SUMÁRIO

1. INTRODUÇÃO

Este manual foi preparado visando implementar e melhorar a gestão da Segurança da Informação, com foco em modelo para os Sistemas utilizados no âmbito do TCE/AL. A adoção das sugestões elencadas devem ser uma decisão estratégica paraa organização. É esperado que a implementação do controle dos níveis de acesso seja escalada conforme as necessidades da organização, por exemplo, um sistema simples requer uma solução simples.

2. REFERÊNCIAS

O Manual em tela foi elaborado com base nas principais referências que tratam de conceitos, regras e responsabilidades relacionadas à segurança das permissões de acesso às informações do TCE-AL. Dentre elas, destacam-se:

Lei Federal nº 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados (LGPD);

Lei nº 8.790 de 29 de dezembro de 2022 – Lei Orgânica do Tribunal de Contas de Alagoas;

Lei nº 12.527 de 18 de novembro de 2011 – Leia de Acesso à Informação (LAI);

Política Corporativa de Segurança da Informação do TCE-AL;

Política de Privacidade e Proteção de Dados Pessoais do TCE-AL;

Manual de Classificação e Tratamento de Informações Sigilosas;

Política de Gerenciamento de Senhas do TCE-AL;

Política de Controle de Acesso Lógico e Físico do TCE-AL;

Política de Gestão de Backup e Recuperação de Dados;

Política de Gestão de Riscos de TI;

Política de Desenvolvimento Seguro na DTI do TCE-AL;

Norma ISO/IEC 27001:2022 para Gestão da Segurança da Informação, Segurança

Cibernética e Proteção à Privacidade;

Norma ABNT NBR 14724:2011 – Informação e Documentação – Apresentação Trabalhos Acadêmicos;

Regimento Interno do TCE/AL;

Resolução de Sigilo, Tratamento, Disponibilidade e Integridade da Informação do TCE/AL;

Resolução de Classificação e Tabela de Temporalidade de Documentos do TCE-AL.

3. CONCEITOS E DEFINIÇÕES

Acessos: é a resultante dos direitos de execução/permissão relacionado a um objeto de sistema;

Autenticação: processo pelo qual a conta ou usuário é validado pelo sistema e autorizado de acordo com as permissões atribuídas;

Contas: são objetos criados no seu ambiente de rede ou em sistemas que definem uma identidade, que pode ser um usuário, computador, sala de reunião, servidor ou qualquer outro que necessite ter uma determinada ação em algum sistema;

Controle de acesso: para o usuário executar determinadas tarefas na sua estrutura de TI, acessar recursos de sistemas e realizar algumas alterações em seus dispositivos pessoais, faz-se necessário o uso de algum mecanismo de controle de acesso;

Papéis: são as diferentes funções dentro de um sistema ou ambiente analisado. Neste caso, ao invés de atribuir as permissões ao usuário, define-se as permissões por papéis e enquadram-se os usuários a cada tipo de papel existente, como por exemplo, Administrador, Auditor, Gerente de sistema;

Permissões: são os direitos de executar uma ou mais ações em objetos de um sistema. Isto é, um objeto pode ser um arquivo, registro de um banco de dados, tela de um sistema,

impressão de um determinado arquivo, entre outros. Neste caso, o objeto pode ser definido como a área/registro de informação a ser analisada;

Sessão: quando o usuário é autenticado e acessa um determinado sistema ele inicia uma sessão. É possível um usuário ter várias sessões ativas paralelamente e, durante uma sessão, é possível ter mais de um papel.

Unidade Gestora: é a Unidade Orçamentária ou administrativa investida do poder de gerir recursos orçamentários e financeiros, próprios ou sob descentralização. São unidades que fazem a gestão de recursos públicos.

Usuários: sujeito da ação de executar, acessar, monitorar e/ou intervir em um sistema. Pode ser indivíduos ou agentes autônomos, como agentes de softwares;

4. RESPONSABILIDADES

4.1. DA DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

Receber, analisar, aprovar, provisionar, revogar e monitorar os perfis de acesso de todos os recursos no TCE-AL.

4.2. DOS GESTORES DAS ÁREAS

Responsáveis por identificar as necessidades de acesso da sua equipe, solicitar e revisar periodicamente as permissões de acesso.

Informar a DTI sobre qualquer mudança nas necessidades de acesso da equipe (incluindo transferências, demissões ou mudanças de funções).

5. REQUISITOS DE ACESSO

Uma organização precisa identificar e gerenciar muitas atividades para funcionar efetivamente. No caso das solicitações para acesso ao ambiente e serviços tecnológicos gerenciados pela DTI no TCE-AL (a exemplo de sistemas e aplicações), deve existir um controle prévio de quem deve estar habilitado para acessar determinado sistema, conforme diretrizes definidas na **Política de Controle de Acesso Lógico e Físico do TCE-AL**.

5.1. CONTROLE HIERÁRQUICO

Considerando que o Tribunal de Contas do Estado de Alagoas é uma pessoa jurídica de direito público, este possui uma estrutura organizada prevista em Lei, possuindo por consequência um escalonamento vertical dos setores e cargos.

Deste controle decorrem as faculdades de supervisão, coordenação, orientação, fiscalização, aprovação, revisão e avocação das atividades administrativas. E ainda, por meio dele, as autoridades acompanham, orientam e reveem as atividades dos servidores.

Nesse sentido, as solicitações que envolvam permissões de acesso aos Sistemas e Aplicações deverão observar a organização interna do Tribunal, levando em consideração o cargo de chefia (direção) e em sua ausência quem o substituirá.

Nos casos de ausência de previsão legal do cargo, deverá ser observada a designação, nomeação ou qualquer outra formalidade de investidura no cargo equivalente à chefia do setor.

5.2. FLUXO

Ao ser nomeado, o servidor deverá acessar o **Formulário Solicitação de Acessos a Novo Colaborador** na página corporativa - Intranet da DTI no TCE-AL e preencher os campos adequadamente, após esse procedimento, obterá o login e senha de acesso aos sistemas e aplicações de acordo com o cargo/função que está designado.

No caso, de existirem outras necessidades com relação ao acesso de usuários, as solicitações de criação/liberação e/ou revogação/exoneração de perfil de acesso sempre devem ser formalizadas mediante ofício, em nome da pessoa que ocupa cargo de chefia no setor, considerando o regimento interno vigente a ser direcionado ao Diretor(a) de Tecnologia e Informática.

5.3. ESCOPO

O Ofício deverá constar:

- Nome completo;
- Matrícula;
- CPF;
- Função exercida pelo usuário solicitado.

5.4. PERMISSÕES

O nível de acesso de cada sistema deve sempre ser compatível com a função exercida pelo usuário. Isso implica dizer que a Diretoria de Tecnologia e Informática, ao recepcionar os formulários de solicitação, deverá avaliar se no escopo do pedido consta a função/atividade do usuário e se ela condiz com a permissão solicitada.

6. PROPOSTA DE PADRONIZAÇÃO

6.1. REGRAS DE NEGÓCIO

Os Sistemas e/ou Aplicações devem atender por completo às regras de negócio necessárias para o cumprimento da Legislação vigente, seja com relação às atividades de controle externo (Ex. protocolo online, acompanhamento processual das partes, transparência e publicidade),

seja com relação às atividades da área meio (Ex. unificação de serviços, eficiência, acesso facilitado ao cidadão, segurança da informação e privacidade).

6.2. REQUISITOS MÍNIMOS DE SISTEMAS/APLICAÇÕES

6.2.1. TIPO DE ACESSO

Atualmente, o login dos usuários internos do TCE-AL, são definidos de acordo com o nome/sobrenome. É recomendável adotar o tipo de acesso mais tradicional de *login*, sendo a primeira credencial o documento (CPF) e depois a senha. Estabelecendo o referido tipo de acesso padrão para todos os Sistemas e/ou Aplicações, podendo subsidiariamente ter outras opções de identificação, seja por certificado digital token ou em nuvem.

Com fulcro na segurança dos dados e no tráfego das informações é importante que a Instituição siga uma **Política de Gerenciamento de Senhas do TCE-AL**, nela devem estar incluídos os critérios para unificação de senhas. Assim, cada usuário terá uma única senha pessoal para acessar todos os sistemas que lhe competem. Isso impacta positivamente no trabalho da equipe de suporte na DTI do TCE/AL, reduzindo os chamados comuns de “esqueci minha senha” por parte dos servidores, cidadãos e fornecedores, permitindo que o processo flua rapidamente. O acesso via login único facilita os controles de bloqueio e acesso das estações online de trabalho da equipe, bem como, quando o servidor é desligado, suspenso ou está em gozo de férias, garantindo a segurança das aplicações e/ou sistemas acessados, conforme regras definidas na **Política de Controle de Acesso Lógico e Físico do TCE-AL**.

6.2.2. PERFIL DE ACESSO

O perfil de acesso serve para representar uma categoria de usuário dentro da Instituição, se baseando nos papéis e privilégios associados a essa categoria específicade usuário, assim as Aplicações e/ou Sistemas contratados devem obedecer ao princípio de segregação das funções,

priorizando o **local (área) e função ocupada pelo usuário** para atribuir um perfil de acesso correspondente, fazendo a correlação com os módulos e ações (Ex. consultar, deletar, assinar, imprimir) aplicáveis à execução do trabalho.

O objetivo principal da gestão de perfis de acesso é ocultar elementos que um usuário não tem necessidade de acesso na funcionalidade. Se um usuário não tem direitos sobre um objeto ou uma ação através de regras de controle de acesso definidas na **Política de Controle de Acesso Lógico e Físico do TCE-AL**, um perfil não deve conceder visibilidade às ações ou informações que são restritas por políticas de controle de acesso relacionadas.

Nesse sentido, é vedado:

a) a existência de perfis que tenham acesso a todos os módulos, com exceção do perfil master;

b) a criação de perfis de acesso que permitam que um usuário de nível/função hierarquicamente mais baixa tenha acesso a mais privilégios que o usuário de nível/função superior;

c) ocupantes da mesma função/atividade não devem ter perfis de acesso diferentes (com mais privilégios);

d) duplicidade de perfis de acesso;

e) visibilidade a módulos não utilizados pelo TCE/AL;

Ao implantar um novo Sistema na Instituição é necessário elaborar um mapeamento de perfis que tenha como resultado quais são os perfis de acesso e/ouperfis de negócio necessários para cada função na organização.

6.2.3. HISTÓRICO DE ACESSO

O registro de *logs* tem como objetivo principal a detecção de ações impróprias nos sistemas de informação. Devem ser tomados cuidados para que esse monitoramento esteja de acordo com requisitos legais e preserve a salvo as informações pessoais e confidenciais.

Os requisitos mínimos são:

a) registros de hora e data de login e logout de cada usuário;

b) tentativas de acesso negadas, origem dos acessos;

c) arquivos acessados (leitura, escrita, geração e exclusão);

d) alterações de privilégios;

e) mudanças nas listas de acessos;

f) erros de software e hardware;

g) tráfego de rede;

h) tempo de conexão;

i) alertas e desativação de controles de rede e

j) alterações na configuração de sistemas.

A avaliação de riscos, conforme diretrizes definidas na **Política de Gestão de Riscos de TI**, pode facilitar na determinação de um nível de monitoramento mais adequado às reais necessidades da organização.

6.2.4. BACKUP DE DADOS

A responsabilidade de backup dos dados armazenados nas estações de trabalho é dos usuários.

Os dados armazenados nos servidores disponibilizados na rede, bem como, nos sistemas utilizados pelo TCE-AL são mantidos pela DTI.

Recomenda-se o backup mensal com retenção anual e em casos excepcionais, a redução temporal, considerando a existência de espaço para armazenamento.

O requisito mínimo é que o backup garanta a segurança dos dados sensíveis e exista uma padronização do ciclo de vida da informação desde a coleta inicial até o arquivamento e eliminação. Segundo os artigos 15 e 16 da Lei Geral de Proteção de Dados, o término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

" Art. 15. (...)

I - Verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

II - Fim do período de tratamento;

III - Comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, **resguardado o interesse público**; ou

IV - Determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

I - Cumprimento de obrigação legal ou regulatória pelo controlador;

II - Estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III - Transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

IV - Uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados."

O período de retenção e descarte das informações devem sempre obedecer a legislação em vigor e o grau de temporalidade estabelecido pela Instituição, seguindo diretrizes definidas na **Política de Gestão de Backup e Recuperação de Dados**.

6.2.5. CRIPTOGRAFIA

Deve-se adotar controles de segurança ao armazenar as informações para garantir que os dados necessários sejam criptografados (criptografia de informações altamente sensíveis quando armazenadas - como dados de verificação de autenticação – mesmo que estejam no lado servidor, usando sempre algoritmos conhecidos, padronizados e bem testados). A identificação das causas de eventuais erros se dá por meio da análise de registros de logs (de toda a rede, se necessário), checagem de configurações e ainda pela verificação de falhas não corrigidas em sistemas de informação.

Recomenda-se utilizar um protocolo de segurança que garanta a integridade de dados entre os aplicativos de comunicação, objetivando assegurar que a conexão entre navegador, aplicativos e serviços seja segura e confiável.

6.2.6. ANONIMIZAÇÃO

Promoção de mecanismos que garantam a proteção de dados pessoais e de dados pessoais sensíveis a exemplo do disposto no artigo 5º, inciso III e XI que conceituam como dado anonimizado, o dado relativo a titular que não possa ser identificado,considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento e a anonimização, como a

utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança.

6.2.7. POLÍTICAS DE PRIVACIDADE E TERMOS DE USO

É um conjunto de termos que determinam de que forma a Instituição trata os dados do usuário. Essas diretrizes são adotadas visando esclarecer os visitantes do site/sistema/aplicação sobre as finalidades dos dados coletados durante as suas operações. Vale salientar que se trata de exigência legal, tanto da LGPD, quanto do Marco Civil da Internet.

Cada interação do usuário em determinada aplicação gera obrigações e responsabilidades tanto para ele quanto para a Instituição em si e, por isso, devem ser minuciosamente delimitadas. Se faz necessário estabelecer normas de utilização da aplicação pelo usuário/cliente, bem como, delinear os limites da responsabilidade do proprietário do software, site ou aplicativo.

6.2.8. CONTROLE DE ACESSO DE TERCEIROS

Deve ser assegurado durante a formalização dos acordos que o serviço prestado por terceiros, especialmente quando a atividade requeira acesso, tratamento, transmissão, gestão da informação, sistemas ou recursos que tratam informações da Instituição, atendem aos requisitos de segurança conforme as boas práticas da ISO 27001 e a legislação em vigor.

No caso de desenvolvimento/sustentação de aplicações e/ou sistemas, mediante regras definidas na **Política de Desenvolvimento Seguro na DTI do TCE-AL**, deve-se:

a) considerar os padrões de segurança e privacidade praticados no mercado;

b) descrever os recursos de segurança e os dados acessados pelas aplicações, os quais

devem ser avaliados pela DTI do TCE/AL;

c) utilizar rotinas de validação de integridade para prevenir erros, seja involuntário ou intencional;

d) realizar a análise de segurança no código-fonte.

Nesse sentido, considerando que o acesso de terceiros, poderá incluir o acesso a base de dados, infraestrutura onde as aplicações estão hospedadas e a própria aplicação (código fonte), estes devem ser concedidos seguindo o princípio de privilégios mínimos,ou seja, apenas aos dados e às operações de que precisam para executar seus trabalhos. Eventuais privilégios adicionais, podem ser concedidos desde que o ambiente seja acessado em conjunto (mecanismo de acesso assistido através de ferramenta Guacamole) com um responsável técnico especializado do TCE/AL. Neste sentido, após o término das atividades revogar os acessos adicionais concedidos preliminarmente para estes fins, mediante regras definidas na **Política de Controle de Acesso Lógico e Físico do TCE-AL**.

6.2.9. CLASSIFICAÇÃO DA INFORMAÇÃO

Os Sistemas e/ou Aplicações a serem implantados no TCE/AL, devem obedecer às regras de provisionamento do negócio, incluindo um estudo sobre a necessidade de publicidade e sigilo das informações para que estejam de acordo com a legislação em vigor. Assim, se um sistema é de uso apenas corporativo, deverá obedecer a classificação da informação, tempo de retenção e destinação final estabelecidos pelo órgão nos documentos **Manual de Classificação e Tratamento de Informações Sigilosas** e **Resolução de Classificação e Tabela de Temporalidade de Documentos do TCE-AL**.

Não devem ser produzidos ou inseridos nas aplicações e/ou sistemas informatizados do TCE-AL documentos ou processos cujo teor da informação se enquadre nas hipóteses de classificação em grau de sigilo conforme os arts. 23 e 24 da Lei nº 12.527, de 2011 e, salvo quando

essas ferramentas disponibilizarem funcionalidades adequadas para o tratamento da informação classificada.

No caso de Sistemas e/ou Aplicações que ofereçam qualquer serviço de uso externo, ao cidadão ou jurisdicionado, possuindo como obrigatoriedade a publicidade de determinada informação ou fase processual, do mesmo modo, os mesmos deverão estar adequados à legislação em vigor.

As informações devem ser qualificadas em níveis de classificação, analisando o nível de proteção em segurança da informação, assim, os sistemas/aplicações deverão obedecer aos critérios de classificação constantes na **Resolução de Sigilo do TCE AL**.

Para se ter um controle das informações já classificadas, é recomendável que, os sistemas informatizados utilizados gerem um Número Único de Protocolo (NUP) – sequência numérica que compõe o Código de Indexação de Documento que contém Informação Classificada (CIDIC).

Nos casos em que a informação gerada for identificada como passível de classificação em grau de sigilo, posteriormente à sua produção ou inserção em sistema informatizado, deve-se seguir os procedimentos estabelecidos no **Manual de Classificação e Tratamento de Informações Sigilosas.**

Vale salientar que, a classificação da informação em grau de sigilo deve ser motivada de acordo com os critérios definidos em Lei, a classificação deve ser formalizada pela autoridade competente, observados os procedimentos estabelecidos e inexistindo a permanência das razões da classificação, a informação deve ser desclassificada.

Desse modo os sistemas devem estar configurados para possibilitar as referidas ações.

6.2.10. MANUAL DO SISTEMA

Cada sistema deve fornecer um guia prático, rápido e resumido para orientações dos seus usuários.

7. CONTROLE DE DOCUMENTOS E REGISTRO

Código	Responsável pela guarda	Permissão de acesso	Meio de arquivo	Indexação	Local de arquivo	Tempo de Arquivo	Forma de Disposição
MN-DTI-001	DTI	Restrito ao setor	Eletrônico	Alfabética	Base de Conhecimento	Permanente	Não aplicável

8. ANEXOS

Não se aplica.

9. HISTÓRICO DAS REVISÕES

Revisão	Descrição das alterações	Data
00	Emissão Inicial	21/03/2024
01	Revisão realizada pelas equipes Governança/Coordenação e Lideranças de Serviço, conforme segue: - Inclusão dos itens 2. Referência e 3. Responsabilidades; - Alteração/Inclusão de texto no item 4.2 Fluxo; - Alteração no texto do item 5.2.1. Tipo de Acesso; - Alteração/Inclusão de texto no item 5.2.4. Backup de Dados; - Alteração/Inclusão de texto no item 5.2.8. Controle de Acesso de Terceiros; Atualização do conteúdo revisado pela equipe de Processos/Projetos. Revisão Ortografia e Gramática.	13/05/2024 21/05/2024 22/05/2024
02	Formatação do texto; Inclusão de texto no item 7. Referências	12/06/2024

03	Inclusão de texto no item 2. Referências; Inclusão de texto no item 5. Requisitos de Acesso; Inclusão de texto no item 5.2. Fluxo; Inclusão de texto no item 6.2.1. Tipo de Acesso; Inclusão de texto no item 6.2.2. Perfil de Acesso; Inclusão de texto no item 6.2.8. Controle de Acesso de Terceiros; Inclusão de texto no item 6.2.9. Classificação da Informação; Correções ortográficas;	09/10/2024

Elaborado por: **Equipe de Processos e Projetos e Governança LGPD**	Analisado e Aprovado por: **Diretoria DTI**
Data da Elaboração: 21/03/2024	Data da Aprovação: 15/10/2024