores de outros órgãos públicos, os familiares dos servidores, dentre outros;
- O acesso de familiares dos servidores aos respectivos locais de trabalho será admitido em caráter excepcional, e desde que autorizados previamente;
- Autorizado o ingresso nos termos previstos anteriormente, o visitante receberá o crachá referente ao andar em que poderá transitar ou, quando for o caso, o de “VISITANTE – Trânsito Livre”;
- A identificação de pessoas não autoriza a entrada à área restrita da edificação, sendo necessária a identificação do membro ou servidor que receberá o indivíduo para a concessão de acesso à área restrita da edificação;
- O advogado identificar-se-á na recepção do Tribunal, mediante apresentação da carteira da Ordem dos Advogados do Brasil – OAB, recebendo o crachá “ADVOGADO – Trânsito Livre”;
- Fica vedado o ingresso de pessoa(s) trajando vestimenta inadequada ao ambiente do TCE-RO, tais como bermudas(s), short(s), camiseta(s) de física, boné(s), capacete(s), miniblusa(s) ou outros assemelhados;
- Quando da entrada de jurisdicionados e cidadãos nas dependências da Corte de Contas, será observado o disposto no item II do artigo 3º, para o sexo masculino, e artigo 4º para o sexo feminino, da Portaria n. 549, de 06 de julho de 2015, excetuando-se crianças de até 12 (doze) anos (Art. 6º);
- Deverão ser entregues pelo portador, por ocasião de sua entrada no prédio, mediante recibo, quaisquer objetos que apresentem ameaça à segurança e considerados perigosos pelos integrantes da equipe de segurança privada, policiais militares ou Assessoria de Segurança Institucional, os quais serão restituídos na saída;
- Não será vedado o acesso, nem caberá embaraço, e será proibida qualquer medida que resulte em constrangimento e discriminação concernente ao visitante, jurisdicionado ou pessoa que não dispõe de condição financeira, educação escolar ou social suficientes para entender as exigências convencionais e que necessita da prestação de serviços do Tribunal, havendo que prevalecer o bom senso e a razoabilidade nesse tipo de atendimento;
- São vedados o ingresso e a permanência de cobradores, angariadores de donativos ou congêneres, bem como a prática de comércio nas dependências do Tribunal, ressalvados os eventos autorizados pela Administração;



- Não é permitido qualquer tipo de panfletagem ou propaganda, salvo mediante autorização prévia do Secretário Geral de Administração e Planejamento;
- As rotas de fuga e saída de emergência das edificações deverão permanecer desobstruídas, sendo vedada a instalação permanente ou provisória de quaisquer barreiras físicas ou depósito, mesmo que temporário, de móveis ou documentos, que dificultem ou impeçam o regular fluxo de pessoas em tais locais.

### **3. ACESSO DE AUTORIDADES:**

- Os Chefes de Poderes serão recebidos, na entrada principal ou acesso da garagem pela Assessoria de Segurança Institucional e Chefia de Gabinete da Presidência e encaminhados ao local de destino ou indicado pelo cerimonial;
- As demais autoridades e personalidades convidadas para sessão solene serão recebidas pelas assessorias respectivas;
- Todas as autoridades constituídas que forem aos Gabinetes de Conselheiros deverão ser acompanhadas por uma das recepcionistas ou membros da ASI;
- As autoridades previamente indicadas pelos Gabinetes dos Conselheiros, dos Conselheiros Substitutos, do Procurador Geral do Ministério Público de Contas, Procuradores do Ministério Público de Contas e demais autoridades, após se identificarem junto à recepção do Tribunal de Contas e receberem o respectivo crachá, serão conduzidas pelas recepcionistas ou assessores de segurança aos locais de destino, somente quando solicitado.

## **II. PROCEDIMENTOS QUANTO À PROTEÇÃO PESSOAL**

- 1.** A segurança pessoal geral dentro da estrutura do Tribunal de Contas se desenvolve através da atividade de policiamento ostensivo, tipo guarda, nas instalações, realizado pela Assessoria de Segurança Institucional, Polícia Militar e pelo serviço de vigilância privado, coibindo ações que ponham em risco a integridade dos servidores durante a jornada de trabalho;
- 2.** A segurança pessoal das autoridades da Corte e Presidência é desenvolvida pela Assessoria de Segurança Institucional, de acordo com as diretrizes estabelecidas pelo Conselheiro Presidente, incluindo as ações de atendimento individualizado e de acompanhamento externo das representações oficiais, ficando a ASI à disposição a qualquer hora do dia;
- 3.** As situações excepcionais, que demandem atendimento da ASI, no tocante à segurança pessoal, tanto de autoridades como de servidores da Corte, em especial o apoio às atividades de

auditoria, do Ministério Público de Contas e do Corregedor, serão atendidas, somente mediante autorização expressa do Conselheiro Presidente;

4. Os crachás de acesso individuais são de utilização obrigatória e não deverão ser compartilhados;
5. A presença de pessoas estranhas ao setor de trabalho, nas áreas restritas, sigilosas ou livres do TCE-RO, deverá ser comunicada imediatamente à equipe de segurança da instalação física e à Assessoria de Segurança Institucional;
6. Não deverão ser fornecidas quaisquer informações pessoais sobre servidores e membros do TCE-RO por telefone;
7. A utilização das instalações físicas do TCE-RO fora dos horários regulares de expediente administrativo deverá ser previamente autorizada pelo chefe imediato, por escrito, e comunicado à equipe de segurança da edificação, a qual deverá registrar o evento em controle próprio;
8. Nos casos de acionamento de alarme de incêndio, os usuários da edificação deverão imediatamente interromper suas tarefas e dirigir-se às rotas de fuga de edificação, utilizando as escadarias, atendendo às orientações das equipes de segurança da instalação física e brigadistas.

### **III. PROCEDIMENTO EM DIA DE PAGAMENTO:**

1. Atenção especial a pessoas e veículos suspeitos nos arredores das edificações do TCE-RO;
2. Não realização de saques vultosos nos caixas automáticos localizados no interior das instalações físicas do TCE-RO;
3. Discrição quanto aos valores recebidos a título de pagamento.

### **IV. PROCEDIMENTO EM SITUAÇÕES DE MANIFESTAÇÕES E TUMULTOS**

1. Acionamento da Polícia Militar para apoio via 190;
2. Acionamento da Assessoria de Segurança Institucional;
3. Fechamento dos portões de acesso à edificação;
4. Estabelecimento de um ponto de controle de acesso e de saída da edificação junto aos portões externos da mesma;

5. Liberação dos bloqueios dos portões externos da edificação somente após a liberação do local por parte da Polícia Militar e Assessoria de Segurança Institucional.

#### **V. PROCEDIMENTO EM SITUAÇÕES DE BRIGAS OU RIXAS NO INTERIOR DAS EDIFICAÇÕES**

1. A composição das partes;
2. Comunicar a equipe de segurança da instalação física;
3. Comunicar a Assessoria Segurança Institucional;
4. Acionamento da Polícia Militar via 190.

#### **VI. PROCEDIMENTOS EM SITUAÇÕES ENVOLVENDO BOATOS PERNICIOSOS**

1. Interromper a proliferação do boato;
2. Comunicar a Assessoria de Segurança Institucional.

#### **VII. PROCEDIMENTOS QUANDO DA OCORRÊNCIA DE ATOS DE VANDALISMO NO INTERIOR E NO EXTERIOR DAS EDIFICAÇÕES**

1. A composição das partes;
2. O acionamento da Polícia Militar via 190 e perícia, caso haja dano ao patrimônio do TCE-RO;
3. Comunicar de imediato a Assessoria de Segurança Institucional.

#### **VIII. PROCEDIMENTOS EM CASO DE INVASÃO OU TENTATIVA DE INVASÃO**

1. O acionamento da Polícia Militar, via 190, para apoio, registro de ocorrência policial e acionamento da perícia, caso tenha ocorrido dano ao patrimônio;
2. O fechamento dos portões externos de acesso à edificação;
3. O estabelecimento de um ponto de controle de acesso e de saída da edificação junto aos portões externos da mesma;
4. A liberação do bloqueio dos portões externo da edificação somente após a liberação do local por parte da Polícia Militar e Assessoria de Segurança Institucional.

**IX. PROCEDIMENTO QUANTO AOS TERCEIRIZADOS:**

1. É vedado o acesso de terceirizados às áreas de segurança classificadas como sigilosas ou restritas, salvo mediante liberação e acompanhamento por servidores ou membros do TCE-RO;
2. Os terceirizados deverão obrigatoriamente apresentar o crachá de identificação no acesso principal, bem como no interior do TCE-RO;
3. Os terceirizados designados para limpeza dos gabinetes dos Conselheiros, Procuradores e Auditores deverão ser extrema confiança e ainda assinar termo onde se comprometam com o sigilo de documentos por ventura vistos, devendo preferencialmente estar acompanhados por algum assessor do Gabinete;
4. Os terceirizados previstos para executar serviços conforme item anterior devem ser cadastrados na ASI;
5. A empresa terceirizada deverá disponibilizar ao TCE-RO cadastro com fotos de seus funcionários, bem como certidões circunstanciadas negativas de antecedentes criminais;
6. Toda e qualquer substituição de terceirizado deverá ser comunicada previamente por escrito ao TCE-RO, com prazo mínimo de 72 horas;
7. A contratação de novos terceirizados deverá ser precedida de solicitação de avaliação individual dos pretensos contratados por parte da Assessoria de Segurança Institucional;
8. Toda e qualquer alteração encontrada por funcionários terceirizados deverá ser comunicado de imediato ao Chefe do setor competente.

**X. PROCEDIMENTO NO CASO DE OCORRÊNCIA DE VAZAMENTO DE INFORMAÇÕES:**

Deve ser coletada a maior quantidade de dados possível a respeito do vazamento e ser efetuada a imediata comunicação à ASI do TCE-RO.

**XI. PROCEDIMENTOS QUANTO À SEGURANÇA DA SALA DE SERVIDORES DE DADOS E COMUNICAÇÃO**

1. Após o encerramento dos horários regulares de expediente administrativo, o acesso de servidores e terceirizados a essa área sigilosa somente poderá ser autorizado pelo **Secretário da Secretaria Estratégica de Tecnologia da Informação e Comunicação** ou, pela **ASI**, nos casos de emergência;

2. O fornecimento de credenciais de acesso a essa sala deverá ser avaliado pelo **Secretário da Secretaria Estratégica de Tecnologia da Informação e Comunicação**.

## **XII. PROCEDIMENTOS QUANTO AO CIRCUITO FECHADO DE TV – CFTV:**

1. O Circuito Fechado de TV deverá operar continuamente, sendo controlado por servidor integrante da ASI ou empresa terceirizada (vigilância privada);
2. O CFTV será regulamentado mediante Resolução do Conselho Superior de Administração, para fins de uso das imagens, acessos, backup e definição de responsabilidades;
3. Deverá proporcionar o controle visual das instalações físicas interna e externamente;
4. A **Secretaria Estratégica de Tecnologia da Informação e Comunicação** controlará o software, manutenção e backup de imagens do CFTV;
5. Comunicar toda e qualquer alteração a ASI;

## **XIII. PROCEDIMENTOS QUANTO AO CONTROLE DE CLAVICULÁRIO:**

1. Todas as chaves de fechamento das aberturas de instalação física deverão possuir cópias identificadas, devidamente organizadas e armazenadas em claviculário;
2. O claviculário deverá ser instalado em área de segurança de classificação restrita, sendo seu controle gerenciado pelo encarregado da administração da edificação;
3. O claviculário deverá dispor de mecanismo de segurança que permita materializar sua eventual violação;
4. A utilização de chaves do claviculário estará condicionada à autorização do encarregado por seu controle ou em caso de emergência.

## **XIV. PROCEDIMENTOS EM CASO DE OCORRÊNCIA ENVOLVENDO SUBSTÂNCIAS PROIBIDAS (ENTORPECENTES E OUTROS)**

1. A composição das partes envolvidas;
2. Acionamento da Polícia Militar para registro da ocorrência policial e comunicação imediata à ASI.

## **XV. PROCEDIMENTOS EM CASO DE OCORRÊNCIA ENVOLVENDO ARTEFATOS OU SUSPEITA DE BOMBA**

1. Isolar o local onde foi encontrado o objeto suspeito;
2. Não permitir a entrada de funcionários por nenhum dos acessos ao interior do TCE-RO;
3. Acionar imediatamente a Polícia Militar via 190;
4. Comunicar à ASI.

#### **XVI. PROCEDIMENTOS EM CASO DE SEQUESTRO DE PESSOAS**

1. A comunicação imediata à Assessoria de Segurança Institucional;
2. A ASI acionará os demais Órgãos policiais para as demais providências, de acordo com a situação apresentada.

#### **XVII. PROCEDIMENTOS EM CASO DE INCÊNDIO**

1. Os integrantes da brigada de incêndio e da equipe de segurança da edificação deverão identificar e confirmar o foco de incêndio e adotar as medidas cabíveis para controlar as chamas, conforme previsão no **Plano de Emergência de Combate a Incêndios e Atuação em Sinistros**;
2. Acionamento do Corpo de Bombeiros via 193;
3. Os demais usuários da edificação deverão preparar-se para o abandono da instalação física;
4. Manter as portas “corta fogo” sempre fechadas;
5. Caso seja necessário, proceder ao abandono da edificação, pelas escadas;
6. Interromper imediatamente as tarefas que estejam sendo executadas;
7. Seguir fielmente as orientações da brigada de incêndio ou da equipe de segurança.
8. Não utilizar elevadores;
9. Utilizar somente as rotas de fuga predeterminadas;
10. Procurar manter a calma e o silêncio durante o abandono da edificação;
11. Não retornar ao local de trabalho sem a liberação da área de risco por parte da equipe de segurança da instalação física.

#### **XVIII. PROCEDIMENTOS EM SITUAÇÃO DE ATENTADOS**

1. O acionamento da Polícia Militar de imediato;
2. Comunicar à ASI;
3. A adoção das ações de abandono de edificação, se cabíveis.

#### **XIX. PROCEDIMENTOS QUANTO AO ESTACIONAMENTO DE VEÍCULOS**

1. Observar a disposição de vagas predeterminadas pelo administrador do setor de transporte e garagem;
2. Estacionar de acordo com as normas previstas no código de trânsito brasileiro;
3. Não estacionar em fila dupla, evitando notificações pelos órgãos de fiscalização de trânsito;
4. Evitar deixar bens visíveis nos bancos dos veículos.

#### **XX. PROCEDIMENTO EM SITUAÇÕES ENVOLVENDO ACESSO DE PESSOAS ARMADAS NO TCE-RO**

1. É vedado o acesso às instalações físicas do TCE-RO de pessoas portando armas de fogo ou objetos que, por sua forma e finalidade de empregos, possam constituir-se como armas brancas;
2. O acesso de pessoas armadas será permitido a Membros do TCE-RO, Membros do Ministério Público de Contas, demais Membros dos Ministérios Públicos e da Magistratura, Chefes de Poderes e Policiais em serviço, Integrantes das Forças Armadas, terceirizados de empresa de segurança privada que prestem serviços de vigilância patrimonial e outras autoridades, desde que autorizadas pela Presidência do TCE e que sejam detentores de porte de arma, conforme legislação em vigor;
3. Os que portarem arma de fogo em decorrência de autorização legal ou licença concedida por Órgão competente e que não se enquadrem nos itens anteriores, enquanto permanecerem nas dependências do Tribunal de Contas, deverão deixar a arma, mediante cautela padrão na sala da Assessoria de Segurança Institucional;
4. No plenário ou salas de audiências onde ocorrem as sessões julgadoras, fica vedado o acesso de pessoas portando armas ou objetos vulnerantes que atentem contra a segurança, com exceção dos integrantes da Assessoria de Segurança Institucional ou outros policiais designados para segurança das sessões do pleno e/ou audiências;
5. Empregados de empresas de transportes de valores, quando em serviço, também têm acesso liberado, devendo ser informado à ASI via email antecipadamente;



6. Integrantes da ASI lotados nesta Corte têm livre acesso;
7. No caso de identificação de pessoas portando arma de fogo que não se enquadrem na situação prevista nos itens 2, 3 e 5, deverá ser acionada a ASI para verificação do registro e do porte de arma pertinentes, bem como para adoção das medidas de acionamento da Polícia Militar, se necessário (se configurado o crime de porte ilegal de arma);
8. A busca pessoal deverá ser realizada sempre que, ao adentrar ou sair da edificação, houver o acionamento de dispositivos eletrônicos que indiquem a presença de metais ou materiais que provoquem o acionamento de tais dispositivos;
9. A busca pessoal deverá, sempre que possível, ser realizada em ambiente reservado, de forma a não expor o indivíduo revistado ao público em geral.

## **XXI. PROCEDIMENTO NAS SESSÕES DE JULGAMENTO, ESPECIAIS E CERIMONIAIS**

1. Durante as sessões, um membro da equipe da ASI permanecerá na assistência do plenário, apto para atuar, se necessário, diante de uma situação de possível risco à integridade física dos presentes, ou por solicitação direta do Presidente da Sessão, e outro na antessala de acesso das autoridades, quando necessário, mediante prévia análise;
2. No plenário ou salas de audiências onde ocorrem as sessões julgadoras, fica vedado o acesso de pessoas portando armas ou objetos vulnerantes que atentem contra a segurança, com exceção dos integrantes da Assessoria de Segurança Institucional ou outros policiais designados para segurança das sessões do pleno e/ou audiências;
3. Nas sessões ordinárias e especiais, um membro da ASI ficará ao lado da porta principal do auditório, na parte externa, apto para atuar na manutenção da ordem, visando proporcionar o bom andamento dos trabalhos, quando necessário;
4. Nas cerimônias oficiais desenvolvidas nas dependências do TCE-RO, a ASI atuará de acordo com um planejamento especificamente elaborado para o evento, colaborando com o cerimonial na recepção de autoridades e convidados, gerenciando o bloqueio de vias de trânsito, o estacionamento e o acesso às dependências do prédio e ao local do evento.

## **XXII. PROCEDIMENTOS PREVISTOS PARA O SERVIÇO DE SEGURANÇA E VIGILANCIA OSTENSIVO ARMADO PRESTADO PELA EMPRESA CONTRATADA**

A segurança patrimonial das dependências do TCE-RO será desenvolvida pela empresa de vigilância terceirizada de forma ininterrupta, na modalidade de guarda, sob a coordenação,



fiscalização, acompanhamento e apoio da Assessoria de Segurança Institucional, estando responsável por guarnecer os prédios da Sede, anexo, estacionamento e demais patrimônios da Corte, quando sob sua vigilância e responsabilidade. As Normas Gerais de Ação n. 001 e 003 da ASI definem as atribuições, competências e obrigações dos vigilantes nos postos de serviço da sede e residências.

Porto Velho-RO, 13 de novembro de 2015.

**JOSÉ ITAMIR DE ABREU – TC PM**  
Assessor de Segurança Institucional

**JOSÉ EULER POTYGUARA PEREIRA DE MELLO**  
Conselheiro Presidente do TCE-RO