TRIBUNAL DE CONTAS DO ESTADO DE RONDÔNIA

RESOLUÇÃO N. 392/2023/TCE-RO

Dispõe sobre a Política de Controle de Acesso do Tribunal de Contas do Estado de Rondônia (PCA/TCE-RO) e define as diretrizes para limitar o acesso à informação e aos Recursos de Tecnologia da Informação, estabelecendo controles de acesso, garantindo a segurança e níveis adequados de proteção e dá outras providências.

O PRESIDENTE DO TRIBUNAL DE CONTAS DO ESTADO DE RONDÔNIA, no uso das atribuições legais que lhe conferem os artigos 3º e 66, I, da Lei Complementar nº 154, de 26 de julho de 1996, c/c o art. 173, II, "b", do Regimento Interno do TCE-RO,

CONSIDERANDO a importância de aprimorar e sistematizar a política e as práticas institucionais relacionadas à segurança da informação, as quais contribuem para assegurar o suporte necessário ao pleno exercício das funções do TCE-RO;

CONSIDERANDO a hierarquia das políticas indicadas no Anexo A da NBR ISO/IEC 27003:2020, que prevê uma política de segurança da informação;

CONSIDERANDO a coleta, recepção, produção, utilização, arquivamento, armazenamento, transferência e a veiculação de informações essenciais ao exercício das competências constitucionais legais e regulamentares deste Tribunal, e que tais informações devem ser preservadas, bem como seu eventual sigilo resguardado;

CONSIDERANDO que as informações do TCE-RO devem ser preservadas, integralmente, por diferentes formas, seja física ou eletrônica, estando suscetíveis a incidentes por sinistros naturais, extravios, furtos, mau uso, acessos não autorizados e colapsos de *softwares* e *hardwares*;

CONSIDERANDO a Lei nº 12.527, de 18 de novembro de 2011 – Lei de Acesso à Informação (LAI), que regula o acesso a informações, bem como a Lei nº 12.965, de 23 de abril de 2014 – Lei do Marco Civil da Internet, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;

CONSIDERANDO os termos da Resolução nº 269/2018/TCE-RO, que aprovou o Código de Ética dos Servidores do Tribunal de Contas do Estado de Rondônia;

CONSIDERANDO os termos da Resolução nº 287/2019/TCE-RO, que instituiu o Comitê de Segurança da Informação e Comunicação (COSIC), no âmbito do Tribunal de Contas do Estado de Rondônia, com o objetivo de estabelecer diretrizes e propor políticas, normas e procedimentos gerais relacionados à gestão informacional e do conhecimento;

CONSIDERANDO a Portaria nº 123, de 30 de março de 2021, que aprovou a implantação do Programa Corporativo de Gestão da Segurança da Informação e Privacidade de Dados (PCGSIPD), com base nas normas da família NBR ISO/IEC 27000, a fim de maximizar o nível de confidencialidade, integridade e disponibilidade das informações e processos críticos de informação do TCE-RO, além de adequar-se à Lei nº 13.709, de 2018 (LGPD), por meio de ações voltadas à aplicação de diretrizes, de forma a potencializar o desempenho do Tribunal nos aspectos de segurança da informação, privacidade e proteção de dados;

CONSIDERANDO a necessidade de implementação, manutenção e monitoramento do PCGSIPD do TCE-RO, para assegurar *compliance* com as leis e regulamentações aplicáveis à segurança da informação e à privacidade, inclusive, às relacionadas ao tratamento de dados pessoais;

CONSIDERANDO os termos da Resolução nº 355/2021/TCE-RO, que dispõe sobre a Política de Gestão de Documentos Arquivísticos do Tribunal de Contas do Estado de Rondônia, objetivando a salvaguarda do patrimônio documental, por seu valor de prova e informação e de instrumento de apoio à administração, à cultura e ao desenvolvimento científico;

CONSIDERANDO que a segurança da informação e privacidade é responsabilidade de todos no âmbito deste Tribunal de Contas, principalmente dos gestores e da alta direção, consistindo em aspectos de liderança, estrutura organizacional e processos que garantam que a informação tenha o devido tratamento no TCE-RO;

CONSIDERANDO a necessidade de aprimorar os mecanismos de proteção e de segurança das informações, ativos e serviços de tecnologia da informação do TCE-RO, bem como de adequar o arcabouço normativo em função de novos paradigmas, como armazenamento em nuvem e trabalho remoto;

CONSIDERANDO as boas práticas em segurança da informação preconizadas pelas normas ABNT NBR ISO/IEC 27001:2013, 27002:2013, 27003:2011, 27004:2017, 27005:2011, 27014:2013, 27701:2020, 29100:2020, 16167:2013 e 31000:2018;

CONSIDERANDO que a proteção da privacidade, no contexto do tratamento de dados pessoais, é uma necessidade da sociedade, bem como um tópico de legislação e/ou regulamentação dedicada em todo o mundo e, ainda, o disposto sobre a Gestão da Privacidade da Informação na norma ABNT NBR ISO/IEC 27701:2019;

CONSIDERANDO a recomendação do Tribunal de Contas da União (TCU), registrada no item 9.1.3 do Acórdão nº 1.603/2008, aos órgãos governantes para que: orientem sobre a importância do gerenciamento da Segurança da Informação, promovendo, inclusive mediante normatização, ações que visem estabelecer e/ou aperfeiçoar a gestão da continuidade do negócio, a gestão de mudanças, a gestão de capacidade, a classificação da informação, a gerência de incidentes, a análise de riscos, a área específica para gerenciamento da Segurança da Informação, a Política de Segurança da Informação e os procedimentos de controle de acesso; e

CONSIDERANDO que a norma ABNT NBR ISO/IEC 27002:2013 recomenda revisões periódicas da política corporativa de segurança da informação e privacidade das instituições;

CONSIDERANDO as informações colacionadas no Processo-SEI n. 02097/2023 e no Pce n. 01681/2023,

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º A Política de Controle de Acesso do Tribunal de Contas do Estado de Rondônia (PCA/TCE-RO) define as diretrizes para limitar o acesso à informação e aos Recursos de Tecnologia da Informação, estabelecendo controles de acesso, garantindo a segurança e níveis adequados de proteção, englobando os seguintes aspectos:

I - contas de usuários (identificação); e

II - autenticação e autorização.

Parágrafo único. Esta norma complementar integra a Política Corporativa de Segurança da Informação do Tribunal de Contas do Estado de Rondônia (PCSI/TCE-RO).

CAPÍTULO II
DA IDENTIFICAÇÃO DE USUÁRIOS E DAS CONTAS DE ACESSO

Art. 2º São usuários dos Recursos de Tecnologia da Informação do Tribunal de Contas do Estado de Rondônia (RTI/TCE-RO):

I - interno: membro ou servidor ativo que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo TCE-RO;

II - inativo: membro emérito, servidor inativo ou pensionista do Tribunal que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo TCE-RO;

III - colaborador: prestador de serviço terceirizado, estagiário ou qualquer outro colaborador do Tribunal que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo TCE-RO;

IV - externo: pessoa que utiliza serviços digitais do TCE-RO de forma identificada e que não se enquadre nas definições contidas nos incisos I, II e III deste artigo; e

V - visitante: pessoa que não se enquadra na definição disposta nos incisos I, II, III e IV deste artigo, com acesso temporário, somente à internet disponibilizada no âmbito do TCE-RO.

Art. 3º Cada usuário possuirá uma única conta para acesso aos RTI/TCE-RO, exceto nos casos explicitamente definidos e autorizados pela Secretaria de Tecnologia da Informação e Comunicação (SETIC).

Art. 4º As contas de usuários são pessoais e intransferíveis, de responsabilidade exclusiva do respectivo titular, e seus privilégios não podem ser estendidos a terceiros.

Parágrafo único. Contas de usuários serão empregadas para registro de operações realizadas pelos respectivos titulares e, no mesmo sentido, as operações passíveis de monitoramento serão registradas unicamente na conta de usuário.

Art. 5º As atividades de criação, atualização e revogação de conta de usuário interno e inativo para acesso aos RTI/TCE-RO serão realizadas pela SETIC, com base nas informações prestadas pela Secretaria de Gestão de Pessoas (SEGESP), salvo nos casos de contas com direitos de acesso privilegiados em sistemas, infraestrutura de redes e demais recursos tecnológicos, cuja competência seja exclusiva da SETIC.

Parágrafo único. A definição e divulgação dos procedimentos a serem executados com vistas à criação, à atualização e à revogação de contas de usuários serão promovidos pela SETIC.

Art. 6º A concessão e o uso de direitos de acesso privilegiado serão restritos e controlados pela SETIC, que deverá:

I - manter um processo de autorização formal, bem como o registro de todas as contas de usuários com acesso privilegiado aos RTI/TCE-RO, os tipos de privilégios concedidos e associados a cada sistema ou processo;

II - assegurar que direitos de acesso privilegiados não sejam concedidos, até que todo o processo de autorização esteja finalizado;

III – garantir que os direitos de acesso privilegiados sejam atribuídos a uma Identificação de Usuário (ID) diferente daquelas usadas nas atividades normais do negócio.

IV - asseverar que as atividades normais do negócio não sejam desempenhadas usando ID privilegiada;

V - analisar criticamente, em intervalos regulares, se as competências dos usuários com direitos de acesso privilegiado estão alinhadas com as suas obrigações, no âmbito do TCE-RO; e

VI - estabelecer e manter procedimentos específicos para evitar o uso não autorizado do ID de usuário de administrador genérico, de acordo com as capacidades de configuração dos sistemas.

§ 1º As senhas associadas às contas que possuem acesso privilegiado devem ser compostas usando uma quantidade mínima de 15 (quinze) dígitos, combinando letras maiúsculas e minúsculas, números e caracteres especiais.

Art. 7º Conta de uso coletivo é permitida, em caráter excepcional e temporária, restrita à finalidade que ensejou a criação, via de regra, para usuários em treinamento ou evento, bem como nos casos em que não seja considerado viável o uso de conta individual.

§ 1º A criação de conta de uso coletivo para finalidade prevista no *caput* será solicitada, por meio da Seção de Serviços e Atendimento em Tecnologia da Informação (SESATI), que analisará as justificativas apresentadas e autorizará o atendimento do pedido ou apresentará solução alternativa.

§ 2º A revogação da conta de uso coletivo, referida no § 1º, será feita imediatamente após a expiração do prazo definido ou antes, caso o demandante comunique não ser mais necessária.

Art. 8º As contas de usuários para acesso aos RTI/TCE-RO têm os seguintes prazos de validade:

I - contas de usuários internos e inativos: enquanto durar o vínculo com o TCE RO;

II - contas de usuários colaboradores: logo após o fim de suas atividades no TCE-RO;

III - contas de usuários estagiários: logo após o fim de suas atividades no TCE-RO;

IV - contas de usuários visitantes e contas de uso coletivo: pelo período necessário para a execução das atividades que motivaram a criação; e

V - contas de usuários externos: pelo período necessário para o acesso aos RTI/TCE-RO.

Parágrafo único. Aos usuários visitantes e externos devem ser aplicadas todas as diretrizes da PCSI/TCE-RO, com as permissões de acesso suficientes e estritamente necessárias às execuções de suas atividades, resguardada a segurança das informações acessadas.

Art. 9º As contas de estagiários e prestadores de serviço devem ficar vinculadas a um grupo específico, controladas e facilmente identificáveis, sendo configuradas para expiração automática a cada 06 (seis) meses. A renovação, se necessária, dar-se-á por meio da autorização do fiscal do contrato, no caso do prestador de serviço, ou do dirigente da unidade responsável pelo estagiário.

§ 1º No ato de criação da conta de acesso à rede para membros, servidores, estagiários e terceirizados, serão criadas também as contas de acesso à intranet, com perfil básico e de correio eletrônico.

§ 2º Não será permitida a criação de contas genéricas de correio eletrônico para as unidades organizacionais, apenas grupos/listas.

Art. 10. A SEGESP deverá informar, imediatamente, à SETIC as aposentadorias, vacâncias, exoneração de membros, servidores, assim como o desligamento de estagiários e prestadores de serviços terceirizados, para as providências necessárias acerca das respectivas contas de usuários, no ambiente do TCE-RO.

§ 1º No caso de servidores cedidos a outros órgãos, o direito de acesso à conta de usuário de rede deve ser bloqueado e o acesso ao correio eletrônico do TCE-RO mantido.

§ 2º O fiscal do contrato e o dirigente da unidade devem informar à SETIC, respectivamente, os casos de desligamento de prestador de serviços ou de estagiário, assim que este ocorrer.

§ 3º O servidor, após aposentado, terá bloqueada/excluída sua conta no sistema de comunicação eletrônica do TCE-RO, devendo informar uma conta de e-mail pessoal à SEGESP para atualização de seus dados cadastrais.

§ 4º A SEGESP deverá apoiar a gestão de identidades, no âmbito do TCE-RO, enviando relatórios tempestivos à SETIC sobre exoneração de membros, servidores, assim como o desligamento de estagiários e prestadores de serviços terceirizados

CAPÍTULO III
DO USO DE SENHAS

Art. 11. A senha associada à conta de usuário é pessoal e intransferível, de responsabilidade exclusiva do respectivo titular, sendo expressamente vedado:

I - compartilhamento com outro(s) usuário(s);

II - registro em local inseguro, em papel ou em meio eletrônico; e

III - envio de senhas, por e-mail ou qualquer outro dispositivo de comunicação em claro.

Art. 12. A senha associada à conta de usuário deverá ser de difícil dedução e, preferencialmente, de fácil memorização, sendo vedada a composição de elementos comumente empregados em ataques cibernéticos, como o de força bruta, a exemplo de:

I - nome e sobrenome do usuário, de membros da família, de amigos, animais de estimação, suas iniciais ou qualquer outro nome, mesmo que embaralhados;

II - informações pessoais, tais como identificador de usuário, matrícula, datas, números de telefone, cartão de crédito, identidade, cadastro de pessoa física, placas, informações sobre veículos ou qualquer outro número de identificação pessoal;

III - nomes de pessoas, de lugares em geral ou próprios;

IV - nomes de equipamentos ou da rede que está sendo utilizada;

V - palavras que constam em dicionários de qualquer idioma;

VI - letras ou números repetidos ou sequenciados em teclado padrão QWERTY; e

VII - locais ou objetos que possam ser associados a partir do ativo.

Art. 13. As regras mínimas de formação de senhas de contas de usuários serão definidas pela Infraestrutura de Tecnologia da Informação e Comunicação (COINFRA).

§ 1º Mecanismo de validação de senhas verificará o atendimento com a regra de formação de senha segura, no momento do cadastro.

§ 2º O usuário repetirá a entrada da nova senha para confirmá-la e minimizar riscos de erros de digitação.

§ 3º Mensagem de advertência será mostrada ao usuário, caso a senha preenchida não atenda à regra de formação definida, ou, se houver implementação, quando existir indícios de que tenha sido vazada a partir de consulta às bases de dados especializadas.

§ 4º A nova senha será diferente das três senhas utilizadas anteriormente, a fim de garantir rotação de senhas.

§ 5º A nova senha ou parte dela poderá ser confrontada com bases conhecidas de senhas triviais e/ou vulneráveis.

Parágrafo único. Caso o sistema gere a primeira senha no momento do cadastro, o usuário será obrigado a modificá-la imediatamente após o primeiro *login*, por meio de procedimento capaz de impedir, temporariamente, a execução das demais atividades, enquanto o usuário não realizar a alteração da senha.

Art. 14. A senha associada à conta de usuário será alterada em periodicidade a ser definida pela COINFRA.

Art. 15. A alteração da senha associada à conta de usuário poderá ser efetuada pelo próprio usuário ou mediante pedido à SESATI.

§ 1º O usuário deverá alterar sua senha, sempre que existir indício de comprometimento da segurança de sua conta ou dos RTI/TCE-RO.

§ 2º A COINFRA disponibilizará mecanismo para recuperação de senhas de usuários.

Art. 16. O sigilo da senha associada à conta de uso coletivo, criada nos termos do art. 7º, será mantido entre os usuários autorizados.

Parágrafo único. Alteração de senha de conta de uso coletivo somente poderá ser solicitada por quem demandou a criação da conta ou por parte do responsável pelo treinamento ou evento.

CAPÍTULO IV
DA AUTENTICAÇÃO E DA AUTORIZAÇÃO

Art. 17. A autenticação de contas no ambiente de RTI/TCE-RO será feita, ao menos, por meio de mecanismo de usuário e senha, atendendo a requisitos mínimos a serem definidos e implantados pela COINFRA.

Art. 18. Deverá ser adotada a autenticação em dois fatores, sempre que possível, para acesso a quaisquer serviços ou soluções de TI, exceto nos casos definidos e justificados pela SETIC.

§ 1º Enquanto estiver autenticado, o usuário deverá bloquear o recurso de TI, sempre que se afastar dele ou deixá-lo desassistido.

§ 2º O mecanismo de autenticação automática (auto *login*) deverá ser desabilitado nos recursos de TI.

§ 3º As informações sobre senhas não devem ser salvas localmente, nem incluídas em processos automáticos de acesso (por exemplo, macros ou autocompletamento).

§ 4º Conta de usuário não será empregada em processos de autenticação em serviços de sistema, incluindo rotinas de agendamento de tarefas.

§ 5º Poderão ser requeridos, como meio alternativo de autenticação, mecanismos de segurança adicionais como certificação digital e biometria.

Art. 19. O controle de acesso à nuvem do TCE-RO poderá ser feito por intermédio de serviços de diretórios localizados na própria nuvem do TCE-RO, e atenderá aos seguintes requisitos:

I - sincronização unidirecional de contas e privilégios, ou seja, a atualização de contas e privilégios será procedida a partir da rede do TCE-RO, inclusive no tocante à troca de senhas; e

II - a sincronização não envolverá contas administrativas, as quais serão mantidas na rede do TCE-RO, exceto as definidas pela COINFRA.

Art. 20. A autorização de acesso aos RTI/TCE-RO respeitará o princípio do menor privilégio e a necessidade de conhecer, bem como observará as seguintes diretrizes:

I - a definição da permissão ou revogação de acesso aos recursos de TI será motivada e autorizada pelo dirigente da unidade em que o usuário presta serviço, mediante abertura de chamado no Sistema de Atendimento ao Servidor (SAS), disponibilizado pela SETIC,

fornecendo todos os dados necessários para a realização do cadastro ou mesmo alteração ou exclusão do acesso, se for o caso;

II - a concessão de acesso será preferencialmente automatizada, sendo realizada e atualizada de acordo com os atributos do usuário, a exemplo da unidade de lotação, da função, entre outros; e

III - é responsabilidade do dirigente da unidade, no caso de mudança de lotação de usuário, comunicar à SETIC, mediante abertura de chamado no SAS, solicitando que as permissões que foram concedidos, em razão das atividades realizadas na unidade, sejam revogadas, exceto se houver a necessidade de continuidade do serviço.

Art. 21. As situações, abaixo identificadas, são passíveis de bloqueio da conta de usuário:

I - conta sem uso, por período igual ou superior a 30 (trinta) dias, ressalvadas as contas de usuários externos;

II - quando o servidor ativo não estiver em efetivo exercício por prazo igual ou superior a 15 (quinze) dias, em função de licenças e de afastamentos previstos na legislação; ou

III - nos casos de envio de alerta para a unidade COINFRA e de habilitação de mecanismo de verificação por desafio cognitivo, em função de erros sucessivos de autenticação, a fim de mitigar riscos de segurança decorrentes de tentativas de comprometimento da conta de usuário.

§ 1º O bloqueio de conta, a que se refere o inciso I, poderá ser realizado automaticamente, observados os procedimentos estabelecidos pela SETIC.

§ 2º O bloqueio de conta, em decorrência do disposto no inciso I, pode ser revogado pela SESATI, mediante solicitação do usuário.

§ 3º O bloqueio e a posterior liberação do uso da conta, na hipótese prevista no inciso II, são realizados pela SESATI, a partir de solicitação encaminhada pela SEGESP.

§ 4º O bloqueio de conta de usuário poderá ser realizado conforme critérios de risco de segurança da informação e privacidade definidos pela COINFRA.

§ 5º As contas de usuários externos sem utilização, por mais de 03 (três) anos, poderão ser excluídas, nos casos e hipóteses definidas pela SETIC.

CAPÍTULO V
DOS REGISTROS DE EVENTOS

Art. 22. Os registros (logs) de eventos das atividades do usuário, bem como as exceções, as falhas e os eventos de segurança da informação devem ser produzidos, mantidos e analisados criticamente pela SETIC, em intervalos regulares, e devem conter no mínimo as seguintes informações:

I - identificação do usuário (ID);

II - datas e horários de entrada (*logon*) e saída do sistema (*logoff*);

III - identificação do dispositivo que originou o acesso;

IV - registros das tentativas de acesso ao sistema (aceitas e rejeitadas);

V - registros das tentativas de acesso aos RTI/TCE-RO (aceitas e rejeitadas); e

VI - quando for o caso, as informações acerca dos recursos computacionais, aplicativos, arquivos de dados e utilitários utilizados, bem como os tipos de operações efetuadas.

Art. 23. Para a proteção e o monitoramento dos recursos dos registros de eventos (*logs*) contra acesso não autorizado, adulteração ou exclusão, a SETIC deverá, no mínimo:

I - possuir e manter um servidor de log com o registro de acesso dos usuários, inclusive dos administradores de rede e de sistemas;

II - garantir que as atividades dos administradores e operadores de rede e de sistemas sejam registradas e os registros (*logs*) protegidos e analisados, criticamente, em intervalos regulares;

III - assegurar que os administradores de sistemas e de rede não tenham permissão de exclusão ou desativação dos registros (*logs*) de suas próprias atividades;

IV - executar e manter cópia de registros (*logs*), em tempo real, para um sistema fora do controle do administrador ou operador de rede e de sistemas, para salvaguarda dos registros, controle e monitoramento de conformidade das atividades dos usuários administradores dos sistemas e de rede;

V - garantir que as informações dos registros de eventos (*logs*) e os seus recursos sejam protegidos contra acesso não autorizado e adulteração;

VI - possuir utilitários de sistemas adequados e/ou ferramentas de auditoria para realizar a racionalização e investigação do arquivo de *log*, com o propósito do monitoramento de segurança da informação; e

VII - implantar e garantir que os relógios – de todos os sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança – sejam sincronizados, com uma única fonte de tempo precisa, auxiliando na exatidão dos registros (*logs*) que podem ser requeridos em investigações ou como evidências, em casos legais ou disciplinares.

Art. 24. Os registros (*logs*) de eventos podem conter dados confidenciais e informação de identificação pessoal, nestes casos se faz necessário que a SETIC adote as medidas apropriadas para assegurar a proteção da privacidade, nos termos da legislação e da normatização pertinentes.

Art. 25. O acesso privilegiado, com perfil de administrador dos sistemas e rede, deve ser concedido à conta específica do usuário. Não deve existir conta genérica de administrador de recursos de TI, no âmbito do TCE-RO, salvo em casos de necessidade justificada e acompanhada de parecer prévio da SETIC, com análise de aceitação dos riscos associados.

Art. 26. O acesso privilegiado, com perfil de administrador, somente deve ser concedido a usuários da SETIC que necessitem deste perfil no desempenho de suas tarefas na administração dos RTI/TCE-RO, excetuando-se os casos de necessidade justificada e acompanhada de parecer prévio da SETIC acerca da possibilidade de aceitação dos riscos associados.

CAPÍTULO VI
DOS PAPÉIS E RESPONSABILIDADES

Art. 27. São responsabilidades dos usuários relacionadas ao emprego de credenciais de acesso aos RTI/TCE-RO:

I - salvaguardar senhas, certificados digitais e quaisquer outros meios empregados na autenticação dos RTI/TCE-RO, sob sua respectiva responsabilidade;

II - proceder à troca periódica de senhas, sob sua respectiva responsabilidade;

III - revisar, periodicamente, privilégios recebidos e solicitar a revogação dos considerados não mais necessários;

IV - reportar incidentes de segurança que tiver conhecimento;

V - colaborar para o tratamento de incidentes de segurança;

VI - observar orientações desta Corte de Contas, no tocante às boas práticas e às configurações específicas de segurança da informação e proteção de dados pessoais;

VII - usar, em estrito interesse e razões de serviço, os dispositivos, equipamentos, sistemas e serviços colocados à sua disposição para o exercício funcional; e

VIII - observar o disposto na PCSI/TCE-RO, quanto à salvaguarda de informações produzidas ou custodiadas pelo Tribunal, bem como à proteção dos RTI/TCE-RO.

Art. 28. Todo membro, servidor e estagiário que ingressar no TCE-RO deve assinar um termo de confidencialidade e responsabilidade para ter acesso às informações e aos recursos de Tecnologia da Informação (TI), sendo de responsabilidade da SEGESP, o armazenamento seguro do termo, em meio físico ou eletrônico.

Parágrafo único. No caso de prestador de serviço ou fornecedor que necessite acesso às informações ou aos recursos de TI, o fiscal do contrato ficará responsável por recolher a(s) assinatura(s) no(s) termo(s) de confidencialidade e responsabilidade, seguindo-se do arquivamento dele(s) no respectivo processo de contratação.

Art. 29. São responsabilidades das Coordenadorias de Infraestrutura de TI (COINFRA) e de Sistemas de Informação (CSI), como administradoras do serviço de autenticação dos RTI/TCE-RO:

I - garantir a disponibilidade de serviços de Controle de Acesso (CA), de acordo com os níveis definidos;

II - definir os perfis e permissões de acesso para as funcionalidades e informações das soluções e serviços de TI;

III - definir e revisar, periodicamente, as regras para conceder, revogar e modificar perfis e permissões de acesso a usuários;

IV - implantar e manter atualizados mecanismos e procedimentos de proteção contra ataques externos e internos relacionados ao CA, incluindo mecanismos de validação de senhas;

V - gerenciar contas configuradas;

VI - impedir a transmissão de senhas em texto claro pela rede e armazená-las com criptografia;

VII - implementar o Protocolo de Transferência de Hipertexto Seguro (HTTPS) e regras de identificação e autorização criptografadas, impedindo o tráfego e o armazenamento de senhas em texto claro em todos os sistemas *web* e portais do TCE-RO;

VIII - armazenar dados de usuário e senha apenas em Sistemas Gerenciadores de Banco de Dados (SGBDs);

IX - realizar triagem, análise, notificação e resposta a incidentes de segurança da informação relacionados aos serviços de CA;

X - realizar identificação periódica e notificação de vulnerabilidades, bem como monitorar a aplicação de correções (*patches*) em sistemas e serviços de CA; e

XI - executar, manter e restaurar cópias de segurança (*backup*) de informações disponíveis em serviços de CA.

Art. 30. A SETIC deverá garantir e manter o acesso ao(s) *Data Center*(s) do TCE-RO restrito e autorizado, somente a:

I - servidores lotados na SETIC;

II - servidores agentes de segurança institucional; e

III - alta administração da Corte de Contas.

Parágrafo único. As pessoas não contempladas nos incisos I, II e III só poderão ter acesso se acompanhadas por servidores da SETIC, ou sem autorização, por motivo de força maior.

Art. 31. O monitoramento por Circuito Fechado de Televisão (CFTV) deve ser implementado e mantido, nos perímetros de acesso ao(s) *Data Center*(s) desta Corte de Contas.

Parágrafo único. O tempo de retenção das imagens gravadas pelo sistema de CFTV que cobrem os perímetros de acesso ao(s) *Data Center*(s) deve ser de, no mínimo, 03 (três) meses.

CAPÍTULO VII
DAS DISPOSIÇÕES FINAIS

Art. 32. O presente normativo utilizará o Glossário de termos do Anexo I e, ainda, o Glossário constante da PCSI/TCE-RO para promover compreensão comum e consistente de conceitos, em função da natureza específica do tema.

Art. 33. A violação ou a inobservância aos dispositivos desta Resolução poderá ser considerada incidente de segurança da informação e implicar, isolada ou cumulativamente, nas sanções previstas na PCSI/TCE-RO e/ou em políticas complementares, bem como civis e penais, nos termos da legislação pertinente, assegurados aos envolvidos o contraditório e a ampla defesa.

Art. 34. As unidades provedoras de TI adotarão as medidas necessárias para operacionalizar o disposto nesta norma, bem como detalharão especificidades do presente normativo.

Art. 35. A revisão desta PCA/TCE-RO poderá ocorrer, a qualquer tempo, quando houver mudanças significativas com impacto nos processos ou requisitos de segurança da informação e privacidade, devendo ser realizada, no máximo, a cada 04 (quatro) anos, de modo a atualizá-la frente a novos requisitos corporativos e legais.

Art. 36. A SETIC poderá, sem aviso prévio, bloquear, restringir acesso ou solicitar imediatamente a troca de senhas de qualquer conta de usuário com comportamento considerado suspeito e que possa causar risco de segurança ao ambiente tecnológico e ao negócio do TCE-RO.

Art. 37. Compete ao Presidente do TCE-RO, mediante ato normativo, criar, alterar ou excluir anexos desta Resolução, a partir de subsídios encaminhados pela unidade de segurança da informação, privacidade e proteção de dados pessoais e aprovados pelo Comitê de Segurança da Informação e Comunicação (COSIC).

Art. 38. Esta Resolução entra em vigor na data de sua publicação.

Porto Velho, 17 de julho de 2023.

(assinado eletronicamente)
PAULO CURI NETO
Conselheiro Presidente

TRIBUNAL DE CONTAS DO ESTADO DE RONDÔNIA

ANEXO I DA RESOLUÇÃO Nº 392, DE 17 DE JULHO DE 2023

APRESENTAÇÃO

Este Glossário fornece definições de termos, aplicáveis à Política de Controle de Acesso do Tribunal de Contas do Estado de Rondônia, para promover uma compreensão comum e consistente de conceitos sobre o tema. É complementar ao Glossário da Política Corporativa de Segurança da Informação (PCSI/TCE-RO).

GLOSSÁRIO

A

Acesso privilegiado: capacidade de um usuário ou sistema acessar recursos, informações ou funcionalidades que estão fora do alcance da maioria dos outros usuários ou sistemas. Deve ser concedido apenas a usuários confiáveis que precisem dele para realizar suas funções, como administradores de sistemas, de redes e de segurança.

Acesso remoto: ingresso, por meio de uma rede, aos dados de um computador fisicamente distante da máquina do usuário. Esse acesso permite a visualização da tela do usuário.

Ataque por força bruta: consiste em enumerar todos os possíveis candidatos de uma solução e verificar se cada um satisfaz o problema. Tem como objetivo testar combinações, palavras de forma consecutivas e, por meio de tentativa e erro, descobrir a senha de acesso.

Ativos da informação: qualquer dispositivo de *software* ou *hardware* que agrega valor ao negócio e compõe a infraestrutura de rede de dados do Tribunal, assim como também os locais onde se encontram esses dispositivos.

C

CFTV (Circuito Fechado de Televisão): técnica de segurança que usa câmeras de vigilância para monitorar e gravar imagens de um determinado local.

Classificação: atribuição, pela autoridade competente, de grau de sigilo a dados, informações, documentos, materiais, áreas ou instalações da instituição.

Conta de usuário estagiário: conta temporária, com duração equivalente ao período necessário para realizar atividades de estágio no TCE-RO, com prazo de expiração a ser especificado pelas unidades provedoras de TI.

Conta de usuário externo: conta temporária, com duração equivalente ao período necessário para realizar atividades no TCE-RO, com prazo de expiração predefinido pelas unidades provedoras de TI.

Conta de usuário visitante e conta de uso coletivo: contas temporárias, com duração equivalente ao período necessário para realizar atividades no TCE-RO, com prazo de expiração predefinido pelas unidades provedoras de TI.

Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso aos recursos de tecnologia da informação.

Custodiante: qualquer pessoa física ou jurídica, interna ou externa, ou unidade do Tribunal que detém a posse, mesmo que transitória, de informação produzida ou recebida pelo TCE-RO.

D

Data center: instalação física centralizada onde se encontram computadores corporativos, rede, armazenamento e outros equipamentos de TI que dão suporte às operações de negócios.

I

Informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado.

L

***Log* ou registro de auditoria:** registro de eventos relevantes em um dispositivo ou sistema computacional.

Logoff: procedimento seguro de saída do sistema.

Logon: procedimento seguro de entrada no sistema.

M

Medidas de segurança: medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade e disponibilidade da informação classificada em qualquer grau de sigilo.

N

Níveis de acesso: especificam o quanto de cada recurso ou sistema o usuário pode utilizar.

P

Perfil básico: acesso exclusivo à intranet e aos serviços de internet gerenciados pela SETIC.

Perfil de acesso: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso.

Prestador de serviço: pessoa envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que devem receber credencial diferenciada de acesso.

Proprietário da informação: membro ou servidor do TCE-RO que tenha a guarda das informações produzidas ou que estejam sob responsabilidade do setor onde estão lotados. São responsabilidades do proprietário da informação atribuir os níveis de classificação que uma informação

requer, reclassificar esta informação quando necessário e autorizar o acesso à informação aos usuários do TCE-RO.

Q

Quebra de segurança da informação: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação.

R

Rede de telecomunicações: estrutura que pode ser composta de várias sub-redes, dependendo do tipo de serviço que é provido ao usuário final. As redes de telecomunicações estão sendo aperfeiçoadas para suportar a transmissão de informações com a introdução de novas tecnologias, tanto do lado dos equipamentos da rede (elementos de rede) quanto dos meios de transmissão (redes de transporte) e dos sistemas de operação para gerenciamento de redes de telecomunicações.

S

Segregação de funções: o pedido, a autorização e a administração de acessos devem ser realizados por pessoas diferentes.

Segurança da informação: proteção da informação contra ameaças a sua confidencialidade, integridade, disponibilidade e autenticidade, para minimizar riscos, garantir a eficácia das ações do negócio e preservar a imagem do TCE-RO.

Sigilo: segredo de conhecimento restrito a pessoas credenciadas; proteção contra revelação não autorizada.

T

Termo de responsabilidade: termo assinado pelo usuário, comprometendo-se em manter a confidencialidade acerca de assuntos classificados como sigilosos dos quais tenha tomado conhecimento ou tido acesso em razão de seu ofício no TCE-RO, zelando pela proteção dos documentos, materiais, áreas e sistemas de informação, sob sua responsabilidade, e usando, em estrito interesse e razões de serviço, os dispositivos, equipamentos e sistemas colocados à sua disposição para o exercício funcional.

Trilha de auditoria: registro ou conjunto de registros gravados em arquivos de log ou outro tipo de documento ou mídia, que possam indicar, de forma cronológica e inequívoca, o autor e a ação realizada em determinada operação, procedimento ou evento.

U

Usuário: membro, servidor, prestador de serviço ou fornecedor do TCE-RO que obteve autorização do Proprietário da Informação pela área interessada para acesso aos Ativos de Informação, formalizada por meio da assinatura do Termo de Responsabilidade e/ou pedido de concessão de acesso.

Usuário colaborador: prestador de serviço terceirizado, estagiário ou qualquer outro colaborador do Tribunal que tenha acesso, de forma autorizada, às informações produzidas ou custodiadas por esta Corte.

Usuário externo: pessoa que utiliza serviços digitais do TCE-RO, de forma identificada.

Usuário inativo: membro emérito, servidor inativo ou pensionista do Tribunal que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo TCE-RO.

Usuário interno: membro ou servidor ativo que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo TCE-RO.

Usuário visitante: pessoa com acesso temporário, somente à internet no âmbito desta Corte de Contas.